V1.0

User Guide

www.tenda.cn

3G622R+
3G 300Mbps Wireless Router

Copyright Statement

CONTENTS

Chapter 1 Introduction

Thank you for purchasing Tenda 3G622R+ 11N Wireless Router!

3G622R+ is a high speed 3G 11N Wireless Router, which complies with the latest IEEE802.11n and IEEE802.11b/g standards and provides up to 300Mbps wireless receiving and transmitting rate with its wireless transmitting distance 6 times farther than G-products. It includes Wireless AP, Router, 4-Port Switch, and Firewall in one, and basically provides three ways to access the Internet sharing with other computers. The first way is to share 3G Internet connection with all network users using a 3G USB modem card to connect the USB port of the Router. It is especially suitable for the users who are not convenient in using fixed broadband or those who need to share the Internet movably.

The second way is to use the unique wireless WAN feature to access wireless broadband. When wireless broadband signals provided by ISP are not strong enough in some Wi-Fi hot area, you can set the wireless WAN feature to amplify wireless signals and share the Internet with other computers.

The third way is to connect the Router's WAN port with the traditional DSL or Cable broadband line to access the Internet. With powerful compatibility, it can break through some access restricted area to share the Internet with multiple computers easily.

Besides those access ways, WDS (Wireless Distribution System) enables you to bridge other wireless Routers and extend wireless coverage area. Meanwhile, QoS bandwidth control is used to control downloading speeds of the specific computers. Then, the included “Setup Wizard” is developed by Tenda especially for less IT-savvy users to install the device within seconds.

In a word, 3G622R+ is your premier choice to share the Internet via 3G, wireless broadband, and wired broadband access ways.

1.1 Product Features

- Includes Wireless AP, Router, 4-Port Switch, and Firewall in one
- Supports WPS (Wi-Fi Protected Setup) encryption method
- Complies with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3 and IEEE 802.3u standards
- Supports over 6 times transmission distance of 11G products
- Supports 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods
- Supports RTS/CTS protocol and data partitioning function
- Provides one 10/100Mbps Auto-Negotiation

Ethernet WAN port

- Provides four 10/100Mbps Auto-Negotiation Ethernet LAN ports
- Provides one USB 2.0 port for 3G modem card connection
- Supports xDSL/Cable MODEM, static and dynamic IP in community networking
- Supports remote/local Web management
- Supports WMM to better smooth your voice and video
- Supports wireless Roaming technology for high-efficient wireless connections
- Supports SSID stealth mode and access control based over MAC address (up to 30 entries)
- Supports Auto MDI/MDIX
- Provides syslog to record the status of the Router
- Supports auto negotiation/manual mode for 802.11b/802.11g/802.11n
- Supports UPnP and DDNS
- Supports Firefox 1.0, IE5.5 or above
- Supports LAN access control over Internet connection
- Supports SNTP
- Supports virtual server, DMZ host
- Built-in firewall for hacker's attack prevention
- Supports auto wireless channel selection
- Supports WDS wireless network extension

- Supports URL Monitor
- Supports QoS function

1.2 Package Contents

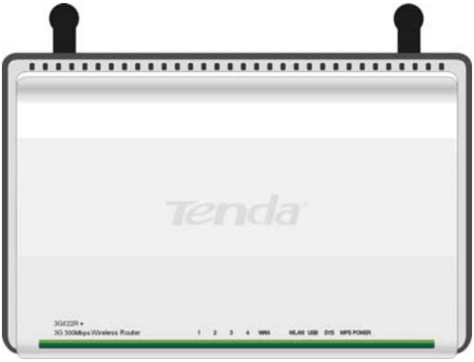
Please unpack the box and check the following items:

- One 3G622R+ 11N Wireless Router
- One Quick Installation Guide
- One Power Adapter
- One CD-ROM

If any of the listed items are missing or damaged, please contact the Tenda reseller from whom you purchased for replacement immediately.

1.3 LED Indicator and Port Description

Front Panel and LED Indicator Show



LED indicator description on front panel: (from R to L)

- **POWER**

  When turns green, Always ON indicates the power connects well.

- **WPS**

  When blinking, it indicates the device is negotiating with client in WPS mode.

- **SYS**

  When turns green, blinking indicates the system runs well.

- **USB**

  When turns green, Always ON indicates the USB port is connected well; Blinking indicates it is transmitting or receiving data packets.

- **WLAN**

  Wireless signal LED indicator. When turns green, blinking indicates the wireless function is enabled.

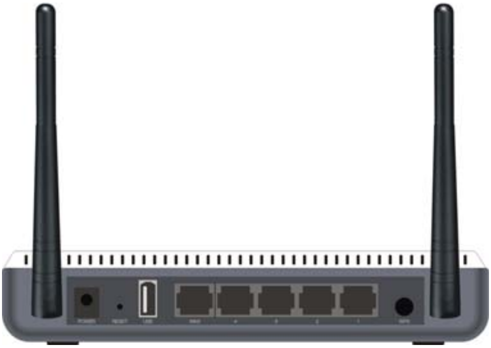
- **WAN**

  Wide area network LED indicator. Always ON indicates it is connected with Ethernet device; Blinking indicates it is transmitting data packets.

- **LAN (4,3,2,1)**

  Wired local network LED indicator. Always ON indicates it is connected with Ethernet device; Blinking indicates the device is transmitting data packets.

Back Panel Show：



Rear Panel： （From L to R）

- **POWER**

  The port is for power adapter connection. Please use the included power adapter.

- **RESET**

  The system reset button. Press this button for 7 seconds, the settings configured in this device will be deleted and it will restore the settings to the default one.

- **USB**：

  The USB2.0 port provided for 3G USB modem card to connect the Internet.

- **WAN**

  The 100Mbps Ethernet port can be connected with MODEM, Switch, Router and other Ethernet devices.

It is always connected with DSL Modem, Cable Modem, or direct Internet line provided by ISP to access the Internet.

- **LAN (1, 2, 3, 4)**

  4 10/100Mbps Ethernet ports can be connected with Ethernet switch, Ethernet router and NIC card.

- **WPS**

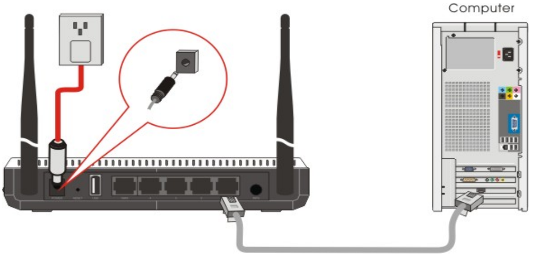
  Wi-Fi Protected Setup button, Press it for 1 second, the WPS feature will be enabled and WPS indicator will be shown blinking.

Chapter 2 Hardware Installation

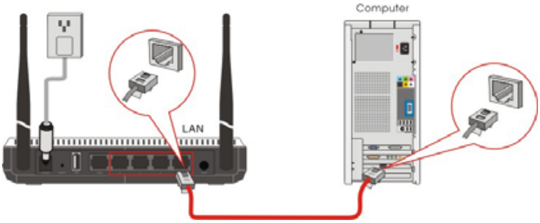
2.1 How to Install the Router

After you unpack the box, please follow the steps below to connect the device. For better wireless performance, please put the device in the middle of wireless coverage area.

1. Please use the included power adapter to power on the Router. (IMPORTANT: Use of a different power adapter could cause damage and void the warranty for this product.)

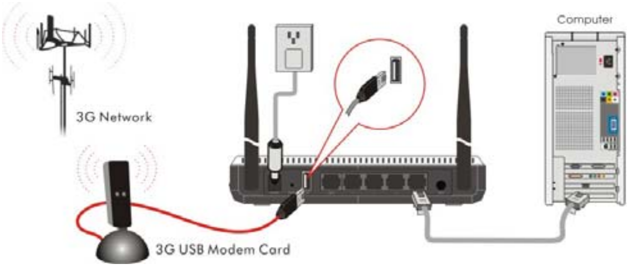


2. Please connect the LAN port of the Router to the network adapter of your computer with a cable.

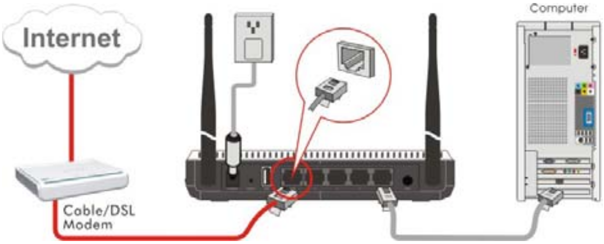


3. Connection between the Router and Network

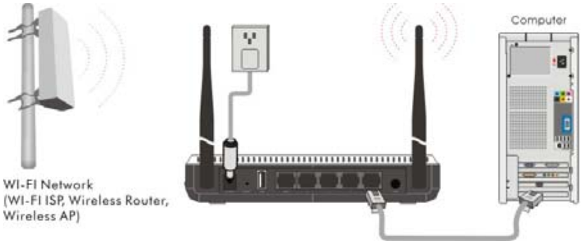
A. If you have a 3G USB modem card, please connect it to the Router's USB port to share 3G network.



B. If you are provided the wired broadband by your ISP to access the Internet, please connect the Router's WAN port with the Internet access line.



C. If you are provided the wireless broadband by your ISP to access the Internet or you want to amplify wireless signals, please set the Router's wireless WAN feature.

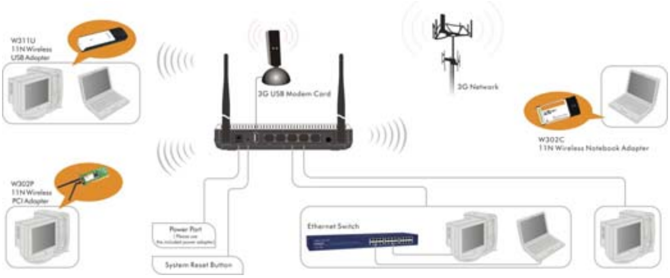


4. Please insert the included CD-ROM into the CD-ROM drive. You can run the “Setup Wizard” automatically or click the “Setup” button manually and then follow the instructions to finish installation or enter the Router’s Web-based utility to set the device. (For more details please refer to chapter 3.)

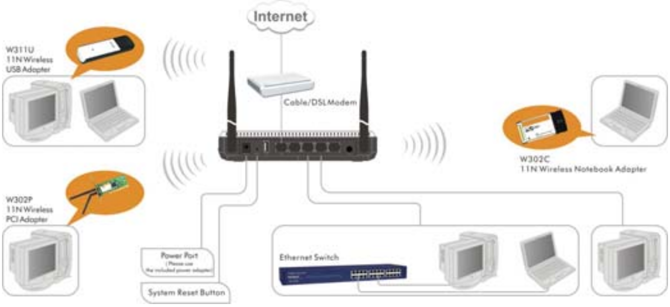
2.2 Network Application Plan

Usually Wireless LAN Network is deployed in a planned environment where each access point is located in a steady place with certain wireless coverage area for communication service. Generally speaking, it is in the center of the area to reduce “dead spot”.

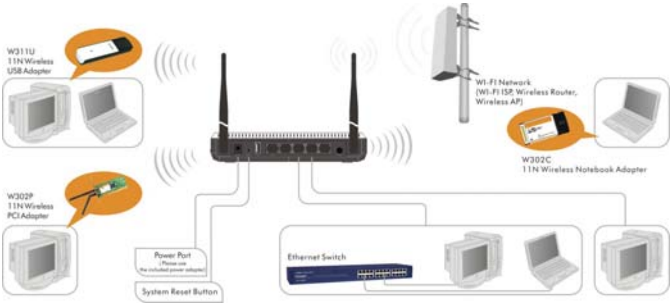
1. Application Plan for 3G Network Connection



2. Application Plan for Wired Broadband Connection



3. Application Plan for Wireless Broadband Connection



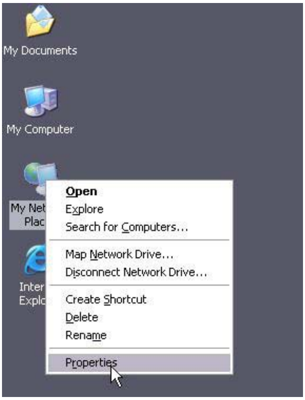
Chapter 3 How to Login to the Router

The chapter mainly presents how to enter the Router's Web page. After you have finished the hardware installation (Please refer to chapter2.), the following steps will assist you to set the network configurations for you computer.

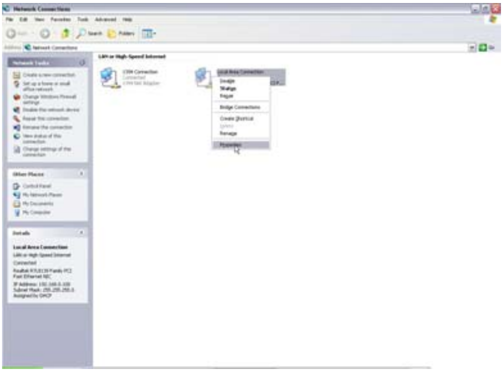
3.1 How to Set the Network Configurations

1. On your computer desktop right click "My Network

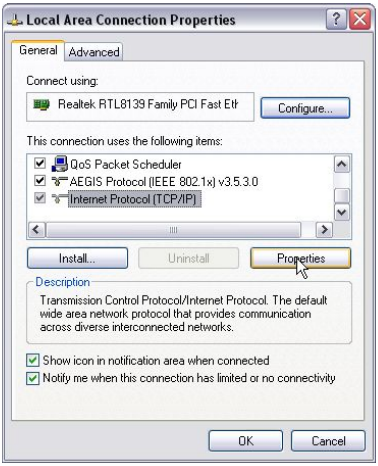
Places” and select “Properties”.



2. Right click "Local Area Network Connection" and select "Properties".



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


Local Area Connection Properties

Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.5.3.0
☑ Internet Protocol (TCP/IP)

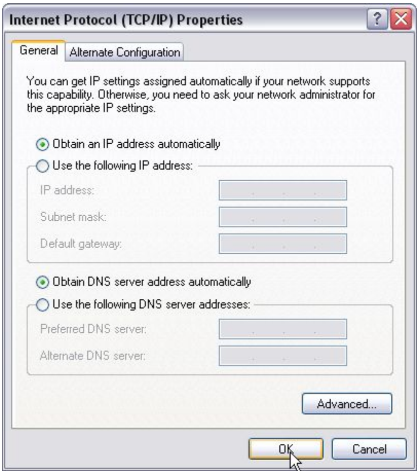
Description

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

4. Select “Obtain an IP address automatically” or select “Use the following IP address (S)”.

A. “Obtain an IP address automatically” as the following diagram:



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

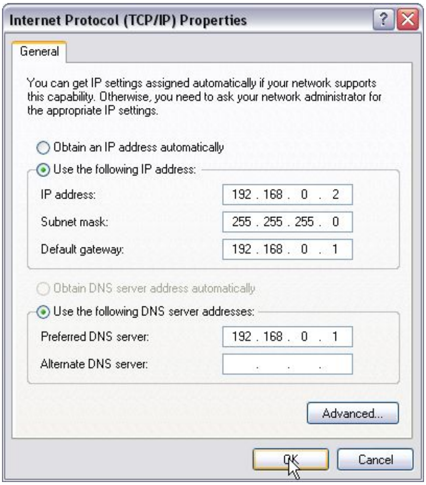
B. “Use the following IP address (S)”

IP Address: 192.168.0.XXX: (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

DNS Server: Certainly you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click “OK” to save the configurations.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

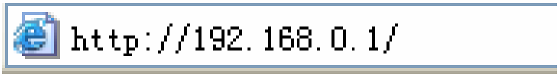
Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

Tip: If you are not sure of the DNS server address, we recommend you to select "Obtain an IP address automatically (O)" and "Obtain a DNS server address automatically".

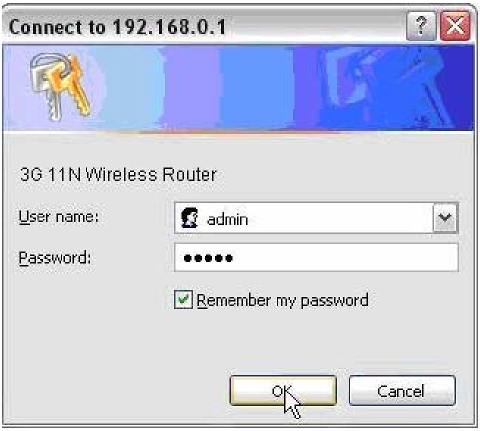
3.2 Login to the Router

1. To access the Router's Web-based interface, launch a web browser such as Internet Explorer and enter the Router's default IP address, http://192.168.0.1. Press "Enter".



http://192.168.0.1/

2. Input the "admin" in both User Name and Password. Click "OK".



Connect to 192.168.0.1

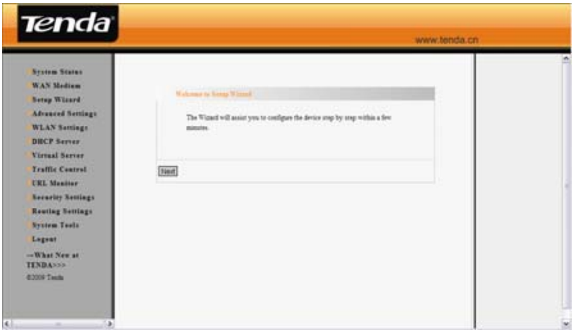
3G 11N Wireless Router

User name: admin

Password: ●●●●●

☑ Remember my password

3. If you enter the correct user name and password, the screen will be the next one.



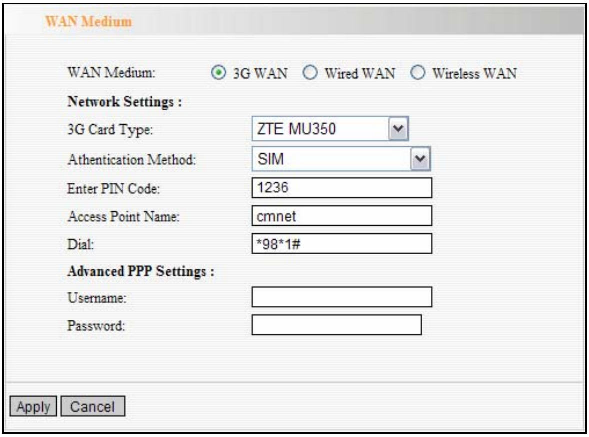
Welcome to Setup Wizard

The Wizard will assist you to configure the device step by step within a few minutes.

Chapter 4 WAN Medium Type

4.1 WAN Medium Type

The Router provides three access medium types. If you are provided the 3G broadband by your ISP to access the Internet, you can connect the 3G USB modem card to the Router's USB port and select 3G WAN to set the device. If you are provided the wired WAN access broadband such as ADSL MODEM, CABLE MODEM or ISP broadband access line, you can connect the access line directly to the WAN port on the Router's rear panel. In addition, if you are provided the wireless broadband by your ISP, you can access the Internet conveniently.



WAN Medium

WAN Medium: ● 3G WAN ○ Wired WAN ○ Wireless WAN

Network Settings :

3G Card Type: ZTE MU350

Athentication Method: SIM

Enter PIN Code: 1236

Access Point Name: cmnet

Dial: *98*1#

Advanced PPP Settings :

Username:

Password:

- **3G WAN:** If you have a 3G USB modem card and you want to share 3G signals and access the

Internet, please select this type.

- **Wired WAN:** In this type the WAN link line must be wired. Please connect the access line to the WAN port on the Router's rear panel. The default type is wired WAN.
- **Wireless WAN:** If you are provided the wireless WAN to access the Internet or you want to amplify the wireless signals, you can use this type.

Please select the different WAN medium type according to the different access ways provided by your ISP. After saving and rebooting the device, you can enter the "Setup Wizard" menu to set the connection type.

Chapter 5 Quick Setup Guide

This chapter deals with how to access the Internet quickly.

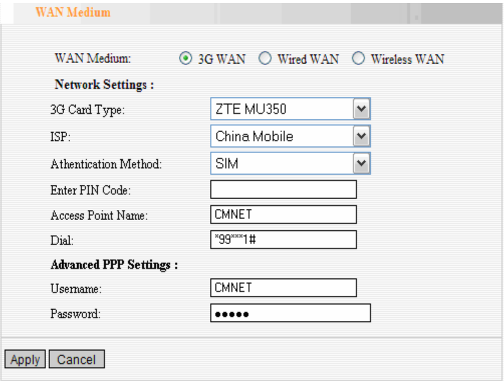
After you enter the Router's Web-based interface from the Internet Explorer, please select the access medium type provided by your ISP in "WAN Medium". After saving and rebooting the device, please select your connection type (PPPOE, Dynamic IP, and Static IP etc.) provided by your ISP to finish the basic settings. Please follow this guide to connect your Router to the Internet.

5.1 Setup Wizard

5.1.1 3G Broadband Connection (via 3G WAN)

If you have a 3G USB modem card and you want to share 3G signals and access the Internet, please select “3G WAN” in “WAN Medium” after you enter the Router’s Web-based interface.

Please follow the diagram below:



WAN Medium

WAN Medium: ● 3G WAN ○ Wired WAN ○ Wireless WAN

Network Settings :

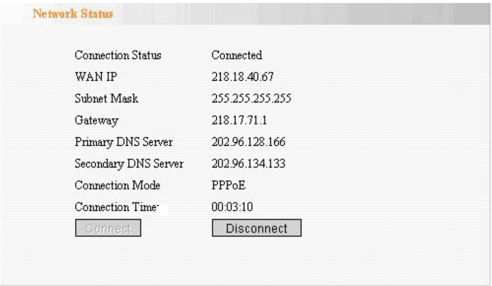
3G Card Type:	ZTE MU350
ISP:	China Mobile
Athentication Method:	SIM
Enter PIN Code:	
Access Point Name:	CMNET
Dial:	*99***1#

Advanced PPP Settings :

Username:	CMNET
Password:	●●●●●

During the installation, please select the type of 3G modem card and 3G ISP, then click “Apply” to finish the settings. Other parameters will come out automatically. Thus, it is very easy and fast for you to access the internet.

For example: If you have ZTEMU350 3G card and the ISP is China Mobile, you can select the card type and ISP from the list, and then click “Apply” to finish the settings. After that, please go to system status to look over wan port status. If it shows connected, you can access the internet.



Network Status

Connection Status	Connected
WAN IP	218.18.40.67
Subnet Mask	255.255.255.255
Gateway	218.17.71.1
Primary DNS Server	202.96.128.166
Secondary DNS Server	202.96.134.133
Connection Mode	PPPoE
Connection Time	00:03:10

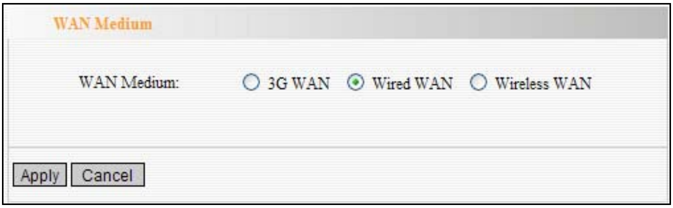
Notice: After you have finished the settings and you still can't access the Internet, please use the wired broadband to connect the Internet and visit our Website. You can search the Model No. of your 3G USB Modem card in the compatible products list to download the corresponding upgrading firmware.

If you still can't access the Internet, please contact the 3G modem card reseller and provide the Model No. of the 3G modem card you have, we'll try our best to help you to solve the problem.

5.1.2 Wired Broadband Connection (via Wired WAN)

If you are provided the wired broadband by your ISP to access the Internet, please select "Wired WAN" in the "WAN Medium" setup page after you enter the Router's Web-based interface. It takes effect after saving and rebooting the device.

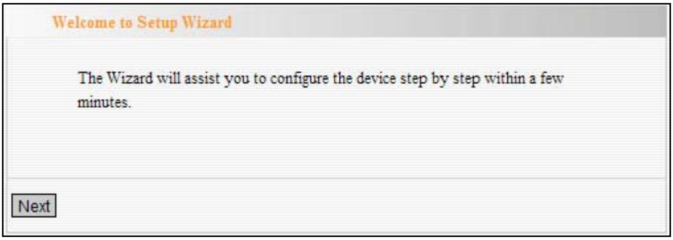
Shown as the diagram below:



WAN Medium

WAN Medium: ○ 3G WAN ● Wired WAN ○ Wireless WAN

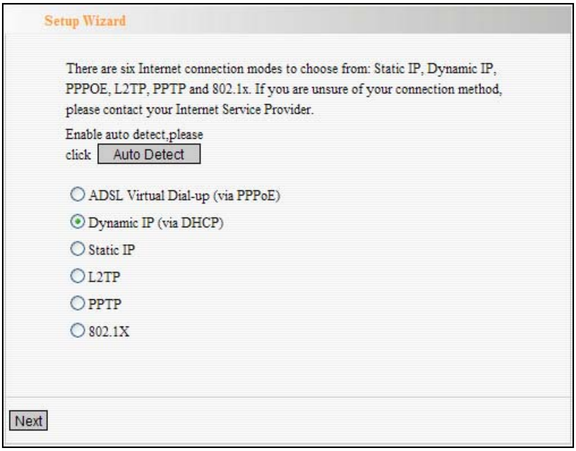
After saving and rebooting the device, you will enter the Router's Web-based interface again. Please click "Next" as the diagram below:



Welcome to Setup Wizard

The Wizard will assist you to configure the device step by step within a few minutes.

The screen will show as the diagram below. The Router supports multiple access ways such as ADSL PPPOE Dial, Dynamic IP, static IP, etc. In this chapter, we introduce you three common access way settings. If you are not sure of your access way, you can enable the auto-detect function to select your access way.



Setup Wizard

There are six Internet connection modes to choose from: Static IP, Dynamic IP, PPPOE, L2TP, PPTP and 802.1x. If you are unsure of your connection method, please contact your Internet Service Provider.

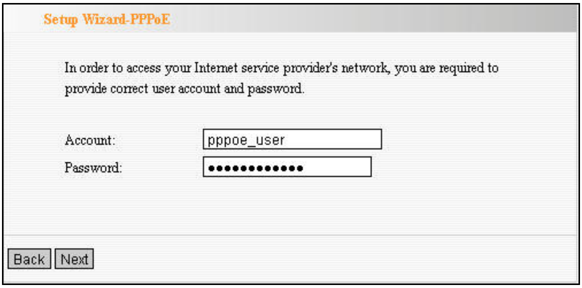
Enable auto detect,please click

○ ADSL Virtual Dial-up (via PPPoE)
● Dynamic IP (via DHCP)
○ Static IP
○ L2TP
○ PPTP
○ 802.1X

➢ ADSL Virtual Dial-up (via PPPoE)

Enter the Account and Password provided by your ISP, and click “Next”.

For example：



Setup Wizard-PPPoE

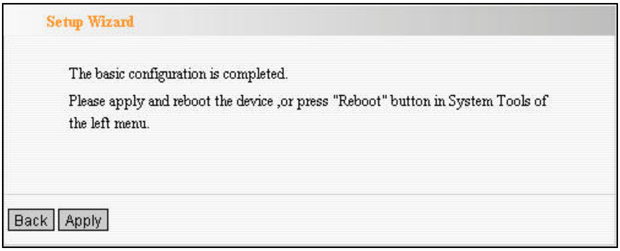
In order to access your Internet service provider's network, you are required to provide correct user account and password.

Account: pppoe_user
Password: ●●●●●●●●●●●●●

➢ Dynamic IP (via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like other modes.

Click “Next” and “Apply” to finish the settings.



Setup Wizard

The basic configuration is completed.

Please apply and reboot the device ,or press "Reboot" button in System Tools of the left menu.

- **Static IP**

In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click “Next”.

For example：

ISP provides the following TCP/IP parameters as follows：

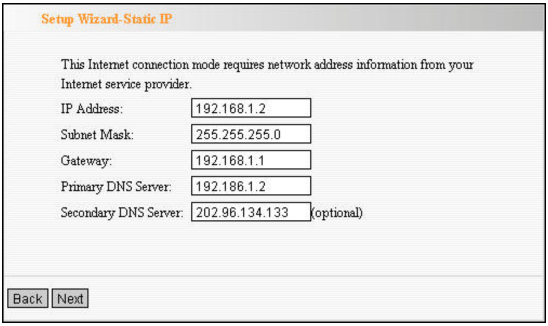
IP Address：192.168.1.2

Subnet Mask：255.255.255.0

Gateway：192.168.1.1

Primary DNS Server：192.168.1.2

Alternate DNS Server：202.96.134.133

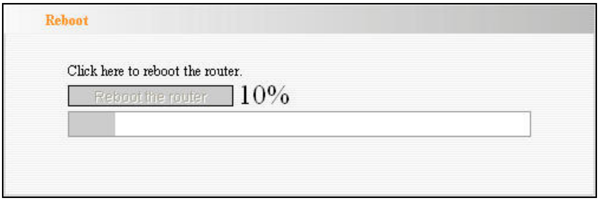


Setup Wizard-Static IP

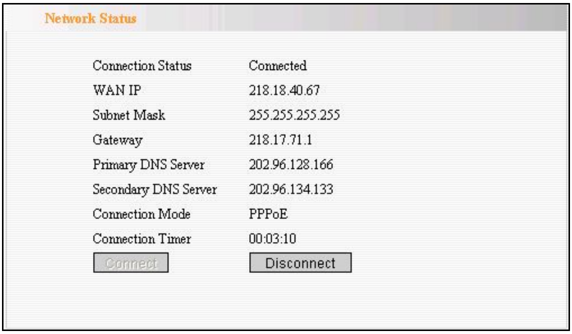
This Internet connection mode requires network address information from your Internet service provider.

IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
Primary DNS Server:	192.186.1.2
Secondary DNS Server:	202.96.134.133 (optional)

Click "Apply" to complete the setup wizard. The Router will record the settings you made. To activate the settings, it is recommended to select "Reboot the Router" from "System Tool" of the left menu. It is rebooting now, please wait for a few minutes and DO NOT power off it.



After rebooting the Router, you can click the "Running Status" on the right menu to check the connection between the Router and ISP device. If the status information of the WAN port appears as the diagram show, it means you have finished the Router's basic settings and you can surf on line now. If you want to configure more, please refer to the following chapters.



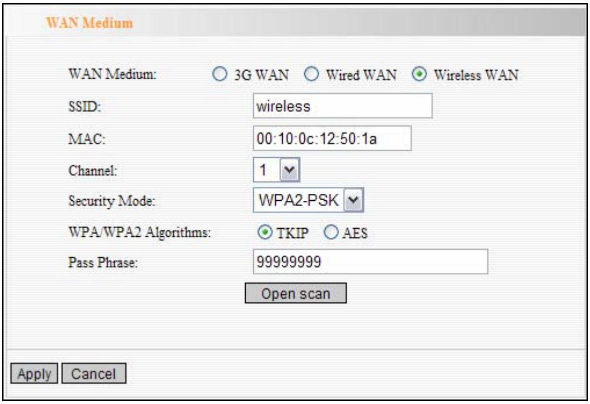
Network Status

Connection Status	Connected
WAN IP	218.18.40.67
Subnet Mask	255.255.255.255
Gateway	218.17.71.1
Primary DNS Server	202.96.128.166
Secondary DNS Server	202.96.134.133
Connection Mode	PPPoE
Connection Timer	00:03:10

5.1.3 Wireless Broadband Connection (via Wireless WAN)

If you are provided the wireless broadband by your ISP to access the Internet or you want to amplify wireless signals, please select “Wireless WAN” in “WAN Medium” page after you enter the Router’s setup page.

Shown as the diagram below:



WAN Medium

WAN Medium: ○ 3G WAN ○ Wired WAN ● Wireless WAN

SSID: wireless

MAC: 00:10:0c:12:50:1a

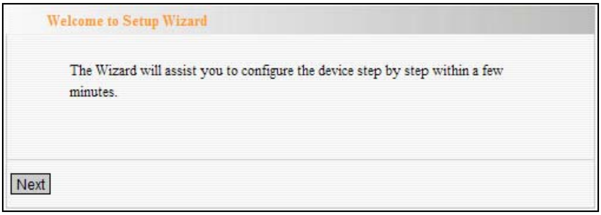
Channel: 1

Security Mode: WPA2-PSK

WPA/WPA2 Algorithms: ● TKIP ○ AES

Pass Phrase: 99999999

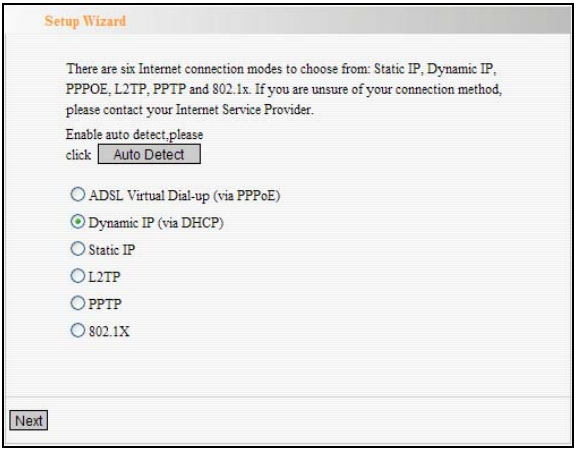
Please enter the wireless SSID, MAC address, channel, security mode parameters provided by your Wi-Fi ISP. If you are not clear, please click" Auto Scan" to finish the settings. Select and save the settings, and you will enter the Router's Web interface again after rebooting the Router. Then click "next" as the diagram show.



Welcome to Setup Wizard

The Wizard will assist you to configure the device step by step within a few minutes.

The screen will show as the diagram below. The Router supports multiple access ways such as ADSL dial-up, Dynamic IP, and Static IP etc. In this chapter, we introduce you three common access way settings. If you are not sure of your ISP access way, you can enable the auto-detect function to select your access way.



Setup Wizard

There are six Internet connection modes to choose from: Static IP, Dynamic IP, PPPOE, L2TP, PPTP and 802.1x. If you are unsure of your connection method, please contact your Internet Service Provider.

Enable auto detect,please click Auto Detect

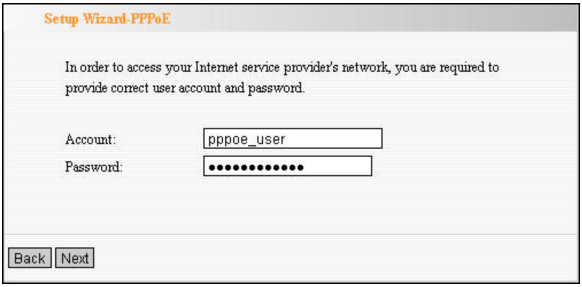
○ ADSL Virtual Dial-up (via PPPoE)
● Dynamic IP (via DHCP)
○ Static IP
○ L2TP
○ PPTP
○ 802.1X

➢ ADSL Virtual Dial-up (via PPPoE)

This way is used when the Router is connected to the wireless modem or you want to amplify wireless signals and share the Internet with multiple computers. Enter the Account and Password provided by your ISP, and click "Next". If you are not clear, please contact your ISP.

For example：

If the Account is pppoe_user and Password is 123456, you need to enter the information as the diagram below. Please enter the Account and Password provided by your ISP.



Setup Wizard-PPPoE

In order to access your Internet service provider's network, you are required to provide correct user account and password.

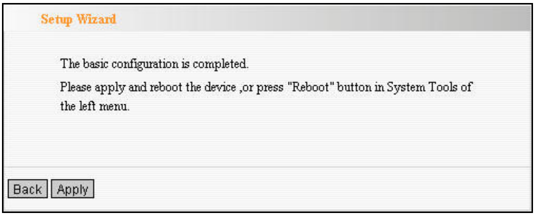
Account: pppoe_user

Password: ●●●●●●●●●●●●●

➢ Dynamic IP (via DHCP)

If you are provided the Dynamic IP connection mode by your ISP or you want to amplify wireless signals, please select "Obtain the IP address automatically". Click "Next" and "Save" to finish settings.

If the IP address of the WAN port is not 0.0.0.0 on the Router's running status Web page, it means you can access the Internet now. Generally speaking, the wireless signals are amplified and you can share the Internet with multiple computers.



Setup Wizard

The basic configuration is completed.

Please apply and reboot the device ,or press "Reboot" button in System Tools of the left menu.

Notice: When you open the wireless WAN feature or when you have a wireless router before and you want to amplify wireless signals, please pay attention to the IP address the previous router distributed. If the IP address belongs to the range: 192.168.0.x, you need to change the LAN IP address to different range such as 192.168.2.1. Only this way, you can amplify the wireless signals and access the Internet. Please refer to chapter 6.1 for changing method.

The wireless broadband which connected to ISP doesn't need to change its LAN IP.

- **Static IP**

In this screen, if you are provided the static IP, please select "Ethernet Broadband, Static IP Address" and fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway, Primary DNS server and Alternate DNS Server fields and click “Next”.

For example：

ISP provides the following TCP/IP parameters as follows：

IP Address：192.168.1.2

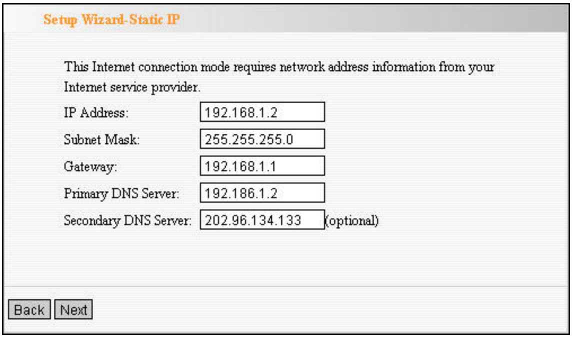
Subnet Mask：255.255.255.0

Gateway：192.168.1.1

Primary DNS Server：210.21.196.6

Secondary DNS Server：211.5.88.88

You need to fill in the related parameters.

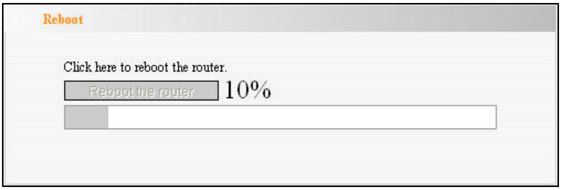


Setup Wizard-Static IP

This Internet connection mode requires network address information from your Internet service provider.

IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
Primary DNS Server:	192.186.1.2
Secondary DNS Server:	202.96.134.133 (optional)

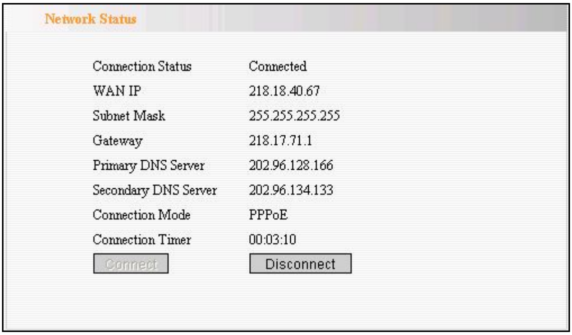
Click “Save” to complete the setup wizard. The Router will record the settings you made. To activate the settings, it is recommended to select “Reboot the Router” from “System Tool” of the left menu. It is rebooting now, please wait for a few minutes and DO NOT power off it. Please use the new parameters to run the Router.



Reboot

Click here to reboot the router.

After rebooting the Router, you can click the "Running Status" on the right menu to check the connection between the Router and ISP device. If the status information of the WAN port appears as the diagram show, it means you have finished the Router's basic settings and you can surf on line now. If you want to configure more, please refer to the following chapters.



Network Status

Connection Status	Connected
WAN IP	218.18.40.67
Subnet Mask	255.255.255.255
Gateway	218.17.71.1
Primary DNS Server	202.96.128.166
Secondary DNS Server	202.96.134.133
Connection Mode	PPPoE
Connection Timer	00:03:10

Notice:

The difference between wired WAN and wireless WAN is the connection medium type. Generally speaking, the standard twisted-pair is used to connect the Router's WAN port in wired WAN connection type. However, wireless signals in standard 2.4GHZ frequency range are used as the transmitting medium in wireless WAN connection type. When you use wireless WAN or 3G WAN, please make sure that the wireless network exists and the intensity and performance of wireless signals are OK. The methods to confirm the wireless feature are very simple.

The following methods are used to confirm the wireless feature by connecting one computer to the Internet via wireless broadband.

1. Confirm 3G signals. Please connect your computer with a 3G modem card to access the Internet. If the signals are OK and the speed is fast at the place, you can connect the wireless Router here to share 3G connection and access the Internet.

2. Confirm Wi-Fi signals. Connect your computer to wireless broadband or other wireless Router by a wireless adapter. If it can access the Internet, it means you can use the wireless feature of the Router and amplify wireless signals at this place. If the computer can’t find wireless signals at some place, you need to change the Router’s place for receiving better signals and using wireless WAN feature better.

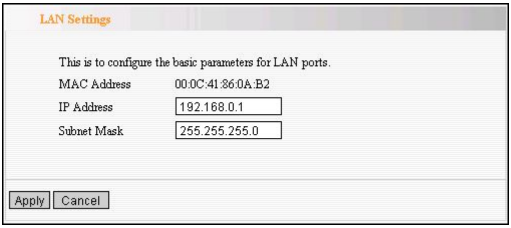
3. Confirm wired WAN signals. The wired WAN access way is the most traditional among the three access ways of the Router. If you can use one computer to access the Internet, you can use the wired WAN

function of the Router.

Chapter 6 Advanced Settings

6.1 LAN Settings

LAN Settings are for the basic TCP/IP parameters of LAN ports.



LAN Settings

This is to configure the basic parameters for LAN ports.

MAC Address 00:0C:41:86:0A:B2

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

- **MAC Address:** The Router's physical MAC address as seen on your local network is unchangeable.
- **IP Address:** The Router's LAN IP addresses (not your PC's IP address). 192.168.0.1 is the default value.
- **Subnet Mask:** It's shown the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value.

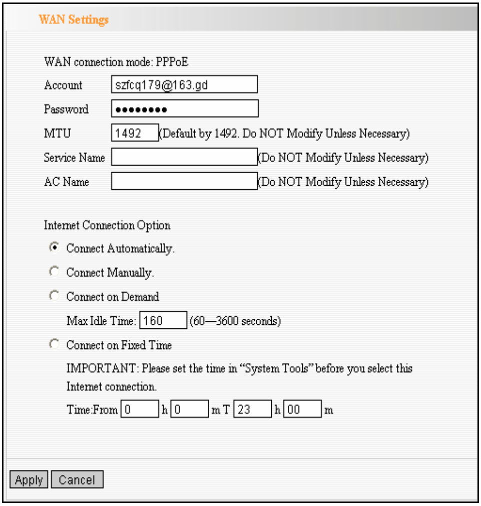
Notice:

Once you modify the IP address, you need to remember it for the Web-based Utility login next time.

6.2 WAN Settings

After you have selected the ISP connection type in "Setup Wizard" and you want to modify the related settings, here you can modify and configure the settings in details.

Virtual Dial-up（PPPoE）



WAN Settings

WAN connection mode: PPPoE

Account: szfcq179@163.gd

Password: ●●●●●●●●●

MTU: 1492 (Default by 1492. Do NOT Modify Unless Necessary)

Service Name: (Do NOT Modify Unless Necessary)

AC Name: (Do NOT Modify Unless Necessary)

Internet Connection Option

● Connect Automatically.

○ Connect Manually.

○ Connect on Demand

Max Idle Time: 160 (60—3600 seconds)

○ Connect on Fixed Time

IMPORTANT: Please set the time in "System Tools" before you select this Internet connection.

Time:From 0 h 0 m T 23 h 00 m

- **WAN Connection Mode:** Show your current connection mode.
- **Account:** Enter them provided by your ISP.
- **Password:** Enter them provided by your ISP.
- **MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1492. Do NOT modify it unless necessary. But if some specific website or web

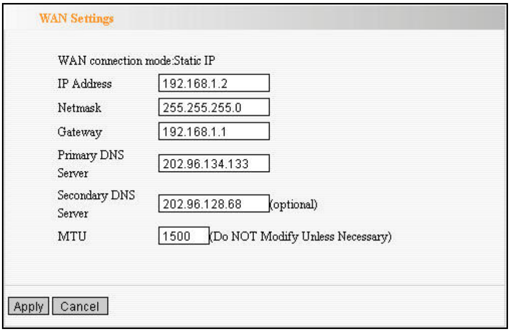
application software can not be open or enabled, you can have a try to change the MTU value as 1450, 1400, etc.

- **Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. Do NOT modify it unless necessary.
- **AC Name:** Enter it if provided. Do NOT modify it unless necessary.
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect Manually:** Connect to the Internet by users manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix.

Notice:

The "Connect on Fixed Time" can be deployed only when you have set the current time in "Time Settings" from "System Tools".

Static IP



WAN connection mode:Static IP

IP Address 192.168.1.2

Netmask 255.255.255.0

Gateway 192.168.1.1

Primary DNS Server 202.96.134.133

Secondary DNS Server 202.96.128.68 (optional)

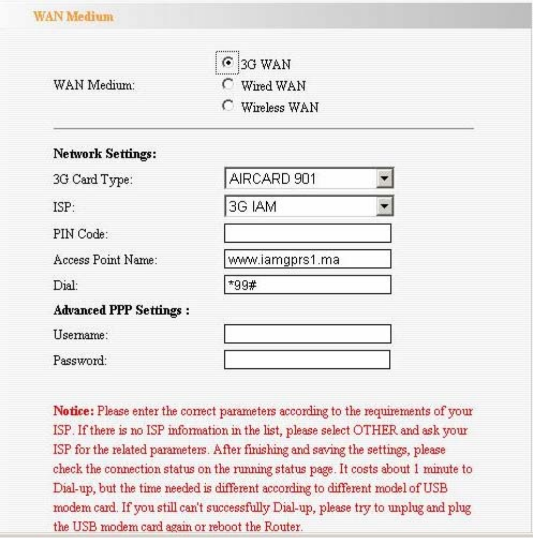
MTU 1500 (Do NOT Modify Unless Necessary)

If your connection mode, static IP is chosen, you can modify the following addressing information.

- **IP Address:** Here enter the WAN IP address provided by your ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask here.
- **Gateway:** Enter the WAN Gateway here.
- **Primary DNS Server:** Enter the Primary DNS server provided by your ISP.
- **Secondary DNS Server:** Enter the secondary DNS.

As for PPTP and L2TP connection settings, please refer to the “Wizard Setup” in chapter 5.

3G WAN:



WAN Medium

WAN Medium: ● 3G WAN ○ Wired WAN ○ Wireless WAN

Network Settings:

3G Card Type: AIRCARD 901

ISP: 3G IAM

PIN Code:

Access Point Name: www.iamgprs1.ma

Dial: *99#

Advanced PPP Settings :

Username:

Password:

Notice: Please enter the correct parameters according to the requirements of your ISP. If there is no ISP information in the list, please select OTHER and ask your ISP for the related parameters. After finishing and saving the settings, please check the connection status on the running status page. It costs about 1 minute to Dial-up, but the time needed is different according to different model of USB modem card. If you still can't successfully Dial-up, please try to unplug and plug the USB modem card again or reboot the Router.

Network settings

- **3G modem card type:** choose the Model No. of your 3G USB modem card.
- **PIN code:** SIM card personal identification code. Enter them provided by your ISP.
- **Access Point Name:** Enter them provided by your ISP.
- **Dial:** Dial number, consult ISP for correct parameters.

Advanced PPP Settings

- **User Name:** PPP Authentication User Name. Some ISP need to enter this value.

- **Password:** PPP Authentication Password. Some ISPs need to enter this value.

Internet connection option:

There are four kinds of connection methods: connect automatically, connect manually, connect on demand and connect on fixed time. Please select one of them according to your needs.

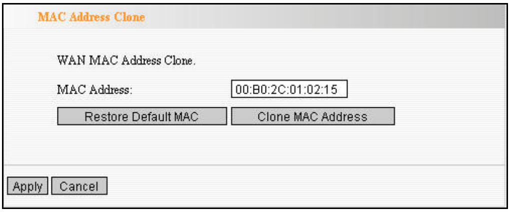
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect Manually:** Connect to the Internet by users manually.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix.

Note: it is suggested you choosing Connect on Demand without running up bills, because it can disconnect the internet automatically when there is no data transmitting or the computer closed. If you access the internet, it will dial up automatically which is very convenient.

If your ISP doesn't offer you the related parameters, you do not need to enter them. After configuring the settings correctly, click "Apply" button and wait for 60 seconds. Then you can access the Internet.

6.3 MAC Address Clone

This page is for the Router's MAC address to WAN.



MAC Address Clone

WAN MAC Address Clone.

MAC Address: 00:B0:2C:01:02:15

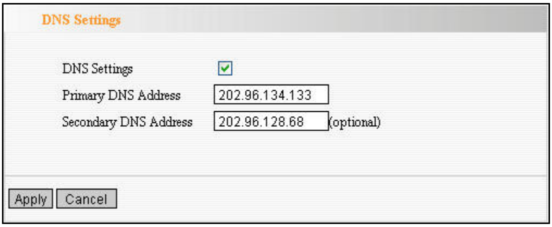
Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

- **MAC Address:** The MAC address to be registered with your Internet service provider.
- **Clone MAC Address:** Register your PC's MAC address.
- **Restore Default MAC Address:** Restore to the default hardware MAC address.

6.4 DNS Settings

DNS is short for Domain Name System (or Service), an

Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.



DNS Settings

DNS Settings ☑

Primary DNS Address 202.96.134.133

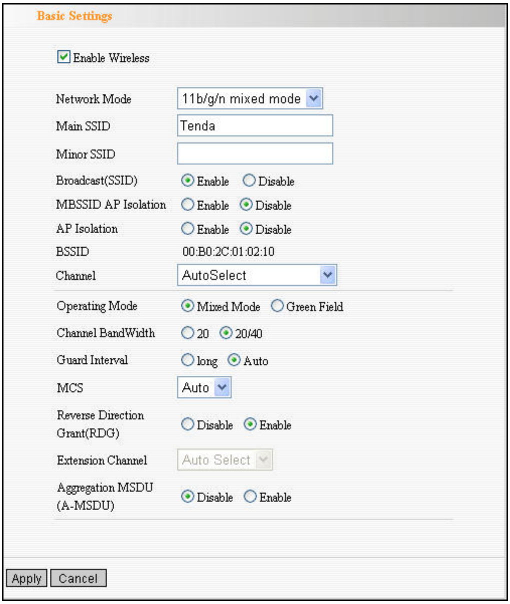
Secondary DNS Address 202.96.128.68 (optional)

- **DNS:** Click the checkbox to enable the DNS server. The Router's DHCP sever will answer the client's requests and distribute DNS address.
- **Primary DNS Address:** Enter the necessary address provided by your ISP.
- **Secondary DNS Address:** Enter the second address if your ISP provides, which is optional.

Notice: After the settings are completed, reboot the device to activate the modified settings.

Chapter 7 Wireless Setting

7.1 Basic Settings



Basic Settings

☑ Enable Wireless

Network Mode	11b/g/n mixed mode
Main SSID	Tenda
Minor SSID	
Broadcast(SSID)	● Enable ○ Disable
MBSSID AP Isolation	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
BSSID	00:B0:2C:01:02:10
Channel	AutoSelect
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	Auto Select
Aggregation MSDU (A-MSDU)	● Disable ○ Enable

- **Enable Wireless:** Check to enable the Router's wireless features; uncheck to disable it.
- **Network Mode：** Select one mode from the following. The default is 11b/g/n mode.

11b mode： Allow the wireless client to connect with the device in 11b mode at the maximum speed of 11Mbps.

11g mode： Allow the 11g/11n-compliant client device to connect with the AP at the maximum speed of 54Mbps.

11b/g mode: Allow the 11b/g-compliant client device to connect with the AP with auto-negotiation speed, and 11n wireless client to connect the device with 11g speed.

11b/g/n mode： Allow 11b/g/n-compliant client device to connect with the AP with auto-negotiation speed

- **Main SSID**：SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSID and the main SSID is necessary.
- **Minor SSID**：It is optional.
- **Broadcast (SSID):** Select "Enable" to enable the device's SSID to be visible by wireless clients. The default is enabled.
- **MBSSID AP Isolation**： One access control feature based on wireless MAC address. When this feature is enabled, wireless clients connected with the same SSID can not communicate with each other. For example, configure main SSID as AP1, minor SSID as AP2. PC1 and PC2 connect to AP1

via wireless adapter, and configure PC1 and PC2 in the same segment. After the feature is enabled, two PCs can not communicate and share network resource each other, but they can communicate with wireless clients connected with AP2. This feature is to isolate the communication of wireless clients connected with the same SSID.

- **AP Isolation:** One access control feature based on SSID. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. When this feature is enabled, wireless clients connected with the Main SSID and Minor SSID can not communicate with each other, which can secure the wireless network strongly. For example, configure main SSID as AP1, minor SSID as AP2. PC1 connects to AP1 via wireless adapter; PC2 connecting to AP2. After the feature is enabled, two PCs can not communicate and share network resource each other. This feature is to isolate the communication of wireless clients connected with different SSID.

  Tip: If you want to isolate all connected wireless client's communication, please enable MBSSID AP Isolation and AP Isolation simultaneously.

- **BSSID**：Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.

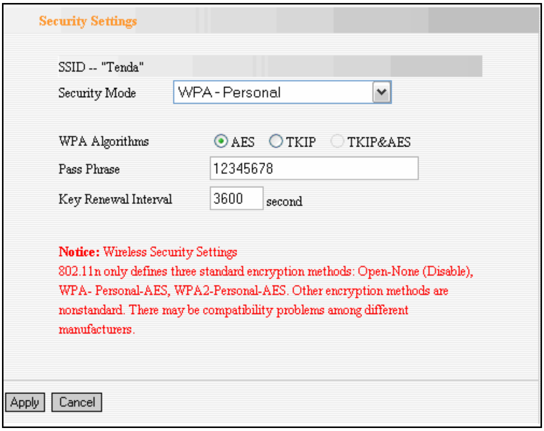
- **Standard Channel**：Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- **Extension Channel**：To increase data throughput of wireless network, the extension channel range is used in 11n mode.
- **Channel Bandwidth** ：Select the channel bandwidth to improve the wireless performance. When the network has 11b/g and 11n clients, you can select the 40M; when it is an 11n network, select 20/40M to improve its throughput.

7.2 Wireless Security Setting

It is used to configure the AP network's security setting. Here presents the common six (ten in all) encryption methods, including WPA-personal, WPA2-personal, Mixed WEP, WPA-enterprise, WPA2-enterprise, etc.

7.2.1 WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.



Security Settings

SSID -- "Tenda"

Security Mode: WPA - Personal

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Pass Phrase: 12345678

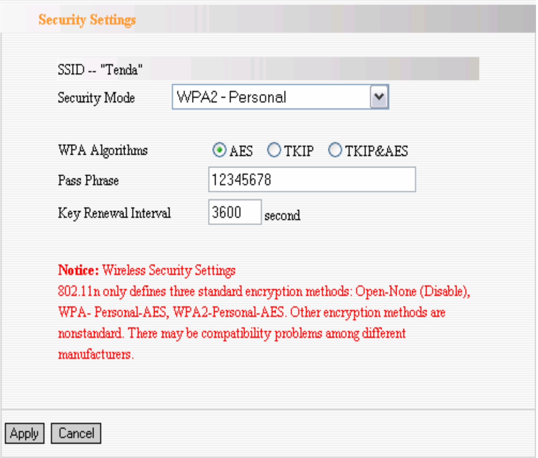
Key Renewal Interval: 3600 second

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Pass Phrase:** Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key’s renewal period.

7.2.2 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) or WPA (Wi-Fi Protected Access). Besides TKIP encryption, new AES encryption mode is provided.



Security Settings

SSID -- "Tenda"

Security Mode: WPA2 - Personal

WPA Algorithms: ● AES ○ TKIP ○ TKIP&AES

Pass Phrase: 12345678

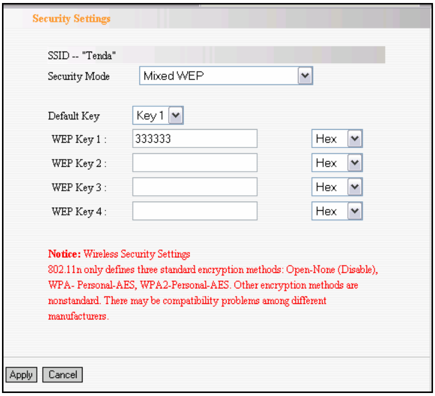
Key Renewal Interval: 3600 second

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **WPA Algorithms**: Provides TKIP [Temporal Key Integrity Protocol], AES [Advanced Encryption Standard] or TKIP&AES mixed mode.
- **Pass Phrase**: Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval**: Set the key's renewal period.

7.2.3 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window:



Security Settings

SSID -- "Tenda"

Security Mode: Mixed WEP

Default Key: Key 1

WEP Key 1 : 333333 Hex

WEP Key 2 : Hex

WEP Key 3 : Hex

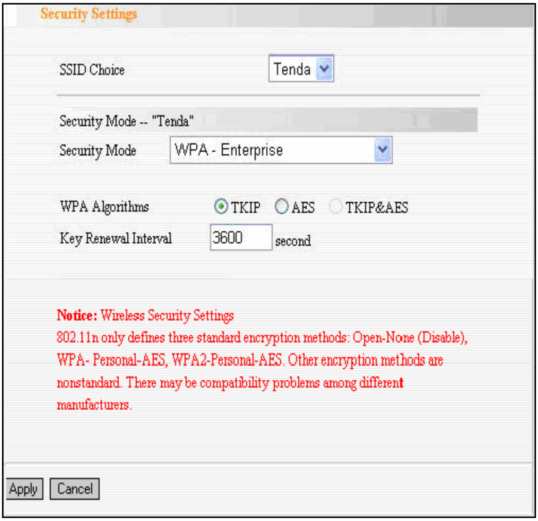
WEP Key 4 : Hex

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **Select SSID：** Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.
- **Security Mode：** From the drop-down menu select the corresponding security encryption modes.
- **WEP Key：** Set the WEP key with the format of ASCII and Hex.
- **Key Explanation:** You can enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) Or 10/26 hex characters.
- **Default Key：** Select one key from the four configured keys as the current available

7.2.4 WPA- Enterprise

This security mode is used when a RADIUS server is connected to the device. Select "WPA-Enterprise" from the drop-down menu to enter the following window:



SSID Choice: Tenda

Security Mode -- "Tenda"

Security Mode: WPA - Enterprise

WPA Algorithms: ● TKIP ○ AES ○ TKIP&AES

Key Renewal Interval: 3600 second

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

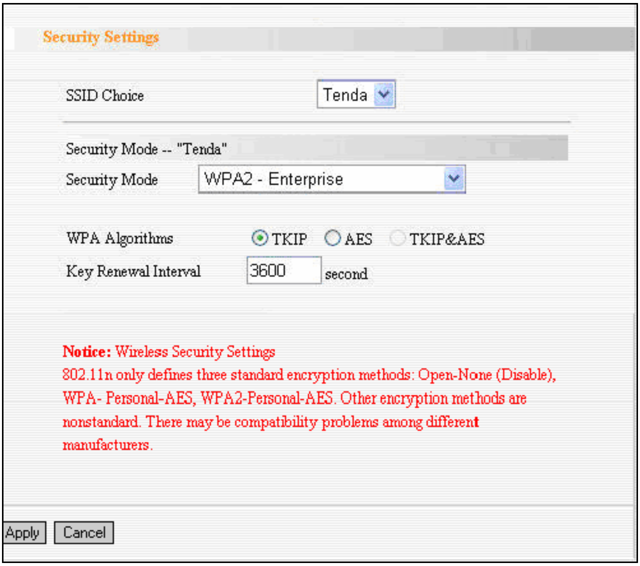
- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Key Renewal Interval:** Set the key's renewal period.
- **Radius Server Address:** Enter the IP address of the Radius server.
- **Radius Server port:** Enter the authentication

port of the Radius server. The default is 1812.

- **Shared Key：** Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout：** The authentication interval period between the Router and authentication server.

7.2.5 WPA2-Enterprise

This security mode is based on Radius authentication server and WPA2 encryption method. WPA2 is used when a RADIUS server is connected to the device. Select “WPA2-Enterprise” from the drop-down menu to enter the following window:



Security Settings

SSID Choice: Tenda

Security Mode -- "Tenda"

Security Mode: WPA2 - Enterprise

WPA Algorithms: ● TKIP ○ AES ○ TKIP&AES

Key Renewal Interval: 3600 second

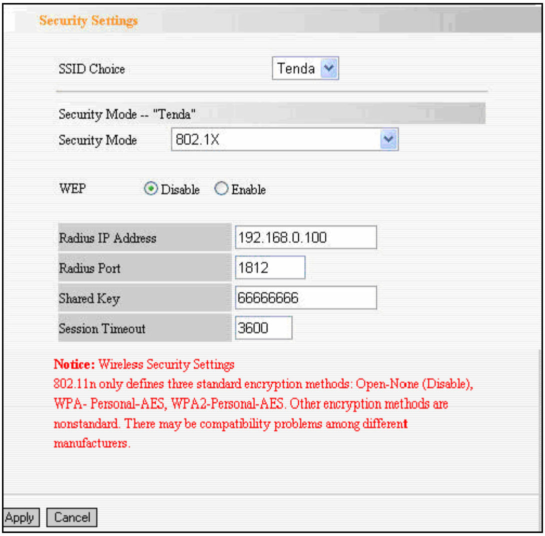
Notice: Wireless Security Settings

802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **WPA Algorithms：**Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Key Renewal Interval：**Set the key’s renewal period.
- **Radius Server Address：**Enter the IP address of the Radius server.
- **Radius Server port：**Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key：**Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout：** The authentication interval period between the Router and authentication server. The default is 3600s.

7.2.6 802.1X

This security mode is used when a RADIUS server is connected to the device. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn’t authenticated successfully, you can keep this port “disable” which just allows 802.1x authentication protocol message to pass. Select "802.1 x" from the drop-down menu to enter the following window:



SSID Choice: Tenda

Security Mode -- "Tenda"

Security Mode: 802.1X

WEP ● Disable ○ Enable

Radius IP Address	192.168.0.100
Radius Port	1812
Shared Key	66666666
Session Timeout	3600

Notice: Wireless Security Settings
802.11n only defines three standard encryption methods: Open-None (Disable), WPA- Personal-AES, WPA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

- **WEP:** Click "Enable/Disable" to enable or disable the WEP algorithm.
- **Radius Server Address:** Enter the IP address of the Radius server.
- **Radius Server Port:** Enter the authentication port of the Radius server. The default is 1812.
- **Shared Key :** Enter the shared key for authentication server with 8~63 ASCII characters.
- **Session Timeout:** The authentication interval period between AP and authentication server. The

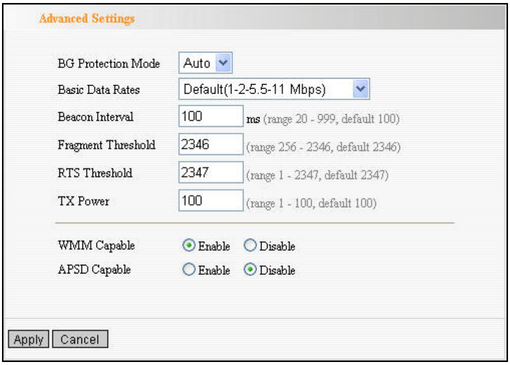
default is 3600s.

Note: To improve security level, do not use too easy characters. If you are not familiar with these ten security modes, it is recommended to use "WPA-Personal" mode.

Wireless Security Settings 802.11n only defines three standard encryption methods: Open-None (Disable), WPA-Personal-AES, PA2-Personal-AES. Other encryption methods are nonstandard. There may be compatibility problems among different manufacturers.

7.3 Advanced Settings

This section is to configure the advanced wireless setting of the Router, including the BG Protection Mode, Basic Data Rates, Fragmentation Threshold, RTS Threshold, and WMM etc.



Advanced Settings

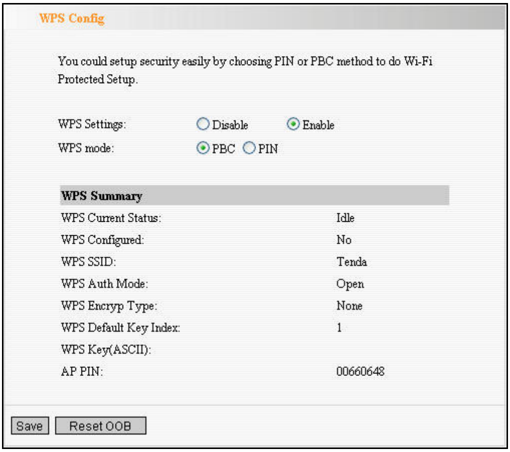
BG Protection Mode	Auto	
Basic Data Rates	Default(1-2-5.5-11 Mbps)	
Beacon Interval	100	ms (range 20 - 999, default 100)
Fragment Threshold	2346	(range 256 - 2346, default 2346)
RTS Threshold	2347	(range 1 - 2347, default 2347)
TX Power	100	(range 1 - 100, default 100)
WMM Capable	● Enable ○ Disable	
APSD Capable	○ Enable ● Disable	

- **BG protection Mode:** Auto by default. It is for 11b/g wireless client to connect 11n wireless network smoothly in a complicated wireless area.
- **Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Here, default value is (1-2-5.5.-11Mbps…). It is recommended not to modify this value.
- **Beacon Interval:** Set the beacon interval of wireless radio. Default value is 100. It is recommended not to modify this value.
- **Fragment Threshold:** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes. It is recommended not to modify this value.
- **RTS Threshold:** RTS stands for “Request to Send”. This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2346. It is recommended not to modify this value in SOHO environment.
- **TX Power:** Set the output power of wireless radio. The default value is 100.
- **WMM Capable:** It will enhance the data transfer performance of multimedia data when they’re being transferred over wireless network. It is recommended to enable this option.

- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

7.4 WPS Settings

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the device through encrypted contents. The users only enter PIN code or press WPS button on the panel to configure it without selecting encryption method and secret keys by manual. In the "Wireless settings" menu, click "WPS settings" to enter the next screen.



WPS Config

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Settings: ○ Disable ● Enable

WPS mode: ● PBC ○ PIN

WPS Summary

WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	Tenda
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII):	
AP PIN:	00660648

- **WPS settings**: To enable or disable WPS function. The default is "disable".
- **WPS mode**: Provide two ways: PBC (Push-Button

Configuration) and PIN code.

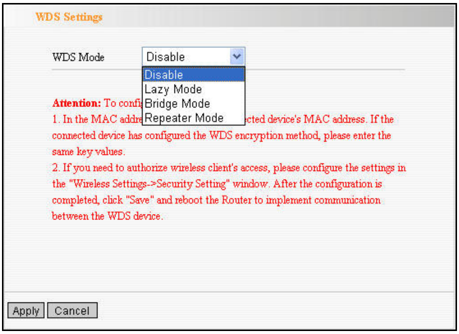
- **PBC：** Select the PBC or press the WPS button on the front panel of the device for about one second (Press the button for about one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports up to 32 clients access.)
- **PIN：** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client.
- **WPS Summary：** Show the current state of Wi-Fi protected setting, including authorized mode, encryption type, default key and other information.
- **WPS Current Status：** Idle means WPS in idle state. Start MSC process means the process has been started and waits for being connected. Configured means the negotiation is successful between server and clients.
- **WPS Configured：** "yes" means WPS feature is enabled and goes into effect. "not used" means it is not used. Usually the AP-security has been enabled, here will displayed "not used".
- **WPS SSID：** Show the main SSID set by WPS.
- **WPS Auth. Mode：** The authorization mode

deployed by WPS, generally WPA/WPA2-personal mode.

- **WPS Encrypt Type：** The encryption type used by WPS, generally AES/TKIP.
- **WPS key：** The effective key generated by AP automatically.
- **AP PIN（KEY）：** The PIN code used by default.
- **Reset OOB：** When this button is pressed, the WPS client will be idle state, and WPS indicator will be turned off. AP will not respond the WPS client's requests and the set the security mode as WPA mode.

7.5 WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.



Attention: To confi

1. In the MAC addre cted device's MAC address. If the connected device has configured the WDS encryption method, please enter the same key values.

2. If you need to authorize wireless client's access, please configure the settings in the "Wireless Settings->Security Setting" window. After the configuration is completed, click "Save" and reboot the Router to implement communication between the WDS device.

Lazy: In this mode, the connected device can be Bridge mode or Repeater mode and enter the Router's BSSID to establish the connection.

Bridge Mode: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table.

Repeater Mode： In this mode, add the opposing MAC address into each own AP MAC address table by manual or scanner to enlarge and extend the wireless radio.

Encrypt Type: Select one from WEP, TKIP, AES for security here.

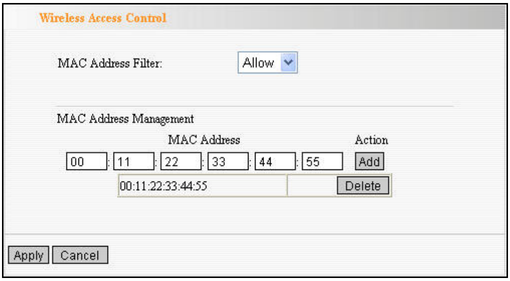
Pass phrase: Enter the encrypted key for wireless devices.

AP MAC Address: Input the MAC address of another (opposing) wireless router you want to connect.

NOTE: It is recommended that two wireless routers keep the same bandwidth, channel number, and security settings. Apply the settings and reboot the Router to activate it.

7.6 Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management to allow or block the specific clients to access the wireless network. Select “Wireless Setting->Access Control” to display the following screen:



Wireless Access Control

MAC Address Filter: Allow

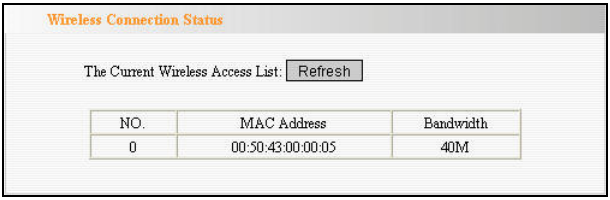
MAC Address Management

MAC Address	Action
00 : 11 : 22 : 33 : 44 : 55	Add
00:11:22:33:44:55	Delete

- **MAC Address Filter**：Enable/disable MAC address filter. Select “off” to malfunction MAC address; “disable” to prevent the MAC addresses in the list from accessing the wireless network; “Allow” to allow the MAC address in the list to access the wireless network.
- **MAC Address Management**：Input the MAC address to implement the filter policy. Click “Add” to finish the MAC add operation.
- **MAC Address list**：Show the added MAC addresses. You can add or delete them.

7.7 Connection Status

This page shows wireless client’s connection status, including MAC address, Channel bandwidth, etc. Select “Wireless Setting->connection status” to enter the following screen:



Wireless Connection Status

The Current Wireless Access List:

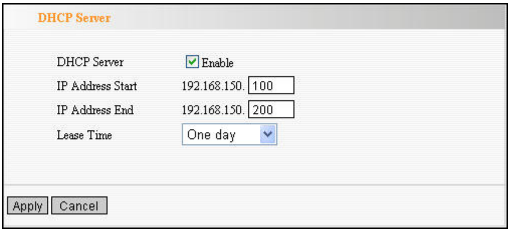
NO.	MAC Address	Bandwidth
0	00:50:43:00:00:05	40M

- **MAC Address**: Shows current MAC addresses of the hosts connecting to the Router.
- **Bandwidth**: Shows current frequency bandwidth the wireless client used.

Chapter 8: DHCP Server

8.1 DHCP Settings

DHCP (Dynamic Host Control Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating "Obtain an IP Address Automatically". So specifying the starting and ending address of the IP Address pool is needed.



DHCP Server

DHCP Server ☑ Enable

IP Address Start 192.168.150. 100

IP Address End 192.168.150. 200

Lease Time One day

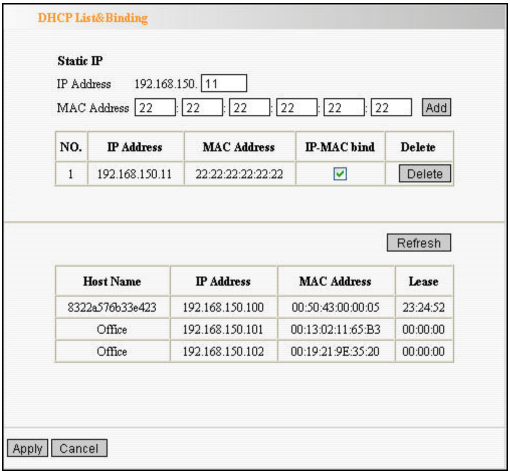
- **DHCP Server:** Activate the checkbox to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP address pool for DHCP server distribution.
- **Lease Time:** The length of the IP address lease.

For example:

If the lease time is an hour, then DHCP server will reclaim the IP address each hour.

8.2 DHCP List and Binding

The Static IP assignment is to add a specifically static IP address to the assigned MAC address. You can view the related information in the DHCP server list.



IP Address 192.168.150. 11

MAC Address 22 : 22 : 22 : 22 : 22 : 22 Add

NO.	IP Address	MAC Address	IP-MAC bind	Delete
1	192.168.150.11	22:22:22:22:22:22	☑	Delete

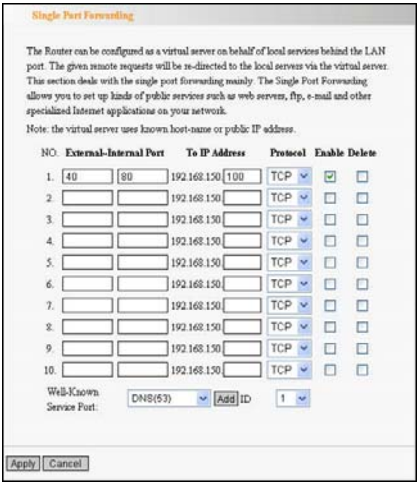
Host Name	IP Address	MAC Address	Lease
8322a576b33e423	192.168.150.100	00:50:43:00:00:05	23:24:52
Office	192.168.150.101	00:13:02:11:65:B3	00:00:00
Office	192.168.150.102	00:19:21:9E:35:20	00:00:00

- **IP Address:** Enter the IP address which needs to be bound.
- **MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click "Add" to add the entry in the list.
- **Hostname:** The name of the computer which is added a new IP address.
- **Lease Time:** The left time length of the corresponding IP address lease.

Chapter 9 Virtual Server

9.1 Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.



Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

Note: the virtual server uses known host-name or public IP address.

NO.	External-Internal Port		To IP Address	Protocol	Enable	Delete
1.	40	80	192.168.150. 100	TCP	☑	□
2.			192.168.150.	TCP	□	□
3.			192.168.150.	TCP	□	□
4.			192.168.150.	TCP	□	□
5.			192.168.150.	TCP	□	□
6.			192.168.150.	TCP	□	□
7.			192.168.150.	TCP	□	□
8.			192.168.150.	TCP	□	□
9.			192.168.150.	TCP	□	□
10.			192.168.150.	TCP	□	□

Well-Known Service Port: DNS(53) Add ID 1

- **External Port:** This is the external (WAN) port number for server or Internet application, for example, port 21 for ftp service.

- **Internal Port:** This is the port number of LAN computer set by the Router. The Internet traffic from the external port will forward to the internal port. For example：you can set the internal port NO.66 to act as the external port NO.21 for ftp service.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Add:** Add the selected well-known port to the policy ID.

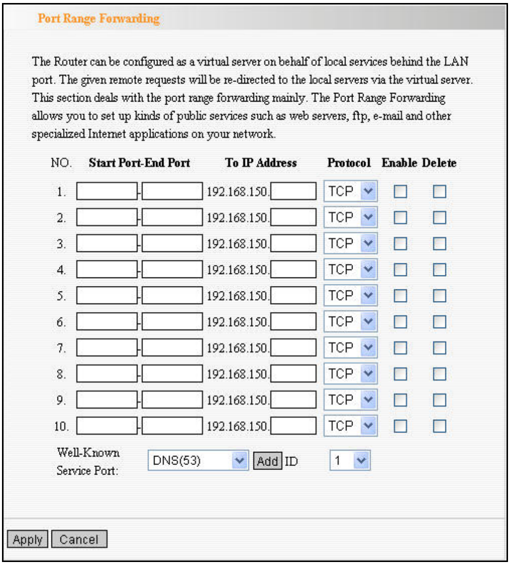
For example:

You can establish a WEB server at the computer with the IP address of 192.168.0.10 in LAN and the server use the port of 80. If you can visit the WEB server in WAN when you enter http://x.x.x.x:40, you can enter 40 at the “WAN Ports “on this page and enter 80 at the “LAN Ports”. “LAN IP” set 192.168.0.10. “Protocol” selects all. It takes effect after saving the settings.

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

9.2 Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.



Port Range Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

NO.	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.	-	192.168.150.	TCP	□	□
2.	-	192.168.150.	TCP	□	□
3.	-	192.168.150.	TCP	□	□
4.	-	192.168.150.	TCP	□	□
5.	-	192.168.150.	TCP	□	□
6.	-	192.168.150.	TCP	□	□
7.	-	192.168.150.	TCP	□	□
8.	-	192.168.150.	TCP	□	□
9.	-	192.168.150.	TCP	□	□
10.	-	192.168.150.	TCP	□	□

Well-Known Service Port: DNS(53) Add ID 1

- **Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.
- **IP Address:** Enter the IP address of the PC where you want to set the applications.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application.
- **Delete/Enable:** Click to check it for corresponding operation.
- **Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.
- **Add:** Add the selected well-known port to the policy ID.

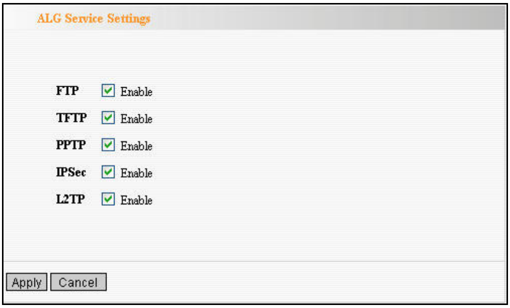
For example:

The server at the IP address of 192.168.0.10 in LAN provides WEB service at the port of 80 and Telnet service at the port of 23. If you want the clients on the Internet to visit this server, please set the device as the diagram above.

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

9.3 ALG Service Settings

In the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications etc.



ALG Service Settings

FTP ☑ Enable

TFTP ☑ Enable

PPTP ☑ Enable

IPSec ☑ Enable

L2TP ☑ Enable

In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

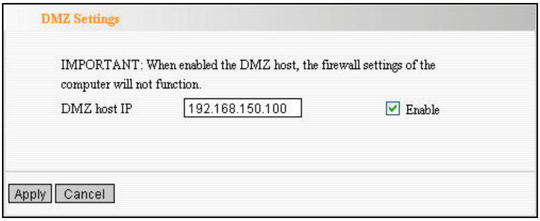
Usually allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.

In the default ALG settings, the following protocols have enabled. It is recommended to keep the settings unchanged.

1. FTP
2. TFTP
3. PPTP
4. IPSec
5. L2TP

9.4 DMZ Settings

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.



DMZ Settings

IMPORTANT: When enabled the DMZ host, the firewall settings of the computer will not function.

DMZ host IP 192.168.150.100 ☑ Enable

- **DMZ Host IP Address:** The IP address of the computer you want to expose.
- **Enable:** Click the checkbox to enable the DMZ host.

For example:

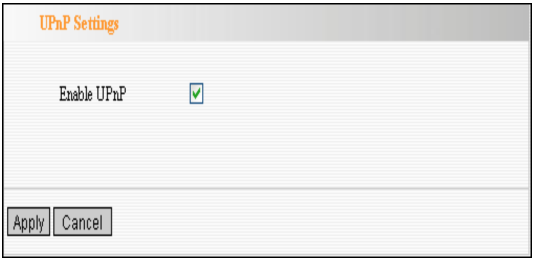
Set the computer at the IP address of 192.168.0.10 in LAN as a DMZ Host to intercommunicate with another host on the Internet.

IMPORTANT:

When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

9.5 UPNP Settings

It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.



UPnP Settings

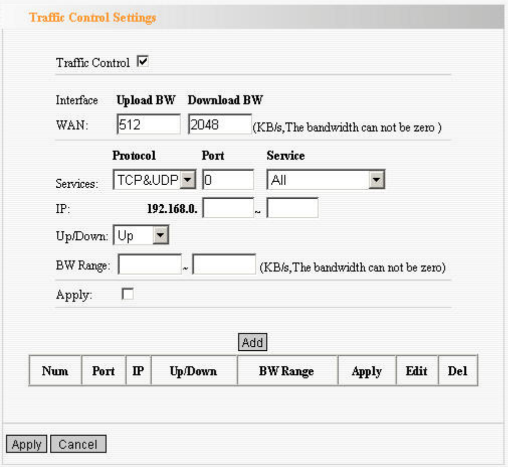
Enable UPnP ☑

- **Enable UPnP:** Click the checkbox to enable the UPnP.

Chapter 10 Traffic Control

10.1 Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.



Traffic Control Settings

Traffic Control ☑

Interface Upload BW Download BW

WAN: 512 2048 (KB/s,The bandwidth can not be zero)

Protocol Port Service

Services: TCP&UDP 0 All

IP: 192.168.0. ~

Up/Down: Up

BW Range: ~ (KB/s,The bandwidth can not be zero)

Apply: □

Add

Num	Port	IP	Up/Down	BW Range	Apply	Edit	Del

Apply Cancel

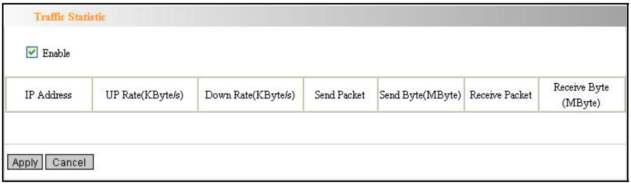
- **Enable Traffic Control:** To enable or disable the internal IP bandwidth control. The default is disabled.
- **Interface:** To limit the uploading and downloading bandwidth in WAN port.
- **Service:** To select the controlled service type, such as HTTP service.
- **IP Starting Address:** The first IP address for traffic control.
- **IP Ending Address:** The last IP address for traffic control.
- **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- **Bandwidth:** To specify the uploading/downloading

Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.

- **Apply:** To enable the current editing rule. If not, the rule will be disabled.
- **Add:** After edit the rule, click the "add to list" button to add the current rule to rule list.
- **Apply:** Click "Save" to activate the current rule.
- **Cancel:** Click "Cancel" to drop all setting saved last time.

10.2 Traffic Statistics

Traffic statistics is used to show the LAN PC's traffic information.



Traffic Statistic

☑ Enable

IP Address	UP Rate(KByte/s)	Down Rate(KByte/s)	Send Packet	Send Byte(MByte)	Receive Packet	Receive Byte (MByte)

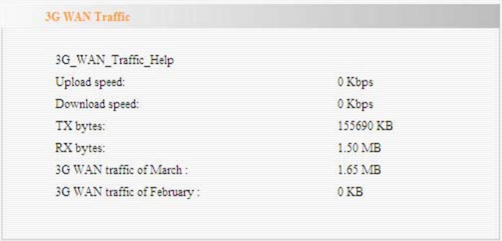
- **Enable traffic statistics:** check to enable traffic statistics. Usually traffic statistics is disabled, which can improve the Router's data handling. The default is disabled. If it is enabled, the page will update the PC's traffic information automatically and be refreshed every 5 seconds.
- **IP address:** The IP address to be shown.
- **Upstream rate:** the speed of upstream data per second (Kbyte/S).

- **Downstream rate:** the speed of downstream data per second (Kbyte/S).
- **Sending packet:** The PC's packets sending from the PC.
- **Sending byte:** The byte (Mbyte) sending from the PC.
- **Receiving packet:** The PC's packets received from the Router.
- **Receiving byte:** The PC's byte (Mbyte) received from the Router.

Chapter 11 3G WAN Traffic and Connection Timer

11.1 3G WAN Traffic

In 3G WAN mode, 3G WAN traffic function is supported. Click "3G WAN traffic" you can check the router's Internet traffic, transmission rate, transmission data volume and traffic for nearly two months, so that you can know how much the traffic that the 3G modem card accesses the Internet without running up bills.



3G WAN Traffic

3G_WAN_Traffic_Help

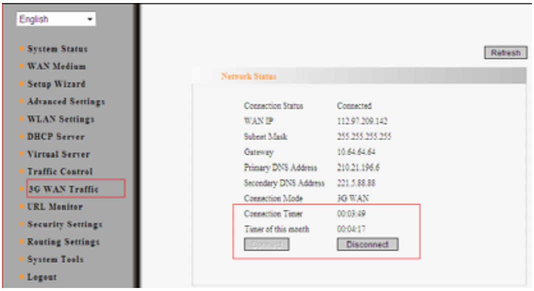
Upload speed:	0 Kbps
Download speed:	0 Kbps
TX bytes:	155690 KB
RX bytes:	1.50 MB
3G WAN traffic of March :	1.65 MB
3G WAN traffic of February :	0 KB

Notice: this function is only for 3G WAN.

In 3G Router mode, 3G WAN traffic is used to calculate the traffics of WAN port. Click "3GWAN Traffic" then you can inquiry the status such as the status

11.2 Connection Timer

In 3G WAN mode, Connection Timer function is supported. Click "System Status" then you can see the WAN port connection time, internet access time of this month and other status.



Network Status

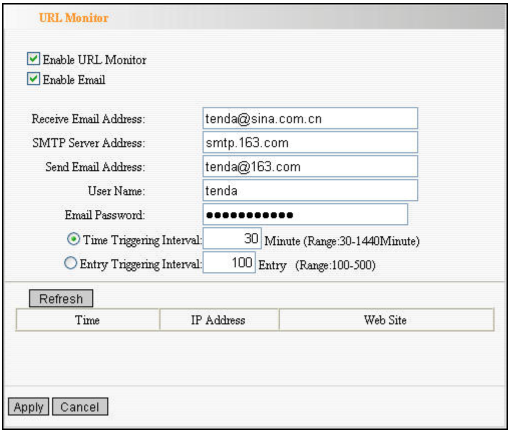
Connection Status	Connected
WAN IP	112.97.209.142
Subnet Mask	255.255.255.255
Gateway	10.64.64.64
Primary DNS Address	210.21.196.6
Secondary DNS Address	221.5.88.88
Connection Mode	3G WAN
Connection Timer	00:03:49
Timer of this month	00:04:17

Note: The result of 3G WAN Traffic and Connection Timer are only for reference. This device can only calculate the status that the 3G modem card plugs into the device. The actual statistics is subject to the ISP.

Chapter12 URL Monitor

12.1 URL Monitor

This feature is used to record user's Internet activity, so in terms of this feature, the administrator can check out and control what they can do and have done.



URL Monitor

☑ Enable URL Monitor

☑ Enable Email

Receive Email Address: tenda@sina.com.cn

SMTP Server Address: smtp.163.com

Send Email Address: tenda@163.com

User Name: tenda

Email Password: ●●●●●●●●●●●●

● Time Triggering Interval: 30 Minute (Range:30-1440Minute)

○ Entry Triggering Interval: 100 Entry (Range:100-500)

Time	IP Address	Web Site

- **Enable URL Monitor:**

  After checking this feature, the Router will record LAN computer's URL information, including the visiting Website, your LAN IP address and the time. The Router can record up to 500 entries. If the record is more than 500 entries, the counter will clean all records and restart the URL record again. If the Router is powered off and restarts the device, the records will be also lost. The default setting is disabled.

- **Enable Email:** To enable this feature, the URL records will be sent to specified e-mail, which can be solved the problem that the records will be lost when it is over 500 entries.
- **Receive E-mail Address:** Input the received E-mail's address here. For example: tenda@sina.com.cn
- **SMTP Server Address:** Input the SMTP server address here. If you are not clear what your SMTP server's address is, you can find them from Help page of the registered e-mail. For example: smtp.sohu.com, smtp.163.com, etc.
- **Send Email Address:** Input the sending email address here.
- **User Name:** Input the sending e-mail's user name.
- **Email Password:** Input the sending e-mail's password.
- **Time Triggering Interval:** To set sending e-mail's time interval. The time ranges from 30 to

1440 minutes.

For example: if you input 30 here, it means the Router will send an email from “Send Email Address” to “Receive Email Address” in every 30 minutes. And then the device will clean all records and start the recording again.

- **Entry Triggering Interval:** To set sending e-mail’s entry interval. The entry ranges from 100 to 500.

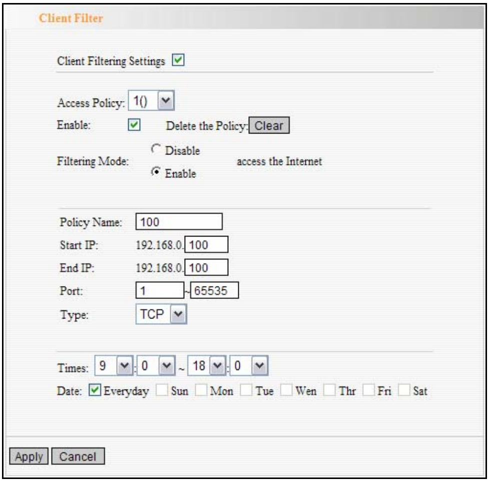
For example:

If you input 100 here, it means the Router will send an email from “Send Email Address” to “Receive Email Address” every 100 entries. And then the device will clean all records and start the recording again.

Chapter 13 Security Settings

13.1 Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.



Client Filter

Client Filtering Settings ☑

Access Policy: 1()

Enable: ☑ Delete the Policy: Clear

Filtering Mode: ○ Disable ● Enable access the Internet

Policy Name: 100

Start IP: 192.168.0.100

End IP: 192.168.0.100

Port: 1 ~ 65535

Type: TCP

Times: 9 : 0 ~ 18 : 0

Date: ☑ Everyday □ Sun □ Mon □ Tue □ Wen □ Thr □ Fri □ Sat

- **Client Filter:** Check to enable client filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **IP Start/End:** Enter the starting/ending IP address.
- **Port No.:** Enter the port range based over the protocol for access policy.
- **Protocol:** Select one protocol (TCP/UDP/Both)

from the drop-down menu.

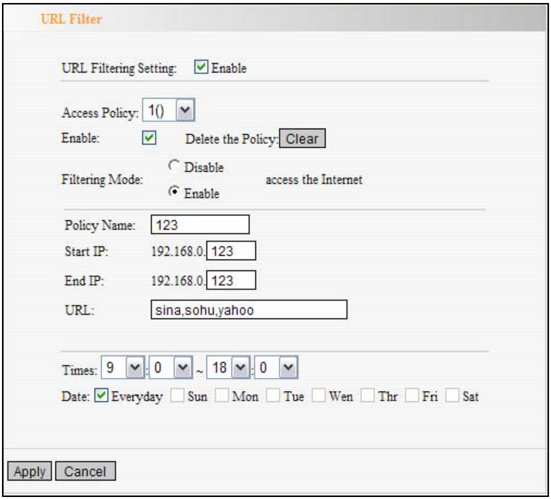
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.

For example:

If you don’t want the computer at the IP address of 192.168.0.100 to access the Internet from 9：00 to 18：00 everyday without restrictions to other computers in LAN, you need to set the packet filtering list as the above diagram.

13.2 URL Filter Settings

In order to control the computer to have access to websites, you can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.



URL Filter

URL Filtering Setting: ☑ Enable

Access Policy: 1()

Enable: ☑ Delete the Policy: Clear

Filtering Mode: ○ Disable ● Enable access the Internet

Policy Name: 123

Start IP: 192.168.0. 123

End IP: 192.168.0. 123

URL: sina,sohu,yahoo

Times: 9 : 0 ~ 18 : 0

Date: ☑ Everyday □ Sun □ Mon □ Tue □ Wen □ Thr □ Fri □ Sat

- ➢ **URL Filter:** Check to enable URL filter.
- ➢ **Access Policy:** Select one number from the drop-down menu.
- ➢ **Enable:** Check to enable the access policy.
- ➢ **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- ➢ **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- ➢ **Policy Name:** Enter a name for the access policy selected.
- ➢ **Start/End IP:** Enter the starting/ending IP address.
- ➢ **URL Strings:** Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.
- ➢ **Times:** Select the time range of client filter.

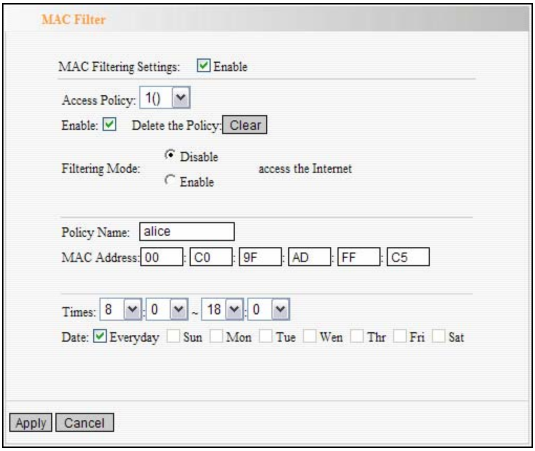
- **Days:** Select the day(s) to run the access policy.
- **Save:** Select Save to enable the settings.

For example:

If you want the computer at the IP address of 192.168.0.123 to access the Internet from 9：00 to 18：00 everyday and only can search the WEB pages contain the strings such as sina, sohu, and yahoo, you need to set the packet filtering list as the above diagram. (Notice: different strings need to be aparted by a comma.)

13.3 MAC Address Filter

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.



MAC Filtering Settings: ☑ Enable

Access Policy: 1()

Enable: ☑ Delete the Policy:

Filtering Mode: ● Disable ○ Enable access the Internet

Policy Name: alice

MAC Address: 00 : C0 : 9F : AD : FF : C5

Times: 8 : 0 ~ 18 : 0

Date: ☑ Everyday □ Sun □ Mon □ Tue □ Wen □ Thr □ Fri □ Sat

- **MAC Address Filter:** Check to enable MAC address filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** Check to enable the access policy.
- **Clear the Policy:** Click “Clear” button to clear all settings for the policy.
- **Filter Mode:** Click one radio button to enable or disable to access the Internet.
- **Policy Name:** Enter a name for the access policy selected.
- **MAC Address:** Enter the MAC address you want to run the access policy.
- **Times:** Select the time range of client filter.
- **Days:** Select the day(s) to run the access policy.
- **Apply**： Click to make the settings go into effect.

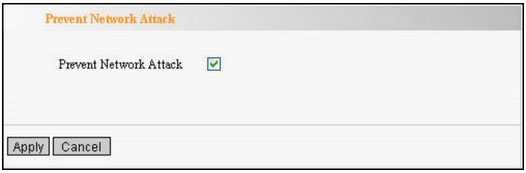
For example:

If you want to configure the host with MAC address 00:C0:9F:AD:FF:C5 not to access the Internet at 8：00-18：00, you need to set it as above.

13.4 Prevent Network Attack

This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically.

The attacker’s IP address can be found from the “System Log”.



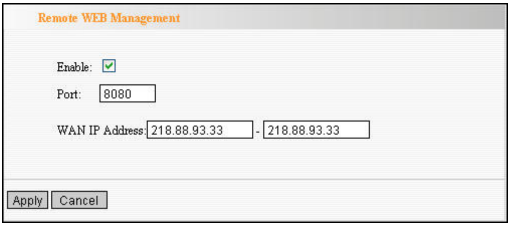
Prevent Network Attack

Prevent Network Attack ☑

- **Prevent Network Attack:** Check to enable it for attack prevention.

13.5 Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the "Enable".



Remote WEB Management

Enable: ☑

Port: 8080

WAN IP Address: 218.88.93.33 - 218.88.93.33

- **Enable:** Check to enable remote web management.
- **Port:** The management port open to outside access. The default value is 80.
- **WAN IP Address:** Specify the range of the WAN IP address for remote management.

Note：

1. If you want to login the device's Web-based interface via port 8080, you need use the format of WAN IP address: port (for example http://219.134.32.101: 8080) to implement remote login.

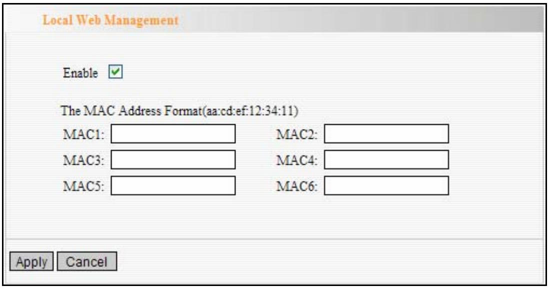
2. If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 218.88.93.33-218.88.93.35, then only the IP addresses as 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the Router.

For example:

If you want to configure the IP address 218.88.93.33 to access the device's web interface, please set it as above.

13.6 Local Web Management

Local web management, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.



Local Web Management

Enable ☑

The MAC Address Format(aa:cd:ef:12:34:11)

MAC1:
MAC2:
MAC3:
MAC4:
MAC5:
MAC6:

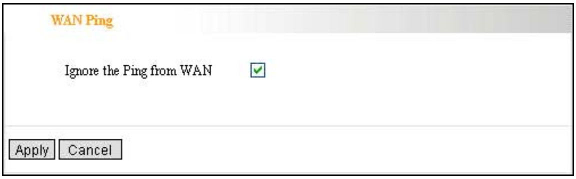
- **Enable:** Check to enable the local web management.
- **MAC Address:** Enter the MAC addresses of LAN computers.

Note：1. In the default state, this feature is not enabled. All computers in the LAN can login the Web.

2. For example, if you only allow the MAC address with 00:11:22:33:E4:F5 to access the web, please set it as above.

13.7 WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.



WAN Ping

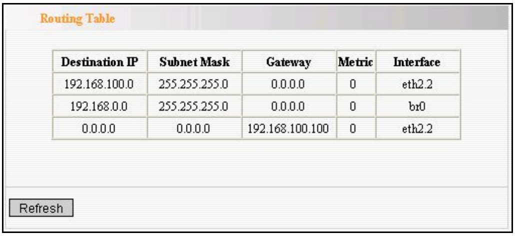
Ignore the Ping from WAN ☑

- **Ignore Ping from WAN:** Check to ignore the ping request and give no reply.

Chapter 14 Routing Setting

14.1 Routing Table

The main duty for a router is to look for a best path for every data frame, and transfer this data frame to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.

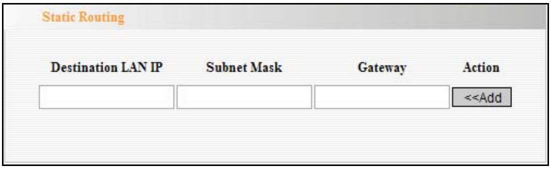


Routing Table

Destination IP	Subnet Mask	Gateway	Metric	Interface
192.168.100.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
0.0.0.0	0.0.0.0	192.168.100.100	0	eth2.2

14.2 Static Routing

This page is used to configure the Router's static routing.



- **Destination LAN IP:** The address of the remote host with which you want to construct a static route.

- **Subnet Mask:** The network portion of the Destination LAN IP.
- **Gateway:** The gateway of the next hop, usually the Router or host’s IP address.

Note：

1. The gateway must keep the same segment with the Router’s LAN IP address.

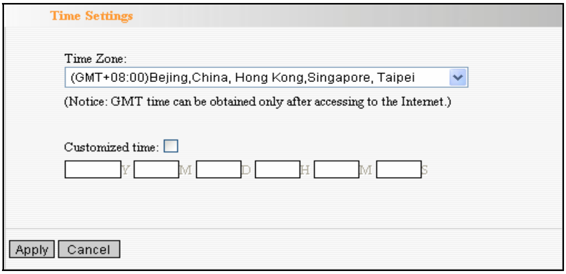
2. If the destination IP address is one host’s IP address, the Subnet mask should be 255.255.255.255.

3. If the destination IP address is an IP address range, the subnet mask should match the IP address. For example, if the IP is 10.0.0.0, subnet mask should be 255.0.0.0; if the IP is 10.1.2.0, subnet mask should be 255.255.255.0.

Chapter 15 System Tools

15.1 Time Settings

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.



Time Settings

Time Zone:

(GMT+08:00)Bejing,China, Hong Kong,Singapore, Taipei

(Notice: GMT time can be obtained only after accessing to the Internet.)

Customized time: □

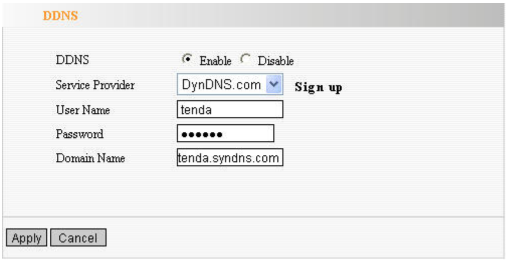
- **Time Zone:** Select your time zone from the drop-down menu.
- **Customized time:** Enter the time you customize.

Note:

When the Router is powered off, the time setting will be lost. Before the Router will obtain GMT time automatically, you need connect with the Internet and obtain the GMT time, or set the time on this page first. Then the time in other features (e.g. firewall) can be activated.

15.2 DDNS

The DDNS (Dynamic Domain Name System) is supported in this Router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select “Enable” and a DDNS service provider to sign up.



DDNS

DDNS	● Enable ○ Disable
Service Provider	DynDNS.com Sign up
User Name	tenda
Password	••••••
Domain Name	tenda.syndns.com

- **Main Features:**

  Owing to ISP most times provides dynamic IP address, DDNS is used to capture the changeable IP address and match the fixed domain. Then users can have access to the Internet to communicate with others.

  DDNS can help you establish virtual host in your home and company.

- **DDNS:** Click the radio button to enable or disable the DDNS service.
- **Service Provider:** Select one from the drop-down menu and press “Sign up” for registration.
- **User Name:** Enter the user name the same as the registration name.
- **Password:** Enter the password you set.
- **Domain Name:** Enter the domain name which is optional.

For example:

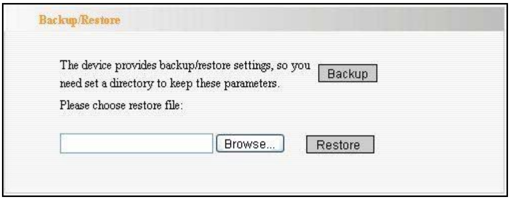
In the local host 192.168.0.10 establish a Web server, and register in 3322.org as follows:

User name	tenda
Password	123456
Domain Name	tenda.vicp.net

After mapping the port in the virtual server, setting account information in DDNS server and in the address field entering http://tenda.3322.org, you can access the Web page.

15.3 Backup/Restore Settings

The device provides backup/restore settings, so you need set a directory to keep these parameters.



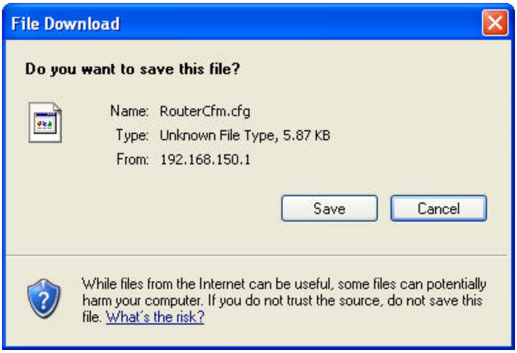
Backup/Restore

The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

- **Backup Setting:**

  Click “Backup” button to back up the Router’s settings and select the path for save.



File Download

Do you want to save this file?

Name: RouterCfm.cfg

Type: Unknown File Type, 5.87 KB

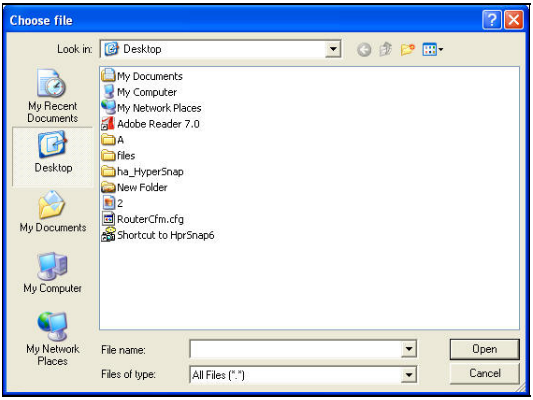
From: 192.168.150.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Click “Save” to save the configuration files.

- **Restore Setting:**

Click “Browse” button to select the backup files.



Choose file

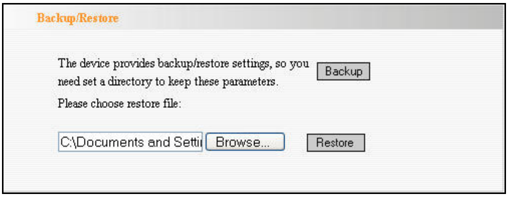
Look in: Desktop

My Documents
My Computer
My Network Places
Adobe Reader 7.0
A
files
ha_HyperSnap
New Folder
2
RouterCfm.cfg
Shortcut to HprSnap6

File name:

Files of type: All Files (*.*)

Click “Restore” button to restore previous settings.



Backup/Restore

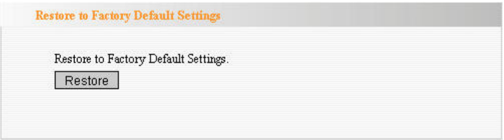
The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

C:\Documents and Setti

15.4 Restore to Factory Default Setting

This button is to reset all settings to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.



Restore to Factory Default Settings

Restore to Factory Default Settings.

- **Restore:** Click this button to restore to default settings.
- **Factory Default Settings:**

  User Name: admin

  Password: admin

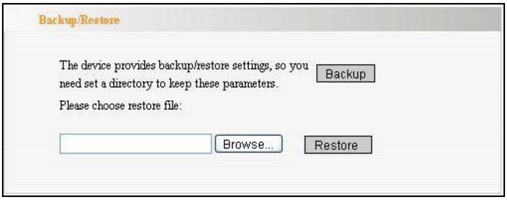
  IP Address: 192.168.0.1

  Subnet Mask: 255.255.255.0

NOTE: After restoring to default settings, please restart the device, then the default settings can go into effect.

15.5 Upgrade Firmware

The Router provides the firmware upgrade by clicking the "Upgrade" after browsing the firmware upgrade packet which you can download from www.tenda.cn.



Backup/Restore

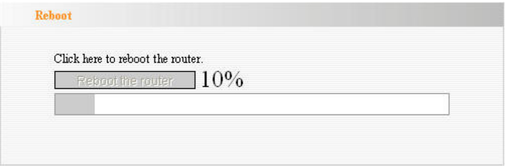
The device provides backup/restore settings, so you need set a directory to keep these parameters.

Please choose restore file:

- **Browse:** click this button to select the upgrade file.
- **Upgrade:** click this button to start the upgrading process. After the upgrade is completed, the Router will reboot automatically.

15.6 Reboot the Router

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.



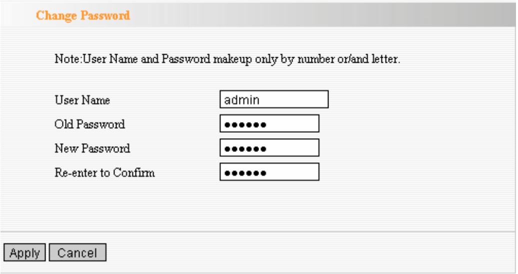
Reboot

Click here to reboot the router.

Reboot the router: Click this button to reboot the device.

15.7 Password Change

This section is to set a new user name and password to better secure your router and network.



Change Password

Note:User Name and Password makeup only by number or/and letter.

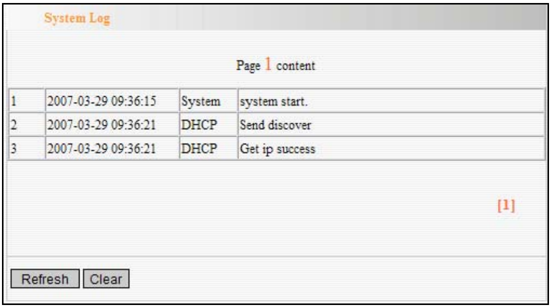
User Name	admin
Old Password	••••••
New Password	••••••
Re-enter to Confirm	••••••

- **User Name:** Enter a new user name for the device.
- **Old Password:** Enter the old password.
- **New Password:** Enter a new password.
- **Re-enter to Confirm:** Re-enter to confirm the new password.

NOTE: It is highly recommended to change the password to secure your network and the Router.

15.8 System Log

The section is to view the system log. Click the “Refresh” to update the log. Click “Clear” to clear all shown information. If the log is over 150 records, it will clear them automatically.



System Log

Page 1 content

1	2007-03-29 09:36:15	System	system start.
2	2007-03-29 09:36:21	DHCP	Send discover
3	2007-03-29 09:36:21	DHCP	Get ip success

[1]

- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the current shown log.

15.9 Logout

After you have finished the settings completely, in logout page click “Yes” to logout the web management page.

Appendix Ⅰ：Glossary

3G

3G, the 3rd Generation, refers to the third digital communication technology. It can manage multi-media such as image, audio, and video streams etc. and provide different communication services such as web browse, telephone session, and electronic business etc.

CDMA2000

CDMA2000, also called CDMA Multi-Carrier, is one of the current three 3G standards in the world which was put forward by an American company. The system derives from narrow frequency CDMAOne digital standard. You can upgrade the original CDMAOne structure to 3G with cheap construction cost.

WCDMA

WCDMA (Wideband CDMA), also called CDMA Direct Spread, is the broadband CDMA technology which was put forward by Europe. It is the standard of 3G technology which was developed from GSM network. The standard has put forward the evolved strategy. The system can be established on the present GSM network. The system provider can change into this system easily and it would be accepted widely in Asia. Thus, W-CDMA has a born advantage in market and is one of the three 3G standards in the world.

Channel

An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID

Service Set Identifier, An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP

Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommended using.

WPA/WPA2

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

802.1x Authentication

Static WEP key is difficult to manage. When you change the key, you need to inform everyone. Once the key is disclosed, there is no security. In addition, since static WEP encryption has serious security holes, the WEP key can be decrypted by receiving multiple data. 802.1X was first used in the wired Ethernet connection to prevent illegal users using the network. Later, people discovered that 802.1x authentication can be used to solve the security problems of wireless network connection. The EAP-TLS of 802.1x accomplished the bidirectional authentication between the users and networks. It can either prevent the illegal users using the network or the users connecting to the illegal AP. 802.1x uses dynamic WEP encryption to prevent the decryption of WEP Key. In order to solve the distributing problems of digital certificates, people improve the TLS certificate into TTLS and PEAP. Thus, users can use the traditional Username authentication method to access the Internet.

Appendix Ⅱ: Troubleshooting

In this part some questions and problems shown during the Router's usage and installation will be given suggesting answers. If your problems are not in the list, please log into our website www.tenda.cn or send an E-mail to support@tenda.cn, and we will reply you in the earliest time.

1. Why can't I login to the Web interface of the Router after entering the IP address in the address field?

Step 1: check the Router if it works well. Once the device is powered on for a few seconds, the SYS indicator on the panel will be turned on. If it is not, please contact us.

Step 2: check the network cables if it is good and the corresponding indicator is "Always ON". Sometimes, the indicator is "Always ON", but it does not mean it gets through.

Run "Ping" command and check if it can ping the Router's LAN IP address 192.168.0.1. If it is OK, please make sure your browser does not access the Internet by proxy server. If the ping fails, you can press the "RESET" button for 7 seconds to restore to default settings. And then repeat the ping operation. If it still does not work, please contact us.

2. Forget the login password and can not enter the setting page. What can I do?

Press the “RESET” button for 7 seconds to restore the Router to default settings.

3. The computer connected with the Router shows IP address conflict. What can I do?

Check if there are other DHCP servers in the LAN. If there have, disable them.

The default IP address of the Router is 192.168.0.1 and please maker sure the address is not occupied by other devices. If there are two computers with the same IP addresses, please modify one.

4. I can not use E-mail and access the Internet. What can I do?

It happens in ADSL connection and Dynamic IP users. And you need modify the default MTU value (1492). Please in the “WAN Setting” modify the MTU value with the recommended value as 1450 or 1400.

5. How can I configure and access the Internet via Dynamic IP?

In Setup Wizard of the Web utility interface, select “Dynamic IP” connection type and click “Save” to activate it. As some ISPs bind the user computer’s MAC address, you need to clone the Router’s WAN MAC address to the bind21ing PC’s MAC address. Select “MAC Address Clone” in “Advanced Setting” to input your computer’s MAC address and click “Apply” to activate it.

6. How to share my computer’s source with other users in Internet?

If you want Internet users to access the internal server via the Router such as e-mail server, Web, FTP, you can configure the “Virtual Server” to come true.

Step 1: create your internal server, make sure the LAN users can access these servers and know related service port. For example, Web server’s port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: in the Router’s web click “Virtual Server” and select “Single Port Forwarding”.

Step 3: input the external service port given by the Router, for example, 80.

Step 4: input the internal Web service port, for example, 80.

Step 5: Input the internal server’s IP address. If your Web server’s IP address is 192.168.0.10, please input it.

Step 6: select the communication protocol used by your internal host: TCP, UDP, ICMP.

Step 7: click “Apply” to activate the settings.

The following table has listed the well-known application and service port:

Server	Protocol	Service Port
WEB Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
NetMeeting	TCP	1503、1720
MSN Messenger	TCP/UDP	File 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

7. Why can’t I use my 3G Modem Card to connect the Internet?

a. Please make sure that you have inserted a SIM card into your 3G Modem Card, you have enabled the ISP 3G data Internet business, and you can use your 3G Modem Card to access the Internet by connecting it to the computer directly.

b. Please make sure that your 3G Modem Card is connected to the Router’s USB port well.

c. Please make sure that your 3G Modem Card Model is compatible with the Router. You can search the related model No. on the compatible product list.

d. Please make sure that the 3G modem card model selected in the 3G Web interface matches the practical product and the settings you entered match the parameters by your ISP.

e. Please download the latest upgrading firmware. After trying the steps above, if you still can't access the Internet, please contact us and we will try our best to solve the problems for you.

8. Why can't I use wireless WAN function to access the Internet?

a. Please make sure that the wireless adapter can access the Internet when connected to the computer, wireless signals scanned by the adapter are strong enough, and quality of signals is good enough. If it can scan too many wireless signals, we recommend you to use 11b/g mode for reducing interference.

b. Please make sure that the needed parameters such as SSID, MAC address etc. are correct. It is recommended to use Auto Scan to finish the settings in the setup process.

c. Please make sure that IP address range obtained at WAN port are different as the one obtained at LAN port. If they are at the same range, you can modify the LAN IP address to solve the problem.

d. Please do not detach any antenna of the wireless Router when you are using the Router.

After trying all the above steps, if you still can’t access the Internet, you can contact us for assistant.

9. Why do the charges increase after using a 3G Modem Card?

a. At present, 3G Modem Card charges according to the traffic or the time. It is recommended to pull out your 3G Modem Card or turn off the power of the Router when you are not using Internet for avoiding unnecessary charges.

b. The traffic when multiple computers are sharing one Internet access line is more intensive than the traffic when only one computer is using the Internet.

After trying all the above steps, if you still can’t access the Internet, you can contact us for support.

If you still have some problems, please contact our customer service or log on our website.

Website: http://www.tenda.cn

➢ Technical Support

- **Toll Free:** 400-6622-666 (For Mainland China Only)
- **Toll Free:** 1-800-570-5892 (For USA only)
- **Tel:** +86 (755) 2344 2820

- **Skype:** tendasz
- **MSN:** tendasz@hotmail.com
- **Email:** support@tenda.com.cn

➢ Headquarter Shenzhen:

- **Add:** Tenda Industrial Zone, No.34-1 Shilong Road, ShiyanTown, BaoanDistrict, Shenzhen,China. 518108
- **Tel:**(86)755-27657180
- **Fax:** (86)755-27657178
- **Email:** sales@tenda.com.cn
- **Technical Support:** support@tenda.com.cn

AppendixⅢ: Complied 3G Modem Card List

Brand	Model	Brand	Model
Tenda	3G189C	D-LINK	DWM_162 U5
HUAWEI	EC169	D-LINK	DWM_162
HUAWEI	EC169 New	DCWL	390
HUAWEI	EC1260 China	Ruijie	EV2000
HUAWEI	EC1260 New	GXZG	GX100C
HUAWEI	EC1260 India	MACAO	CTM H21
HUAWEI	EC1261	WEWINS	U602D
HUAWEI	ET128	ChangHe	868
HUAWEI	E1750	HiNet	E220
HUAWEI	EC226	TURKCELL	E176G
HUAWEI	E1630 TMobile	Vodafone	E220

HUAWEI	E176G	Vodafone	K3520
HUAWEI	E176 Chile	Cricket	UM185C
HUAWEI	E180	Cricket	A600
HUAWEI	EC170 BT	T-Mobile	UMG181
HUAWEI	EC168C_Reliance	AT&T	USBConnect mercury
HUAWEI	EC168C_Tata	AT&T	GI0322
HUAWEI	MD-@ HSUPA	Sprint	USB 598
HUAWEI	E160E	Sprint	U300
HUAWEI	E1550	Sprint	U760
HUAWEI	EZ220 3G UK	Verizon	USB760
HUAWEI	BASE e.plus E169	Verizon	UMW190VW
Vtion	E1916	Verizon	UMW190
ZTE	MU351	Verizon	UMW175VW
ZTE	AC580	Ttec	WS 119
ZTE	AC581	Ttec	WS220
ZTE	AC581 New1	CCU	680
ZTE	AC581 New2	CCU	650
ZTE	AC560	Intertel leader	C810
ZTE	AC560-New	Sierra	USB306
ZTE	MF626 Chile	BeiFang Qingniao	EC805U
ZTE	MF626 TMobile	DTM	5731E
ZTE	AC2736	DeUnite	DU360
ZTE	AC2746	DeUnite	DU456
ZTE	AC8710	DeUnite	DU458
ZTE	MF637U	JinXunChi	EV169
ZTE	MU350	TIMESPOWER	WM2080A-110
ZTE	MF622	T-Linking	T-Linking
ZTE	MF627	ChangHong	CH600

ZTE	AC2726	Datang	AirCard 901
ZTE	AC2726 Reliance		MC727
ZTE	AC8710 TATA		LKT 828
ZTE	AC8700 BSNL		Modem LC625
			CM810EV

Remark:

1. The 3G modem cards in the above list are compatible with this 3G Router. Please confirm that the 3G modem card you purchased is in the compatibility list. Only the cards in the compatibility list can be supported by this Router.
2. We will keep updating the firmware to support the new 3G modem cards. If you find that our Router can not support your 3G modem card, please visit our official website www.tenda.cn to download new firmware.
3. Huawei EC226、EC122、E176G, Viton E1916，ZTE MU351 and GXZG LKT828 are added in V0.5.
4. You are recommended to use the extended USB line to connect your 3G modem card with the 3G Router to reach a better effect.
5. New functions supported in this version:
   a. Dial on demand: when there is no access to the Internet, the network will be automatically disconnected to save network costs.
   b. 3G WAN Traffic and Connection Timer function are supported so that you can clearly know the using time and traffics without running up bills.

SHENZHEN TENDA TECHNOLOGY CO., LTD
www.tenda.cn