

Contents

Chapter 1: Introduction	1
Package Contents	1
Chapter 2: Getting to Know the Wireless-N Broadband Router.....	2
The Rear Panel.....	2
The Front Panel.....	3
Hardware Installation.....	4
Chapter 3: Getting to Connect the Wireless-N Broadband Router	5
How to Set the Network Configurations for My Computer	5
How to Check the Network Connection	7
Chapter 4: Basic Configurations	9
How to Access the Web-based Configuration Utility	9
Setup Wizard	110
Chapter 5: Advanced Settings	15
LAN Settings	14
WAN Settings—PPPoE	16
WAN Settings—Static IP	17
WAN Settings—L2TP	177
WAN Settings—PPTP	178
MAC Address Clone.....	18
DNS Settings	21

Chapter 6: Wireless Settings	22
Basic Settings	23
Wireless Security Settings	24
WEP	24
WPA-Personal	25
WPA2-Personal	26
WPA-Enterprise	27
WPA2-Enterprise	27
802.1x	28
WPS	28
WDS	28
Advanced Wireless Settings	30
Wireless Access Control	36
Wireless Connection Status	37
 Chapter 7: DHCP Server	 38
DHCP Server List	39
 Chapter 8: Virtual Server	 40
Single Port Forwarding	40
Port Range Forwarding	42
DMZ Settings	43
UPnP Settings	40
 Chapter 9: Security Settings	 41
Client Filter Settings	44
DNS Filter Settings	45

MAC Address Settings	46
Prevent Network Attack	47
Remote Web Management	47
Local Web Management	48
Wan Ping	48
Chapter 10: Routing Settings	49
Routing Table	49
Static Route	49
Chapter 11: System Tools	49
Time	50
DDNS	50
Backup/Restore	51
Firmware Upgrade	52
Restore to Factory Default Settings	50
Reboot	51
Change Password	51
System Log	55
Appendix A: Product Features	56

Chapter 1: Introduction

Thank you for choosing the LW310 Wireless-N Broadband Router. It employs the advanced MIMO (Multi Input, Multi Output) technology and integrates router, wireless access point, four-port switch and firewall in one, which will allow you to share Internet access over the four switched ports or via the wireless broadcast. Compatible with IEEE 802.11n (Draft 2.0) standard, it can connect with existing 802.11b/g PCI, USB and Notebook adapters. Up to 300Mbps transmission rate allows you to enjoy real-time activities such as video streaming, online gaming and so on.

Besides, the Wireless-N Broadband Router supports all of the latest wireless security features, such as 64/128-bit WEP encryption, WPS (PBC and PIN) encryption method, packet filtering and port forwarding, to prevent unauthorized access and protect your network against malicious attack.

Moreover, the user-friendly Setup Wizard on the CD-ROM can assist you to set up the Wireless-N Broadband Router easily. It also can be managed or configured through Local/Remote easy-to-use Web-based utility. So it is the best choice for SOHOs and small-sized enterprises.

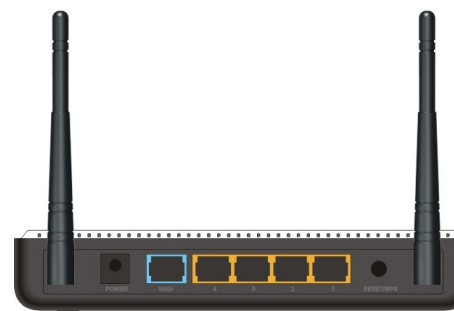
Package Contents

- ◆ One LW310 Wireless-N Broadband Router
- ◆ One Ethernet Network Cable
- ◆ One Power Adapter
- ◆ One CD-ROM

Chapter 2: Getting to Know the Wireless-N Broadband Router

The Rear Panel

Here is the description of the back panel. The RJ-45 ports for cable connection and Reset button are located on the back panel as shown below.

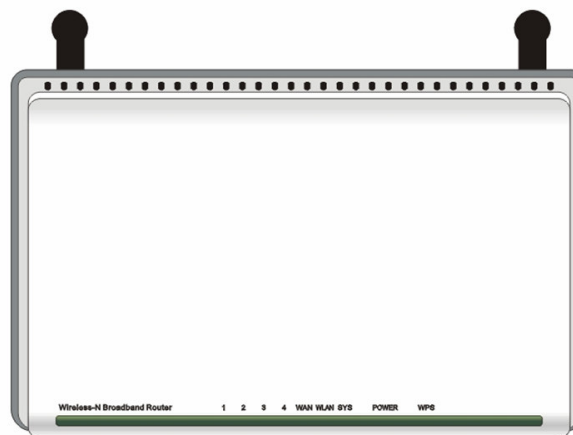


Connections:

Rear Panel Interface	Description
1-4 (LAN Ports)	Connect to Ethernet devices (such as computers, switches, hubs).
RESET/WPS	Note: After pressing the RESET button for 7 seconds, the configurations you have set will be deleted and the device will restore to the factory default settings. If you press this button for 1 second, the WPS (PBC) function is enabled.
WAN	Connect to DSL Modem, Cable Modem or community broadband
POWER	Receptor for the supplied power adapter.

The Top Panel

There are the Router's LED indicators on the top panel.



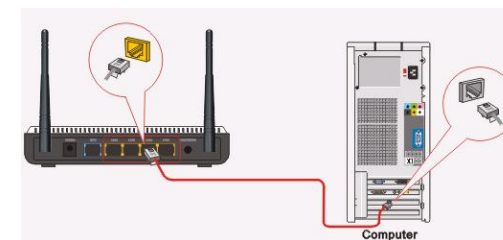
LEDS:

LED Indicator	Status	Description
POWER	Always ON	The POWER indicator is Always ON when it is powered on and works properly.
SYS	Blinking	The SYS is blinking regularly when the system works normally.
WAN	Always ON	Indicates the correct connection of the WAN ports.
	Blinking	Indicates the Router is transmitting/receiving data packets.
WLAN	Blinking	Indicates the wireless signal is OK.
LAN(1/2/3/4)	Always ON	Indicates the correct connection of the LAN ports.

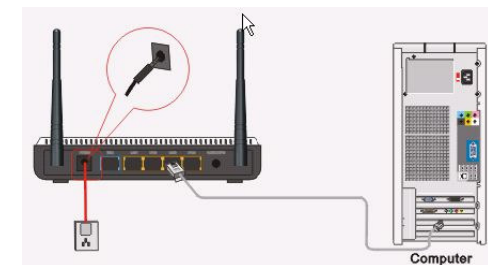
	Blinking	Indicates the Router is transmitting/receiving data packets.
WPS	Blinking	Indicates the Router is negotiating with WPS clients in WPS Mode (PBC).

Hardware Installation

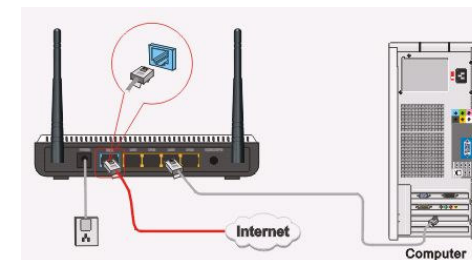
1. Please connect the LAN port of the router to the network adapter of your computer with one cable.



2. Please use the delivery-attached power adapter to power the router.



3. Please connect your broadband line provided by your ISP to the WAN port of your router.



IMPORTANT: Please use the included power adapter. Use of a different power adapter could cause damage and void the warranty for this product.

Chapter 3: Getting to Connect the Wireless-N Broadband Router

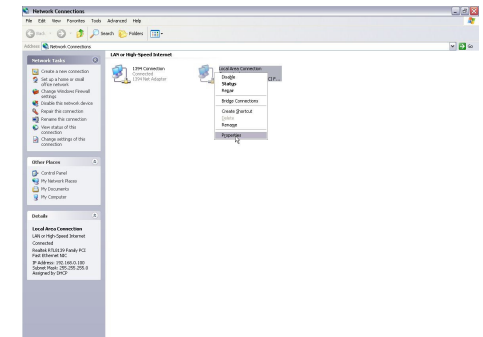
For easy and fast configuration, the following steps for network configuration are required.

How to Set the Network Configurations for My Computer

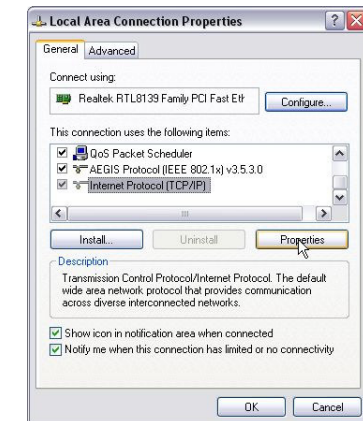
Right click “**My Network Places**” and select “**Properties**”.



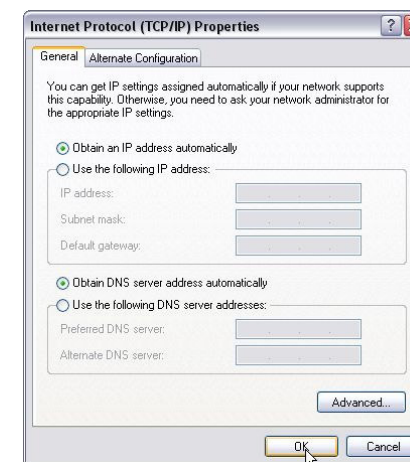
Right click **“Local Area Network Connection”** and select **“Properties”**.



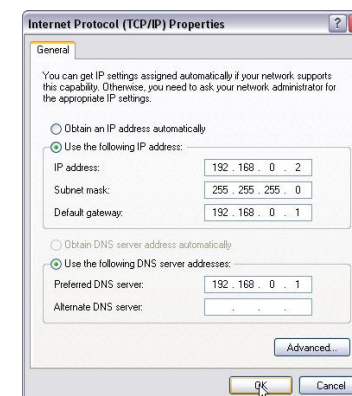
Select **“Internet Protocol (TCP/IP)”** and click **“Properties”**.



Select “**Obtain an IP address automatically**” and “**Obtain DNS server address automatically**”. Click “**OK**” to save the configurations.

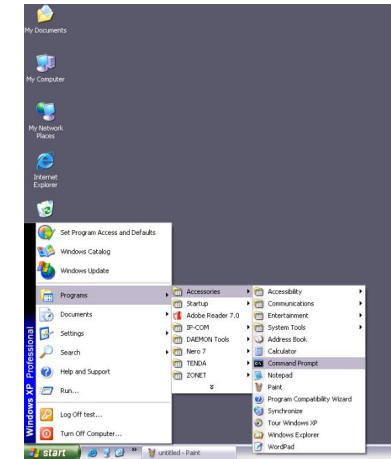


Or select “**Use the following IP address**” and enter the IP address, Subnet mask, Default gateway as shown right. Of course, you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click “**OK**” to save the configurations.



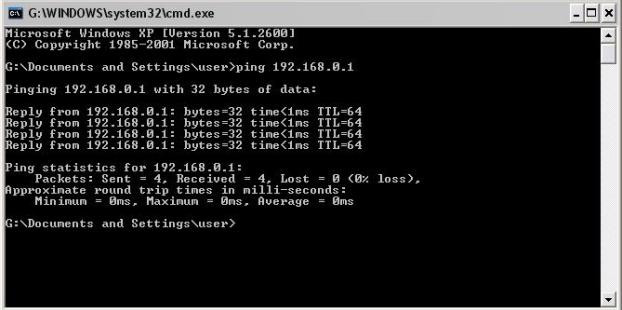
How to Check the Network Connection

Select **“Start”**— **”Programs”**—**“Accessories”**
—**“Command Prompt”**.



Input the “**ping 192.168.31.1**” and press “**Enter**”. If the screen displays as the right figure, it means your PC is connected to your router successfully.

If not, please make sure the hardware installation and network adapter are OK. After all preparations are made, please proceed to Chapter 4 for more and advanced configuration.



```
G:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

G:\Documents and Settings\User>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

G:\Documents and Settings\User>
```

Chapter 4 Basic Configurations

This section is to show you how to configure your new Wireless-N Broadband Router through the Web-based Configuration Utility.

How to Access the Web-based Configuration Utility

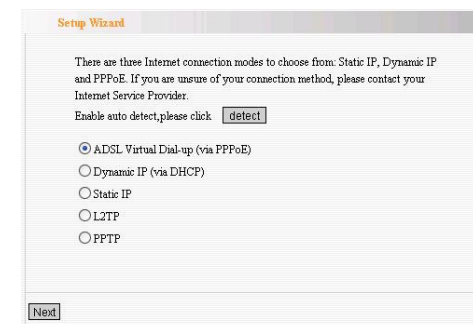
To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, <http://192.168.31.1>. Press **“Enter”**.

Please input the **“sweex”** in User Name and Password is **mysweex**. Click **“OK”**.




Setup Wizard

In the Internet Configuration screen, select one mode of your Internet connection you use. If you are not clear, press the “**Detect**” button or contact your Internet Service Provider, and click “**Next**”.



**→Connection Mode 1: ADSL Virtual Dial-up
(Via PPPoE)**

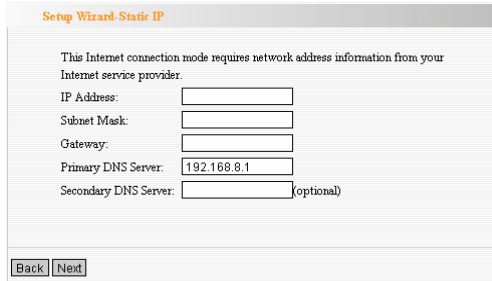
Enter the Account and Password provided by your ISP, and click “**Next**”.

**→Connection Mode 2: 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 Mode 2 or Mode 3.

→Connection Mode 3: 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**”.



→Connection Mode 4: L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP use a L2TP connection, your ISP will provide you with a username and password please fill in the parameters.

L2TP provides two access modes.

If the L2TP offered by your ISP is **Dynamic IP**: Please select Dynamic IP.

If the L2TP offered by your ISP is **Static IP**: Please fill in the parameters provided by your ISP.

After configuration, please click “Next”.

The screenshot shows the 'Setup Wizard L2TP' configuration page. It contains the following fields and values:

Field	Value
L2TP Server IP Address:	0.0.0.0
User Name:	tenda
Password:	*****
IP Address:	Static (selected from dropdown)
Address Mode:	0.0.0.0
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0

At the bottom, there are 'back' and 'next' buttons.

→Connection Mode 5: PPTP

If the connection is “PPP Tunneling Protocol”, please input the following parameters provided by your ISP: Server IP Address, User Name, and Password.

PPTP provides two access modes.

If the PPTP offered by your ISP is **Dynamic IP**: Please select Dynamic IP.

If the PPTP offered by your ISP is **Static IP**: Please fill in the parameters provided by your ISP.

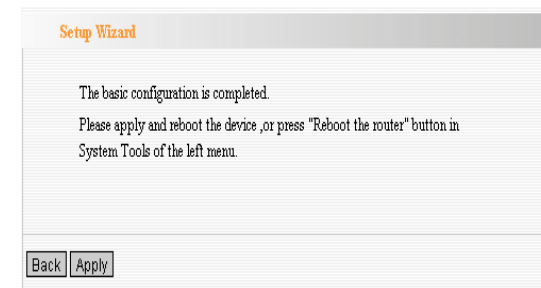
After configuration, please click “Next”.

The screenshot shows the 'Setup Wizard PPTP' configuration page. It contains the following fields and values:

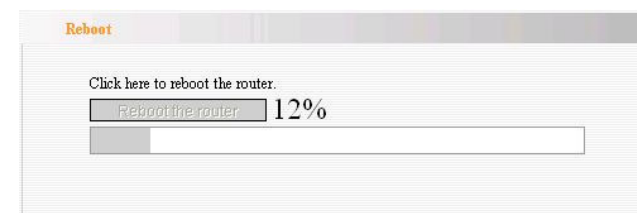
Field	Value
PPTP Server IP Address:	0.0.0.0
User Name:	tenda
Password:	*****
Address Mode:	Static (selected from dropdown)
IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0

At the bottom, there are 'back' and 'next' buttons.

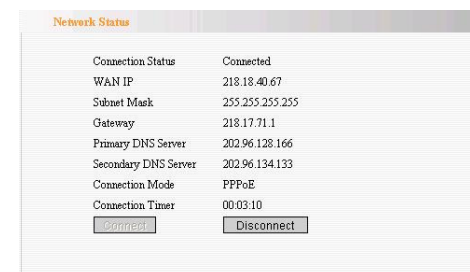
Click “**Apply**”, select “**Reboot**” in **System Tools** of the left menu and press the “**Reboot the router**” button.



It is rebooting now, please wait for a few minutes and **DO NOT** power off it.



Click the “**System Status**” in the left menu of the Web-based Utility to find out the current network and system information. If the “Connection Status” is “Connected”, Congratulations you on completing the Router’s basic settings. You are on the Internet now. If you want to configure more, please proceed to the following explanations for Advanced Settings.



The screenshot shows the 'Network Status' page of a router's web interface. It displays various network parameters in a table format. At the bottom, there are two buttons: 'Connect' and 'Disconnect'.

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
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	

Chapter 5: Advanced Settings

This section is to conduct the advanced configurations for the Router, including LAN Settings, WAN settings, MAC Address Clone and DNS Settings.

LAN Settings

MAC Address: The Router's physical MAC address as seen on your local network, which is unchangeable.

IP Address: The Router's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.31.1 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.

WAN Settings—PPPoE

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

<p>network. The default value is 1492. Do NOT modify it unless necessary.</p> <p>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.</p> <p>AC Name: Enter it if provided. Do NOT modify it unless necessary.</p> <p>Connect automatically to the Internet after rebooting the system or connection failure.</p> <p>Connect Manually: Connect to the Internet by the user manually.</p> <p>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.</p> <p>Connect on Fixed Time: Connect to the Internet during the time you fix.</p>	
--	--

WAN Settings—Static IP

If your connection mode, static IP is chosen, please enter 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

The screenshot shows the 'WAN Settings' page of a router. At the top, there is a header 'WAN Settings' in orange. Below it, the text 'WAN connection mode: Static IP' is displayed. The form contains several input fields: 'IP Address' with the value '192.168.1.2', 'Netmask' with '255.255.255.0', 'Gateway' with '192.168.1.1', 'Primary DNS Server' with '192.168.0.1', and 'Secondary DNS Server' which is empty and followed by '(option)'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

WAN Settings	
WAN connection mode: Static IP	
IP Address	192.168.1.2
Netmask	255.255.255.0
Gateway	192.168.1.1
Primary DNS Server	192.168.0.1
Secondary DNS Server	(option)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WAN Settings—L2TP

L2TP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter L2TP username.

Password: Enter L2TP password.

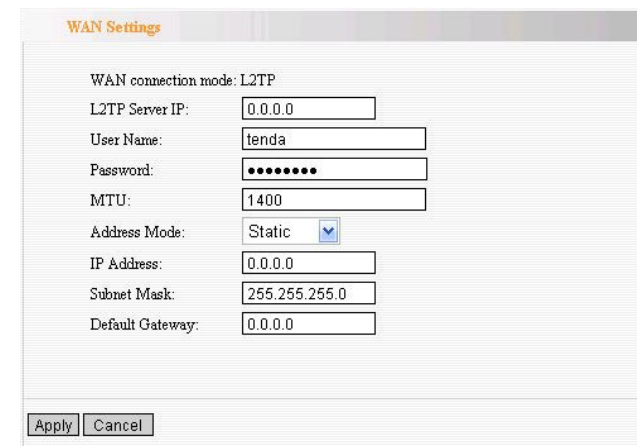
MTU: Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1400 is the default MTU.

Address Mode: Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the L2TP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.



The screenshot shows the 'WAN Settings' page of a router. The 'WAN connection mode' is set to 'L2TP'. The following fields are visible:

Field	Value
L2TP Server IP:	0.0.0.0
User Name:	tenda
Password:	••••••••
MTU:	1400
Address Mode:	Static (selected)
IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0

At the bottom of the form are 'Apply' and 'Cancel' buttons.

WAN Settings—PPTP

PPTP Server IP: Enter the Server IP provided by your ISP.

User Name: Enter PPTP username provided by your ISP.

Password: Enter PPTP password provided by your ISP..

Address Mode: Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

IP Address: Enter the PPTP IP address supplied by your ISP.

Subnet Mask: Enter the Subnet Mask supplied by your ISP.

Default Gateway: Enter the Default Gateway supplied by your ISP.

Setup Wizard - PPTP

PPTP Server IP Address: 0.0.0.0

User Name: tenda

Password:

Address Mode: Static

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

back next

MAC Address Clone

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 the default hardware MAC address.

The screenshot shows a web-based configuration interface for a router. At the top, there is a header bar with the text "MAC Address Clone" in orange. Below this, the text "WAN MAC Address Clone." is displayed. A label "MAC Address:" is followed by a text input field containing the value "02:10:17:F2:AB:12". Below the input field are two buttons: "Restore Default MAC" and "Clone MAC Address". At the bottom of the form, there are two buttons: "Apply" and "Cancel".

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:

Click the checkbox to enable the DNS server.

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.

DNS Settings

DNS Settings ☐

Primary DNS Address

Secondary DNS Address (option)

Apply Cancel

Chapter 6: Wireless Settings

This section mainly deals with the wireless settings, including Basic Settings, Security Setting, Access Control and Advanced Settings.

Basic Settings

Network Mode: Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.

Main SSID: Main Service Set Identifier. It's the "name" of your wireless network.

Minor SSID: Minor Service Set Identifier. It is optional.

Broadcast (SSID): Select "enable" to enable the device's SSID to be visible by wireless clients.

BSSID: It is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP

Channel: From the drop-menu, it is for selecting the working channels of the wireless network. Please select from 1 to 13, or select AutoSelect to select different channels.

Channel Bandwidth : Select wireless work frequency 20M or 20/40M.

HT TxStream: RF Transmit Stream.

HT RxStream: RF Receive Stream.

Basic Settings

Network Mode: 11b/g/n mixed mode

Main SSID: Sweex LW310

Minor SSID:

Broadcast(SSID): ☒ Enable ☐ Disable

AP Isolation: ☐ Enable ☒ Disable

MBSSID AP Isolation: ☐ Enable ☒ Disable

BSSID: 00:B0:0C:02:ED:A6

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

Apply Cancel

--	--

Wireless Security Settings

This page is to configure the wireless security of your Router. Six wireless security modes, WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise and RADIUS, are supported. If you do not want to use wireless security, select Disable from the drop-down menu.

1. 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.

SSID Choice: Select SSID to be configured security. The device supports to configure different security classes between the main SSID and the subordinate SSID.

Security Mode: There are several different security modes; you can choose one from mixed WEP, WPA-Personal, WPA-Enterprise, etc.

Default Key: Select a valid encryption key.

WEP Key1, 2, 3, 4: Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be **ASCII Characters** or **Hexadecimal Digits**

2. 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.

WPA Algorithms: Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

Pass Phrase: Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval: Enter the key renewal period. It is to tell the Router how often to change the keys.

3. WPA2-Personal

WPA2 (Wi-Fi Protected Access version 2), It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.

WPA Algorithms: Select key Algorithms such as TKIP, AES and TKIP&AES.

Pass Phrase: Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval: Enter the key renewal period. It is to tell the Router how often to change the keys.

4. WPA-Enterprise

This Authentication protocol based on RADIUS server. This security mode is used when a RADIUS server is connected to the Router.

Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.

5. WPA2-Enterprise

This security mode is also used when a RADIUS server is connected to the Router.

WPA Algorithms: Select key Algorithms such as TKIP and AES.

Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.

6. 802.1X

This security mode is used when a RADIUS server is connected to the Router. 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.

WEP: Select "enable/disable" WEP encryption which indicates the authentication process between wireless adapter and wireless router.

Radius IP Address: Please input IP address of the radius server here.

Radius Port: Please input the port number of the radius server here.

Shared key: The encryption key that the router is authenticated through RADIUS server.

Session Timeout: The recertification time interval between the router and the server. The default value is 3600s.

⚠ NOTE: To improve security level, do not use those words which can be found in a dictionary or too easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it's worth to use complicated WEP key to improve security level.

WPS Settings

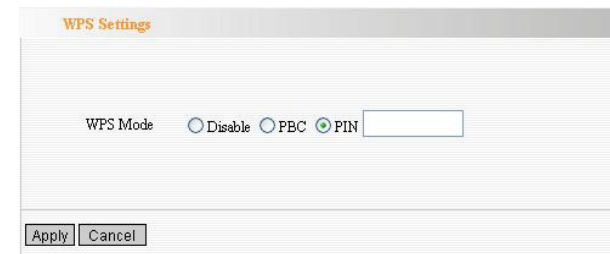
WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the Router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

WPS Mode: Supports two ways to configure WPS settings:

PBC(Push-Button Configuration) and PIN code.

PBC: Select the PBC or press the WPS button on the panel of the Router (Press the button for 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 Router to implement the WPS/PBC negotiation between them. At present, the WPS only support one client access. Two minutes later, the WPS indicator will be off.).

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 client.



WDS Settings

In this mode, you can expand the scope of network by combining up to four other access points together, and every access point can still accept wireless clients.

Lazy Mode: You need configure the router's BSSID into another device, not need input another router's BSSID in it, and then connect together automatically.

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. At the same time, the connecting device should be in Lazy, Repeater or Bridge mode.

Repeater Mode: You can select the mode to extend the distance between the two WLAN devices. Functioning as a WDS repeater, the LW310 connects to both a client card as an AP and to another AP. In typical repeater applications, APs connecting to other APs equipped with WDS functionality must also support WDS. In this mode, you need to add the MAC address of the connecting device into the

WDS Settings

WDS Mode: Bridge Mode (selected), Disable, Lazy Mode, Bridge Mode, Repeater Mode

AP MAC: [input field]

AP MAC: [input field]

AP MAC: [input field]

AP MAC: [input field]

Open Scan

Save Cancel

Router's AP MAC address table and the connecting client should be in Lazy, Repeater or client mode.

Encrypt Type: You can select WEP mode, TKIP mode, AES mode for security here.

Pass phrase: Enter the key, the key format according to encryption you selected.

AP MAC: Input the MAC address of another wireless router.

⚠ **NOTE: Two wireless routers must use the same mode, band, channel number, and security setting!**

Advanced Wireless Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, Beacon Period and DTIM Interval.

BG protection Mode: Auto by default. You can select On or Off.

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...).

Beacon Interval: Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.

Fragment Threshold: Do not modify default value if you don't know what it is, default value is 2346.

RTS Threshold: Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.

TX Power: You can set the output power of wireless radio. Unless you're using this wireless router in a really big space, you may not have to

The screenshot shows the 'Advanced Settings' window of a router. It contains the following fields and options:

- BG Protection Mode:** A dropdown menu set to 'Auto'.
- Basic Data Rates:** A dropdown menu set to 'Default(1-2-5.5-11 Mbps)'.
- Beacon Interval:** A text input field with '100' and a unit dropdown set to 'ms'. A note indicates the range is 20 - 999, with a default of 100.
- Fragment Threshold:** A text input field with '2346'. A note indicates the range is 256 - 2346, with a default of 2346.
- RTS Threshold:** A text input field with '2347'. A note indicates the range is 1 - 2347, with a default of 2347.
- TX Power:** A text input field with '100'. A note indicates the range is 1 - 100, with a default of 100.
- WMM Capable:** Two radio buttons, 'Enable' (selected) and 'Disable'.
- APSD Capable:** Two radio buttons, 'Enable' and 'Disable' (selected).
- At the bottom, there are 'Save' and 'Cancel' buttons.

set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).

WMM Capable: It will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is / not sure if you need it, it's safe to set this option to 'Enable', however, default value is enabling.

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

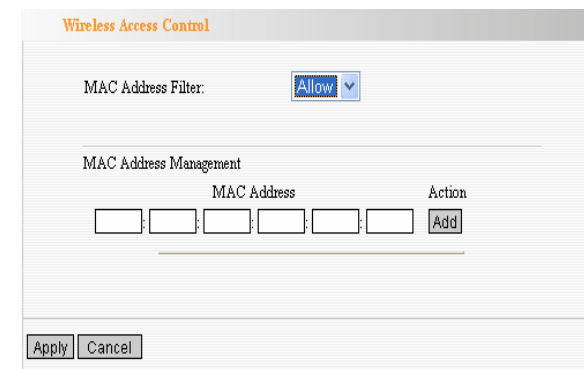
Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management.

MAC Address Filter: If you want to access the router from any external IP Address, please select the “Disable”.

MAC Address: To specify an external IP address, please add the MAC address manually and click “Add”.

MAC Address List: The added MAC addresses are listed here. Click “Delete” to delete the filter management for this MAC address.



The image shows a screenshot of the 'Wireless Access Control' configuration page. At the top, the title 'Wireless Access Control' is displayed in orange. Below it, there is a 'MAC Address Filter' section with a dropdown menu currently set to 'Allow'. Underneath, the 'MAC Address Management' section features a table with two columns: 'MAC Address' and 'Action'. The 'MAC Address' column contains six empty input boxes for manual entry, and the 'Action' column has an 'Add' button. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Wireless Connection Status

This page is to show the current wireless access status. Click “Refresh” to update the wireless connection information.

MAC Address:

Shows the connecting PC’s MAC address.

Bandwidth: displays the channel bandwidth of the host to be connected.



The screenshot shows the 'Wireless Connection Status' page. At the top, there is a title bar with the text 'Wireless Connection Status'. Below the title bar, the text 'The Current Wireless Access List:' is followed by a 'Refresh' button. Underneath, there is a table with three columns: 'NO.', 'MAC Address', and 'Bandwidth'. The table is currently empty.

NO.	MAC Address	Bandwidth
-----	-------------	-----------

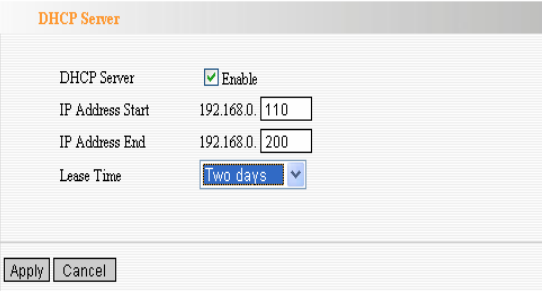
Chapter 7: DHCP Server

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: Activate the checkbox to enable DHCP server.

IP Address Start/End: Enter the range of IP address for DHCP server distribution.

Lease Time: The length of the IP address lease.



The screenshot shows the 'DHCP Server' configuration window. It has a title bar 'DHCP Server' in orange. Below it, there are four rows of configuration options: 'DHCP Server' with a checked 'Enable' checkbox, 'IP Address Start' with a text box containing '192.168.0.' and a spinner box set to '110', 'IP Address End' with a text box containing '192.168.0.' and a spinner box set to '200', and 'Lease Time' with a dropdown menu showing 'Two days'. At the bottom left, there are 'Apply' and 'Cancel' buttons.

DHCP Server	
DHCP Server	<input checked="" type="checkbox"/> Enable
IP Address Start	192.168.0. 110
IP Address End	192.168.0. 200
Lease Time	Two days

Apply Cancel

DHCP Server List

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: Enter one IP address for the computer on the LAN network.

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 time length of the corresponding IP address lease.

DHCP Client List

Static IP

IP Address 192.168.0.

MAC Address : : : : :

NO.	IP Address	MAC Address	Delete
-----	------------	-------------	--------

Host Name	IP Address	MAC Address	Lease
fanyi	192.168.0.110	00:E0:4C:01:9C:92	1days 22:09:25

Chapter 8: Virtual Server

Single Port Forwarding

The LW310 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.**

External Port: This is the external 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

Single Port Forwarding

The W302R 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.	66 21	192.168.0.10	Both	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
8.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
10.		192.168.0.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

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

Apply Cancel

where you want to set the applications.

Protocol: Select the protocol (TCP/UDP/Both) for the application.

Well-Known Service Port: Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

Delete/Enable: Click to check it for corresponding operation.

⚠ 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.

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.

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.

Well-Known Service Port: Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

Delete/Enable: Click to check it for corresponding operation.

Port Range Forwarding

The W302R 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.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/> - <input type="text"/>	192.168.0. <input type="text"/>	TCP <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>

Well-Known Service Port: ID

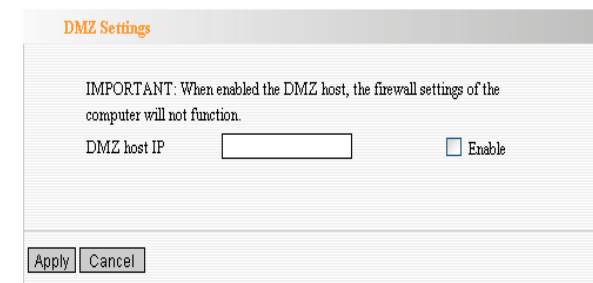
DMZ Settings

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 Host IP Address: The IP address of the computer you want to expose.

Enable: Click the checkbox to enable the DMZ host.

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



DMZ Settings

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

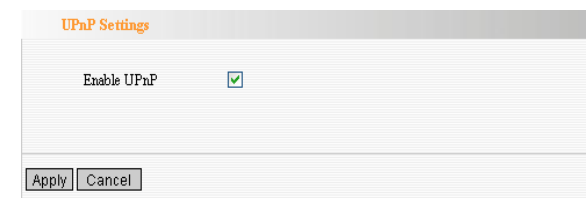
DMZ host IP ☐ Enable

Apply Cancel

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.

Enable UPnP: Click the checkbox to enable the UPnP.



UPnP Settings

Enable UPnP ☒

Apply Cancel

Chapter 9: Security Settings

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: 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.

Client Filter

Client Filtering Settings ☒

Access Policy: 10

Enable: ☒ Delete the Policy:

Filtering Mode: ☒ Disable ☐ Enable access the Internet

Policy Name:

Start IP: 192.168.0

End IP: 192.168.0

Port: -

Type: TCP

Times: 0:00 - 0:00

Date: ☒ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wen ☐ Thr ☐ Fri ☐ Sat

DNS 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.

DNS Filter: Check to enable DNS 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.

DNS: Specify the text strings or keywords in the DNS. If any part of the DNS contains these strings or words, the web page will not be accessible and display.

Times: Select the time range of client filter.

Days: Select the day(s) to run the access policy.

The screenshot shows the 'DNS Filter' configuration page. At the top, 'DNS Filter' is checked. Below it, 'Access Policy' is set to '10'. The 'Enable' checkbox is checked, and there is a 'Clear the Policy' button. Under 'Filtering Mode', the 'Disable' radio button is selected, with the text 'access the Internet' next to it. The 'Policy Name' field is empty. 'Start IP' and 'End IP' are both set to '192.168.0.'. The 'DNS' field is empty. The 'Times' section shows a time range of 0:00 to 0:00. The 'Date' section has 'Everyday' checked, and all other day checkboxes (Sun, Mon, Tue, Wen, Thr, Fri, Sat) are unchecked. At the bottom, there are 'Apply' and 'Cancel' buttons.

MAC Address Settings

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

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.

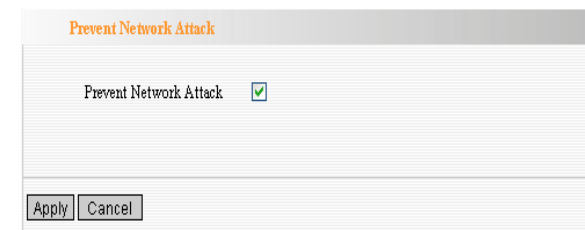
Days: Select the day(s) to run the access policy.

The screenshot shows the 'MAC Filter' configuration page. At the top, 'MAC Filtering Settings' has an 'Enable' checkbox checked. Below it, 'Access Policy' is set to '10'. There is an 'Enable' checkbox checked, a 'Delete the Policy' button, and a 'Clear' button. The 'Filtering Mode' section has two radio buttons: 'Disable' (unselected) and 'Enable' (selected), with the text 'access the Internet' next to the 'Enable' option. Below this, there is a 'Policy Name' text field and a 'MAC Address' field with six input boxes. The 'Times' section shows a time range from 0 to 0. The 'Date' section has checkboxes for 'Everyday', 'Sun' (checked), 'Mon', 'Tue', 'Wen', 'Thr', 'Fri' (checked), and 'Sat'. At the bottom, there are 'Apply' and 'Cancel' buttons.

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: Check to enable it for attack prevention.



The image shows a web interface for "Prevent Network Attack". It has a title bar with the text "Prevent Network Attack" in orange. Below the title bar, there is a label "Prevent Network Attack" followed by a checked checkbox. At the bottom of the interface, there are two buttons: "Apply" and "Cancel".

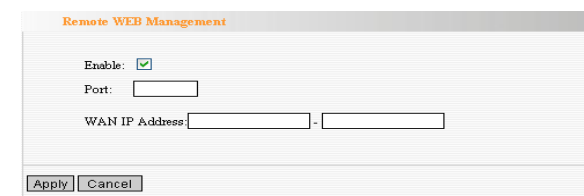
Remote Web Management

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".

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.



The image shows a web interface for "Remote WEB Management". It has a title bar with the text "Remote WEB Management" in orange. Below the title bar, there are three fields: "Enable:" with a checked checkbox, "Port:" with a text input field, and "WAN IP Address:" with two text input fields separated by a hyphen. At the bottom of the interface, there are two buttons: "Apply" and "Cancel".

Local Web Management

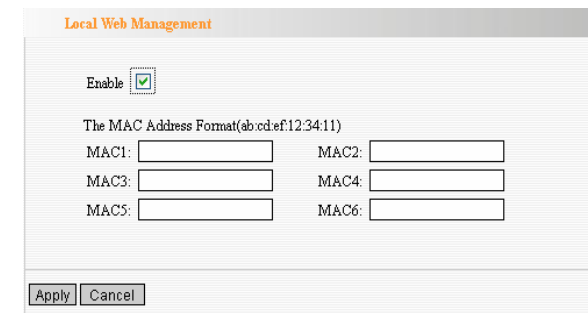
Local web management, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.

Enable:

Check to enable the local web management

MAC1/2/3...:

Enter the MAC addresses of LAN computers.

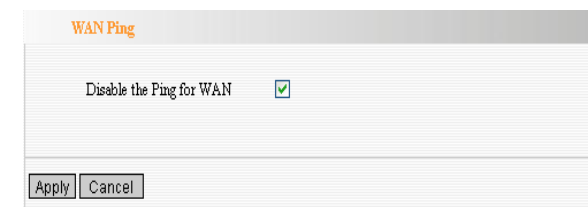


The screenshot shows the 'Local Web Management' configuration window. At the top, the title 'Local Web Management' is displayed in orange. Below the title, there is a section labeled 'Enable' with a checked checkbox. Underneath, a note states 'The MAC Address Format(ab.cd.ef:12:34:11)'. This is followed by six input fields arranged in two columns, labeled MAC1, MAC2, MAC3, MAC4, MAC5, and MAC6. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

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.

Disable the Ping for WAN: Check to enable it.



The screenshot shows the 'WAN Ping' configuration window. The title 'WAN Ping' is displayed in orange at the top. Below the title, there is a section labeled 'Disable the Ping for WAN' with a checked checkbox. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Chapter 10: Routing Settings

Routing Table

The main duty for router is to look for a best path for every data frame, and transfer this data frame to 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

Refresh

Static Route

Static Route is set by administrator in advance is called static route. Usually, it is set according to network configuration when installing the operation system. It would not be changed according to network structure's change.

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.

Static Routing

Destination LAN IP	Subnet Mask	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add

Chapter 11: System Tools

Time

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 Zone: Select your time zone from the drop-down menu.

Customized time: Enter the time you customize.

The screenshot shows the 'Time Settings' page. At the top, it says 'Time Zone:' followed by a dropdown menu currently set to '(GMT+08:00)Beijing,China, Hong Kong,Singapore, Taipei'. Below this is a notice: '(Notice: GMT time can be obtained only after accessing to the Internet.)'. Underneath is a 'Customized time:' section with a checkbox that is unchecked, followed by six input fields for HH, MM, SS, DD, MM, and SS. At the bottom are 'Apply' and 'Cancel' buttons.

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: Click the radio button to enable or disable the DDNS service.

Service Provider: Select one from the

The screenshot shows the 'DDNS' configuration page. It starts with 'DDNS' and two radio buttons: 'Enable' (selected) and 'Disable'. Below is 'Service Provider' with a dropdown menu set to 'DynDNS.org' and a 'Sign up' link. Then are 'User Name', 'Password', and 'Domain Name' (with '(optional)' text) input fields. At the bottom are 'Apply' and 'Cancel' buttons.

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.

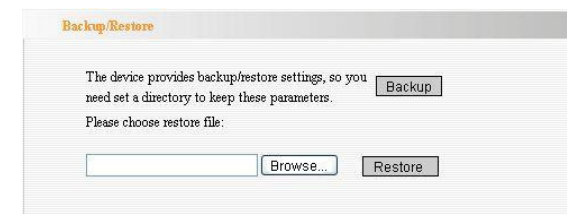
Backup/Restore

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

Backup: Click this button to back up the Router’s configurations.

Browse: Click this button to browse the directory where you Back up or save files.

Restore: Click this button to restore the Router’s configurations.



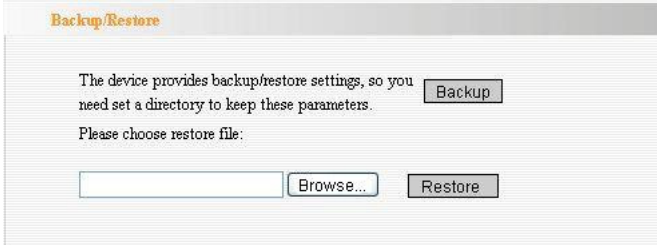
Firmware Upgrade

The Router provides the firmware upgrade by clicking the “Upgrade” after browsing for the firmware upgrade packet which you can download from www.tenda.cn. After the upgrade is completed, the Router will reboot automatically.

Browse: Click this button to browse the directory where you download the firmware upgrade files.

Upgrade: Click this button to start upgrade.

IMPORTANT: Do not power off the system during the firmware upgrade to avoid damaging the device. The Router will reboot after the upgrade.



The screenshot shows a web interface titled "Backup/Restore". It contains the following text and controls:

- Text: "The device provides backup/restore settings, so you need set a directory to keep these parameters."
- Text: "Please choose restore file:"
- Buttons: "Backup", "Browse...", and "Restore".
- Input field: A text box for specifying the restore file path, located below the "Please choose restore file:" text.

Restore to Factory Default Settings

This button is to reset all configurations 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: Click this button to restore to default settings.

Factory Default Settings:

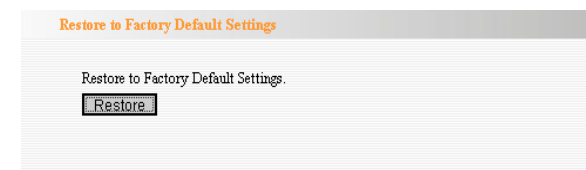
User Name: **admin**

Password: **admin**

IP Address: **192.168.31.1**

Subnet Mask: **255.255.255.0**

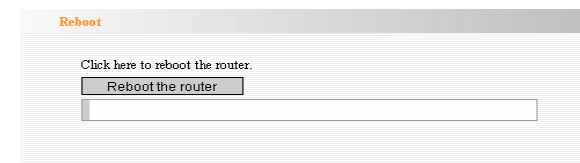
⚠ NOTE: After restoring to default settings, please restart the device, then the default settings can go into effect.



Reboot

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

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

A screenshot of the 'Reboot' web interface. It has a title bar 'Reboot' in orange. Below it, the text 'Click here to reboot the router.' is displayed. Underneath is a button labeled 'Reboot the router'. Below the button is a long, empty text input field.

Change Password

This section is to set a new user name and password to better secure your router and network. Please Note that the new password should be less than 14 characters.

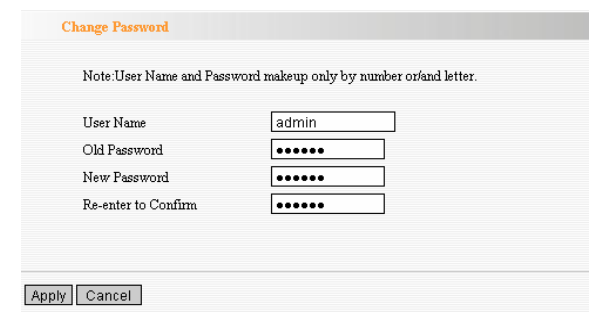
User Name: Enter a new user name for the device.

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.*

A screenshot of the 'Change Password' web interface. It has a title bar 'Change Password' in orange. Below it, a note says 'Note: User Name and Password makeup only by number or/and letter.' There are four input fields: 'User Name' with 'admin' entered, 'Old Password' with seven dots, 'New Password' with seven dots, and 'Re-enter to Confirm' with seven dots. At the bottom are 'Apply' and 'Cancel' buttons.

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.

Refresh: Click this button to update the log.

Clear: Click this button to clear the current shown log.

System Log			
Page 1 content			
1	2000-01-01 00:00:09	DHCP	Send discover
2	2000-01-01 00:00:12	DHCP	Send discover
3	2000-01-01 00:00:15	DHCP	Send discover
4	2000-01-01 00:00:21	System	system start.
5	2000-01-01 00:01:18	DHCP	Send discover
6	2000-01-01 00:01:21	DHCP	Send discover
7	2000-01-01 00:01:24	DHCP	Send discover
8	2000-01-01 00:00:09	DHCP	Send discover
9	2000-01-01 00:00:12	DHCP	Send discover
10	2000-01-01 00:00:15	DHCP	Send discover
[1][2][3]			
Refresh Clear			

Appendix A: Product Features

- ☐ Integrates router, wireless access point, four-port switch and firewall in one
- ☐ Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
- ☐ MIMO technology utilizes reflection signal to increase eight times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
- ☐ Provides 300Mbps receiving rate and 150Mbps sending rate
- ☐ Supports WMM to make your voice and video more smooth
- ☐ Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
- ☐ WPS (PBC and PIN) encryption method to free you from remembering long passwords
- ☐ Supports remote/local Web management
- ☐ Supports wireless Roaming technology and ensures high-efficient wireless connections
- ☐ Supports wireless SSID stealth mode and MAC address access control
- ☐ Supports Auto MDI/MDIX
- ☐ Provides system log to record the status of the router
- ☐ Supports MAC address filtering, NAT, NAPT
- ☐ Supports UPnP and DDNS
- ☐ Supports the access control over 30 MAC addresses
- ☐ Supports DHCP server/client
- ☐ Supports SNTP
- ☐ Supports virtual server and DMZ host
- ☐ Supports auto wireless channel selection
- ☐ Supports WDS function (wireless distribution system)