

Table of Contents

1. ABOUT THIS GUIDE	3
1.1 Navigation of the User's Guide.....	3
2. PRODUCT OVERVIEW	3
2.1 Introduction.....	3
2.2 Features	3
2.3 Panel Layout	4
2.3.1 Front Panel	4
2.3.2 Rear Panel	5
3. HARDWARE INSTALLATION.....	6
3.1 Hardware Installation	6
3.2 Check the Installation.....	6
3.3 Set up the Computer.....	6
4. CONNECTING TO INTERNET.....	8
4.1 Accessing Web page	8
4.2 Changing Password	9
4.3 Setup Wizard.....	9
4.3.1 Router Mode.....	12
4.3.2 Wireless ISP Client Mode.....	16
4.3.3 Wireless Client Mode	17
4.3.4 Repeater Mode	18
4.3.5 Bridge with AP	20
4.3.6 Client Mode.....	20
4.4 Quick Setup	21
4.5 Status.....	23
4.4.1 System status	23
4.4.2 Statistics.....	24
4.4.3 System log	25
5. ADVANCED SETTINGS	25
5.1 Operation mode	26
5.2 TCP/IP Settings.....	27
5.2.1 LAN Interface.....	27
5.2.2 WAN Interface.....	29
5.2.2.1 PPPoE.....	30
5.2.2.2 PPTP.....	31
5.2.2.3 L2TP.....	32
5.2.3 VLAN Settings	32
5.2.4 DHCP&ARP Table	34

5.3 Wireless.....	34
5.3.1 Basic Settings	34
5.3.2 Security Settings	38
5.3.3 Site Survey	38
5.3.4 WDS	39
5.3.5 Advanced Settings	40
5.3.6 Access Control.....	41
5.3.7 WPS Settings	42
5.3.8 Schedule	42
5.4 Route Setup	43
5.4.1 Static Route	43
5.4.2 Routing Table	44
5.5 Firewall	44
5.5.1 IP Filtering.....	45
5.5.2 Port Filtering.....	45
5.5.3 MAC Filtering	46
5.5.4 URL Filtering	46
5.5.5 Port Forwarding.....	47
5.5.6 DMZ.....	47
5.5.7 QoS.....	47
5.5.8 Alias IP & NAT Mapping	48
5.5.9 Session Limit.....	49
5.6 Management.....	50
5.6.1 DDNS	50
5.6.2 Denial-of-Service	50
5.6.3 Upgrade Firmware.....	51
5.6.4 SSH Server	52
5.6.5 Reset to Default Settings	52
5.6.6 Web Login Password	53
5.6.7 TR-069 Config	53
5.6.8 SNMP	54
5.6.9 Date and Time	54
5.6.10 Reboot Router.....	55
5.6.11 Reboot Schedule	55
5.6.12 Run Comment.....	55

Copyright Statement

All the photos and product specifications mentioned in this manual are for references only, as the upgrading of software and hardware. They are subject to change without notice. No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TOTOLINK. If you want to know more about our products information, please visit our website at <http://www.totolink.net>

Copyrights 2014 by TOTOLINK All rights reserved.

1. ABOUT THIS GUIDE

Thank you very much for purchasing this router. This guide will introduce the features of this router and tell you how to connect, use and configure the router to access Internet. Please follow the instructions in this guide to avoid affecting the router's performance by improper operation.

1.1 Navigation of the User's Guide

Product Overview: Describes the router's function and its features.

Hardware Installation: Describes the hardware installation and settings on user's computer.

Connecting to Internet: Tells you how to connect your computer to Internet successfully by the router.

Advanced Settings: Lists all technical functions including Wireless, TCP/IP Settings, Firewall and System of the router.

2. PRODUCT OVERVIEW

2.1 Introduction

This is a high power wireless N router which integrates with internet-sharing router, 4-port switch and firewall all-in-one. It allows users to connect to Internet by DHCP/Static IP/PPPoE(dual access)/PPTP(dual access)/L2TP(dual access) and can deliver high speed wireless data rate. The VLAN function also makes amazing interactive entertainment experience of IPTV be achieved easily. Multiple encryptions including wireless LAN 64/128-bit WEP, WPA/WPA2 and WPA-mixed security are supported by the router. The IP, Port, URL and MAC address filtering function also makes it easy for user management. In view of the above, it will allow you to connect your network wirelessly in an easy and secure way better than ever. It is really a high performance and cost-effective solution for home and small offices.

2.2 Features

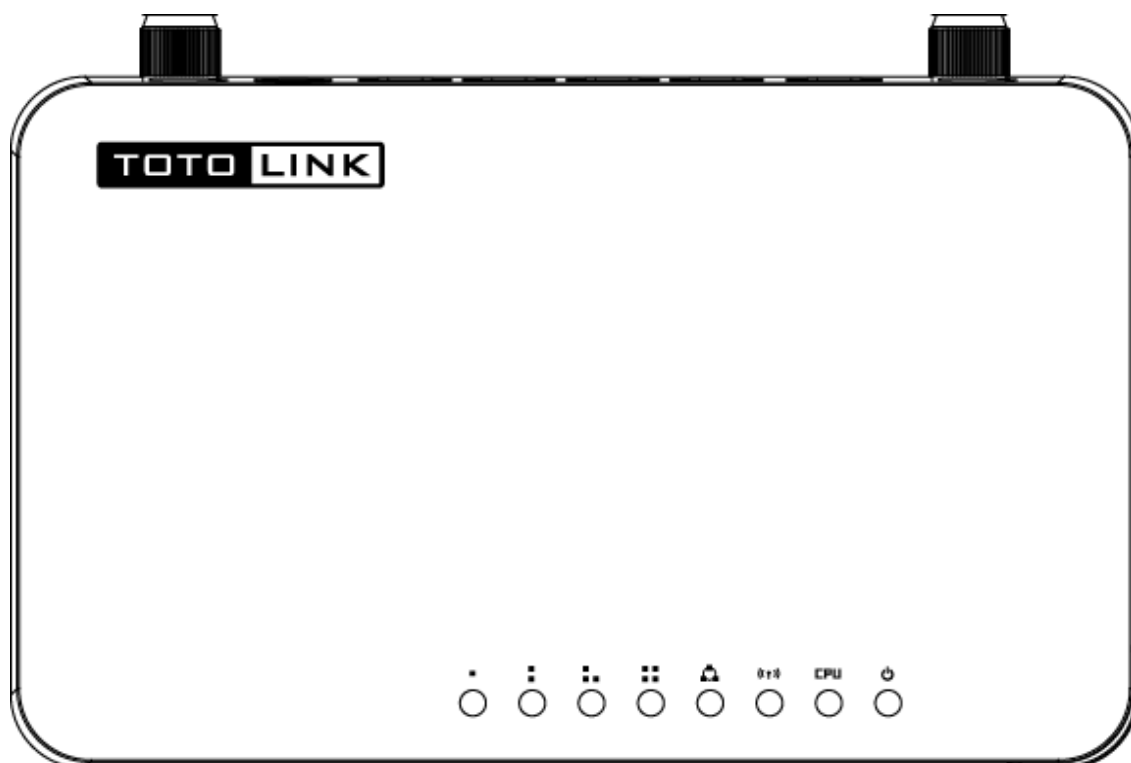
- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Supports DHCP, Static IP, PPPoE, PPTP and L2TP broadband functions and supports dual access.
- Provides six operation modes: Wireless ISP Client Router, Wireless Client, Repeater, Router, Bridge with AP and Client.
- Connects to secure network easily and fast using WPS (one-button).
- High output power expands the wireless coverage and improve connective stability.

- Provides 64/128-bit WEP, WPA/WPA2 and WPA-Mixed security.
- VLAN function for IPTV or other internet services.
- Supports IP, Port, MAC, URL filtering and Port Forwarding.
- QoS function allocates network bandwidth reasonably.
- Setup Wizard simplifies the basic settings of the router.

2.3 Panel Layout

2.3.1 Front Panel

The front panel of this router consists of 8 LEDs, which is designed to indicate connection status.



POWER	This indicator lights blue when the router powered on, otherwise it is off.	
CPU	This indicator blinks blue when router powered on.	
WLAN	This indicator blinks blue when there are wireless devices connected and transmitting data to the router.	
WAN	On	When the WAN port is connected successfully the indicator lights blue.
	Blink	During transmitting or receiving data through the WAN port the indicator blinks blue.
	Off	There is no device linked to the WAN port.

1/2/3/4 LAN	On	When the LAN port has a successful connection, the corresponding indicator lights blue.
	Blink	During transmitting or receiving data through the LAN port the corresponding indicator blinks blue.
	Off	There is no device linked to the LAN port.

2.3.2 Rear Panel

The figure below shows the rear panel of this router.



DC IN	The Power socket is where you will connect the power adapter.
WAN	This port is where you will connect with the cable to access Internet.
1/2/3/4 LAN	This port connects the router to local PC.
RST/WPS Button	The button is on the opposite of the rear panel. Press for about 2~3 seconds, the system LED indicator keep solid light, it means WPS working, while press for about 10 seconds, all LEDs blinks quickly, the device will restore to factory default settings.

3. HARDWARE INSTALLATION

3.1 Hardware Installation

Please connect the router according to the following steps.

1. Connect the Modem to ADSL Filter using RJ11 network cable, LINE port to LINE port.
2. Connect the ADSL's LAN port to Router's WAN port using RJ45 network cable.
3. Connect your PC to any one of router's LAN port.
4. Plug the Power Adapter into the router and then into an outlet.
5. Turn on your computer.
6. Check and confirm that the Power & LAN LED on the router are **ON**.

3.2 Check the Installation

The control LEDs of the router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, WPS, LAN, WLAN and WAN port LEDs of the WLAN Router will light up indicating a normal status.
2. When the WAN Port is connected to Internet successfully, the WAN LED will light up.
3. When the LAN Port is connected to the computer system, the LAN LED will light up.

3.3 Set up the Computer

The default IP address of the router is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description.

Connect the local PC to the LAN port on the router. There are then two ways to configure the IP address for your PC.

◆ Configure the IP address manually

Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (router's default IP address).

◆ Obtain an IP address automatically

Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. Open a command prompt, and type in **ping 192.168.1.1**, then press **Enter**.

```

C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_

```

Figure 3-1 Successful Ping command

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

```

C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>_

```

Figure 3-2 Failure Ping command

If the result displayed is similar to the figure 3-2, it means that your PC has not connected to the router successfully. Please check it following below steps:

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

If correct, the LAN port on the router and LED on your PC's adapter should be lit.

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

Since the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

4. CONNECTING TO INTERNET

This chapter introduces how to configure the basic functions of your router so that you can surf the Internet.

4.1 Accessing Web page

Connect to the router by typing 192.168.1.1 in the address field of web browser. Then press **Enter** key.



Then below window will pop up that requires you to enter valid User Name and Password.



Enter **admin** for User Name and Password, both in lower case letters. Then click **OK** button or press **Enter** key.

Now you will get into the web interface of the device. The Main screen will appear.

Note: If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings**, in the screen that appears, cancel the **Using Proxy checkbox**, and click **OK** to finish it.

Now you have logged into the web interface of the router. First, you will see the System Status page.

ModelNo. N300RH
The Smartest Network Devices

Status

- System Status
- Statistics
- System Log

Setup Wizard
Quick Setup
Operation Mode
TCP/IP Settings
Wireless
Route Setup
Firewall
Management

STATUS

English

System

Uptime	0 day : 0 h : 15 m : 15 s
Internet Uptime	0 day : 0 h : 0 m : 0 s
Firmware Version	TOTOLINK-N300RH-V1.0.0-B20140115.1104
Build Time	Thu Jan 2 10:11:26 CST 2014
389.12	
49%	

WAN Configuration

Connect type	Getting IP from DHCP server...
IP Address	0.0.0.0 / 0.0.0.0 / 0.0.0.0
MAC Address	78:44:76:81:96:c2
ISP's Intranet DNS 1	0.0.0.0
ISP's Intranet DNS 2	0.0.0.0
ISP's Intranet DNS 3	0.0.0.0

Wi-Fi Configuration

Mode	Local AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK_N300RH
Channel Number	5
Encryption	Disabled(AP).Disabled(WDS)

Copyright © 2013 TOTOLINK Ltd., All Rights Reserved

4.2 Changing Password

Now, we recommend that you change the password to protect the security of your router. Please go to **Management—Web Login Password** change the password required to log in your router.

PASSWORD SETUP

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:	<input type="text" value="admin"/>
New Password:	<input type="password" value="....."/>
Confirmed Password:	<input type="password"/>
<input type="button" value="Apply Changes"/>	

User Name: type in the name that you use to login the web interface of the router.

New Password: new password is used for administrator authentication.

Confirm Password: new password should be re-entered to verify its accuracy.

Note: password length is 8 characters maximum, characters after the 8th position will be truncated.

4.3 Setup Wizard

Setup Wizard is provided as part of the web configuration utility. Users can simply finish

the settings on this page to access Internet.

Status	+
Setup Wizard	-
• Setup Wizard	
Quick Setup	+
Operation Mode	+
TCP/IP Settings	+
Wireless	+
Route Setup	+
Firewall	+
Management	+

1. Click on the **Setup Wizard** on the left navigation menu, then the following screen will appear. Click **Next** to continue.

SETUP WIZARD

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

1. Show Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless Basic Setting
6. Wireless Security Setting

Next>>

2. This router provides six operation modes: **Wireless ISP Client Router**, **Wireless Client and Repeater (Range Extender)**, **Router**, **Bridge with AP** and **Client**. As the default mode is Router mode, you just need to click **Next** to continue other settings. Otherwise, click Setup Operation Mode Button to select one operation mode according to need.

1. MODE

This page shows you the selected router mode.

Router

In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Cancel

<<Back

Setup Operation Mode

Next>>

3. After click Setup Operation Mode Button, the operation mode select interface will appear, please choose the proper mode refer to the introduction. Click **Save Changes**.

OPERATION MODE

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

<input type="radio"/> Wireless ISP Client Router	Wirelessly connect to WISP station/hotspot to share Internet to local wireless and wired network
<input type="radio"/> Wireless Client	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
<input type="radio"/> Repeater(Range Extender)	Extend your existing wireless coverage by relaying wireless signal.
<input checked="" type="radio"/> Router	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
<input type="radio"/> Bridge with AP	Combine two local networks via wireless connection.
<input type="radio"/> Client	Acting as a "Wireless Adapter" to connect your wired devices(e.g.Xbox/PS3) to a wireless network.

A: Wireless ISP Client Router

In this mode, it will wirelessly connect to WISP station/hotspot to share Internet to local wireless and wired network.

B: Wireless Client

In this mode, all Ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. You can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

C: Repeater (Range Extender)

In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners. It is good for extending your existing wireless coverage by relaying wireless signal.

D: Router

In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The Wireless port share the same IP to ISP through Ethernet WAN port .The Wireless port acts the same as a LAN port while at AP Router mode. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

E: Bridge with AP

In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can't be connected easily together with a cable.

F: Client

In this mode, the device can be connected to another device via Ethernet port and act as a "Wireless Adapter" to connect your wired device to a wireless network.

4.3.1 Router Mode

After selecting the Router mode in the last step, click next to continue the other settings.

1. This page allows you to maintain the system time synchronizing with a public time server over the Internet. Here, you can specify the device's time zone according to GMT (Greenwich Mean Time). Then click **Next**.

2. TIME ZONE SETTING

You can maintain the system time by synchronizing with a public time server over the Internet.

<input type="checkbox"/> Automatically Adjust Daylight Saving	
Time Zone Select :	(GMT+07:00)Bangkok, Hanoi, Jakarta ▼
SNTP server :	203.117.180.36 - Asia Pacific ▼

Enable NTP client update: NTP means Network Time Protocol which is used to make the computer's time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.

Automatically Adjust Daylight Saving: If the Time Zone you choose implements daylight saving time, please select this option.

Time Zone Select: Select the Time Zone where the router is located.

SNTP server: Please choose the corresponding SNTP server to get right time.

2. This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point.

3. LAN INTERFACE SETUP

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

IP Address: this is the IP address to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Subnet Mask: this is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

3. This interface is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.

4. WAN INTERFACE SETUP

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	DHCP Client ▼
------------------	---------------

Cancel <<Back Next>>

WAN Access Type: there are five methods provided to allow you to access Internet. Please choose the appropriate one according to the information from your ISP (Internet Service Provider).

(1). Static IP

If your ISP has provided the fixed IP that allows you to access Internet, please choose this option.

WAN Access Type:	Static IP ▼
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
ISP's Intranet DNS 1	
ISP's Intranet DNS 2	
ISP's Intranet DNS 3	

Cancel <<Back Next>>

IP Address: the IP address provided by your ISP.

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.

DNS: The Domain Name System (DNS) is an Internet “phone book”, which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requested are forwarded by this router.

(2). DHCP

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically.

WAN Access Type:	DHCP Client ▼
------------------	---------------

Cancel <<Back Next>>

(3). PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection

between two systems that enables encapsulated data transport. It relied on two widely accepted standards: PPP and Ethernet. The router supports dual access in this WAN type, you could choose the proper one according to what your ISP provides for you.

WAN Access Type:	PPPoE ▼
User Name:	<input type="text"/>
Password:	<input type="password"/>

User Name: a specific valid ADSL user name provided by your ISP.

Password: the corresponding valid password provided by your ISP.

(4). PPTP

PPTP means Point to Point Tunneling Protocol is a VPN connection that only applies in Europe. If you choose one of them, please type in all the information that your ISP provided for this protocol:

WAN Access Type:	PPTP ▼
WAN DHCP Type:	<input checked="" type="radio"/> DHCP Client <input type="radio"/> Static IP
Server IP Address:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>

(5). L2TP

L2TP means Layer 2 Tunneling Protocol is a VPN connection that only applies in Europe, Middle East and Africa (MEA) regions. If you choose one of them, please type in all the information that your ISP provided for this protocol:

WAN Access Type:	L2TP ▼
WAN DHCP Type:	<input checked="" type="radio"/> DHCP Client <input type="radio"/> Static IP
Server IP Address:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>

4. The general wireless settings, such as wireless mode, SSID and channel can be configured in this section.

5. WIRELESS BASIC SETTING

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	2.4 GHz (B+G+N) ▼
Mode:	AP ▼
Network Type:	Infrastructure ▼
SSID:	TOTOLINK N300RH Find Wi-Fi networks
Channel Width:	20MHz ▼
Control Sideband:	Upper ▼
Channel Number:	Auto ▼

<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK N300RH_RPT0 Find Wi-Fi networks
--------------------------------------------------------------------------------------------------	-------------------------------------------------------

Cancel <<Back Next>>

Band: In fact, this option allows you to choose the radio standard for operation of your router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n (2.4GHz and/or 5GHz, in this case, only supports 2.4GHz) is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. Here, you can choose the last one 2.4GHz (B+G+N), this mode offers better compatibility.

Mode: Wireless mode specifies the operating mode of the device. The mode depends on the network topology requirements. There are 2 operating modes supported in this software.

AP: This mode allows users with laptop to surf Internet by wireless connection. It's designed to add wireless function for existed wired router which is just suitable for home and small offices.

Client: If you choose this mode, the Channel Number and Channel Width can't be edited.

Note: If you select WDS, you can't change SSID.

SSID---Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in AP or AP+WDS mode. All the client devices within the range will receive broadcast messages from the access point advertising this SSID.

Channel Width---This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

20MHz is the standard channel spectrum width.

40MHz is the channel spectrum with the width of 40MHz (selected by default).

Control Sideband---This function is to control the sideband of the radio channel.

Upper: By default, it is Upper, and the Channel Number is 11.

Lower: If you choose Lower, the Channel Number will change to **Auto** automatically and you can't change the Control Sideband at the same time. The selectable Channel Number now will range from 1 to 9. Only when you choose other Channel Number you will activate the Control Sideband again. If you choose Upper, the Channel Number

selectable will range from 5 to 13.

Channel Number---this option provides selectable channel numbers.

5. By default, the encryption type is disabled. For a secure connection, WPA2 Mixed is recommended for you to protect your network.

6. WIRELESS SECURITY SETUP

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:	WPA2 Mixed ▼
Pre-Shared Key Format:	Passphrase ▼
Pre-Shared Key:	<input type="text"/>

After all the above settings, please click **Finish** button, then page with below messages will pop up:

CHANGE SETTING SUCCESSFULLY!

Do not turn off or reboot the Device during this time.

Please wait 35 seconds ...

When it turns back to the system status interface, you can see the Wi-Fi Configuration Column, The Mode should be Local AP if you have setup Router mode successfully. The numbers of connected clients will be shown here. Now you can surf Internet and enjoy the best wireless experience brought by the router.

<u>Wi-Fi Configuration</u>	
<u>Mode</u>	Local AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK N151RT
Channel Number	3
<u>Encryption</u>	Disabled(AP),Disabled(WDS)
BSSID	d4:bf:7f:0d:aa:2d
<u>WPS Status:</u>	Off
<u>Connected Clients</u>	1

4.3.2 Wireless ISP Client Mode

1. In the Wireless ISP Client Mode, the Time Zone Setting is the same with the Router mode.
 2. The LAN and WAN Interface Setting is the same with the Router mode too.
 3. The wireless basic setting interface is obviously different from the Router mode.
- In this mode, you can enable Universal Repeater in this page.

5. WIRELESS BASIC SETTING

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	2.4 GHz (B+G+N) ▼
Mode:	AP ▼
SSID:	TOTOLINK N151RT <input type="button" value="Find Wi-Fi networks"/>
Channel Width:	20MHz ▼
Control Sideband:	Upper ▼
Channel Number:	Auto ▼

<input checked="" type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK N151RT_RPT0 <input type="button" value="Find Wi-Fi networks"/>
-------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------

4. The settings will take effect soon. Then it will come back to the system status interface, and you can see the WISP status. The signal strength is also shown here.

CHANGE SETTING SUCCESSFULLY!

Do not turn off or reboot the Device during this time.

Please wait 34 seconds ...

Wi-Fi Configuration

Mode	Local AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK_N151RT
Channel Number	11
Encryption	WPA2 Mixed(AP),Disabled(WDS)
BSSID	d4:bf:7f:0d:aa:2d
WPS Status:	Off

WISP status

Mode	Wireless ISP
SSID	TOTOLINK N302R+
Encryption	Disabled
BSSID	b8:55:10:b4:8d:60
Status	Connected
Connected Clients	0
Signal Strength	<div><div></div></div> 84%

4.3.3 Wireless Client Mode

The first three steps are the same with Router mode too. Wireless Basic Setting interface is also different with the Router mode. See below.

Please

Band:	2.4 GHz (B+G+N) ▼	
Mode:	Client ▼	
SSID:	TOTOLINK_N151RT	Find Wi-Fi networks
Channel Width:	20MHz ▼	
Control Sideband:	Upper ▼	
Channel Number:	Auto ▼	

<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK N151RT_RPT0 Find Wi-Fi networks
--------------------------------------------------------------------------------------------------	----------------------------------------------------------

[Cancel](#)
[<<Back](#)
[Next>>](#)

After configuration, it will also come back to the system status interface, and you can see the Wi-Fi Configuration column. The signal strength is also shown here.

Wi-Fi Configuration

Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK_N151RT
Channel Number	10
Encryption	Disabled
BSSID	00:00:00:00:00:00
WPS Status:	Off
Status	Scanning
Signal Strength	<div style="width: 0%;"></div> 0%

4.3.4 Repeater Mode

1. In the Repeater Mode, the Time Zone Setting is the same with the Router Mode.
2. The LAN Interface Setting is the same with the Router Mode too.
3. The WAN interface setting is unvalued in Repeater Mode. See Below:

4. WAN INTERFACE SETUP

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	DHCP Client ▼
------------------	---------------

[Cancel](#)
[<<Back](#)
[Next>>](#)

4. Wireless Basic Setting interface is also different with the Router mode. See below:

5. WIRELESS BASIC SETTING

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	2.4 GHz (B+G+N) ▼
Mode:	AP ▼
SSID:	TOTOLINK N151RT Find Wi-Fi networks
Channel Width:	20MHz ▼
Control Sideband:	Upper ▼
Channel Number:	Auto ▼

<input checked="" type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK N151RT_RPT0 Find Wi-Fi networks
-------------------------------------------------------------------------------------------------------------	-------------------------------------------------------

Cancel <<Back Next>>

5. Click Find Wi-Fi networks Button, the site survey interface will appear. You should click Site Survey button to scan the wireless network, and then choose one as upper AP. After selection please click next to continue the setup wizard.

WIRELESS SITE SURVEY

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
TOTOLINK N302R+	b8:55:10:b4:8d:60	11 (B+G+N)	AP	no	60	<input checked="" type="radio"/>
zion	00:0e:e8:64:07:56	9 (B+G)	AP	WPA-PSK	44	<input type="radio"/>
TOTOLINK ND300	b8:55:10:70:84:94	11 (B+G+N)	AP	no	40	<input type="radio"/>
HUASAN	f8:01:13:92:f4:84	10 (B+G+N)	AP	WPA2-PSK	34	<input type="radio"/>
iptime-n7004ns	00:08:9f:00:00:20	9 (B+G)	AP	WPA-PSK	30	<input type="radio"/>
360ase	00:23:c0:03:11:a0	3 (B+G+N)	AP	WPA2-PSK	22	<input type="radio"/>
04173	00:26:66:6d:39:3c	5 (B+G+N)	AP	no	12	<input type="radio"/>
TOTOLINK N100RE	78:44:76:45:b5:cd	5 (B+G+N)	AP	no	12	<input type="radio"/>
zion-meetingroom	b8:55:10:02:e8:4d	9 (B+G+N)	AP	WPA-PSK/WPA2-PSK	12	<input type="radio"/>
TOTOLINK-208	78:44:76:d6:54:80	1 (B+G)	AP	WEP	10	<input type="radio"/>
Phicomm_3467A8	f0:eb:d0:34:67:a8	3 (B+G+N)	AP	WPA-PSK/WPA2-PSK	10	<input type="radio"/>

Next>>

6. When there comes to this page, you should enter the correct Pre-Shared Key to connect to the network if the network has enabled encryption if the AP you select is encrypted. Then click Connect button.

Encryption:	NONE ▼
-------------	--------

<<Back Connect

7. Just wait for minutes when it comes out this page. The settings will take effect after few minutes.

WIRELESS SITE SURVEY

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.


Please wait...

After configuration, it will also come back to the system status interface, and you can see the Wi-Fi Configuration column.

Wi-Fi Configuration

Mode	Local AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK_N151RT
Channel Number	11
Encryption	Disabled(AP),Disabled(WDS)
BSSID	d4:bf:7f:0d:aa:2d
WPS Status:	Off

WISP status

Mode	Wireless ISP
SSID	TOTOLINK N302R+
Encryption	Disabled
BSSID	b8:55:10:b4:8d:60
Status	Connected
Connected Clients	0
Signal Strength	 74%

4.3.5 Bridge with AP

In Bridge with AP mode, the first three steps are also the same with the Repeater mode. The Wireless Basic Setting interface is shown below:

5. WIRELESS BASIC SETTING

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	2.4 GHz (B+G+N) ▼	
Mode:	AP ▼	
SSID:	TOTOLINK_N151RT	Find Wi-Fi networks
Channel Width:	20MHz ▼	
Control Sideband:	Upper ▼	
Channel Number:	Auto ▼	
<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)		
TOTOLINK N302R+		Find Wi-Fi networks
<div>Cancel <<Back Next>></div>		

4.3.6 Client Mode

The first three steps are the same with the Repeater Mode. The Wireless Basic Setting is different from Repeater Mode. See below:

5. WIRELESS BASIC SETTING

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band:	2.4 GHz (B+G+N) ▼	
Mode:	Client ▼	
SSID:	TOTOLINK_N151RT	Find Wi-Fi networks
Channel Width:	20MHz ▼	
Control Sideband:	Upper ▼	
Channel Number:	Auto ▼	

<input type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	TOTOLINK_N302R+	Find Wi-Fi networks
--------------------------------------------------------------------------------------------------	-----------------	---------------------

Cancel <<Back Next>>

It will come back to status interface, and you can see the Wi-Fi Configuration column in the system status page. If you have setup Client mode successfully, you will see that the Mode is Infrastructure Client here, and the signal strength is also shown in this page.

Wi-Fi Configuration

Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK_N302R+
Channel Number	11
Encryption	Disabled
BSSID	b8:55:10:b4:8d:60
WPS Status:	Off
Status	Connected
Signal Strength	<div><div></div></div> 82%

4.4 Quick Setup

Quick Setup is provided as part of the web configuration utility. Users can simply finish the settings all in one page to access Internet. In this section, you can setup LAN, WAN, WLAN and Time Zone Settings. Please click **Save** button to apply the configuration when you have completed the settings on this page.

QUICK SETUP

<u>LAN Interface Setup</u>		
IP Address:	192.168.1.1	login.viettel.vn
Subnet Mask:	255.255.255.0	
<u>WAN Interface Setup</u>		
WAN Access Type:	DHCP Client ▼	
<u>IPTV</u>		
<input type="checkbox"/> Enabled IPTV		
Internet Vlan ID	35	
IPTV1 Vlan ID	36	<input checked="" type="checkbox"/> Tag
IPTV1 PORT	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input checked="" type="checkbox"/> LAN4	
<u>WLAN Interface Setup</u>		
<input type="checkbox"/> Disable Wireless LAN Interface		
Band:	2.4 GHz (B+G+N) ▼	
Mode:	AP ▼	
SSID:	TOTOLINK N151RT	
Channel Width:	20MHz ▼	
Control Sideband:	Upper ▼	
Channel Number:	Auto ▼	
Data Rate:	Auto ▼	
Encryption:	Disabled ▼	
<u>Time Zone Setting</u>		
<input checked="" type="checkbox"/> Enable NTP client update		
Time Zone Select :	(GMT+07:00)Bangkok, Hanoi, Jakarta ▼	
SNTTP server :	203.117.180.36 - Asia Pacific ▼	

LAN Interface Setup

IP Address: This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

WAN Interface Setup

This part allows you to configure the WAN port parameters so that your computer can access Internet.

IPTV

This part allows you to enable IPTV function and configure the Internet and IPTV VIDs

provided by corresponding service providers and choose the port for IPTV.

WLAN Interface Setup

Band: In fact, this option allows you to choose the radio standard for operation of your router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n (2.4GHz and/or 5GHz, in this case, only supports 2.4GHz) is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. Here, you can choose the last one 2.4GHz (B+G+N), this mode offers better compatibility.

Mode: Wireless mode specifies the operating mode of the device. The mode depends on the network topology requirements. There are 2 operating modes supported in this software.

AP: This mode allows users with laptop to surf Internet by wireless connection. It's designed to add wireless function for existed wired router which is just suitable for home and small offices.

Client: If you choose this mode, the Channel Number and Channel Width can't be edited.

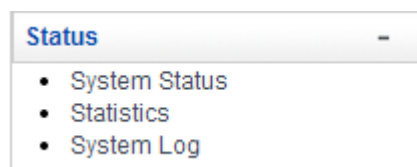
Time Zone Setting:

Enable NTP client update: NTP means Network Time Protocol which is used to make the computer's time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.

Time Zone Select: Select the Time Zone where the router is located.

SNTP server: Please choose the corresponding SNTP server to get right time.

4.5 Status



4.4.1 System status

The System Status provides basic network settings of this router, including LAN, WAN and Wireless configuration. Also, you could get the current running firmware version or firmware related information from this presentation.

STATUS

English ▼

System

Uptime	0day:0h:0m:56s
Internet Uptime	0day:0h:0m:0s
Firmware Version	AN-PHAT-N151RT-V1.0.0-B20140310.1627
Build Time	Mon Mar 10 16:29:21 CST 2014
CPU load	40%
SDRAM utilization	41%

WAN Configuration

Connect type	Getting IP from DHCP server...
IP Address	0.0.0.0 / 0.0.0.0 / 0.0.0.0
MAC Address	d4:bf:7f:0d:aa:30
ISP's Intranet DNS 1	0.0.0.0
ISP's Intranet DNS 2	0.0.0.0
ISP's Intranet DNS 3	0.0.0.0

Wi-Fi Configuration


Mode	Local AP
Band	2.4 GHz (B+G+N)
SSID	TOTOLINK N151RT
Channel Number	3
Encryption	Disabled(AP),Disabled(WDS)
BSSID	d4:bf:7f:0d:aa:2d
WPS Status:	Off
Connected Clients	0

LAN Configuration

Connect type	Fixed IP
IP Address	192.168.1.1 / 255.255.255.0 / 192.168.1.1
DHCP Server	Enabled
MAC Address	d4:bf:7f:0d:aa:2d
LAN-connected clients	1

Signal strength will show on this page in Wireless ISP Client Router mode, Client Router mode, Repeater mode and Client mode. As below:

WISP status

Mode	Wireless ISP
SSID	TOTOLINK N302R+
Encryption	Disabled
BSSID	b8:55:10:b4:8d:60
Status	Connected
Connected Clients	0
Signal Strength	 84%

4.4.2 Statistics

This page shows the counter for sent and received packets regarding to wireless and Ethernet networks.

STATISTICS

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	Sent Packets	1292
	Received Packets	9376
Ethernet LAN	Sent Packets	13091
	Received Packets	7839
Ethernet WAN	Sent Packets	0
	Received Packets	0

Refresh

4.4.3 System log

This page can be used to set remote log server and show the system log.

SYSTEM LOG

This page can be used to set remote log server and show the system log.

<input type="checkbox"/> Enable Log		
<input type="checkbox"/> system all	<input type="checkbox"/> wireless	<input type="checkbox"/> DoS
<input type="checkbox"/> Enable Remote Log	Log Server IP Address:	<input type="text"/>
Save Changes	Refresh	Clear

Enable Log: this option enables the registration routine of the system log messages. By default it is disabled. Below items including system all, wireless, Dos allows you to choose the log type.

Enable Remote Log: enables remote log sending function while System log messages are sent to a remote server.

Log Server IP Address: this is the host IP address where system log messages should be sent.

After finished, please click **Save Changes**.

5. ADVANCED SETTINGS

This chapter allows users to configure advanced settings includes TCP/IP settings, Wireless, Route Setup, Firewall and System Management. These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Also they should not be changed unless you know what effect the changes will have on your wireless router.

5.1 Operation mode

Operation Mode

- Operation Mode

This parameter specifies the operating network modes for the router. Since we have introduced on the **Setup Wizard** section, just refer to **Setup Wizard**

<input type="radio"/> Wireless ISP Client Router	Wirelessly connect to WISP station/hotspot to share Internet to local wireless and wired network
<input type="radio"/> Wireless Client	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
<input type="radio"/> Repeater(Range Extender)	Extend your existing wireless coverage by relaying wireless signal.
<input checked="" type="radio"/> Router	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
<input type="radio"/> Bridge with AP	Combine two local networks via wireless connection.
<input type="radio"/> Client	Acting as a "Wireless Adapter" to connect your wired devices(e.g.Xbox/PS3) to a wireless network.

Save Changes

Operation Mode Help

If you don't know how to choose the correct operation mode, please click Operation Mode Help Button. The interface for help will appear right now. This interface will introduce the difference of different modes.

OPERATION MODE HELP

Client Router:In this mode ,the device enables multiusers to Internet from WISP.The LAN port devieces share the same IP from WISP through Wireless port.While connecting to WISP,the Wireless port works as a WAN port at AP client Router mode.The ethernet port acts as a LAN port

Repeater(Range Extender):In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners

Router:In this mode,the device enables multiusers to share Internet via ADSL/Cable Modem.The Wireless port share the same IP to ISP through ethernet WAN port .The Wireless port acts the same as a LAN port while at AP Router mode

Bridge with AP:In this mode, the device can be used to combine multiple local networks together to the same one via wirelss connections,especially for a home or office where separated networks can not be connected easily together with a cable

Client:In this mode ,the device can be connected to another device via Ethernet port and act as an adaptor to grant your wired devices access to a wireless network,especially for a Smart TV,Mdia Player.or game console only with an Ethernet port

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

<< Back

5.2 TCP/IP Settings

TCP/IP Settings -

- LAN Interface
- WAN Interface
- VLAN Settings
- DHCP&ARP Tables

5.2.1 LAN Interface

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP. This part allows you to configure the parameters for LAN which connects to the LAN port of your Access Point.

LAN INTERFACE SETUP

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

DHCP	Server ▾	
IP Address:	192.168.1.1	login.totolink.com
Subnet Mask:	255.255.255.0	
DNS Type	Attain DNS Automatically ▾	
ISP's Intranet DNS 1		
ISP's Intranet DNS 2		
DHCP Client Range:	192.168.1.10 - 192.168.1.254	
DHCP Lease Time:	480 (1 ~ 10080 minutes)	
Static DHCP:	Set Static DHCP	
Domain Name:	TOTOLINK	
802.1d Spanning Tree:	Disabled ▾	
For IP Routing usage:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
2nd IP Address:	0.0.0.0	
2nd Subnet Mask:	0.0.0.0	

Save Changes

DHCP Clients Table

Hostname	IP Address	MAC Address	Remaining lease time (in seconds)
MQR91X2P79KCP8Y	192.168.1.10	50:46:5d:09:f3:84	28683

IP Address: This is the IP addresses to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

Note: If this IP address changed, you can log into the WEB configuration interface only using the new IP address. AND if the new IP address and the original IP address are not in the same segment, the Virtual Server and DMZ Host service will not work. If you need to enable these functions, you will have to reset this IP address.

Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

DHCP: You can disable or enable this function here.

DHCP Client Range: the range of IP addresses that will be assigned to each computer connected with the router.

DHCP Lease Time: the IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Static DHCP: click the **Set Static DHCP** button to go to the Static DHCP setup interface.

Domain name: this represents the name of your IP address.

802.1d Spanning Tree: Multiple interconnected bridges create larger networks using the IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within the network and to eliminate loops from the topology. If the STP is turned on, the router will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when this router is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the bridge to participate in the Spanning Tree Protocol in this case.

For IP Routing Usage: you can enable or disable this function for IP routing usage. When you enable this function, please enter the second IP address and subnet mask in the corresponding field.

It will come out the Static DHCP Setup interface after you click the **Set Static DHCP** button.

Check the box to enable static DHCP, it allows you to reserve IP addresses and assign the same IP address to the network device with the specified MAC address any time it requests an IP address.

STATIC DHCP SETUP

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

☐ Enable Static DHCP

IP Address	<input type="text"/>
MAC Address	<input type="text"/>
Comment	<input type="text"/>

Save Changes

Static DHCP List:

IP Address	MAC Address	Comment	Select
------------	-------------	---------	--------

Delete Selected

Delete All

5.2.2 WAN Interface

This part allows you to configure the WAN port parameters so that your computer can access Internet. Since we have discussed WAN Access Type on Setup Wizard, we will mainly explain PPPoE, PPTP, L2TP and the other settings here.

WAN INTERFACE SETUP

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	DHCP Client ▼	
Host Name:	<input type="text"/>	
MTU	<input type="text" value="1492"/>	(1400-1492)
Clone MAC Address	<input type="text" value="000000000000"/>	
Web Server Port:	<input type="text" value="80"/>	(default : 80)
SSH Server Port:	<input type="text" value="22"/>	(default : 22)
<input checked="" type="checkbox"/> Enable uPNP		
<input type="checkbox"/> Enable IGMP Proxy		
<input type="checkbox"/> Enable IGMP Snooping		
<input type="checkbox"/> Enable Ping Access on WAN		
<input type="checkbox"/> Enable Web Server Access on WAN		
<input checked="" type="checkbox"/> Enable IPsec pass through on VPN connection		
<input checked="" type="checkbox"/> Enable PPTP pass through on VPN connection		
<input checked="" type="checkbox"/> Enable L2TP pass through on VPN connection		

Save Changes

MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

DNS: Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Clone MAC Address: MAC address is the physical address of your computer's network card. Generally, every network card has one unique Mac address. Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

Enable UPnP: the UPnP (Universal Plug and play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows "Plug and Play" system. You can enable this function so that the router doesn't need to work out which port need to be opened.

Enable IGMP Proxy: IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. If you select this checkbox, the application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.

Enable Ping Access on WAN: enable users use Ping command to access WAN.

5.2.2.1 PPPoE

Select PPPoE option if ISP provides a PPPoE connection. You should enter the following parameters.

WAN Access Type:	PPPoE/Dual Wan Access PPPoE ▼		
PPPoE Connection:			
User Name:	<input type="text"/>		
Password:	<input type="password"/>		
Connection Type:	<input checked="" type="radio"/> Constant		
	<input type="radio"/> Connection on demand		
	Idle Time:	<input type="text" value="5"/>	(1-1000)
	<input type="radio"/> Connection manually		
	<input type="button" value="Connect"/>		<input type="button" value="Disconnect"/>
Service name:	<input type="text"/>		
AC name:	<input type="text"/>		
MTU	<input type="text" value="1442"/>	(1360-1492)	
Clone MAC Address	<input type="text" value="000000000000"/>		

User Name/Password: enter the User Name and Password provided by your ISP.

Connection Type: provides three modes to connect to the Internet.

- **Constant:** the connection can be re-established automatically.
- **Connection on demand:** the Internet connection can be terminated automatically after a specified inactivity period (idle time).
- **Connection manually:** you can click **Connect** or **Disconnect** button to connect/disconnect immediately.

Service Name (AC): this is optional. It describes the service name your ISP provided to

you. Generally, leaving these fields blank will work.

MTU: it means Max Transmit Unit for packet. When using slow links, large packets can cause some delays thereby increasing lag and latency.

Clone MAC Address: MAC address is the physical address of your computer's network card. Generally, every network card has one unique Mac address. Since many ISPs only allow one computer in LAN to access Internet, users can enable this function to make more computers surf Internet.

5.2.2.2 PPTP

You should select PPTP option if ISP provides a PPTP connection and enter the following parameters. Please refer to PPPoE configuration if there are the same parameters.

WAN Access Type:	PPTP/Dual Wan Access PPTP ▼		
User Name:	<input type="text"/>		
Password:	<input type="password"/>		
Server IP Address:	<input type="text"/>		
MPPE:	<input type="checkbox"/> Enable MPPE Encryption <input type="checkbox"/> Enable MPPC compression		
WAN DHCP Type:	<input checked="" type="radio"/> DHCP Client <input type="radio"/> Static IP		
Connection Type:	<input checked="" type="radio"/> Constant <input type="radio"/> Connection on demand		
Idle Time:	<input type="text" value="5"/>	(1-1000)	
	<input type="radio"/> Connection manually <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>		
MTU	<input type="text" value="1460"/>	(1400-1460)	
Clone MAC Address	<input type="text" value="000000000000"/>		

WAN DHCP type: it's available only for PPTP connection. If your ISP provides an extra type to connect to a local area network such as **DHCP Client/Static IP**, you should select the type and enter the right parameters provided by ISP to enable the secondary connection.

MPPE: You can enable MPPE Encryption or MPPC compression here. MPPE provides link encryption. Link encryption encrypts data as it passes between the calling and answering routers. MPPC provides a method to negotiate and utilize compression protocols over PPP encapsulated links.

DNS Type: If you select Set DNS Manually, you will have to type in the DNS address by yourself. It is chosen to Attain DNS by default while you select the DHCP client mode. Besides, it is Set DNS type while you select the Static IP.

5.2.2.3 L2TP

You should select L2TP option if ISP provides a L2TP connection and enter the following parameters. Please refer to PPPoE configuration if there are the same parameters.

WAN Access Type:	L2TP/Dual Wan Access L2TP ▼	
User Name:	<input type="text"/>	
Password:	<input type="password"/>	
Server IP Address:	<input type="text"/>	
WAN DHCP Type:	<input checked="" type="radio"/> DHCP Client <input type="radio"/> Static IP	
Connection Type:	<input checked="" type="radio"/> Constant <input type="radio"/> Connection on demand	
Idle Time:	5 (1-1000)	
	<input type="radio"/> Connection manually <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	
MTU	1460 (1400-1460)	
Clone MAC Address	<input type="text" value="000000000000"/>	

5.2.3 VLAN Settings

VLAN: ☒ Disabled ☐ Enabled ☐ Triple Play

VLAN means Virtual Local Area Network, this function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

VLAN: ☐ Disabled ☒ Enabled ☐ Triple Play

Enable	Ethernet/Wireless	WAN/LAN	Forwarding Rule	Tag	VID(1~4090)	Priority	CFI
<input checked="" type="checkbox"/>	Ethernet Port1	LAN	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Ethernet Port2	LAN	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Ethernet Port3	LAN	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Ethernet Port4	LAN	Bridge ▼	<input checked="" type="checkbox"/>	36	4 ▼	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Wireless 1 Primary AP	LAN	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/>
<input type="checkbox"/>	Wireless 1 Virtual AP1	LAN	NAT ▼	<input type="checkbox"/>	1	0 ▼	<input type="checkbox"/>
<input type="checkbox"/>	Wireless 1 Virtual AP2	LAN	NAT ▼	<input type="checkbox"/>	1	0 ▼	<input type="checkbox"/>
<input type="checkbox"/>	Wireless 1 Virtual AP3	LAN	NAT ▼	<input type="checkbox"/>	1	0 ▼	<input type="checkbox"/>
<input type="checkbox"/>	Wireless 1 Virtual AP4	LAN	NAT ▼	<input type="checkbox"/>	1	0 ▼	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Ethernet Port5	WAN	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/>

[Apply Changes](#)

Enabled: this option enables VLAN function.

Ethernet/Wireless: specifies the WAN port and wireless AP.

WAN/LAN: defines the WAN port or LAN port.

Forwarding Rule: VLAN feature also support forwarding rule as bridge and NAT between LAN port and WAN port.

Tag: enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please type the tag value and specify the priority for the packets sending by LAN.

VID: type the value as the VLAN ID number. The range is from 1 to 4090.

Priority: Type the packet priority number for such VLAN. The range is from 0 to 7.

CFI: enable the CFI function which indicates whether MAC is encapsulated by standard format.

After the VLAN settings, please click **Apply Changes** to finish TCP/IP Settings.

When you choose Triple Play, this configuration page is shown below

VLAN: ☐ Disabled ☐ Enabled ☒ Triple Play

VLAN information	Forwarding Rule	Tag	VID(1-4090)	Priority	Port mapping(LAN & WLAN) P1 P2 P3 P4 W1 W2 W3
Internet	NAT ▼	<input checked="" type="checkbox"/>	35	0 ▼	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
IPTV 1	Bridge ▼	<input checked="" type="checkbox"/>	36	4 ▼	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
IPTV 2	Bridge ▼	<input checked="" type="checkbox"/>	1	0 ▼	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

[Apply Changes](#)

5.2.4 DHCP&ARP Table

ARP means address resolution protocol. This table will show you detailed information about the ARP request your router has detected. DHCP Table presents the DHCP information.

DHCP CLIENTS & ARP TABLE

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

ARP Table		
IP Address	MAC Address	Interface
192.168.1.10	50:46:5d:09:f3:84	br0

DHCP Clients Table			
Hostname	IP Address	MAC Address	Remaining lease time (in seconds)
No HostName	192.168.1.10	50:46:5d:09:f3:84	28209

Refresh

5.3 Wireless



5.3.1 Basic Settings

On this page, you could configure the parameters for Wireless LAN client that may connect to your Access Point. Since we have discussed wireless settings on **Setup Wizard**, here we will focus on the encryption, WMM function and Data Rate.

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N) ▼	
Mode:	AP ▼	Multiple APs
SSID:	TOTOLINK N300RH	Find Wi-Fi networks
Channel Width:	20MHz ▼	
Control Sideband:	Upper ▼	
Channel Number:	Auto ▼	
Broadcast SSID:	Enabled ▼	
WMM:	Enabled ▼	
Data Rate:	Auto ▼	
Associated Clients:	Show Active Clients	
Encryption:	Disabled ▼	

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneously)

TOTOLINK N300RH_RPT0
Find Wi-Fi networks

Apply Changes

Click Multiple APs button, the multiple APs setup interface will appear. You can add other SSID for different needs. What's more, you can setup different encryption for different SSIDs in Security Settings section. We will introduce in **5.2.2 Security Settings**

MULTIPLE APs

This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List	Mode:
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N) ▼	TOTOLINK N1	Auto ▼	Enabled ▼	Enabled ▼	LAN+WAN ▼	Show	AP
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N) ▼	TOTOLINK N1	Auto ▼	Enabled ▼	Enabled ▼	LAN+WAN ▼	Show	AP
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N) ▼	TOTOLINK N1	Auto ▼	Enabled ▼	Enabled ▼	LAN+WAN ▼	Show	AP
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N) ▼	TOTOLINK N1	Auto ▼	Enabled ▼	Enabled ▼	LAN+WAN ▼	Show	AP

Apply Changes

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.

Note: This option will keep Enabled and can't be changed by default.

Data Rate

This defines the data rate (in Mbps) at which the device should transmit wireless packets. You can fix a specific data rate between MCS 0 and MCS 7 also. It is recommended to use Auto option, especially if you are having trouble getting connected or losing data at a higher rate.

MCS means Modulation Coding Scheme. Before 802.11n standard emerges, most Access Points complies with 802.11a/b/g standards and the data rate ranges from 1Mbps to 54Mbps, including only 12 possible physical speed. But when it comes to

802.11n technology, the physical speed can be affected by many factors, such as modulation type, coding rate, space flow quantity, whether 40MHz banding and so on. Combining these factors together will create a lot of selectable physical speed. Thus, 802.11n proposes the term MCS. You can consider this term to be a whole combination of these factors and every digit represents a combination.

Note: If you select 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is MCS7(150Mbps).

Associate Clients: Click Show Active Clients Button it will come to WiFi Station interface.

ACTIVE WIRELESS CLIENT TABLE

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

MAC Address	Mode	Tx Packet	Rx Packe	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---	---

Encryption: This router supports Disabled, WEP, WPA, WPA2, WPA-Mixed security options. By default, it is disabled. Please select one according to the Access Point security policy for a secure network.

Encryption:	WEP ▼
802.1x Authentication:	Disabled
Authentication:	WEP
Key Length:	WPA
Key Format:	WPA2
	WPA-Mixed

1) WEP

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.

Encryption:	WEP ▼
802.1x Authentication:	<input type="checkbox"/>
Authentication:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length:	64 Bits ▼
Key Format:	HEX(10 characters) ▼
Encryption Key:

Key Length: 64-bit/128-bit, by default it is 64-bit.

64-bit—For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10

hexadecimal digitals leading by 0x, such as 0x414234445.)

128-bit—For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Key Format: If you choose 64 bit, there will be two Key Formats selectable: ASCII (5 characters) and Hex (10 characters). If 128-bit, the Key Formats should comply with ASCII (13 characters) or Hex (26 characters)

Encryption Key: Please refer to Key Length to set this parameter.

2) 802.1x Authentication

WPA (Wi-Fi Protected Access) is separated into two categories: WPA/PSK and WPA/802.1x. If you choose 802.1x Authentication, you will have to provide the RADIUS Server IP Address, Port and Password so that the encryption key will be obtained dynamically from RADIUS server.

Encryption:	WEP ▼
802.1x Authentication:	<input checked="" type="checkbox"/>
Authentication:	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length:	<input checked="" type="radio"/> 64 Bits <input type="radio"/> 128 Bits
RADIUS Server IP Address:	<input type="text"/>
RADIUS Server Port:	1812
RADIUS Server Password:	<input type="text"/>

RADIUS Server IP Address: Enter the IP address of RADIUS server.

RADIUS Server Port: the UDP port number that the RADIUS server that is used to authenticate the messages sent between them.

RADIUS Server Password: enter the password.

RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet Service Provider. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

3) WPA/WPA2

Wi-Fi Protected Access (WPA) is the most dominating security mechanism in industry. It is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x. WPA2 means Wi-Fi Protected Access 2, it is the current most secure method of wireless security and required for 802.11n performance.

TKIP--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA.

AES--Advanced Encryption Standard is another cipher for data encryption supported by WPA.

Encryption:	WPA ▼
Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA Cipher Suite:	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
Pre-Shared Key Format:	Passphrase ▼
Pre-Shared Key:	<input type="text"/>

Pre-Shared Key Format/Pre-Shared Key: This is a pre-defined key used for encryption during data transmission. It has two formats: Passphrase and Hex (64 characters). Then you need to enter the Pre-Shared Key, either 8~63 ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as “0x321253abcde...”).

4) WPA Mixed

This option mixes WPA/WPA2 together. It will provide the best security for your router.

Encryption:	WPA-Mixed ▼
Authentication Mode:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Pre-Shared Key Format:	Passphrase ▼
Pre-Shared Key:	<input type="text"/>

Note: Since WEP has been proved vulnerable, you may consider using WPA2 for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and/or privacy on your wireless network.

Enable Universal Repeater Mode: enable the repeater mode and search for wireless networks in range on all the supported channels while device is operating in Access Point.

<input checked="" type="checkbox"/> Enable Universal Repeater Mode (Acting as AP and client simultaneously)	<input type="text" value="TOTOLINK N300RH_RPT0"/>	<input type="button" value="Find Wi-Fi networks"/>
-------------------------------------------------------------------------------------------------------------	---------------------------------------------------	----------------------------------------------------

5.3.2 Security Settings

You can setup wireless security in this page. Setup different encryptions for different SSIDs so that makes your wireless network more secure. It is very practical for protecting your private information.

Select SSID:	Root AP - TOTOLINK N300RH ▼
<input type="button" value="Apply Changes"/>	<input type="button" value="Reset"/>

Encryption:	Disabled ▼
-------------	------------

5.3.3 Site Survey

Utility will search for wireless networks in range on all the supported channels while device is operating in Access Point mode. This page provides a tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal
TOTOLINK N302R+	b8:55:10:b4:8d:60	11 (B+G+N)	AP	no	60
zion	00:0e:e8:64:07:56	9 (B+G)	AP	WPA-PSK	46
TOTOLINK	b8:55:10:70:84:94	11 (B+G+N)	AP	WPA2-PSK	38
HUASAN	f8:01:13:92:f4:84	10 (B+G+N)	AP	WPA2-PSK	36
iptime-n7004ns	00:08:9f:00:00:20	9 (B+G)	AP	WPA-PSK	32
360ase	00:23:c0:03:11:a0	3 (B+G+N)	AP	WPA2-PSK	20
iptime	64:e5:99:00:00:00	5 (B+G+N)	AP	no	16
ChinaNet-qNFG	0c:96:bf:7e:d8:08	9 (B+G+N)	AP	WPA- PSK/WPA2- PSK	14
TOTOLINK-208	78:44:76:d6:54:80	1 (B+G)	AP	WEP	10
TOTOLINK_8fc814	b8:55:10:8f:c8:14	7 (B+G+N)	AP	no	6

Please click **Site Survey** button to search for any Access Point or IBSS. Then they will be showed in the form.

Site Survey reports SSID, BSSID, wireless channel, type, encryption type (if any) and Signal Strength of all the surrounding Access Points which can be found by this device.

5.3.4 WDS

WDS means Wireless Distribution System. It is a protocol for connecting two access points wirelessly. Usually, it can be used for the following application:

1. Provide bridge traffic between two LANs though the air.
2. Extend the coverage range of a WLAN.

To meet the above requirement, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☐ Enable WDS

MAC Address:

Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
<div> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> </div>			

Enable WDS: by default, you can't select the checkbox to enable WDS.

MAC Address: the other AP's MAC Address that you want to communicate with.

Data Rate: please choose the transmission data rate.

Comment: describes the reason why you want to communicate with others.

The WDS Security Setup allows you to set encryption for your WDS connection. You can refer to the Wireless Security Setup.

5.3.5 Advanced Settings

This page handles advanced wireless settings that are only for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Country Region:	Europe 1-13 ▼	
Fragment Threshold:	2346	(256-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20-1024 mc)
Limit Client AP(3-64):	64	(default:64)
Limit Client AP1(3-64):	64	(default:64)
Limit Client AP2(3-64):	64	(default:64)
Limit Client AP3(3-64):	64	(default:64)
Limit Client AP4(3-64):	64	(default:64)
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Protection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
WLAN Partition:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
20/40MHz Coexist:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Multicast to Unicast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%	

Apply Changes

Fragment Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes. The default value is 2347, which means that RTS is disabled.

RTS/CTS (Request to Send/Clear to Send) are the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses **Request to Send/Clear to Send** frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provide clear media for the requesting station to send the data. CTS collision control management has a time

interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Beacon Interval: By default, it is set to 100ms. Higher Beacon interval will improve the device's wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

Preamble Type: this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. By default, Long Preamble is selected.

IAPP: Inter-Access Point Protocol is designed for the enforcement of unique association throughout an ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period. It is enabled by default.

Protection: it is disabled by default.

Aggregation: A part of the 802.11n standard. It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header. It is enabled by default.

Frames- determine the number of frames combined on the new larger frame.

Bytes- determine the size (in **Bytes**) of the larger frame.

Short GI: short Guide Interval. It is to assure the safety of propagation delays and reflections for the sensitive digital data.

WLAN Partition: divides the WLAN to several parts.

20/40MHz Coexist: enable this function will make the device select the channel with better performance automatically. It is disabled by default.

RF Output Power: you can select the output power of the wireless device. The default value is 100%. It will deliver the best performance of the device.

5.3.6 Access Control

Disable ▼
Disable
Allow Listed
Deny Listed

MAC Address:

Comment:

Apply Changes

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected Delete All

By default, Wireless Access Control Mode is disabled.
There are two ways to set the Access Control List:

1. If you select **Allow List** and enter the MAC Address of wireless client, the listed address will have granted access to the Access Point while the other access will be denied.
2. If you select **Deny List** and enter the MAC Address of wireless client, the listed address will have denied access to the Access Point while the other access will be granted.

MAC Address: the wireless MAC address that you allow to access or not.

Comment: describe the reason why you allow or deny the access of the MAC Address.

You need to click **Apply Changes** to make your setting work.

Current Access Control List: this list will show all the current access control that you have set. And you're able to delete some or all of them using the **Delete Selected** or **Delete All** button.

5.3.7 WPS Settings

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2.

☐ Disable WPS

Self-PIN Number:	99956042	
Push Button Configuration:	<button>Start PBC</button>	
STOP WSC	<button>Stop WSC</button>	
Client PIN Number:	<input type="text"/>	<button>Start PIN</button>

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Self-PIN Number: it will show the PIN Number of your device.

Push Button Configuration: click Start PBC button to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes.)

STOP WSC: Click the button to stop WSC function.

Client PIN Number: please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

Current Key Info: If the wireless security (encryption) function of the router is properly configured, you can see the encryption information on the list.

5.3.8 Schedule

This router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocol (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions. You have to set your time before setting schedule.

☐ Enable Wireless Schedule

On	Days	From				To			
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)
<input type="checkbox"/>	Sun ▼	00 ▼	(h)	00 ▼	(m)	00 ▼	(h)	00 ▼	(m)

5.4 Route Setup

Route Setup
-

- Static Route
- Routing Table

5.4.1 Static Route

This page is used to setup dynamic or static routing protocol.

☐ Enable Dynamic Route

NAT: ☒ Enabled ☐ Disabled

Transmit ☒ Disabled ☐ RIP 1 ☐ RIP 2

Receive ☒ Disabled ☐ RIP 1 ☐ RIP 2

☐ Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN ▼

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select
------------------------	---------	---------	--------	-----------	--------

Enable Dynamic Route

You may want to set up your router to route computers or devices on your network to other

local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other users to exchange information about the network. Select the checkbox to enable Dynamic Route function.

Note: Configuring this feature assumes that you have some general networking knowledge.

NAT: by default, this option is selected. Detailed information about this parameter refers to the discussion before.

Transmit: allows your router to send out network information to other routers so other routers can dynamically build routes to your network.

Disabled— disable sending routing information from your router to other routers.

RIP1— sends out routing information to other routers using the RIP version 1 protocol.

RIP2— sends out routing information to other routers using the RIP version 2 protocol.

Receive: allows your router to receive network information from other routers so your router can build routes to other networks.

Disabled— disable receiving routing information from other router to your router.

RIP1— receive routing information from other routers using the RIP version 1 protocol.

RIP2— receive routing information from other routers using the RIP version 2 protocol.

Enable Static Route: this part allows you to specify that a specific target IP addresses passes through a determined gateway manually.

IP Address: type in the target network IP.

Subnet Mask: type in the Netmask.

Gateway: type in the Gateway IP.

Metric: enter the metric or priority of the route. The metric range is 1 to 15, the lowest number 1 being the highest priority.

Interface: click the drop-down list and select the interface on your router where the route is active.

Static Route Table: this table will list the detailed information about the target network IP.

5.4.2 Routing Table

This table shows detail information of all the routing entry.

ROUTING TABLE

This table shows the all routing entry .

Destination	Gateway	Genmask	Metric	Interface	Type
192.168.1.0	0.0.0.0	255.255.255.0	0	LAN	Dynamic

Refresh

5.5 Firewall

While the broadband users demand more bandwidth for multimedia, interactive

applications, or distance learning, security has been always the most concerned. The firewall of this router helps to protect you local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.



5.5.1 IP Filtering

☐ Enable IP Filtering

Local IP Address:

Comment:

Current Filter Table:

Hostname	Local IP Address	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>				

Enable IP filtering: you can select this checkbox to enable IP Filtering function.

Local IP Address: the IP address that you want to filter.

Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP.

Comment: describe the reason why you want to filter the IP address. Just few words are saved there usually.

IP Filter Table: this table will list the detailed information about the IP addresses that will be filtered.

5.5.2 Port Filtering

☐ Enable Port Filtering

Port Range: -

Protocol:

Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

Enable Port Filtering: you can select this checkbox to enable Port Filtering function.

Port Range: the port range that you want to filter.

Protocol: choose which particular protocol type should be filtered. Here you can choose UDP/TCP.

Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.

PORT Filter Table: this table will list the detailed information about the ports that will be filtered.

5.5.3 MAC Filtering

☐ Enable MAC Filtering

MAC Address:

Comment:

Apply Changes

Current Filter Table:

Hostname	MAC Address	Comment	Select
----------	-------------	---------	--------

Delete Selected

Delete All

Enable MAC Filtering: you can check the box to enable MAC Filtering function.

MAC Address: the MAC address that you want to filter.

Comment: describe the reason why you want to filter the MAC address. Just few words are saved there usually.

MAC Filter Table: this table will list the detailed information about the MAC addresses that will be filtered.

5.5.4 URL Filtering

☐ Enable URL Filtering

URL Address:

Apply Changes

Current Filter Table:

URL Address	Select
-------------	--------

Delete Selected

Delete All

Enable URL Filtering: you can select this checkbox to enable URL filtering function.

URL Addresses: type in the keywords contained in URLs that you don't allow LAN users to access.

URL Filter Table: this table will list the detailed information about the keywords contained in URLs that you don't allow LAN users to access.

5.5.5 Port Forwarding

☐ Enable Port Forwarding

IP Address:

Protocol:

Both ▼

Port Range:

 -

Comment:

Apply Changes

Current Port Forwarding Table:

Hostname	Local IP Address	Protocol	Port Range	Comment	Select
Delete Selected					
Delete All					

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding: you can select this checkbox to enable Port Forwarding function.

IP Address: enter the Port's IP address.

Protocol: choose which particular protocol type should be forwarding. Here you can choose Both/UDP/TCP.

Port Range: set the range that the port forward to.

Comment: describe the reason why you want to use port forward function. Just few words are saved there usually.

Port Forwarding Table: this table will list the detailed information about the ports that will be forwarded.

5.5.6 DMZ

☐ Enable DMZ

DMZ Host IP Address:

Apply Changes

DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.

Enable DMZ: you can select this checkbox to Enable DMZ function.

DMZ Host IP Address: type in the IP address of the DMZ host.

5.5.7 QoS

QoS means Quality of Service. Deploying QoS management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network. Since numerous TCP-based applications tend to continually increase their transmission

rate and consume all available bandwidth, we need QoS to control the bandwidth use. On this page, you could set the QoS rules.

<input type="checkbox"/>	Enable QoS
<input type="checkbox"/>	Automatic Uplink Speed
Manual Uplink Speed (Kbps): 4096	
<input type="checkbox"/>	Automatic Downlink Speed
Manual Downlink Speed (Kbps): 4096	
QoS Rule Setting:	
Address Type: <input checked="" type="radio"/> IP <input type="radio"/> MAC	
Local IP Address: <input type="text"/> - <input type="text"/>	
MAC Address: <input type="text"/>	
Mode: Guaranteed minimum bandwidth ▼	
Uplink Bandwidth (Kbps): <input type="text"/>	
Downlink Bandwidth (Kbps): <input type="text"/>	
Comment: <input type="text"/>	
<input type="button" value="Apply Changes"/>	

Current QoS Rules Table:

Local IP Address	MAC Address	Port Range	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select
------------------	-------------	------------	------	------------------	--------------------	---------	--------

Automatic Uplink Speed: this option allows you to set the total uplink speed automatically.

Manual Uplink Speed (Kbps): set the uplink speed by entering a number in the blank.

Automatic Downlink Speed: this allows you to set the total downlink. By default, it is 4096Kbps as well.

Manual Downlink Speed (Kbps): set the uplink speed by entering a number in the blank.

QoS Rule Setting

Address type: it allows users control the bandwidth by IP or MAC.

Local IP Address: enter the IP address range if address type is IP.

MAC address: enter the MAC address if address type is MAC.

Mode: Guaranteed minimum bandwidth and restricted maximum bandwidth are selectable.

Uplink Bandwidth: please set the max uplink bandwidth.

Downlink Bandwidth: please set the max downlink bandwidth.

Current QoS Rules Table: this table will list the detailed parameter about QoS.

Click **Apply Changes** to finish the setting.

5.5.8 Alias IP & NAT Mapping

Alias IP means virtual IP. You can choose to enable this function according to your requirement. NAT Mapping function is very useful for a domestic network with one wireless router and a few devices with private IP addresses.

☐ Enable Alias IP

IP Address:

Subnet Mask:

Apply Changes

Alias IP Table

IP Address	Subnet Mask	Interface	Select

Delete Selected

Delete All

☐ Enable Nat Address Mapping

Public IP Address:

Private IP Address:

Comment:

Apply Changes

Current NAT Address Mapping Table

Public IP Address	Private IP Address	Comment	Select

Delete Selected

Delete All

Public IP Address: enter the public IP address provided by corresponding service provider.

Private IP Address: enter the private IP address of your PC.

5.5.9 Session Limit

After enabled session limit, you can set the maximum number of sessions.

SESSION LIMIT

☐ Enable Session Limit

Local IP Address:

Session Limit Number:

127 (2~127)

Comment:

Apply Changes

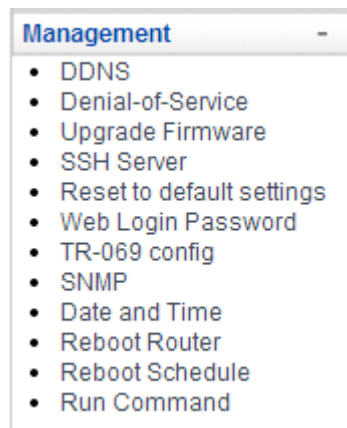
Current Session Limit:

Local IP Address	Session Limit Number	Comment	Select

Delete Selected

Delete All

5.6 Management



5.6.1 DDNS

DDNS means Dynamic Domain Name System. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. This router supports three service providers: DynDNS, TZO and NOIP.

<input checked="" type="checkbox"/> Enable DDNS	
Service Provider	DynDNS ▼
Auto-Update interval	2 Min(s)(1~14400)
Domain Name	host.dyndns.org
User Name/Email	
Password/Key	
<input type="button" value="Save Changes"/>	

Enable DDNS: please select this checkbox to enable DDNS function.

Service Provider: choose one service provider where you have applied for free DDNS service.

Domain Name: type in the domain name you registered from the DDNS provider.

User Name/Email: enter the User Name or Email you registered from the DDNS provider.

Password/Key: enter the Password or Key you set for the User Name.

Click **Save Changes** to finish the setting.

5.6.2 Denial-of-Service

The DoS Prevention functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the

vulnerabilities of the protocol or operation system.

<input type="checkbox"/> Enable DoS Prevention	Select ALL	Clear ALL
<input type="checkbox"/> Whole System Flood: SYN	1000	Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	1000	Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	1000	Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	250	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	500	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	500	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	500	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	100	Packets/Second
<input type="checkbox"/> TCP/UDP PortScan	Low ▼	Sensitivity
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		
<input type="checkbox"/> TCP Scan		
<input type="checkbox"/> TCP SynWithData		
<input type="checkbox"/> UDP Bomb		
<input type="checkbox"/> UDP EchoChargen		
<input type="checkbox"/> Enable Source IP Blocking	10	Block time (sec)

Apply Changes

Enable DoS Prevention: check this box to enable DoS prevention function.

This page shows the attack types that DoS prevention function can detect:

Whole System Flood: SYN	ICMP Smurf
Whole System Flood: FIN	IP Land
Whole System Flood: UDP	IP Spoof
Whole System Flood: ICMP	IP TearDrop
Per-Source IP Flood: SYN	PingofDeath
Per-Source IP Flood: FIN	TCP Scan
Per-Source IP Flood: UDP	TCP SynWithData
Per-Source IP Flood: ICMP	UDP Bomb
TCP/UDP PortScan	UDP EchoChargen

Sensitivity: you can select Low or High sensitivity.

You can click **Select ALL** or **Clear ALL** to select prevention type.

5.6.3 Upgrade Firmware

New version of firmware will be released to improve the various efficiency or to fix some bugs. Following the steps show below so as to realize upgrading. This page allows you to upgrade the Access Point firmware to new version.

Please note: DO NOT power off the device during the upload because it may crash the

system.

UPGRADE FIRMWARE

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version:	AN-PHAT-N151RT-V1.0.0-B20140310.1627	
Select File:	<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Upload"/>		

Firmware version: shows the current firmware version.

Choose File: select the firmware version you want to upgrade on your computer.

Click **Upload** to upgrade the firmware version.

5.6.4 SSH Server

☐ Enable SSH

SSH User	<input type="text" value="root"/>
SSH Password	<input type="password" value="....."/>

Enable SSH Server: SSH means Secure Share. It is the most secure protocol specially used for remote login and other web service.

Server User: type in a name for the SSH server.

SSH Password: type in the password for security.

5.6.5 Reset to Default Settings

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. Besides, you can reset the current configuration to factory default.

SAVE/RELOAD SETTINGS

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:	<input type="button" value="Save..."/>	
Load Settings from File:	<input type="button" value="Choose File"/>	No file chosen <input type="button" value="Upload"/>
Reset Settings to Default:	<input type="button" value="Reset"/>	

Save Settings to File: click **Save...** button to download the current settings of the Access Point to your computer.

Load Settings from File: if you want to reload the settings from the file saved before, you could click **Choose File** button to choose the right file then click **Upload** button.

Reset Settings to Default: this **Reset** button is provided to allow you to restore the router settings to the default factory settings.

5.6.6 Web Login Password

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup.

User Name:	<input type="text" value="admin"/>
New Password:	<input type="password" value="....."/>
Confirmed Password:	<input type="password"/>
<input type="button" value="Apply Changes"/>	

User Name: specifies the name of the system user.

New Password: new password used for administrator authentication should be specified.

Confirm Password: new password should be re-entered to verify its accuracy.

5.6.7 TR-069 Config

TR-069 stands for CPE WAN Management Protocol. It is a protocol for communication between Customer Premise Equipment (CPE) and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework. On this page you can configure the TR-069 CPE and change the setting of ACS.

TR069:	<input checked="" type="radio"/> Off <input type="radio"/> On
ACS:	
URL	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>
Enable periodic information:	<input checked="" type="radio"/> Off <input type="radio"/> On
Interval periodic updates:	<input type="text" value="0"/>
Connection Request:	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Path:	<input type="text"/>
Port:	<input type="text" value="0"/>
<input type="button" value="Apply Changes"/>	

Certificat Management:

CA Certificat:

No file chosen

TR069: enable or disable TR069 function by choosing On or Off. After enabled this function, it is very convenient for the ISP to manage all of customer devices.

ACS:

URL: enter the URL of ACS which is provided by your ISP

User Name & Password: provided by your ISP.

Enable periodic information: choose On to enable the periodic information update.

Interval periodic updates: please enter the time as the interval for periodic updates in the field (the interval should be decimal number (0~9) while other characters are invalid).

Connection Request

User Name: enter the CPE Connection Request User Name.

Password: enter CPE Connection Request Password.

Port: enter the CPE connection port number for connecting to ACS.

5.6.8 SNMP

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

<input type="checkbox"/> Enable SNMP	
Name :	TOTOLINK N151RT
Location :	AP
Contact :	Router
Read/Write Community :	private
Read-Only Community :	public
<input type="button" value="Save Changes"/>	

System Name/ Location/ Contact: set the administrator name, physical location and contact method.

5.6.9 Date and Time

Current Time :	Yr 2014	Mon 3	Day 10	Hr 16	Mn 56	Sec 23
<input type="button" value="Copy Computer Time"/>						
Time Zone Select :	(GMT+07:00)Bangkok, Hanoi, Jakarta ▼					
<input checked="" type="checkbox"/> Enable NTP client update						
<input type="checkbox"/> Automatically Adjust Daylight Saving						
SNTP server :	<input checked="" type="radio"/> 203.117.180.36 - Asia Pacific ▼					
	<input type="radio"/> (Manual IP Setting)					
<input type="button" value="Save Changes"/>						

You can specify the device's time zone according to GMT (Greenwich Mean Time) or copy computer time as the current time only by clicking the **Copy Computer Time** button.

Enable NTP client update: NTP means Network Time Protocol which is used to make the

computer's time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption. You need to check this box to activate this page.

Time Zone Select: Select the Time Zone where the router is located.

SNTP server: Please choose the corresponding SNTP server to get right time.

5.6.10 Reboot Router

You can just click **Reboot** to reboot the router.

Reboot Router

Reboot Router

5.6.11 Reboot Schedule

After enabled the Reboot schedule, the router will automatically reboot at the time that you set here. You have to set your time before setting schedule.

☐ Enable Reboot Schedule

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

3 (0-23 hour):

0 (0-59 min)

Save Changes

5.6.12 Run Comment

You can run system command in this page, just enter the command in the System Command bar and click Run button.

SYSTEM COMMAND

This page can be used to run target system command.

System Command:

Apply