

TEW-751DR

2x2 802.11a+b+g+n
Dual Band Concurrent
Wireless Router

User's Guide

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1:

Safety of Information Technology Equipment

EN 50385: (2002-08)

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1 (2009-05)




Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for Broadband Data Transmission Systems

















This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.



 Český [Czech]	TRENDnet tímto prohlašuje, že tento TEW-751DR je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-751DR overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre TRENDnet, dass sich das Gerät TEW-751DR in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen

	einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-751DR vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this TEW-751DR is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-751DR cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΤΡΕΝΔnet ΔΗΛΩΝΕΙ ΟΤΙ ΤΕW-751DR ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-751DR est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-751DR è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
 Latvīski [Latvian]	Ar šo TRENDnet deklarē, ka TEW-751DR atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-751DR atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-751DR in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-751DR jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-751DR megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-751DR jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	TRENDnet declara que este TEW-751DR está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-751DR v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
 Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TEW-751DR spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi	TRENDnet vakuuttaa täten että TEW-751DR tyyppinen laite on direktiivin

[Finnish]	1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-751DR står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

TABLE OF CONTENTS

ABOUT THIS GUIDE	1
Purpose	1
Terms/Usage	1
Overview of this User's Guide	1
INTRODUCTION	2
Applications:	3
Supported Features:	3
Wireless Performance Considerations	4
UNPACKING AND SETUP.....	5
Unpacking	5
Setup	5
HARDWARE INSTALLATION.....	6
Front Panel.....	6
Rear Panel	7
Side Panel.....	8
Hanging Way	8
Hardware connections.....	9
Connecting the WLAN Router	9
Check the installation	10
PC NETWORK TCP/IP SETTINGS.....	11
Windows 95/98/ME.....	11
Windows 2000	12
Windows XP	13
Windows Vista / 7.....	16
CONFIGURATION.....	18
Login to the WLAN Router through Wireless LAN.....	18
Login to the WLAN Router	18
Using the Web Browser	19
Setup Wizard.....	19
Advanced configuration.....	28
Main	28
Local Network	28
Internet Setup.....	30
Time and Date.....	34
Wireless	35
Basic Setting	35
Security	37
Advanced Wireless	40
Wi-Fi Protected Setup.....	40
Status	41
Device Information	41
Log	42
Log Setting.....	44

Statistic	45
Wireless Client.....	46
Routing.....	46
Static	46
Dynamic.....	47
Routing Table	48
Access.....	49
Virtual Server.....	52
Special AP	53
DMZ	54
Dynamic DNS.....	55
Firewall Settings	56
Management.....	57
Password.....	57
Remote Management	58
Tools.....	59
Restart.....	59
Settings	59
Firmware.....	60
Ping Test	60
<i>TECHNICAL SPECIFICATIONS</i>	61
158 x 109 x 34mm (6.2 x 4.3 x 1.3in)	61
250g (7.4oz).....	61
<i>LIMITED WARRANTY</i>	62

ABOUT THIS GUIDE

Congratulations on your purchase of this TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router. This integrated access device combines Internet gateway functions with wireless LAN and Gigabit Ethernet switch. It provides a complete solution for Internet surfing and office resource sharing, and it is easy to configure and operate for every user.

Purpose

This manual discusses how to install the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

Terms/Usage

In this guide, the term “the WLAN Router” refers to your TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

Overview of this User’s Guide

Introduction. Describes the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router and its features.

Unpacking and Setup. Helps you get started with the basic installation of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

Identifying External Components. Describes the front panel, rear panel and LED indicators of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

Connecting the WLAN Router. Tells how you can connect the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router to your xDSL/Cable Modem.

Technical Specifications. Lists the technical (general, physical and environmental, performance and Routers settings) specifications of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

INTRODUCTION

The 2x2 802.11a+b+g+n Dual Band Concurrent Wireless Router delivers unsurpassed Dual Band wireless speed, coverage, and reliability with up to 14x the speed and 6x the coverage of a wireless g connection*.

Concurrent Dual Band technology creates two separate 300Mbps wireless n networks at the same time—one on the 2.4GHz frequency and the other on the less congested 5GHz frequency.

Gigabit Ethernet ports offer exceptional wired throughput performance. Multiple Input Multiple Output (MIMO) antenna technology reduces wireless dead spots, advanced wireless encryption protects your digital content, and WMM® Quality of Service (QoS) technology prioritizes gaming, Internet calls, and video streams. Wi-Fi Protected Setup (WPS) connects WPS compliant computers at the touch of a button. Wirelessly stream HD multimedia using the uncongested 5GHz frequency while surfing the Internet using the 2.4GHz frequency.

With the explosive growth of the Internet, accessing information and services at any time, day or night has become a standard requirement for most people. The era of the standalone PC is waning. Networking technology is moving out of the exclusive domain of corporations and into homes with at least two computers.

This integrated access device combines Internet gateway functions with wireless LAN and Fast Ethernet switch. Designed for the business and home, it saves you the cost of installing a separate modem and ISP line for each computer, while providing ready connection for the users, with or without the network wires.

Broadband network access is also gaining ground. However, allowing more than two computers to access the Internet at the same time means less affordable, higher costs. Thus, there is a need to share one public IP address over a single Internet connection to link the home with the Internet.

The scarcity of IP addresses and using a shared Internet connection through an Internet sharing device can solve high network access costs. All linked computers can make full use of broadband capabilities over such a device.

This device not only comes equipped with a wide range of features, but also can be installed and configured right out of the box. This device supports a simple local area network and Internet access share, offering great cost savings.

The local area network connects home computers while also allowing any of the computers to access the Internet, share resources, or play online games—the basis of the family computing lifestyle.

Applications:

Broadband Internet access: Several computers can share one high-speed broadband connection through wireless or wired (WLAN, LAN and WAN-Internet).

Resource sharing: Share resources such as printers, scanners and other peripherals.

File sharing: Exchange data, messages, and distribute files thus making good use of hard disk space.

Online gaming:

Through the local area network, online gaming and e-commerce services can be easily setup.

Firewall: A built-in firewall function — for security and anti-hacking systems.

Supported Features:

- Wi-Fi compliant with IEEE 802.11a/n (5GHz band) and IEEE 802.11b/g/n (2.4GHz band) standards
- 4 x 10/100/1000Mbps Auto-MDIX LAN port and 1 x 10/100/1000Mbps WAN port (Internet)
- Supports Cable/DSL modems with Dynamic IP, Static IP, PPPoE, PPTP and L2TP connection types
- High-speed data rates up to 600Mbps using two IEEE 802.11n connections (2.4GHz band + 5GHz band)
- 2 fixed external antennas support high speed performance and great coverage with MIMO technology
- Network Address Translation (NAT) firewall
- Wi-Fi Protected Setup (WPS) button for simple network connectivity
- Universal Plug and Play (UPnP) and Application Level Gateway support for Internet applications such as email, FTP, gaming, remote desktop, Net Meeting, telnet and more
- Provides additional security with Internet Access Control (MAC Address, Domain, and IP Filtering)
- Easy remote management via Web browser
- Wireless security support for WEP, WPA & WPA2
- Indoor coverage up to 100 meters (330ft.)*
- Outdoor coverage up to 300 meters (980ft.)*
- Works with Windows, Linux and Mac operating systems

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
3. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.
6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.

Unpacking

Open the box of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router and carefully unpack it. The box should contain the following items:

- ◆ TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router
- ◆ CD-Rom (User's Guide)
- ◆ Multi-Language Quick Installation Guide
- ◆ Power adapter
- ◆ Network cable 1.5m (4.9ft)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the WLAN Router can be performed properly using the following methods:

- ◆ The power outlet should be within 1.82 meters (6 feet) of the Broadband Router.
- ◆ Visually inspect the DC power jack and make sure that it is fully secured to the power adapter.
- ◆ Make sure that there is proper heat dissipation and adequate ventilation around the Broadband Router. Do not place heavy objects on the Broadband Router.
- ◆ Fix the direction of the antennas. Try to place the Wireless Router in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

HARDWARE INSTALLATION

Front Panel

The figure below shows the front panel of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.



Front Panel

POWER

This indicator lights green when the hub is receives power, otherwise it is off.

Status

This indicator blinking green means the WLAN Router is working successfully. Otherwise, this indicator always on or off means the function of the WLAN Router has failed.

WAN (Link/ACT)

The indicators light green when the WAN port is connected to a xDSL/Cable modem successfully.

The indicators blink green while the WAN port was transmitting or receiving data from the xDSL/Cable modem.

WLAN (ACT)

This indicator lights green when there are wireless devices connected and transmitting data to the WLAN Router.

LAN (Link/ACT)

These indicators light green when the LAN ports were connected successfully. These indicators blinking green while the LAN ports were accessing data.

Rear Panel

The figure below shows the rear panel of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.



Rear Panel

Antenna

There are two 2dBi gain antennas on the rear panel for wireless connection.

LAN (1-4)

Four RJ-45 10/100Mbps Auto-MDIX ports for connecting to either 10Mbps or 100Mbps Ethernet connections.

WAN

In the four port broadband Router, there is an RJ-45 10/100Mbps Auto-MDIX port for the WAN that connects to the xDSL/Cable modem for Internet connectivity.

POWER

Plug the power adapter to this power jack

RESET

Use a pin-shaped item to push to reset this device to factory default settings (Hold for 15 seconds and release). It will be a useful tool when the manager forgot the password to login, and needs to restore the device back to default settings.

POWER SWITCH

Use the power on/off switch to turn the device on or off.

Side Panel

The figure below shows the side panel of the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router.



Side Panel

WPS

Push and hold this button for 3 seconds and release it to initiate the Wi-Fi Protected Setup process.

Hanging Way

User can mount the device on a wall. Mount the Nylon screw anchors into a cement wall and then drive a screw into the Nylon screw anchors. It does not need to mount the Nylon screw anchors into a wood wall. Hook the mounting holes of the switch back on the screws and completed the wall-mount.

Hardware connections

Connecting the WLAN Router



1. Plug in one end of the network cable to the WAN port of the WLAN Router.
2. Plug in the other end of the network cable to the Ethernet port of the xDSL or Cable modem.
3. Use another network cable to connect to the Ethernet card on the computer system; the other end of the cable connects to the LAN port of the WLAN Router. Since the TEW-751DR 600Mbps Wireless N Dual Band Concurrent Router has four gigabit Ethernet ports, you can connect up to four computers directly to the unit. Then you do not have to buy a switch to connect these computers since one WLAN Router functions both as a connection-sharing unit and as a switch.

Check the installation

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

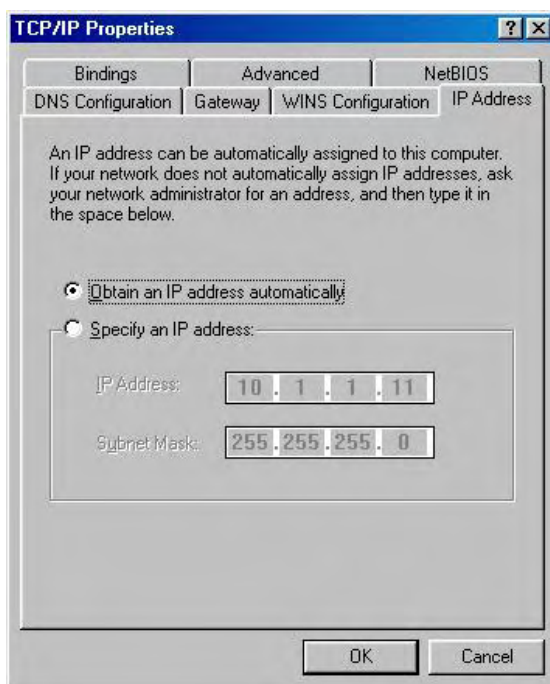
1. With the power source on, once the device is connected to the broadband modem, the Power, LAN, WLAN and WAN port LEDs of the WLAN Router will light up indicating a normal status.
2. When the WAN Port is connected to the ADSL/Cable modem, the WAN LED will light up.
3. When the LAN Port is connected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

PC NETWORK TCP/IP SETTINGS

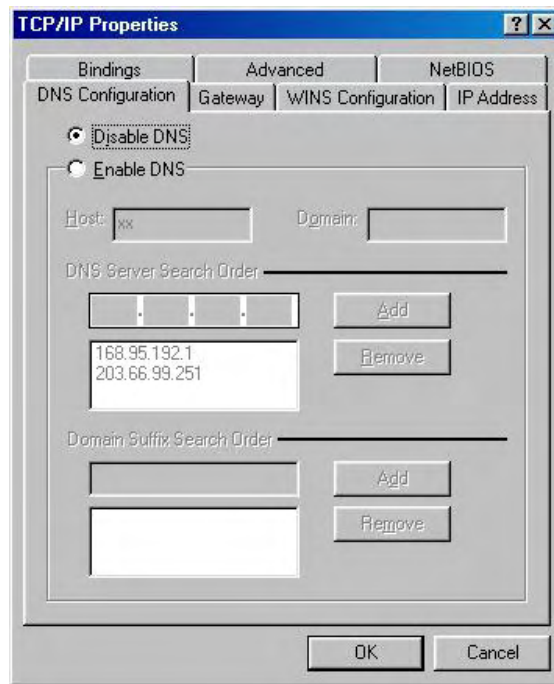
The network TCP/IP settings differ based on the computer's operating system (Win95/98/ME/NT/2000/XP/Vista) and are as follows.

Windows 95/98/ME

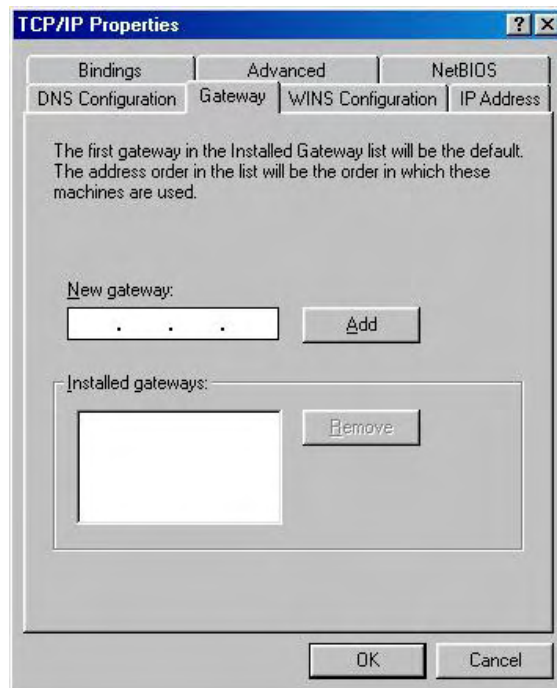
1. Click on the **“Network neighborhood”** icon found on the desktop.
2. Click the right mouse button and a context menu will be show.
3. Select **“Properties”** to enter the TCP/IP setting screen.
4. Select **“Obtain an IP address automatically”** on the **“IP address”** field.



5. Select **“Disable DNS”** in the **“DNS”** field.



6. Select **“None”** for the **“Gateway address”** field.

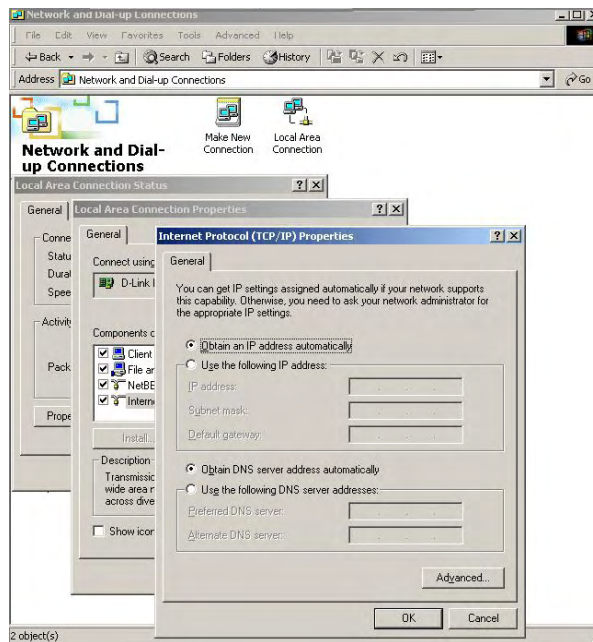


Windows 2000

Double click on the **“My Computer”** icon on the desktop. When **“My Computer”** window opens, select **“Control Panel”** and then open the **“Network dialup connection”** applet. Double click on the **“Local area network connection”** icon. Select **“Properties”** to enter the TCP/IP setting window.

1. In the **“Local area network status”** window, click on **“Properties.”**
2. In the **“Local area network connection”** window, first select TCP/IP setting and then select **“Properties.”**

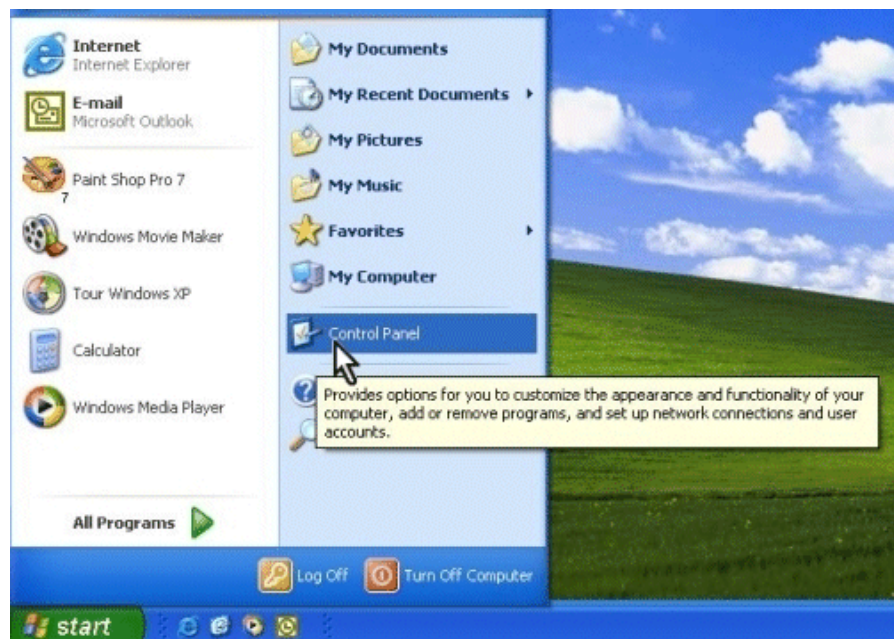
3. Set both “IP address” and “DNS” to Automatic configuration.



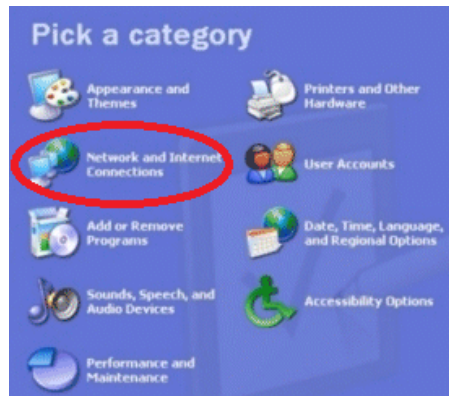
Windows XP

Point the cursor and click the right button on the “My Network Place” icon. Select “properties” to enter the TCP/IP setting window.

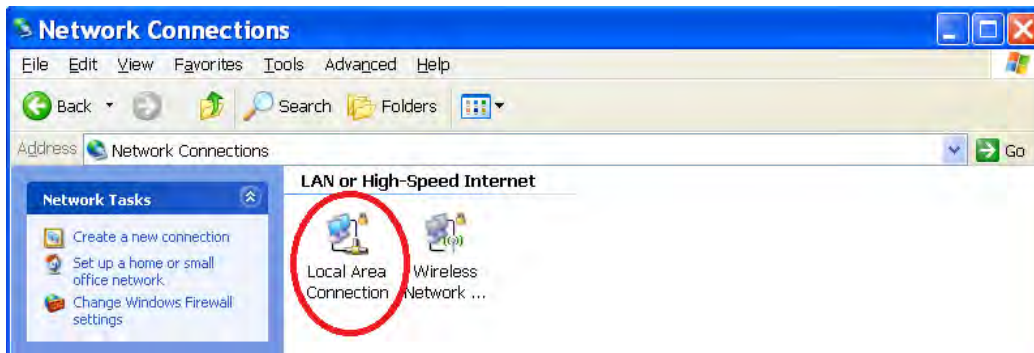
1. Click “**Start**” button, and click on “**Control Panel**”.



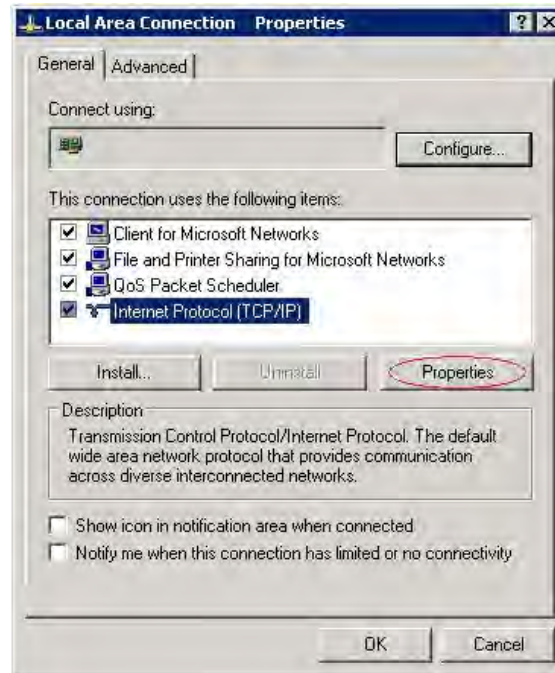
2. Click on “**Network and Internet Connections**” and click on “**Network Connections**”. Note: In Classic, double-click on “**Network Connections**”.



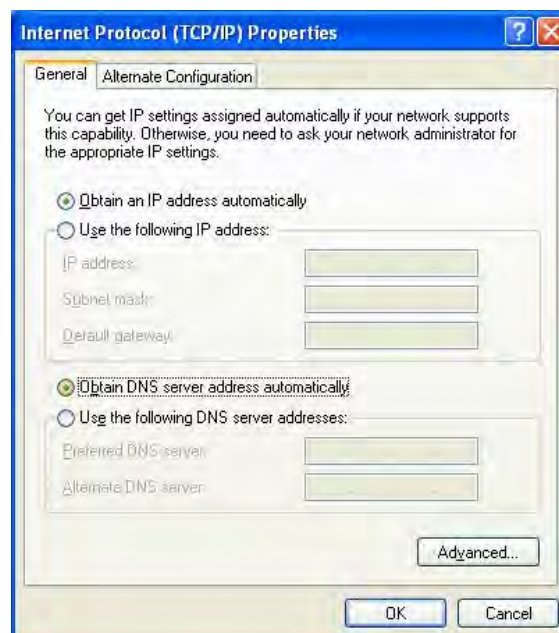
3. Right click **“Local Area Connection”** and select **“Properties”**.



4. Click on **“Internet Protocol (TCP/IP)”** and click on **“Properties”**.

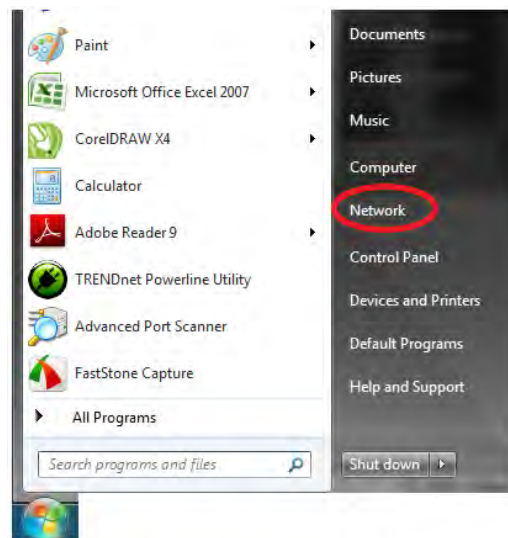


5. Set **“IP address”** to **“Obtain an IP address automatically.”**
6. Set **“DNS”** to **“Obtain DNS server address automatically.”**

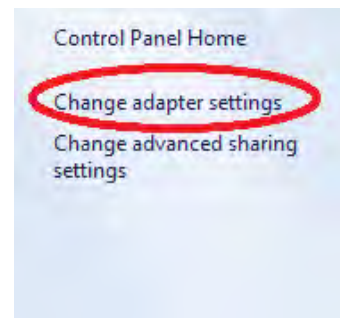
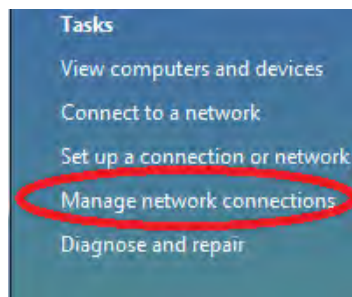


Windows Vista / 7

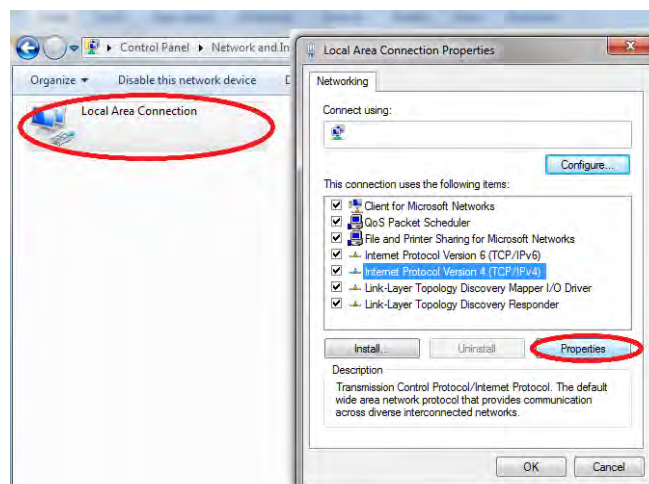
1. Click on the **“Start/Windows”** button. Right click on **“Network”** and select **“Properties”**.



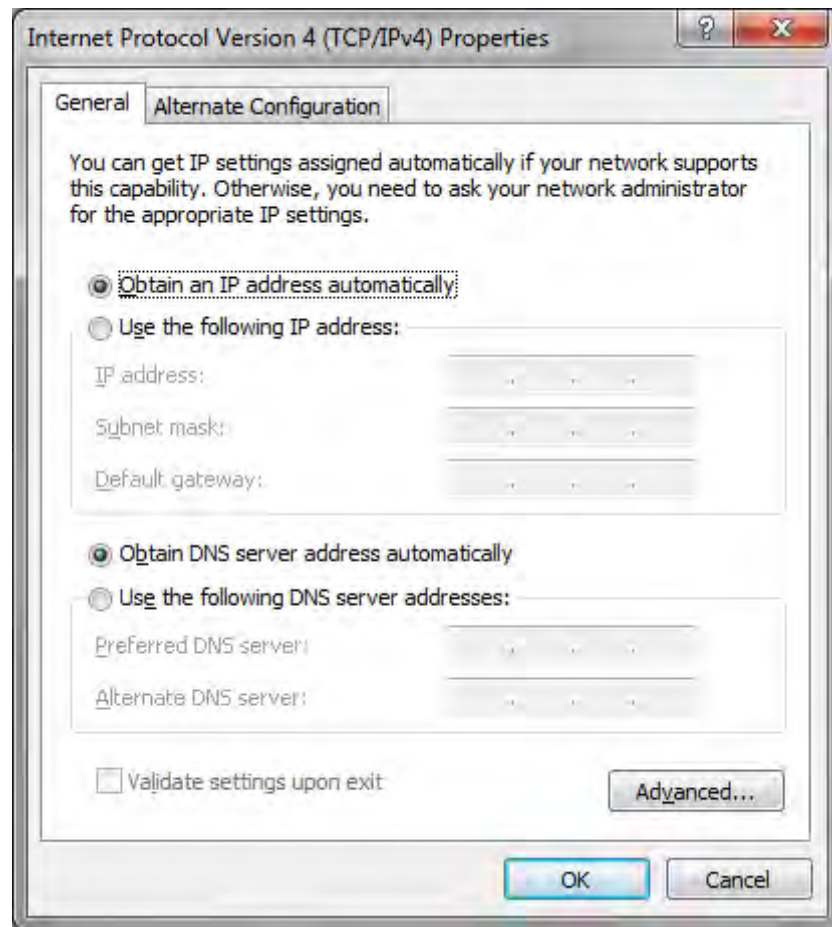
2. **Window Vista:** Click on **“Manage Network Connections.”**
Windows 7: Click on **“Change adapter settings”**.



3. Right click **“Local Area Connection”** and select **“Properties”**. Click on **“Internet Protocol Version 4 (TCP/IPv4)”** and click **“Properties”**.



4. Set "IP address" to "Obtain an IP address automatically."
5. Set "DNS" to "Obtain DNS server address automatically."



CONFIGURATION

First make sure that the network connections are functioning normally.

This WLAN Router can be configured using Internet Explorer 6.0 or newer web browser versions.

Login to the WLAN Router through Wireless LAN

Before configuring the WLAN Router through WLAN, make sure that the SSID, Channel and the WEP is set properly.

The default setting of the WLAN Router that you will use:

- ✓ SSID: TRENDnet751_2.4GHz, TRENDnet751_5GHz
 - ✓ Channel: Auto Channel
 - ✓ 802.11 Mode: 802.11a/n mixed mode (5GHz band), 802.11b/g/n mixed mode (2.4GHz band)
 - ✓ Channel bandwidth: 20Mhz
 - ✓ Security: Disabled
-

Login to the WLAN Router

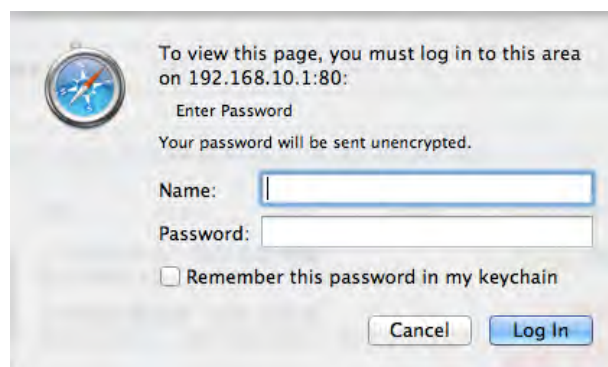
Before you configure this device, note that when the WLAN Router, make sure the host PC must be set on the **IP subnet** that can be accessed by the xDSL/Cable modem. For example, when the default network address of the xDSL/Cable modem Ethernet interface is 192.168.10.x, then the host PC should be set at 192.168.10.xxx (where xxx is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Using the Web Browser

1. Open Internet Explorer 6.0 or above Internet browser.
2. Enter IP address <http://192.168.10.1> (the factory-default IP address setting) to the URL web address location.



3. When the following dialog box appears, enter the user name and password to login to the main configuration window, the default username and password is ***“admin”***.



Setup Wizard

Setup wizard is provided as part of the web configuration utility. User can simply follow the step-by-step process to get the wireless Router configuration ready to run in 4 easy steps by clicking on the “Wizard” button on the function menu. The following screen will appear. Please click “Next” to continue.

Step 1: Wireless Basic Setting

Click “Enable” to enable Wireless LAN.

Enter a unique SSID (Wireless Network Name). Choose something that you would easily identify when searching for available wireless networks (using laptops, smart phones, etc.); Select a specified wireless channel or auto select a best wireless channel. Click Next.

Setup Wizard [Help]

Wireless Basic Setting (2.4G)

Device Name	wlan1
Device	<input checked="" type="checkbox"/> Enable
SSID	TRENDnet751_2.4GHz
BSSID	00:E0:4C:81:86:82
Wireless Channel	Auto
Wireless Mode	802.11n + 802.11g + 802.11b

Wireless Basic Setting (5G)

Device Name	wlan0
Device	<input checked="" type="checkbox"/> Enable
SSID	TRENDnet751_5GHz
BSSID	00:E0:4C:81:86:87
Wireless Channel	Auto
Wireless Mode	802.11a + 802.11n

[Back] [Next] [Cancel]

Step 2: Set The Wireless Security:

Click on the Security Mode drop-down list to select your wireless security type.

Setup Wizard [Help]

Security Configuration (2.4G)

Security Mode	None
Security Configuration	
Security Mode	WEP

[Back] [Next] [Cancel]

Selecting WEP:

If selecting WEP (Wired Equivalent Privacy), please review the WEP settings to configure and click Next to save the changes.

Setup Wizard [Help]

Security Configuration (2.4G)

Security Mode	WEP
Authentication Type	<input type="radio"/> Auto <input checked="" type="radio"/> Open System <input type="radio"/> Shared Key

Security Encryption (WEP) Key

Encryption Strength	64bit
Key Format	ASCII
Passphrase	<input type="text"/> [Generate]
Key1	<input checked="" type="radio"/>
Key2	<input type="radio"/>
Key3	<input type="radio"/>
Key4	<input type="radio"/>

Security Configuration (5G)

Security Mode	None
---------------	------

[Back] [Next] [Cancel]

- **Authentication** - Choose Open System, Shared Key or Auto.

Note: It is recommended to use Open System because it is known to be more secure than Shared Key.

- **Encryption Strength** - Choose the key length 64-bit or 128-bit.

Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.

- **Key Format** - Choose HEX or ASCII.

Note: It is recommended to use ASCII because of the much larger character set that can be used to create the key.

- **Key 1-4**

- This is where you enter the password or key needed for a computer to connect to the router wirelessly
- You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
- Choose a key index 1, 2, 3, or 4 and enter the key.
- When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

Selecting WPA, WPA-Auto or WPA2 (WPA2 recommended):

The screenshot shows a 'Setup Wizard' window with a 'Help' button in the top right. The main section is 'Security Configuration (2.4G)'. It contains several rows: 'Security Mode' with a dropdown menu set to 'WPA'; 'Authentication Type' with radio buttons for 'PSK' (selected) and 'EAP'; 'Encryption Type' with radio buttons for 'TKIP', 'AES', and 'TKIP and AES' (selected); and 'Group Rekey Time' with a text box containing '86400' and '(seconds)'. Below this is a 'Passphrase' section with a 'Confirmed Passphrase' text box containing 'wlan1WPA'. Underneath is another section 'Security Configuration (5G)' with a 'Security Mode' dropdown menu set to 'None'. At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.

First, from the Security Mode row, select WPA, WPA-Auto, or WPA2.

Then from the Authentication Type row, select either PSK or EAP

- **PSK** stands for Passphrase Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).

*Note: **EAP** requires an external RADIUS server, **PSK** only requires you to create a passphrase.*

The following section outlines options when selecting PSK (Preshared Key Protocol):

Select a Cipher Type:

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** or **WPA2** security, it is recommended to use **AES**.

Create your Wireless security Passphrase (password or key):

- **Passphrase** – Enter the passphrase.

This is the password or key that is used to connect your computer to this router wirelessly

Confirmed Passphrase – Re-enter the passphrase.

Note: 8-63 alphanumeric characters (a,b,C,?,,/,1,2, etc.)*

The following section outlines options when selecting EAP (Extensive Authentication Protocol).

Select a Cipher Type:

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** or **WPA2** security, it is recommended to use **AES**.

The screenshot shows a 'Setup Wizard' window with a 'Help' button in the top right. The main section is 'Security Configuration (2.4G)'. It contains a 'Security Mode' dropdown menu set to 'WPA2'. Below that are three rows of radio button options: 'Authentication Type' with 'PSK' and 'EAP' (selected), 'Encryption Type' with 'TKIP', 'AES' (selected), and 'TKIP and AES', and 'Group Rekey Time' with a text box containing '86400' and '(seconds)' next to it. The next section is 'RADIUS Information' with three text input fields: 'RADIUS Server IP' (0.0.0.0), 'RADIUS Server Port' (1812), and 'RADIUS Server Key'. Below that is 'Security Configuration (5G)' with a 'Security Mode' dropdown set to 'None'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

RADIUS Server - Configure the RADIUS server settings:

- **RADIUS Server IP** - Enter the IP address of the RADIUS server.
- **RADIUS Server Port** - Enter the port your RADIUS server is configured to use for RADIUS authentication.

Note: It is recommended to use port 1812.

- **RADIUS Server Key** - Enter the shared secret used to authorize your router with your RADIUS server.

Step 3: Internet Setup:

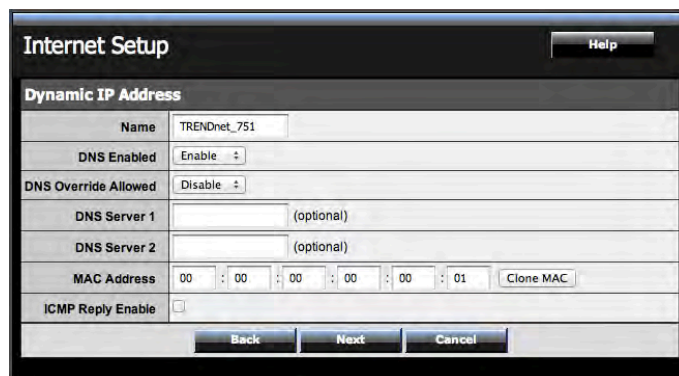
The WLAN Router will attempt to auto detect your Internet Connection.

Dynamic IP Address:



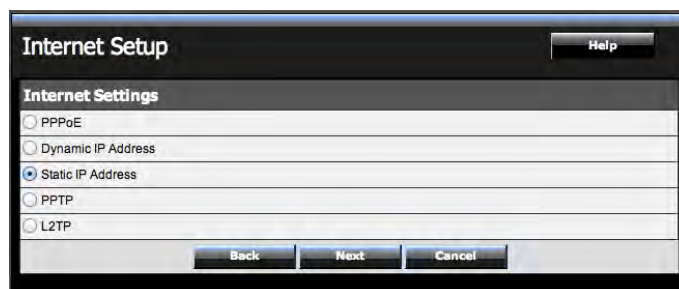
The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section. The 'Dynamic IP Address' option is selected with a radio button. Other options include PPPoE, Static IP Address, PPTP, and L2TP. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

Choose "Dynamic IP Address" to have the WLAN Router assign IP addresses automatically.



The screenshot shows the 'Internet Setup' window with the 'Dynamic IP Address' configuration section. Fields include: Name (TRENDnet_751), DNS Enabled (Enable), DNS Override Allowed (Disable), DNS Server 1 and 2 (optional), MAC Address (00 : 00 : 00 : 00 : 00 : 01 with Clone MAC button), and ICMP Reply Enable (checkbox). Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

Static IP Address:



The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section. The 'Static IP Address' option is selected with a radio button. Other options include PPPoE, Dynamic IP Address, PPTP, and L2TP. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

If the Internet Service Provider (ISP) assigns a static IP address, choose this option and enter the assigned WAN IP Address, WAN Subnet Mask, WAN Gateway Address and DNS Server Addresses for the WLAN Router.

Internet Setup Help

Static IP Address

Name	TRENDnet_751
External IP Address	0.0.0.0
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
MAC Address	00 : 00 : 00 : 00 : 00 : 01 Clone MAC
ICMP Reply Enable	<input type="checkbox"/>

Back Next Cancel

PPPoE:

Internet Setup Help

Internet Settings

PPPoE
 Dynamic IP Address
 Static IP Address
 PPTP
 L2TP

Back Next Cancel

PPPoE to obtain IP automatically:

Internet Setup Help

PPPoE

IP Mode of Connection	Dynamic
Name	
User Name	
User Password	
Confirm Password	
Max MRU	1492 (576~1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
PPPoE Service Name	(optional)
MAC Address	00 : E0 : 4C : 81 : 86 : 82 Clone MAC
PPPoE AC Name	(optional)
Connection Trigger	OnDemand
Idle Disconnect Time	300 (30~3600 seconds)
LCP Interval	20 (0~86400 seconds)
ICMP Reply Enable	<input type="checkbox"/>

Back Next Cancel

If connected to the Internet using a PPPoE (Dial-up xDSL) connection, and the ISP provides a User Name and Password, then choose this option and enter the required information.

PPPoE with a Specify IP address:

The screenshot shows the 'Internet Setup' window with the 'PPPoE' section selected. The 'IP Mode of Connection' is set to 'Static'. The 'IP Address' field contains '0.0.0.0' and the 'Subnet Mask' field contains '255.255.255.0'. Other fields include 'Name', 'User Name', 'User Password', 'Confirm Password', 'Max MRU' (1492), 'DNS Enabled' (Enable), 'DNS Override Allowed' (Disable), 'DNS Server 1' and 'DNS Server 2' (optional), 'PPPoE Service Name' (optional), 'MAC Address' (00 : E0 : 4C : 81 : 86 : 82), 'PPPoE AC Name' (optional), 'Connection Trigger' (OnDemand), 'Idle Disconnect Time' (300), 'LCP Interval' (20), and 'ICMP Reply Enable' (unchecked). Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

If connected to the Internet using a PPPoE (Dial-up xDSL) connection, and the ISP provides a IP address, Subnet mask, User Name, Password and a Static IP Address, choose this option and enter the required information.

PPTP:

The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section. The 'PPTP' option is selected with a radio button. Other options include 'PPPoE', 'Dynamic IP Address', 'Static IP Address', and 'L2TP'. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

If connected to the Internet using a PPTP xDSL connection, enter your IP, Subnet Mask, Gateway, Server IP, PPTP Account and PPTP Password.

The screenshot shows the 'Internet Setup' window with the 'PPTP' section selected. The configuration fields are as follows:

VPN IP Mode of Connection	Dynamic
VPN Server IP	0.0.0.0
MPPE	Disable
Name	
User Name	
User Password	
Confirm Password	
Max MRU	1492 (576-1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
MAC Address	00 : E0 : 4C : 81 : 86 : 82 Clone MAC
Connection Trigger	OnDemand
Idle Disconnect Time	300 (30-3600 seconds)
LCP Interval	20 (0-86400 seconds)
ICMP Reply Enable	<input type="checkbox"/>

Buttons: Back, Next, Cancel, Help

L2TP:

The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section selected. The options are:

- PPPoE
- Dynamic IP Address
- Static IP Address
- PPTP
- L2TP

Buttons: Back, Next, Cancel, Help

If connected to the Internet using a L2TP (Dial-up xDSL) connection and the ISP provides a Server IP, Account and Password information, choose this option and enter the required information.



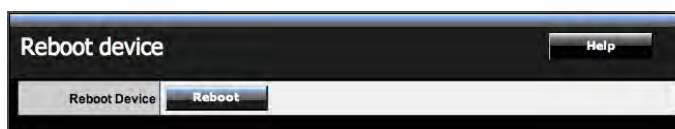
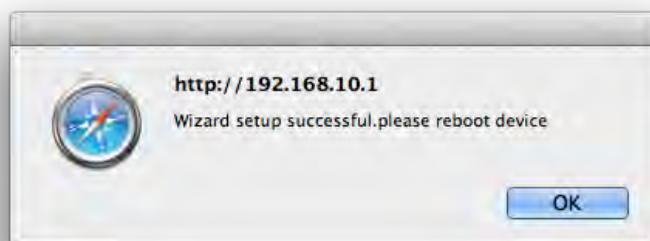
The screenshot shows the 'Internet Setup' window with the 'L2TP' tab selected. The configuration fields are as follows:

Field	Value	Range/Notes
VPN IPMode of Connection	Dynamic	
VPN Server IP	0.0.0.0	
Name		
User Name		
User Password		
Confirm Password		
Max MRU	1492	(576-1492)
DNS Enabled	Enable	
DNS Override Allowed	Disable	
DNS Server 1		(optional)
DNS Server 2		(optional)
MAC Address	00 : E0 : 4C : 81 : 86 : 82	Clone MAC
Connection Trigger	OnDemand	
Idle Disconnect Time	300	(30-3600 seconds)
LCP Interval	20	(0-86400 seconds)
ICMP Reply Enable	<input type="checkbox"/>	

Buttons at the bottom: Back, Next, Cancel.

Step 4: Setup completed

The Setup wizard is now completed. The new settings will be effective after the WLAN Router restarts. Please click "Reboot" to reboot the WLAN Router.



Advanced configuration

Main

The screen enables users to configure the **Internet Setup**, **Local Network**, and **Time and Date** settings.

Local Network

This page allows the user to configure LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.

LAN Setting:

LAN	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Local Domain Name	domain.name (optional)
DNS Relay	<input checked="" type="checkbox"/> Enable

IP Address: This is the IP address of the WLAN Router. The default IP address is 192.168.10.1.

Subnet Mask: Type the subnet mask for the WLAN Router in the text box. The default subnet mask is 255.255.255.0.

Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "TEW-751DR".

DNS Relay: Checked to enable the DNS Relay feature.

DHCP Setting

DHCP Option: select the which DHCP method to be use on the WLAN Router

- Disabled: Disable the DHCP feature.
- DHCP Server: Selected the DHCP Server to allow the WLAN Router to automatically assign IP addresses to devices connecting to the LAN/WLAN. DHCP Server is enabled by default.
- DHCP Relay: Selected the DHCP Relay to allow the LAN/WLAN users getting the IP address from specified DHCP server.

When selected **DHCP Server**:

The screenshot shows the 'DHCP Setting' window. At the top, 'DHCP Option' has three radio buttons: 'Disabled', 'DHCP Server' (which is selected), and 'DHCP Relay'. Below this, there are several input fields: 'IP Pool Starting Address' (192.168.10.33), 'IP Pool Ending Address' (192.168.10.254), 'Subnet Mask' (255.255.255.0), and 'Router IP Address' (192.168.10.1). There are also two 'Using WAN' options, both set to 'Disabled'. 'Primary DNS Servers' and 'Secondary DNS Servers' are both set to 80.58.61.250. 'Lease Time' is set to 86400 seconds. At the bottom, there are checkboxes for 'Sub Range IP Enable' and 'Extra Option Enable', both of which are unchecked. 'Apply' and 'Cancel' buttons are at the very bottom.

All DHCP client computers are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of the client.

IP Pool Starting Address: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the WLAN Router.

IP Pool Ending Address: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the WLAN Router.

Primary/Secondary DNS Server: Type an IP address to specific the DNS Servers.

Lease Time: The lease time specifies the amount of connection time a network user be allowed with their current dynamic IP address.


When selected **DHCP Relay**:

The screenshot shows the 'DHCP Setting' window. At the top, 'DHCP Option' has three radio buttons: 'Disabled', 'DHCP Server', and 'DHCP Relay' (which is selected). Below this, there is one input field: 'DHCP Server IP' (192.168.33.253). At the bottom, there are 'Apply' and 'Cancel' buttons.

DHCP Server IP: Type an IP address of the specified DHCP server.

Internet Setup

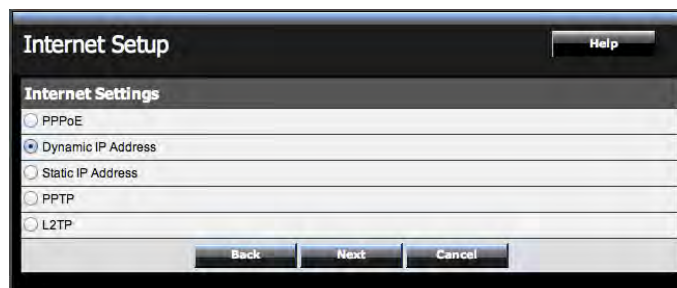
This screen enables users to set up the WLAN Router Internet connection.



The screenshot shows the 'Internet Setup' window with a 'Help' button in the top right. Under the 'Internet Settings' section, the following options are listed with radio buttons: PPPoE (selected), Dynamic IP Address, Static IP Address, PPTP, and L2TP.

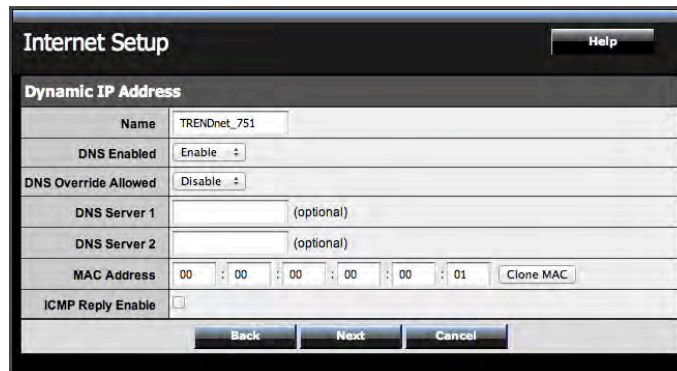
Connection Type: Select the connection type, either Dynamic IP Address, Static IP, PPPoE, PPTP or L2TP.

When selected the **Dynamic IP Address** for Internet connection:



The screenshot shows the 'Internet Setup' window with a 'Help' button in the top right. Under the 'Internet Settings' section, the following options are listed with radio buttons: PPPoE, Dynamic IP Address (selected), Static IP Address, PPTP, and L2TP. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

Choose "Dynamic IP Address" to have the WLAN Router assign IP addresses automatically.

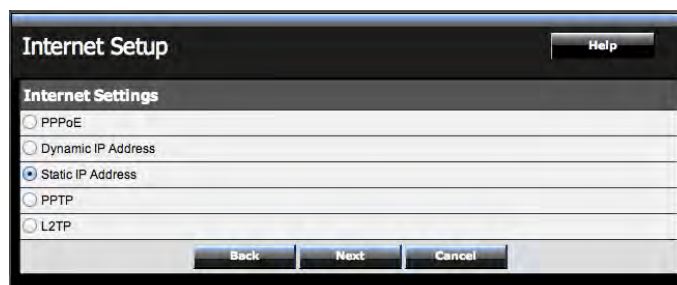


The screenshot shows the 'Internet Setup' window with a 'Help' button in the top right. The 'Dynamic IP Address' section is active and contains the following fields and controls:

Name	TRENDnet_751
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
MAC Address	00 : 00 : 00 : 00 : 00 : 01 Clone MAC
ICMP Reply Enable	<input type="checkbox"/>

At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

When selected the **Static IP Address** for Internet connection:



The screenshot shows the 'Internet Setup' window with a 'Help' button in the top right. Under the 'Internet Settings' section, the following options are listed with radio buttons: PPPoE, Dynamic IP Address, Static IP Address (selected), PPTP, and L2TP. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

If the Internet Service Provider (ISP) assigns a static IP address, choose this option and enter the assigned WAN IP Address, WAN Subnet Mask, WAN Gateway Address and DNS Server Addresses for the WLAN Router.

The screenshot shows the 'Internet Setup' window with the 'Static IP Address' section selected. The fields are filled with the following values:

Name	TRENDnet_751
External IP Address	0.0.0.0
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
MAC Address	00 : 00 : 00 : 00 : 00 : 01 <input type="button" value="Clone MAC"/>
ICMP Reply Enable	<input type="checkbox"/>

Buttons at the bottom: Back, Next, Cancel.

When selected the **PPPoE** for Internet connection:

The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section selected. The options are:

- PPPoE
- Dynamic IP Address
- Static IP Address
- PPTP
- L2TP

Buttons at the bottom: Back, Next, Cancel.

PPPoE with a Dynamic IP:

The screenshot shows the 'Internet Setup' window with the 'PPPoE' section selected. The fields are filled with the following values:

IPMode of Connection	Dynamic
Name	
User Name	
User Password	
Confirm Password	
Max MRU	1492 (576~1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
PPPoE Service Name	(optional)
MAC Address	00 : E0 : 4C : 81 : 86 : 82 <input type="button" value="Clone MAC"/>
PPPoE AC Name	(optional)
Connection Trigger	OnDemand
Idle Disconnect Time	300 (30~3600 seconds)
LCP Interval	20 (0~86400 seconds)
ICMP Reply Enable	<input type="checkbox"/>

Buttons at the bottom: Back, Next, Cancel.

If connected to the Internet using a PPPoE (Dial-up xDSL) connection, and the ISP provides a User Name and Password, then choose this option and enter the required information.

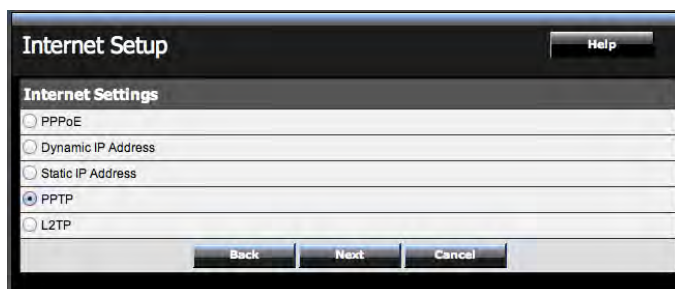
PPPoE with a Static IP:

The screenshot shows the 'Internet Setup' window with the 'PPPoE' section selected. The 'IP Mode of Connection' is set to 'Static'. The 'IP Address' is 0.0.0.0 and the 'Subnet Mask' is 255.255.255.0. The 'Name' field is empty. The 'User Name' and 'User Password' fields are empty. The 'Confirm Password' field is empty. The 'Max MRU' is 1492 (range 576-1492). 'DNS Enabled' is set to 'Enable'. 'DNS Override Allowed' is set to 'Disable'. 'DNS Server 1' and 'DNS Server 2' are empty (optional). 'PPPoE Service Name' is empty (optional). 'MAC Address' is 00 : E0 : 4C : 81 : 86 : 82 with a 'Clone MAC' button. 'PPPoE AC Name' is empty (optional). 'Connection Trigger' is set to 'OnDemand'. 'Idle Disconnect Time' is 300 (range 30-3600 seconds). 'LCP Interval' is 20 (range 0-86400 seconds). 'ICMP Reply Enable' is unchecked. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Internet Setup		Help
PPPoE		
IP Mode of Connection	Static	
IP Address	0.0.0.0	
Subnet Mask	255.255.255.0	
Name		
User Name		
User Password		
Confirm Password		
Max MRU	1492 (576-1492)	
DNS Enabled	Enable	
DNS Override Allowed	Disable	
DNS Server 1		
DNS Server 2		
PPPoE Service Name		
MAC Address	00 : E0 : 4C : 81 : 86 : 82 Clone MAC	
PPPoE AC Name		
Connection Trigger	OnDemand	
Idle Disconnect Time	300 (30-3600 seconds)	
LCP Interval	20 (0-86400 seconds)	
ICMP Reply Enable	<input type="checkbox"/>	
Back Next Cancel		

If connected to the Internet using a PPPoE (Dial-up xDSL) connection, and the ISP provides a IP address, Subnet mask, User Name, Password and a Static IP Address, choose this option and enter the required information.

When selected the **PPPTP** for Internet connection:



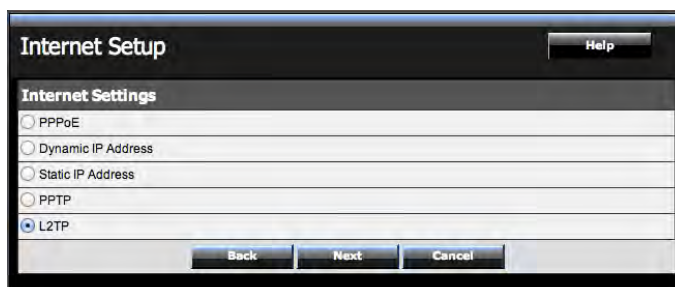
The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section. The 'PPTP' radio button is selected, while others (PPPoE, Dynamic IP Address, Static IP Address, L2TP) are unselected. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

If connected to the Internet using a PPTP xDSL connection, enter your IP, Subnet Mask, Gateway, Server IP, PPTP Account and PPTP Password.



The screenshot shows the 'Internet Setup' window with the 'PPTP' section expanded. Fields include: VPN IP Mode of Connection (Dynamic), VPN Server IP (0.0.0.0), MPPE (Disable), Name, User Name, User Password, Confirm Password, Max MRU (1492), DNS Enabled (Enable), DNS Override Allowed (Disable), DNS Server 1 and 2 (optional), MAC Address (00:E0:4C:81:86:82), Connection Trigger (OnDemand), Idle Disconnect Time (300), LCP Interval (20), and ICMP Reply Enable (checkbox). Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

When selected the **L2TP** for Internet connection:



The screenshot shows the 'Internet Setup' window with the 'Internet Settings' section. The 'L2TP' radio button is selected, while others (PPPoE, Dynamic IP Address, Static IP Address, PPTP) are unselected. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

If connected to the Internet using a L2TP (Dial-up xDSL) connection and the ISP provide a Server IP, Account and Password information, choose this option and enter the required information.

The screenshot shows the 'Internet Setup' window with the 'L2TP' section selected. The configuration fields are as follows:

VPN IP Mode of Connection	Dynamic
VPN Server IP	0.0.0.0
Name	
User Name	
User Password	
Confirm Password	
Max MRU	1492 (576-1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
MAC Address	00 : E0 : 4C : 81 : 86 : 82 Clone MAC
Connection Trigger	OnDemand
Idle Disconnect Time	300 (30-3600 seconds)
LCP Interval	20 (0-86400 seconds)
ICMP Reply Enable	<input type="checkbox"/>

Buttons at the bottom: Back, Next, Cancel.

Time and Date

This screen enables users to set the time and date for the WLAN Router's real-time clock, select properly time zone, and enable or disable daylight saving.

The screenshot shows the 'Time Setting' window with the following configuration:

Time Zone	(GMT+08:00) Hong Kong, Perth, Singapore, Taipei
NTP Enable	<input type="checkbox"/>
Server 1 IP or Domain name	
Server 2 IP or Domain name	
First Poll Frequency	5 (seconds)
ThereAfter Frequency	(hours)
Daylight Saving Enable	<input type="checkbox"/>
Start Time	
End Time	

Buttons: Apply, Cancel.

Manually Set Time

Year	2011	Month	Nov	Day	01
Hour	03	Minute	02	Second	02

Buttons: Set Time, Sync Time.

Local Time: Displays the local time and date.

Time Zone: Select the time zone from the drop-down list.

NTP Enable: Checked to automatically adjust the system time from NTP Server; otherwise, uncheck for manually adjust the system time when you press the **Set Time** or **Sync Time** button.

NTP server 1/2: The Simple Network Time Protocol (SNTP) server allows the WLAN Router to synchronize the system clock to the global Internet through the SNTP Server. Specify the NTP domain name or IP address in the text.

Set the time: Manually setting the WLAN Router system time, press the **Set Time** button to update the system time.

Sync the time: Syncing the WLAN Router system time same with your computer, press the **Sync Time** button to update the system time.

Daylight Saving: Enables users to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

Wireless

This section enables users to configuration the wireless communications parameters for the WLAN Router.

Basic Setting

This page allow user to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.

Wireless device (2.4G)	
Device Name	wlan1
Device	<input checked="" type="checkbox"/> Enable
SSID	TRENDnet751_2.4GHz
BSSID	00:E0:4C:81:86:82
Wireless Channel	2.437 GHz - CH6
Wireless Mode	802.11n + 802.11g + 802.11b

Wireless device (5G)	
Device Name	wlan0
Device	<input checked="" type="checkbox"/> Enable
SSID	TRENDnet751_5GHz
BSSID	00:E0:4C:81:86:87
Wireless Channel	CH40
Wireless Mode	802.11a + 802.11n

Enable/Disable: Enables or disables wireless LAN either 2.4GHz and 5GHz band.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the WLAN Router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the WLAN Router.

802.11 Mode: Select one of the following:

2.4GHz Band (802.11b/g/n)

- **802.11b/g/n mixed** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.
- **802.11b/g mixed** - Select if you are using both 802.11b and 802.11g wireless clients.
- **802.11n only** - Select if you are using 802.11n wireless clients only.
- **802.11g only** - Select if you are using 802.11g wireless clients only.
- **802.11b only** - Select if you are using 802.11b wireless clients only.

5GHz Band (802.11a/n)

- **802.11a/n mixed** - Select if you are using both 802.11a and 802.11n wireless clients.
- **802.11a only** - Select if you are using 802.11a wireless clients only.
- **802.11n only** - Select if you are using 802.11n wireless clients only.

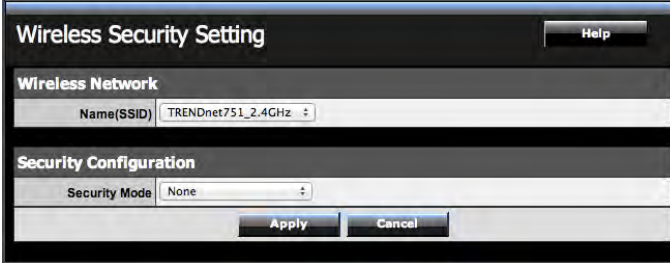
Channel Width: Select the Channel Width:

- **20MHz** – This is the default setting. Select this option if you are not using any 802.11n wireless clients.
- **Auto 20/40 MHz** - Select this option if you are using both 802.11n and non-802.11n wireless devices.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to view the WLAN Router's SSID. Note: Disabling SSID broadcast will disable the WPS function.

WMM: Enable the Wi-Fi Multi-Media will offer Wi-Fi networks stable that improve the user experience for audio, video, and voice applications by prioritizing data traffic.

Security



The screenshot shows the 'Wireless Security Setting' window. Under the 'Wireless Network' section, the 'Name(SSID)' is 'TRENDnet751_2.4GHz'. Under the 'Security Configuration' section, the 'Security Mode' is set to 'None'. There are 'Apply' and 'Cancel' buttons at the bottom.

Security Mode: The authentication type default is set to open system. There are four options: Disabled, WEP, WPA, WPA2 and WPA-Auto.

WEP

If selecting WEP (Wired Equivalent Privacy), please review the WEP settings to configure and click Next to save the changes.



The screenshot shows the 'Wireless Security Setting' window with 'Security Mode' set to 'WEP'. Under 'Security Configuration', 'Authentication Type' has radio buttons for 'Auto', 'Open System' (selected), and 'Shared Key'. Under 'Security Encryption(WEP)Key', 'Encryption Strength' is '64bit' and 'Key Format' is 'HEX'. There is a 'Passphrase' field with a 'Generate' button. Below are four key selection options: 'Key1' (selected), 'Key2', 'Key3', and 'Key4'. 'Apply' and 'Cancel' buttons are at the bottom.

- **Authentication Type** - Choose Open System, Shared Key or Auto.

Note: It is recommended to use Open System because it is known to be more secure than Shared Key.

- **Encryption Strength** - Choose the key length 64-bit or 128-bit.

Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.

- **Key Format** - Choose HEX or ASCII.

Note: It is recommended to use ASCII because of the much larger character set that can be used to create the key.

- **Key 1-4**

- This is where you enter the password or key needed for a computer to connect to the router wirelessly

- You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
- Choose a key index 1, 2, 3, or 4 and enter the key.
- When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

WPA, WPA-Auto or WPA2 (WPA2 recommended):

First, from the Security Mode row, select WPA, WPA-Auto, or WPA2.

Then from the Authentication Type row, select either PSK or EAP

- **PSK** stands for Passphrase Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).

*Note: **EAP** requires an external RADIUS server, **PSK** only requires you to create a passphrase.*

The following section outlines options when selecting PSK (Preshared Key Protocol):

Select a Cipher Type:

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** or **WPA2** security, it is recommended to use **AES**.

Create your Wireless security Passphrase (password or key):

- **Passphrase** – Enter the passphrase.

This is the password or key that is used to connect your computer to this router wirelessly

Confirmed Passphrase – Re-enter the passphrase.

Note: 8-63 alphanumeric characters (a,b,C,?,,/,1,2, etc.)*

The following section outlines options when selecting EAP (Extensive Authentication Protocol).

Select a Cipher Type:

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** or **WPA2** security, it is recommended to use **AES**.

Wireless Security Setting		Help
Wireless Network		
Name(SSID)	TRENDnet751_2.4GHz	
Security Configuration		
Security Mode	WPA	
Authentication Type	<input type="radio"/> PSK <input checked="" type="radio"/> EAP	
Encryption Type	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP and AES	
Group Rekey Time	86400 (seconds)	
RADIUS Information		
RADIUS Server IP	0.0.0.0	
RADIUS Server Port	1812	
RADIUS Server Key		
Apply		Cancel

RADIUS Server - Configure the RADIUS server settings:

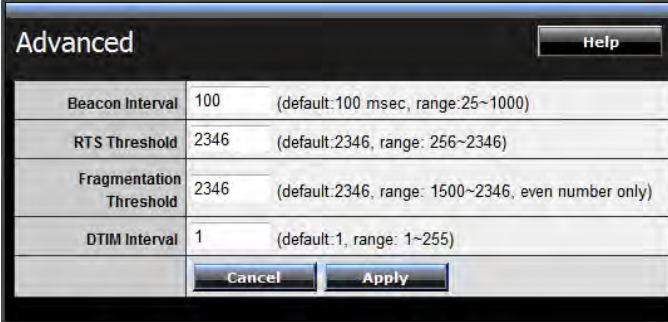
- **RADIUS Server IP** - Enter the IP address of the RADIUS server.
- **RADIUS Server Port** - Enter the port your RADIUS server is configured to use for RADIUS authentication.

Note: It is recommended to use port 1812.

- **RADIUS Server Key** - Enter the shared secret used to authorize your router with your RADIUS server.

Advanced Wireless

This screen enables users to configure advanced wireless functions.



Advanced		Help
Beacon Interval	100	(default: 100 msec, range: 25~1000)
RTS Threshold	2346	(default: 2346, range: 256~2346)
Fragmentation Threshold	2346	(default: 2346, range: 1500~2346, even number only)
DTIM Interval	1	(default: 1, range: 1~255)
Cancel		Apply

Beacon Interval: Type the beacon interval in the text box. User can specify a value from 25 to 1000. The default beacon interval is 100.

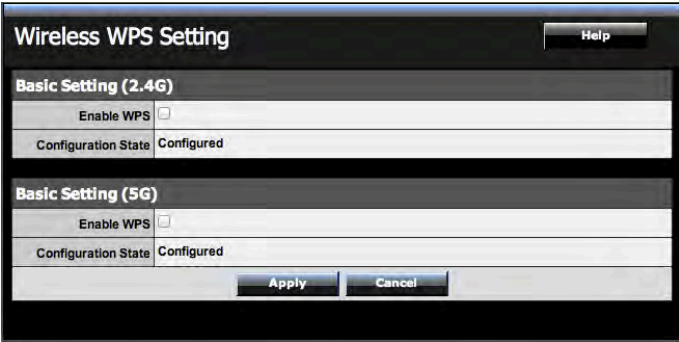
RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2346 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 1500 and 2346 until packet transfer rates are minimized. (NOTE: set this fragmentation threshold value may diminish system performance.)

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. User can specify

Wi-Fi Protected Setup

This screen enables users to configure the Wi-Fi Protected Setup function.



Wireless WPS Setting		Help
Basic Setting (2.4G)		
Enable WPS	<input type="checkbox"/>	
Configuration State	Configured	
Basic Setting (5G)		
Enable WPS	<input type="checkbox"/>	
Configuration State	Configured	
Apply		Cancel

Enable WPS: Enable or Disable the WPS (Wi-Fi Protected Setup) function

Configuration Status: Display the status (Un-configured State/Configured State) information of WPS.

Self-PIN Number: Display the current PIN number of the WLAN Router.

Add Client - PIN: When the **PIN** selected from **Add Client**, type Client's PIN number the client uses to negotiate with the WLAN Router via WPS connection. It is only used when users want their station to join Router's network.

Push Button Configuration: When the **Push Button** selected from **Add Client**, Clicking the **Add** button will invoke the Push Button Configuration (PBC) method of WPS. Push the WPS button on the client side when users want their station to join Router's network.

Status

This selection enables users to view the status of the WLAN Router LAN, WAN and Wireless connections, and view logs and statistics pertaining to connections and packet transfers.

Device Information

This screen enables users to view the WLAN Router's LAN, Wireless and WAN configurations.

The screenshot displays the 'Device Information' page of a router's web interface. It features a 'Help' button in the top right corner. The page is organized into three main sections: WAN, Wireless, and LAN, each with a table of configuration parameters.

Device Information	
Firmware Version:	
Router up time : 0 Day, 0:21:09	
WAN	
MAC Address	00:14:D1:E9:5B:EC
Connection	DHCP client Disconnected <input type="button" value="Renew"/> <input type="button" value="Release"/>
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DNS	0.0.0.0
Wireless	
MAC Address	00:14:D1:E9:5B:EB
Connection	AP Enable
SSID	TRENDnet652
Channel	1
Authentication	Disable
LAN	
MAC Address	00:14:D1:E9:5B:EB
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled DHCP Table

Firmware Version: Displays the latest build of the WLAN Router firmware interface. After updating the firmware in Tools - Firmware, check this to ensure that the firmware was successfully updated.

WAN: This section displays the WAN interface configuration including the MAC address, Connection status, DHCP client status, IP address, Subnet mask, Default gateway, and DNS.

Wireless: This section displays the wireless configuration information, including the MAC address, the Connection status, SSID, Channel and Authentication type.

LAN: This section displays the LAN interface configuration including the MAC address, IP Address, Subnet Mask, and DHCP Server Status. Click “DHCP Table” to view a list of client stations currently connected to the WLAN Router LAN interface. Click “*DHCP Release*” to release all IP addresses assigned to client stations connected to the WAN via the WLAN Router. Click “*DHCP Renew*” to reassign IP addresses to client stations connected to the WAN.

Log

This screen enables users to view a running log of Router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click “*First Page*” to view the first page of the log

Click “*Last Page*” to view the final page of the log

Click “*Previous Page*” to view the page just before the current page

Click “*Next Page*” to view the page just after the current page

Click “*Clear Log*” to delete the contents of the log and begin a new log

Click “*Refresh*” to renew log statistics

Log Help

Page: 1 / 3


Time	Type	Message
Sep 1 01:06:11	daemon.info	dnsmasq[150]: using nameserver 10.10.10.254#53
Sep 1 01:06:11	daemon.info	dnsmasq[150]: reading /etc/resolv.conf
Sep 1 01:05:52	user.notice	syslog: Note: adding VIF, idx=1 FI flags=0x0 IP=10.10.10.107 eth1
Sep 1 01:05:52	user.notice	syslog: Note: adding VIF, idx=0 FI flags=0x0 IP=192.168.10.1 br0
Sep 1 01:05:46	daemon.err	lld2d[2554]: osl_write_pidfile: /var/run/lld2d-br0.pid contains pid 2340 which is still running; aborting
Sep 1 01:05:24	daemon.warn	dnsmasq[150]: no servers found in /etc/resolv.conf, will retry
Sep 1 01:03:59	user.warn	kernel: wlan0: A wireless client is deauthenticated - 00:21:E9:90:0F:41
Sep 1 01:03:48	user.warn	kernel: wlan0: A wireless client is associated - 00:21:E9:90:0F:41
Sep 1 01:03:48	user.warn	kernel: wlan0: A wireless client is associated - 00:21:E9:90:0F:41
Sep 1 00:34:11	user.warn	kernel: wlan0: A wireless client is deauthenticated - 00:21:E9:90:0F:41

Time: Displays the time and date that the log entry was created.

Message: Displays summary information about the log entry.

Log Setting

This screen enables users to set Router Log parameters.



The screenshot shows a 'Log Setting' window with a 'Help' button in the top right corner. The window contains the following fields and options:

- SMTP Authentication:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- SMTP Account:** Text field containing 'user'.
- SMTP Password:** Password field with masked characters.
- SMTP Server:** Empty text field.
- SMTP Server Port:** Empty text field.
- From Email Address:** Empty text field.
- To Email Address:** Empty text field.
- Email Log Now:** Button.
- E-mail Logs:** Radio buttons for 'When log is full' and 'Every Sunday' (selected). Below 'Every Sunday' are dropdown menus for 'at 0' and 'AM'.
- Syslog Server:** Text field containing '0.0.0.0'.
- Log Type:** Checkboxes for 'System Activity' (checked), 'Debug Information' (unchecked), 'Attacks' (checked), 'Dropped Packets' (unchecked), and 'Notice' (checked).
- Buttons:** 'Cancel' and 'Apply' buttons at the bottom.

SMTP Authentication: Selected the Enabled if the SMTP server need for authentication, fill in account name and password in SMTP Account field and SMTP Password field.

SMTP Account: If the SMTP Authentication enabled, fill in the SMTP account name here.

SMTP Password: If the SMTP Authentication enabled, fill in the password of the SMTP account here.

SMTP Server: Type your SMTP server address here.

From Email address: Type an email address for the log to be sent from.

To Email address: Type an email address for the log to be sent to. Click "Email Log Now" to immediately send the current log.

E-mail Logs: Email the logs to specified email receiver.

When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.

Every day, Every Monday ... - The log is sent on the interval specified.

- If "Every day" is selected, the log is sent at the time specified.

- If the day is specified, the log is sent once per week, on the specified day.
- Select the time of day you wish the E-mail to be sent.
- If the log is full before the time specified to send it, it will be sent regardless.

Syslog Server: Type the IP address of the Syslog Server if user wants the WLAN Router to listen and receive incoming Syslog messages.

Log Type: Enables users to select what items will be included in the log:

System Activity: Displays information related to WLAN Router operation.

Debug Information: Displays information related to errors and system malfunctions.

Attacks: Displays information about any malicious activity on the network.

Dropped Packets: Displays information about packets that have not been transferred successfully.

Notice: Displays important notices by the system administrator.

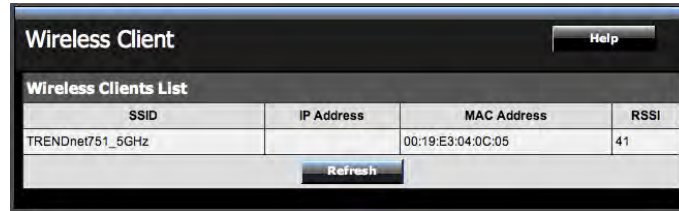
Statistic

This screen displays a table that shows the rate of packet transmission via the WLAN Router's LAN, Wireless and WAN ports (in bytes per second).

Statistic				
Help				
Internet Connections				
LAN Device				
Tx OK	12070	Packets		
Rx OK	12945	Packets		
Tx Error	0	Packets		
Rx Error	0	Packets		
Wireless Port (2.4G)				
Tx OK	45	Packets		
Rx OK	9518	Packets		
Tx Error	0	Packets		
Rx Error	0	Packets		
Wireless Port (5G)				
Tx OK	133	Packets		
Rx OK	228	Packets		
Tx Error	0	Packets		
Rx Error	0	Packets		
LAN Ports				
	LAN1	LAN2	LAN3	LAN4
Link Status	Link down	Link down	Link up	Link down

Wireless Client

This screen enables users to view information about wireless devices that are connected to the WLAN Router.



SSID	IP Address	MAC Address	RSSI
TRENDnet751_5GHz		00:19:E3:04:0C:05	41

Connected Time: Displays the time duration of wireless clients connection to the WLAN Router.

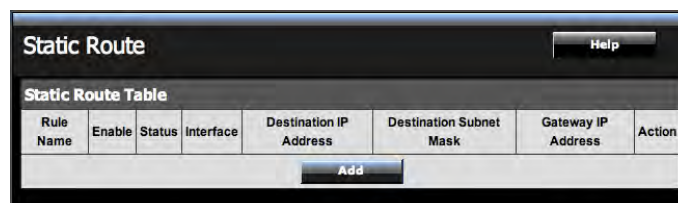
MAC Address: Displays the wireless client's MAC address.

Routing

This selection enables users to set how the WLAN Router forwards data: Static and Dynamic. Routing Table enables users to view the information created by the WLAN Router that displays the network interconnection topology.

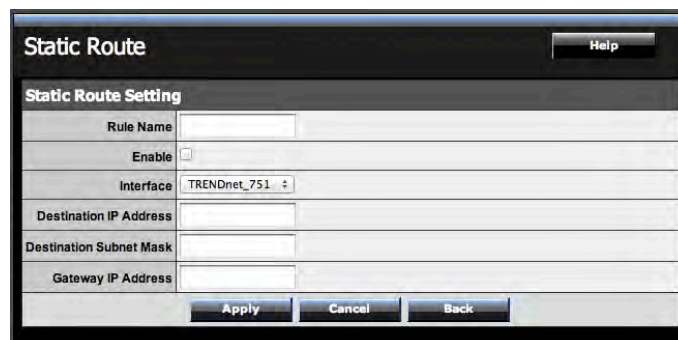
Static

It enables users to create static routes to other IP networks through next hop routers.



Rule Name	Enable	Status	Interface	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Action
-----------	--------	--------	-----------	------------------------	-------------------------	--------------------	--------

Click the **Add** button to adding the static route



Rule Name	<input type="text"/>
Enable	<input type="checkbox"/>
Interface	TRENDnet_751
Destination IP Address	<input type="text"/>
Destination Subnet Mask	<input type="text"/>
Gateway IP Address	<input type="text"/>

Destination IP Address: Type the network IP address (ex. 192.168.2.10 or 192.168.2.0) of the destination network.

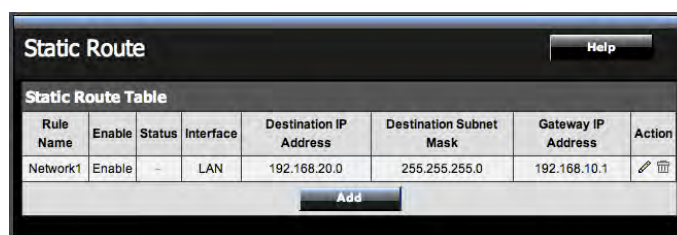
Destination Subnet Mask: Type the subnet mask of the destination network (ex 255.255.255.0).




Gateway IP Address: Type the gateway IP address to the destination network or next hop router IP address. (ex. 192.168.10.10)


Interface: Select an interface, Internet or LAN to map the static route.


Metric: Type the metric (priority) for the static route (1-15). Metric 1 being the highest priority.

Click **Apply** button to add the configuration to the static IP address table at the bottom of the page.



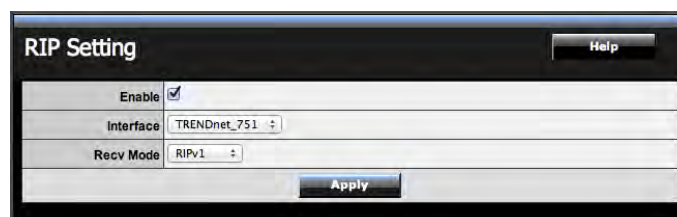
Static Route							
Static Route Table							
Rule Name	Enable	Status	Interface	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Action
Network1	Enable	-	LAN	192.168.20.0	255.255.255.0	192.168.10.1	  

Update : Select one of the entries in the static IP address table at the bottom of the page, and after changing parameters, click “Update” to confirm the changes.

Delete : Select one of the entries in the static IP address table at the bottom of the page and click “Delete” to remove the entry.

Dynamic

It enables users to enable RIPv1 or RIPv2 (Routing Information Protocol) on all of the router interfaces, to transmit and/or receive RIP information to and from other routers also using the RIP protocol. This allows the router to dynamically learn routes and exchange route information of other IP networks between other RIP routers.



RIP Setting	
Enable	<input checked="" type="checkbox"/>
Interface	TRENDnet_751
Recv Mode	RIPv1

Recv Mode:

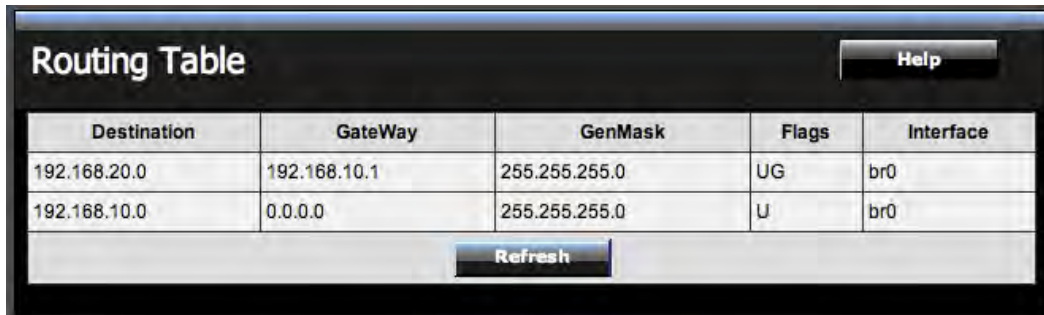
Select the RIP protocol RIPv1, RIPv2, or RIPv1/RIPv2 from drop-down list.

Interface:

Select the network interface from drop-down list.

Routing Table

This screen enables users to view the routing table of the WLAN Router. The routing table is a database created by the WLAN Router that displays the network interconnection topology.



Destination	GateWay	GenMask	Flags	Interface
192.168.20.0	192.168.10.1	255.255.255.0	UG	br0
192.168.10.0	0.0.0.0	255.255.255.0	U	br0

Destination: Displays the destination network IP address.

Network Mask: Displays the destination network subnet mask.

Gateway Address: Displays the gateway address to the destination network.

Interface: Displays whether the interface (WAN) or LAN, where the route is mapped.

Metric: Displays the metric (priority) of the route.

Type: Displays whether the route is dynamically created (automatically generated) or statically created or assigned.

Access

This page enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

Using filters to deny or allow the users to access to the Internet. Three types of filters can be select: MAC, Domain/URL blocking, and Protocol/IP filter.

MAC Filters



MAC Address	Action
-------------	--------

MAC Address Control: Checked to enabling the MAC filter function.

Allow: Only allow computers with MAC address listed in the MAC Table.




Deny: Computers in the MAC Table are denied access to the router, access to your wired/wireless local network (LAN/WLAN), and Internet access.

MAC Address: Type the MAC address of the user's network interface.

Delete  : Select a user from the **MAC Address Control List** at the bottom of the list and click  to remove the selected setting.

Domain/URL Blocking

You could specify the domains that allow users to access or deny by clicking one of the two items. Also, add the specified domains in the text box.



URL	Action
network.com	
xxx.com	
sex	

URL Filter: Check to enable the Domain/URL filter function.

Add FRDN Rule: Enter the domain name which will be deny to access.

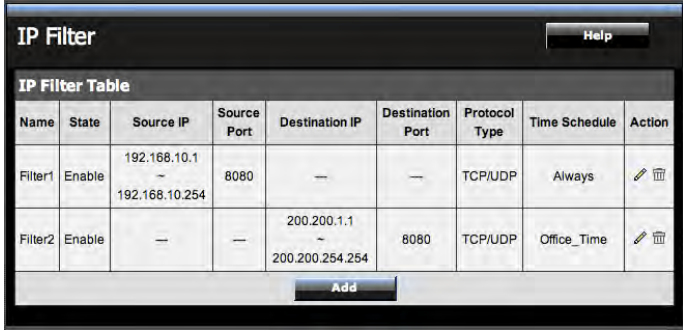
Add Keyword Rule: Enter the keyword in which will be deny to access the domain name which including the keyword.





Add: Click to **Add** button to add domain to the URL list.

Delete : Select a Domain/URL from the table at the bottom of the list and click  to remove the Domain/URL.

IP Filters

This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling within the range are not allowed accessing internet. The IP filter profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)



Name	State	Source IP	Source Port	Destination IP	Destination Port	Protocol Type	Time Schedule	Action
Filter1	Enable	192.168.10.1 ~ 192.168.10.254	8080	--	--	TCP/UDP	Always	 
Filter2	Enable	--	--	200.200.1.1 ~ 200.200.254.254	8080	TCP/UDP	Office_Time	 

Add: Check **Add** button to adding new IP filter rule

Delete : Select a list item and click  to remove the rule from the list.

Edit : Select a list item and click  to edit the rule from the list.

IP Filter Setting	
IP Filter	<input type="checkbox"/> Enable
Filter Name	<input type="text"/>
Start Source IP Address	<input type="text"/>
End Source IP Address	<input type="text"/>
Source Port	<input type="text"/> (port or port:port)
Start Destination IP Address	<input type="text"/>
End Destination IP Address	<input type="text"/>
Destination Port	<input type="text"/> (port or port:port)
Protocol Type	TCP/UDP
Time Schedule	Always <input type="button" value="New Time Schedule"/>

Apply Cancel Back

Enable: Check to enable the IP address filter.

Filter Name: Type the name of the user to be denied access.

Start Source IP Address/End Source IP Address: Type the IP range. **From** the IP addresses falling between this value and the Range End are not allowed to access the Internet.

Protocol Type: Select a protocol (TCP or UDP) to use for the virtual server.

Source Port: Type the port or port range of the protocol.

Apply: Click to add the IP range to the table at the bottom of the screen.

Virtual Server

This screen enables user to create a virtual server via the WLAN Router. If the WLAN Router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The WLAN Router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

Virtual Server Help

Enable Enable Disabled

Name

Protocol TCP ▾

Private Port

Public Port

LAN Server

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTP	TCP 80/80	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	PPTP	TCP 1723/1723	0.0.0.0
<input type="checkbox"/>	NetMeeting	TCP 1720/1720	0.0.0.0

Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select a protocol (TCP or UDP) to use for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

- **Add:** Click to add the virtual server to the table at the bottom of the screen.
- **Update:** Click to update information for the virtual server if the user has selected a listed item and has made changes.
- **Delete:** Select a listed item and click **Delete** to remove the item from the list.
- **Cancel:** Click **Cancel** button to erase all fields and enter new information.

Special AP

This screen enables users to specify special applications, such as games which require multiple connections that are blocked by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

	Name	Trigger Port Range	Incoming Port
<input type="checkbox"/>	Battle.net	Any 6112-6112	Any 6112
<input type="checkbox"/>	Dialpad	Any 7175-7175	Any 51200-51201,51210
<input type="checkbox"/>	ICU II	Any 2019-2019	Any 2000-2038,2025-2051,2069,2085,3010-3030
<input type="checkbox"/>	PC-to-Phone	Any 12053-12053	Any 12120,12122,24150-24220
<input type="checkbox"/>	Quick Time 4	Any 554-554	Any 6970-6999

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the WLAN Router's WAN connection. Click "Disabled" on a profile to prevent users from accessing the application on the WAN connection.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol (TCP, UDP, or * for TCP+UDP) that can be used to access the application.
- **Port Range:** Type the port range that can be used to access the application in the text boxes.

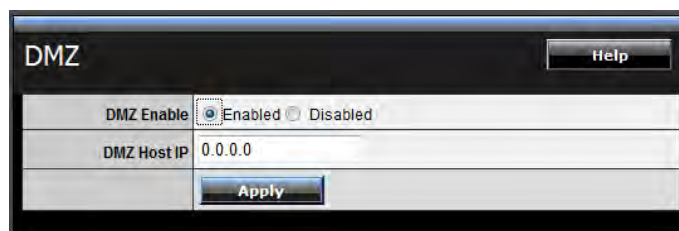
Incoming: Defines which incoming communications users are permitted to connect with.

- **Protocol:** Select the protocol (TCP, UDP, or * for TCP+UDP) that can be used by the incoming communication.
- **Port:** Type the port number that can be used for the incoming communication.
- **Add:** Click to add the special application profile to the table at the bottom of the screen.
- **Update:** Click to update information for the special application if user have selected a list item and have made changes.
- **Delete:** Select a list item and click **Delete** to remove the item from the list.
- **Cancel:** Click **Cancel** button to erase all fields and enter new information.

DMZ

This screen enables users to create a DMZ for those computers that cannot access Internet applications properly through the WLAN Router and associated security settings.

Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.



DMZ		Help
DMZ Enable	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
DMZ Host IP	0.0.0.0	
Apply		

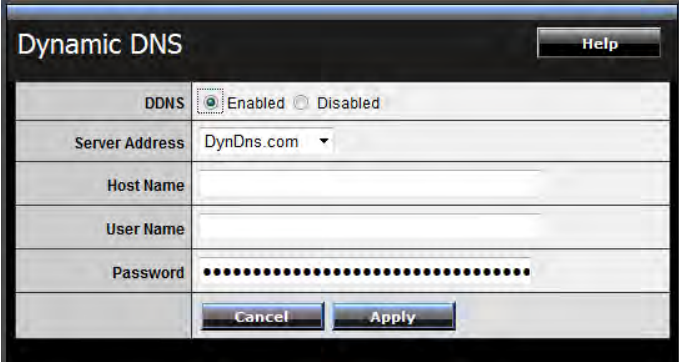
Enable: Click to enable or disable the DMZ.

DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Apply: Click to save the settings.

Dynamic DNS

This synchronizes the DDNS server with your current Public IP address when you are online. First, you need to register your preferred DNS with the DDNS provider. Then, please select the DDNS address in the Server Address and fill the related information in the below fields: Host Name, User Name and Password.



The image shows a software window titled "Dynamic DNS" with a "Help" button in the top right corner. The window contains several configuration fields:

DDNS	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Server Address	DynDns.com ▼
Host Name	<input type="text"/>
User Name	<input type="text"/>
Password
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

Firewall Settings

This screen enables users to set up the firewall. The WLAN Router provides basic firewall functions, by filtering all the packets that enter the WLAN Router using a set of rules. The rules are listed in sequential order--the lower the rule number, the higher the priority the rule has.

	Interface	IP Range Start	IP Range End	Protocol
Source	LAN			
Destination	WAN			TCP

	Action	Name	Source	Destination	Protocol
<input checked="" type="checkbox"/>	Deny	Default	WAN,*	LAN,*	**
<input checked="" type="checkbox"/>	Allow	Default	LAN,*	WAN,*	**

Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Source: Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if the user has selected a listed item and has made changes.

Delete: Select a listed item and click *Delete* button to remove the entry from the list.

New: Click “**New**” to erase all fields and enter new information.

Priority Up: Select a rule from the list and click “**Priority Up**” to increase the priority of the rule.

Priority Down: Select a rule from the list and click “**Priority Down**” to decrease the priority of the rule.

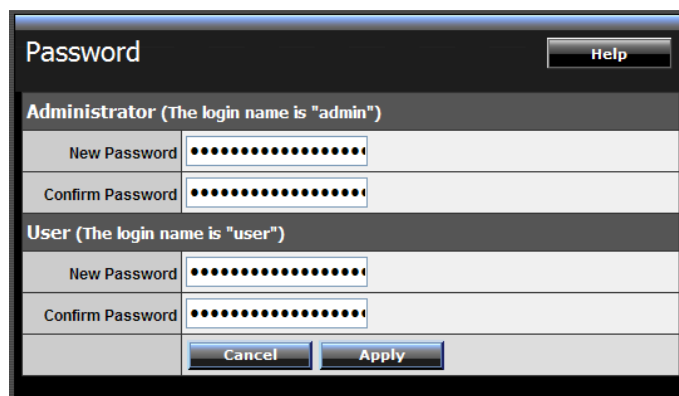
Update Priority: After increasing or decreasing the priority of a rule, click “*Update Priority*” to save the changes.

Management

Management enables users to set up the SNMP and Remote Management features.

Password

This screen enables users to set administrative and user passwords. These passwords are used to gain access to the WLAN Router interface.



The screenshot shows a window titled "Password" with a "Help" button in the top right corner. The window is divided into two sections: "Administrator (The login name is 'admin')" and "User (The login name is 'user')". Each section contains two input fields: "New Password" and "Confirm Password", both of which are currently filled with dots. At the bottom of the window, there are two buttons: "Cancel" and "Apply".

Administrator: Type the password the Administrator will use to log into the system. The password must be typed again for confirmation. The Administrator can also authorize users the ability to configure the WLAN Router.

User: Type the password the User will use to log in to the system. The password must be typed again for confirmation.

Remote Management

This screen enables users to set up remote management. Using remote management, the WLAN Router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.

Remote Management	
HTTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disabled Port: 8080 Remote IP Range: From * To
Allow to Ping WAN Port	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
UPNP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
PPTP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
L2TP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPSec	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Multicast Stream	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Cancel Apply	

HTTP: Enables users to set up HTTP access of the Port number, and Remote IP Range for remote management.

Allow to Ping WAN Port: Type a range of Router IP addresses that can be pinged from remote locations

UPnP Enable: UPnP is short for Universal Plug and Play that is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The WLAN Router is an UPnP-enabled Router and will only work with other UPnP devices/software. If user does not want to use the UPnP functionality, select “Disabled” to disable it.

PPTP: Enables users to set up PPTP access for remote management.

L2TP: Enables users to set up L2TP access for remote management.

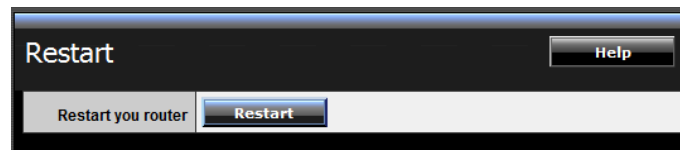
IPSec: Enables users to set up IPSec access for remote management.

Tools

This page enables users to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure WLAN Router settings, upgrade the firmware, and ping remote IP addresses.

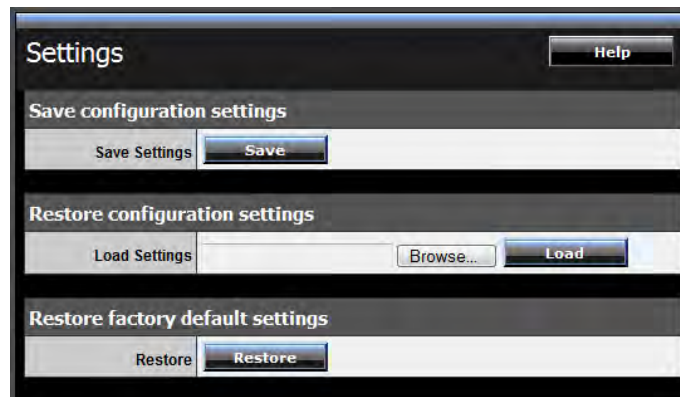
Restart

Click “Restart” to restart the system in the event the system is not performing correctly.



Settings

This screen enables users to save settings as a profile and load profiles for different circumstances. User can also load the factory default settings, and run a setup wizard to configure the WLAN Router and Router interface.



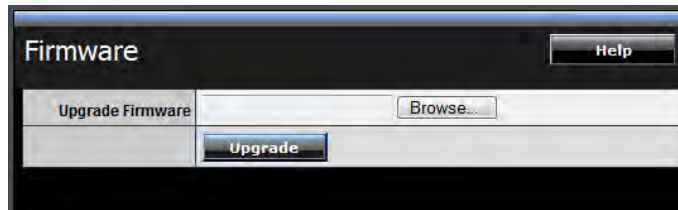
Save Settings: Click “Save” to save the current configuration as a profile that can load when necessary.

Load Settings: Click “Browse” and go to the location of a stored profile. Click “Load” to load the profile's settings.

Restore Factory Default Settings: Click “Restore” to restore the default settings. All configuration changes will lose.

Firmware

This screen enables users to keep the WLAN Router firmware up to date.



Please follow the below instructions:

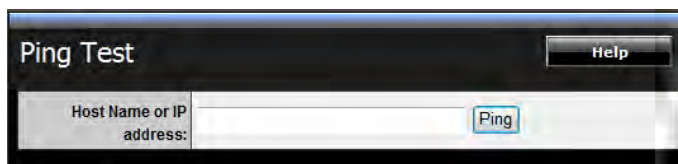
Download the latest firmware from the manufacturer's Web site, and save it to disk.

Click "**Browse**" and go to the location of the downloaded firmware file.

Select the file and click "**Upgrade**" to update the firmware to the latest release.

Ping Test

The ping test enables users to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click Ping.



TECHNICAL SPECIFICATIONS

Hardware	
Standards	IEEE 802.3 (10BASE-T), IEEE 802.3u (100BASE-TX), IEEE 802.11a/b/g/n
WAN	1 x 10/100/1000Mbps Auto-MDIX port (Internet)
LAN	4 x 10/100/1000Mbps Auto-MDIX ports
WPS Button	Enables Wi-Fi Protected Setup (WPS) function
Connection Type	Dynamic IP, Static (Fixed) IP, PPPoE, PPTP, L2TP
UPnP	UPnP IGD 1.0 compliant
DMZ	DMZ host & Virtual Servers
DNS	Static or WAN assigned DNS servers; 3 verified services for DDNS
SNMP	Up to 3 external trap receivers
Internet Access Control	MAC Address Filter, Domain/URL Filter, Protocol/IP Filter
Logging	5 types of event logging; email report
LED Indicator	Power, LAN1~LAN4, WAN, WLAN, Status
Power Switch	On/Off power switch
Power Adapter	12V DC, 1A external power adapter
Power Consumption	3.0 watts (max)
Dimension (L x W x H)	158 x 109 x 34mm (6.2 x 4.3 x 1.3in)
Weight	250g (7.4oz)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F); Storage: -10°~ 70°C (14°F~158 °F)
Humidity	Max. 90% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.412~2.484GHz band
Antenna	2 x 2dBi fixed dipole antennas
Media Access Protocol	CSMA/CA with ACK
Data Rate	802.11b: Up to 11Mbps 802.11a/g: Up to 54Mbps 802.11n: Up to 300Mbps
Security	WEP(HEX/ASCII): 64/128-bit WPA(AES/TKIP): WPA/WPA2-RADIUS, WPA-PSK/WPA2-PSK
Output Power	2.4GHz band (FCC): 25.5dBm 5GHz band (FCC): 16.0dBm
Receiving Sensitivity	802.11b: -85dBm (typical) @ 11Mbps 802.11g: -68dBm (typical) @ 54Mbps 802.11n: -62dBm (typical) @ 300Mbps
Channels	1~ 11 (FCC), 1~13 (ETSI)

LIMITED WARRANTY

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEW-751DR – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

PWP05202009v2



TRENDNET[®]

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>