User's Guide

TRENDnet®

N600 Dual Band Wireless Router

TEW-752DRU

Table of Contents

Product Overview

TEW-752DRU

Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Multi-Language Quick Installation Guide
- 1 x Network cable (1.5m / 5ft.)
- Power Adapter (12V, 1.25A)

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's N600 Dual Band Wireless Router, model TEW-752DRU, offers proven concurrent Dual Band 300 Mbps wireless n networking, Gigabit wired Ethernet ports, and a convenient USB share port. Embedded GREENnet technology reduces power consumption by up to 50%. For your security this router comes pre-encrypted and features guest networks.

Ease of Use

Easy Setup

Get up and running in minutes with the intuitive guided setup

One Touch Connection

Securely connect to the router at the touch of the Wi-Fi Protected Setup (WPS) button

USB Share Port

Plug in a USB flash or storage drive to share content across the network

Security

Pre-Encrypted

For your security the router arrives pre-encrypted with its own unique password

Guest Network

Create a secure isolated network, on each wireless band, for guest internet access only

Parental Controls

Control access to specific websites

Performance

N600 Wireless

Proven concurrent dual band 300 Mbps wireless n

Gigabit Ports

Gigabit ports extend high performance wired connections

Wireless Coverage

Extensive wireless coverage with MIMO antenna technology

Quality of Service (QoS)

Advanced QoS prioritizes video and audio transmissions

Compatibility

Compatible with older Wireless G devices

Energy Savings

Embedded GREENnet technology reduces power consumption by up to 50%

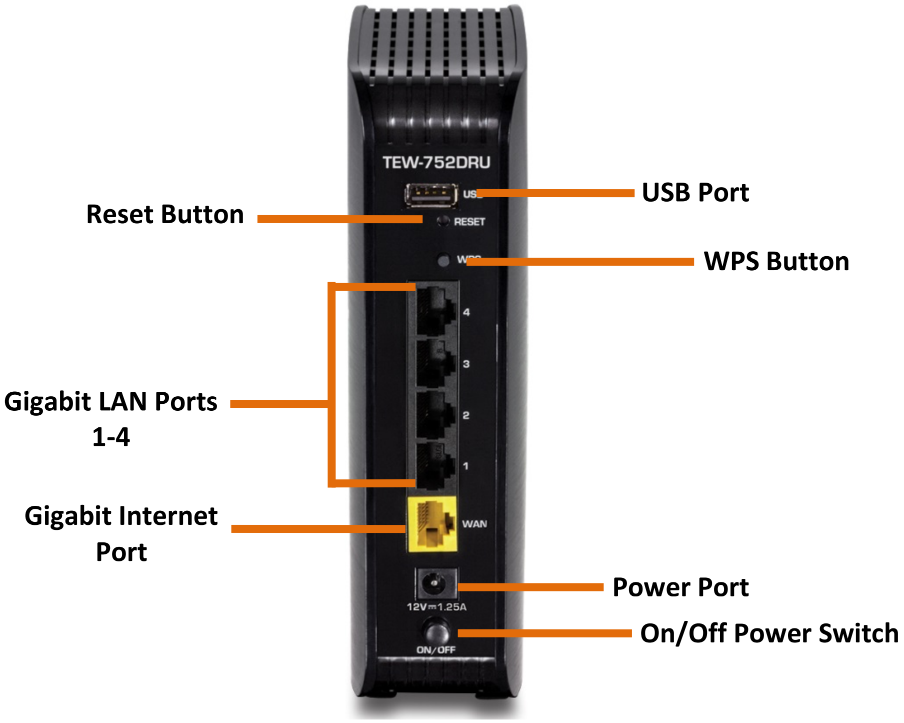
IPv6

IPv6 network support

*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

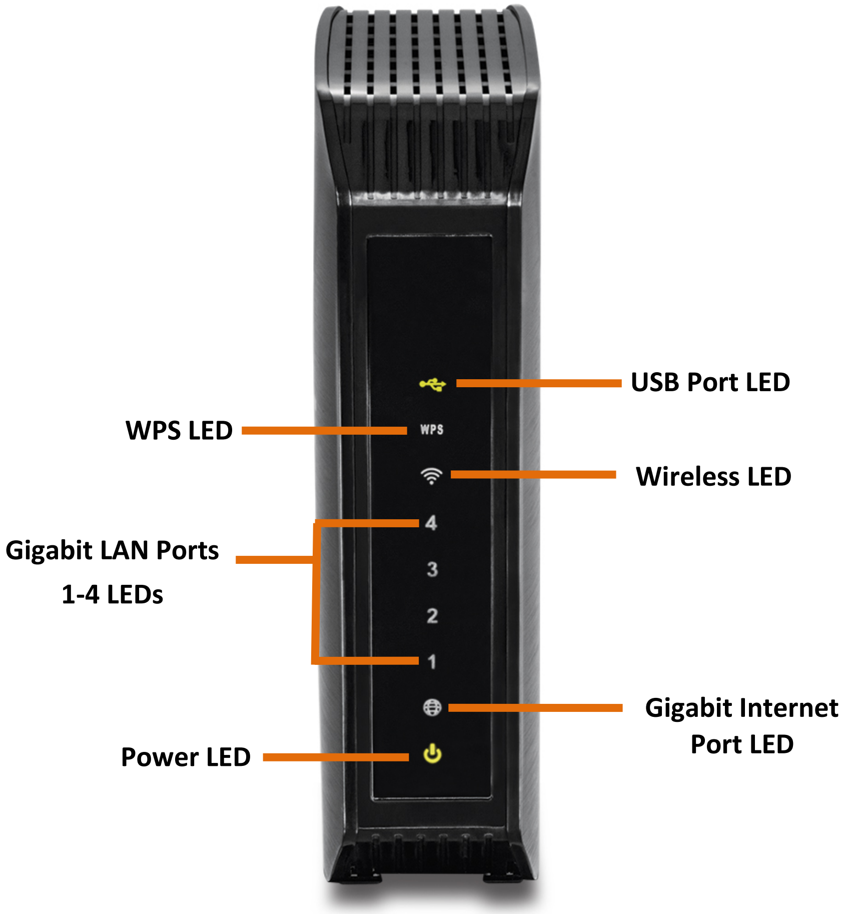
Product Hardware Features

Rear View



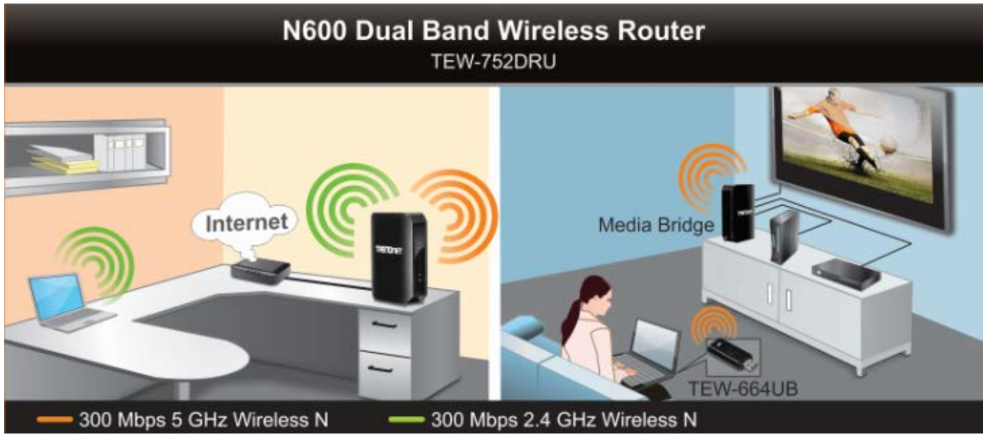
- **USB Port:** Press and hold this button for 10 seconds to reset the router.
- **Reset Button:** Press and hold this button for 10 seconds to reset the router.
- **WPS Button (Wi-Fi Protected Setup):** Push and hold this button for 5 seconds to activate WPS. The Power LED will blink when WPS is activated.
- **Gigabit LAN Ports 1-4:** Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
- **Gigabit Internet Port:** Connect an Ethernet cable from your router Internet port to your modem.
- **Power Port:** Connect the included power adapter from your router power port and to an available power outlet.
- **On/Off Power Switch:** Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).

Front View



- **USB Port LED:** The indicator when a USB device is connected. The indicator will blink during data transmission.
- **WPS LED:** The indicator will blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.
- **Wireless (Link/Activity) LED:** The indicator turns on solid green when wireless is enabled on your router. The indicator will blink during when data is transmitted or received by your wireless client devices connected to your router.
- **Gigabit LAN Ports 1-4 (Link/Activity) LED:** These LED indicators are solid green when the LAN ports 1-4 are physically connected to your wired network devices (which are turned on) with a network or Ethernet cable. These LED indicators will blink green while data is transmitted or received through your router's LAN ports.
- **Gigabit Internet Port (Link/Activity) LED:** This LED indicator is solid green when your router Internet port is physically connected to the modem network or Ethernet port with a network or Ethernet cable (modem turned on). The LED indicator will be blinking green while data is transmitted or received through the Internet port of your router.
- **Power LED:** The indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router. The indicator will also blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.

Application Diagram


N600 Dual Band Wireless Router
TEW-752DRU
Internet
Media Bridge
TEW-664UB
300 Mbps 5 GHz Wireless N
300 Mbps 2.4 GHz Wireless N

The router is installed near the modem (typically supplied by your ISP "Internet Service Provider") and physically connected to it from the router's Internet port to the modem's network port which connects to the Internet. 2.4GHz wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) and the less congested 5GHz wireless signals from the router are broadcasted to other wireless client devices such as TVs, game consoles, or media bridges thereby providing Internet access for all wireless client devices.

Basic Router Setup

Creating a Home Network

What is a network?

A network is a group of computers or devices that can communicate with each other. A home network of more than one computer or device also typically includes Internet access, which requires a router.

A typical home network may include multiple computers, a media player/server, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and Internet cameras.

- **Modem** – Connects a computer or router to the Internet or ISP (Internet Service Provider).
- **Router** – Connects multiple devices to the Internet.
- **Switch** –Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to add more wired connections.

How to set up a home network

1. For a network that includes Internet access, you'll need:

- Computers/devices with an Ethernet port (also called network port) or wireless networking capabilities.
- A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
- A router to connect multiple devices to the Internet.

2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.

3. Set up your router. See "How to setup your router" below.

4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 12.

5. To set up wireless security on your router, see "Wireless Networking and Security" on page 13.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on page 8 for more detailed installation instructions.

Where to find more help

In addition to this User's Guide, you can find help below:

- http://www.trendnet.com/support (documents, downloads, and FAQs are available from this Web page)

Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

1. Obtain IP Address Automatically (Dynamic IP DHCP)

Host Name:_______________ (Optional, if required by ISP for Compatibilty)
Use Unicasting: Enabled / Disabled (Optional, if required by ISP for compatibility)
Primary DNS Server Address: _____. _____._____._____ (Optional)
Secondary DNS Servers Address : _____. _____._____._____ (Optional)
MTU:_______ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

2. Static IP/Fixed IP address

IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask: _____. _____._____._____
Default Gateway IP Address: _____. _____._____._____
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Servers Address : _____. _____._____._____ (Optional)
MTU:_______ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

3. PPPoE Dynamic IP (DHCP) / PPPoE Static IPto obtain IP automatically

Type (Dynamic IP/DHCP or Static IP)
IP Address (Static IP): _____. _____._____._____ (e.g. 215.24.24.129)
Username: _________
Password: ________________
Service Name: _________________ (Optional)
DNS Servers Address 1 (Static IP): _____. _____._____._____
DNS Servers Address 2 (Static IP): _____. _____._____._____ (Optional)
Reconnect Mode: Always / On Demand / Manual (Optional)

MTU:_______ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

4. PPTP
Type (Dynamic IP/DHCP or Static IP)
PPTP IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
PPTP Subnet Mask: _____. _____._____._____ (e.g. 255.255.255.0)
PPTP Gateway:_____. _____._____._____ (e.g. 215.24.24.1)
PPTP Server: _____________________ (e.g. 215.24.24.150)
Username: _________
Password: ________________
Reconnect Mode: Always / On Demand / Manual (Optional)
DNS Servers Address 1 (Static IP): _____. _____._____._____
DNS Servers Address 2 (Static IP): _____. _____._____._____ (Optional)
MTU:_______ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

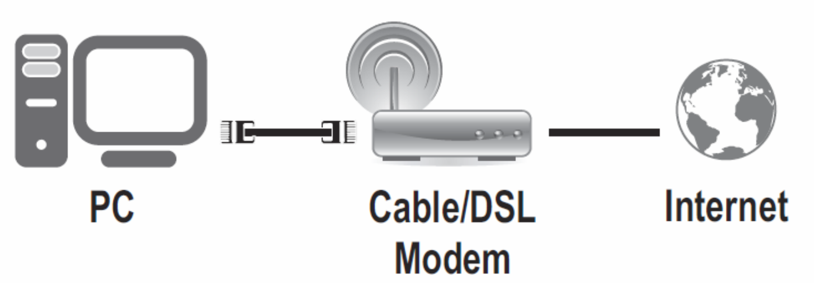
5. L2TP
Type (Dynamic IP/DHCP or Static IP)
L2TP IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
L2TP Subnet Mask: _____. _____._____._____ (e.g. 255.255.255.0)
L2TP Gateway:_____. _____._____._____ (e.g. 215.24.24.1)
L2TP Server: _____________________ (e.g. 215.24.24.150)
Username: _________
Password: ________________
Reconnect Mode: Always / On Demand / Manual (Optional)
DNS Servers Address 1 (Static IP): _____. _____._____._____
DNS Servers Address 2 (Static IP): _____. _____._____._____ (Optional)
MTU:_______ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

5. DS-Lite
Type (DS-Lite DHCP IPv6 or Manual)

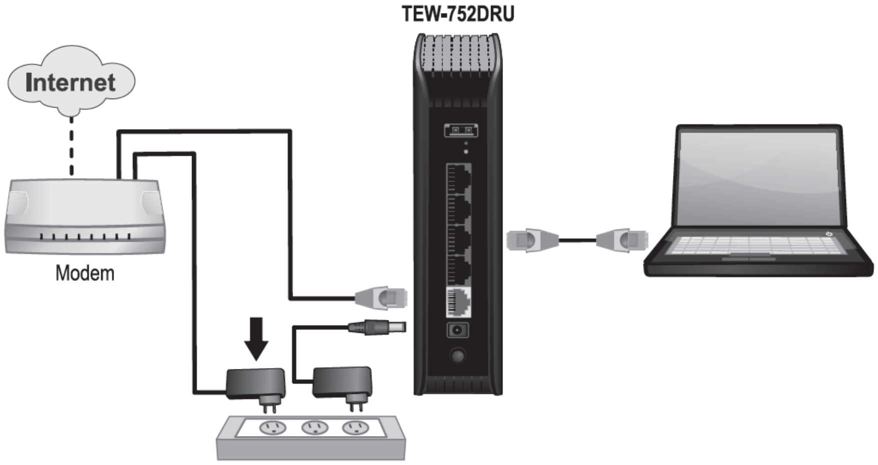
Check with your ISP for the required settings.

Hardware Installation

1. Verify that you have an Internet connection when connecting your computer directly to your modem.

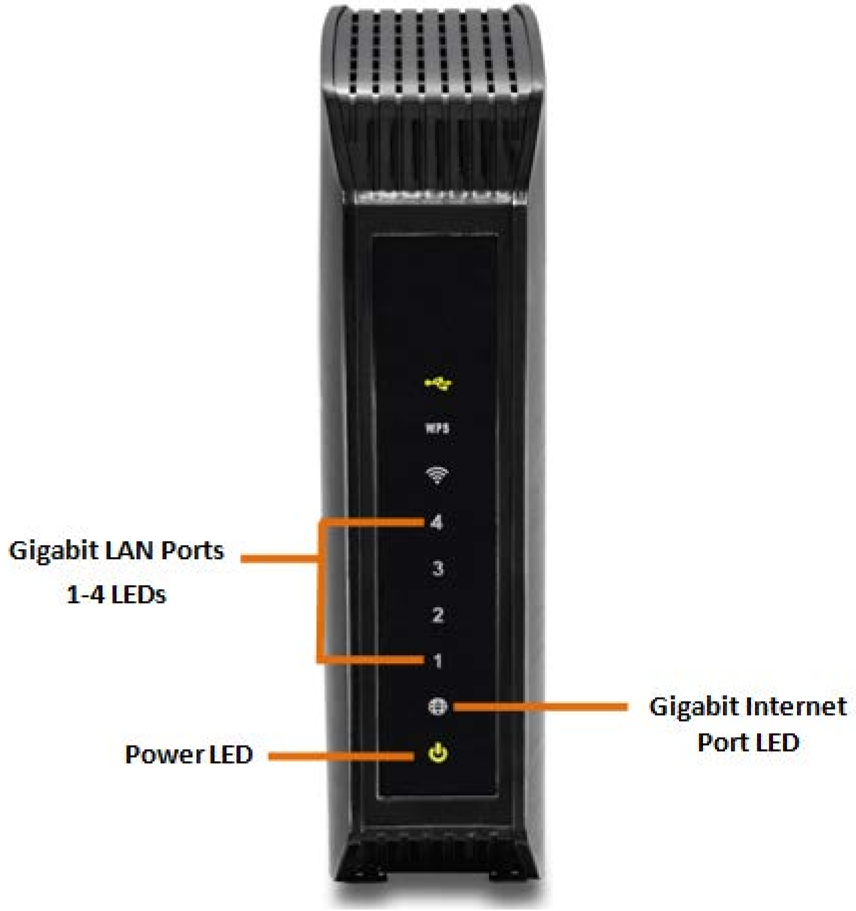


2. Turn off your modem.
3. Disconnect the Network cable from your computer to your modem.
4. Connect your modem to the router Internet port (yellow).
5. Connect your computer to one of the router LAN ports.



6. Connect the power adapter to the router and then to a power outlet.
7. Turn on your modem.

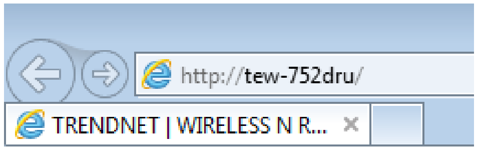
8. Verify that the status LED indicators on the front of the router are illuminated: **Power, Gigabit Internet,** and one of the **Gigabit LAN ports (1,2,3,4)** port where your computer is connected.



Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and the wizard will automatically appear.

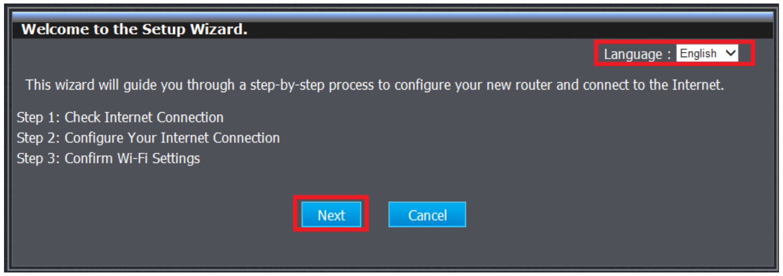
Note: If you have already configured your router before, the wizard will no longer appear automatically. In your web browser, go to http://tew-752dru or you can access the router management using the default IP address http://192.168.10.1. Your router will prompt you for a user name and password. Enter your user name and password and click Main > Wizard.



http://tew-752dru/

TRENDNET | WIRELESS N R...

2. Select your Language and click **Next.**.



Welcome to the Setup Wizard.

Language : English

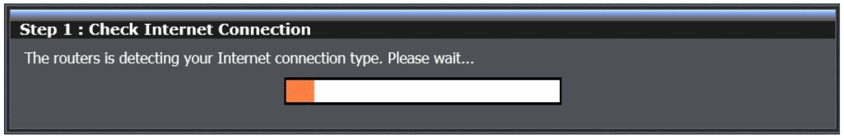
This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

Step 1: Check Internet Connection
Step 2: Configure Your Internet Connection
Step 3: Confirm Wi-Fi Settings

Next Cancel

3. If the wizard is unable to detect your Internet connection type, you will be prompted to select it. Select your Internet connection type and click **Next**.

***Note:** Dynamic IP (DHCP) is typical for most Internet services. You can verify your settings with your Internet Service Provider.*

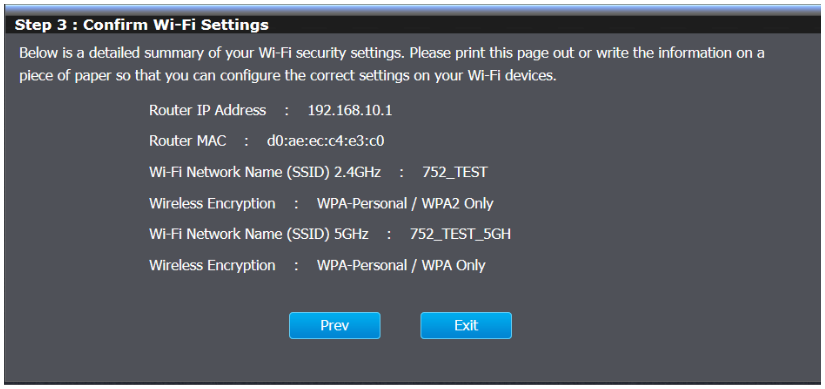


Step 1 : Check Internet Connection

The routers is detecting your Internet connection type. Please wait...

4. Confirm your settings. This window displays your predefined router wireless settings and click **Exit** to complete the wizard**.**

Note: For added security, the router wireless network is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and the pre-assigned network name (SSID) on a sticker on the side of the router and on a label on the bottom of the router. You will need this information to connect to the router. To change the network security key, refer to page 12. If the router is reset to factory defaults, the wireless encryption will reset to the network security key printed on the product labels of the router.



Step 3 : Confirm Wi-Fi Settings

Below is a detailed summary of your Wi-Fi security settings. Please print this page out or write the information on a piece of paper so that you can configure the correct settings on your Wi-Fi devices.

Router IP Address : 192.168.10.1

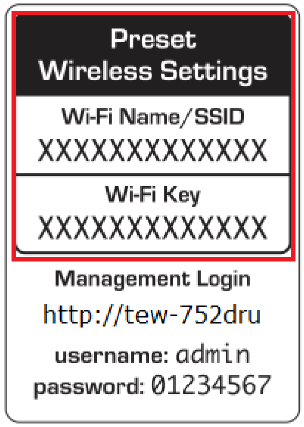
Router MAC : d0:ae:ec:c4:e3:c0

Wi-Fi Network Name (SSID) 2.4GHz : 752_TEST

Wireless Encryption : WPA-Personal / WPA2 Only

Wi-Fi Network Name (SSID) 5GHz : 752_TEST_5GH

Wireless Encryption : WPA-Personal / WPA Only



Preset
Wireless Settings

Wi-Fi Name/SSID
XXXXXXXXXXXXX

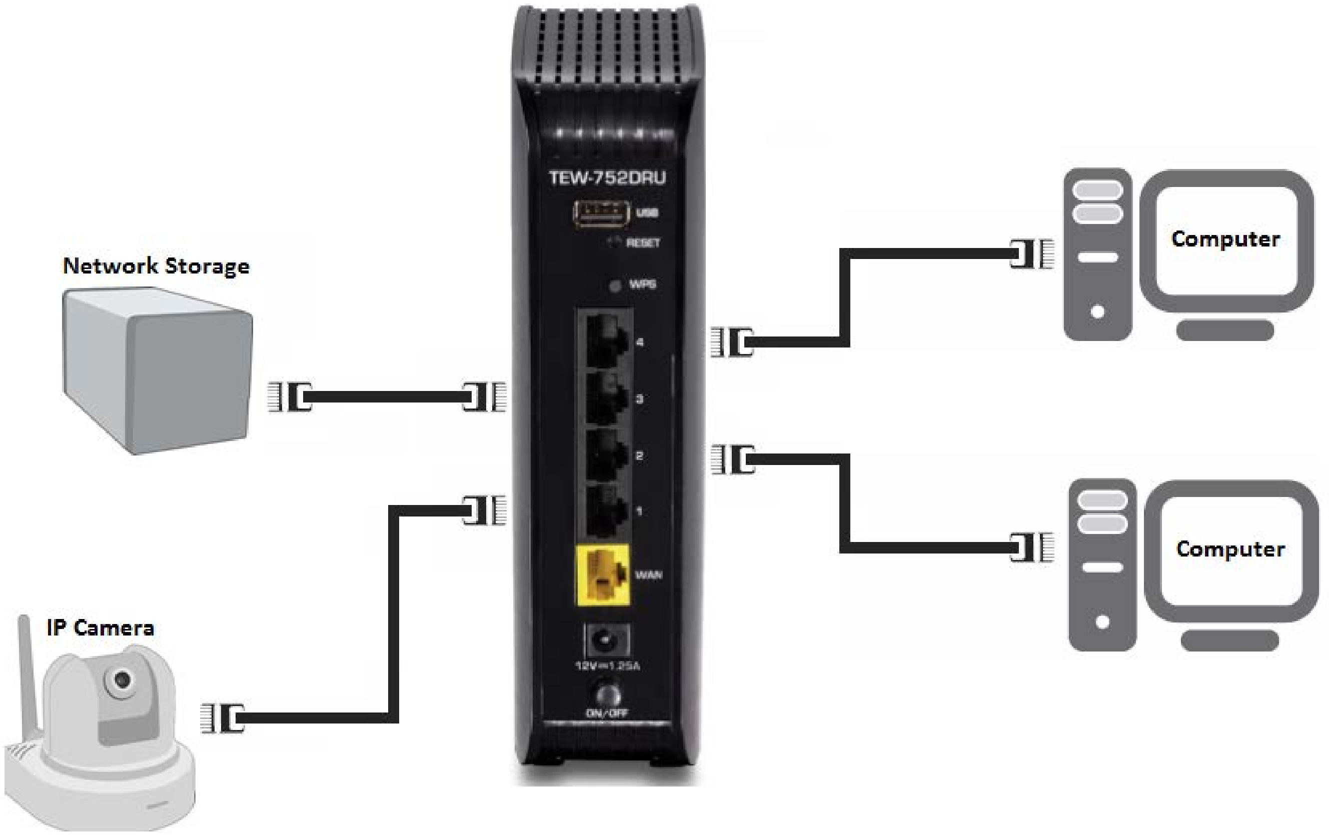
Wi-Fi Key
XXXXXXXXXXXXX

Management Login
http://tew-752dru
username: admin
password: 01234567

Connect additional wired devices to your network

You can connect additional computers or other network enabled devices to your network by using Ethernet cables to connect them to one of the available Gigabit LAN ports labeled 1,2,3,4 on your router. Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device.

Note: *If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured to obtain IP address settings automatically (also called dynamic IP address or DHCP) and to Obtain DNS Server address settings automatically.*



Wireless Networking and Security

How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new router.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware).

It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.).

In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router.
  Note: *This encryption standard will limit connection speeds to 54Mbps.*
- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
  - **WPA-**Auto: This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption. ***Note:*** *WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps*
- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.
  Note: *Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.*Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	**Up to 54Mbps**	**Up to 54Mbps**	**Up to 300Mbps**
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

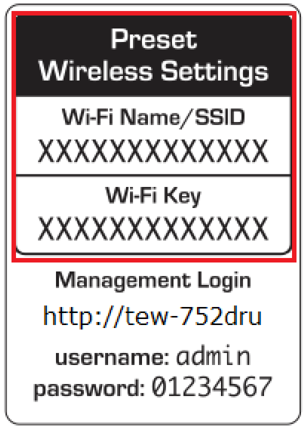
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps)

Secure your wireless network

Wireless > Basic

After you have determined which security type to use for your wireless network (see "How to choose the security type for your wireless network" on page 13), you can set up wireless security.

Note: *By default, your router is configured with a predefined wireless network name (SSID) and security key using WPA2-Personal. The predefined wireless network name and security can be found on the sticker on the side of the router or on the device label at the bottom of the router.*



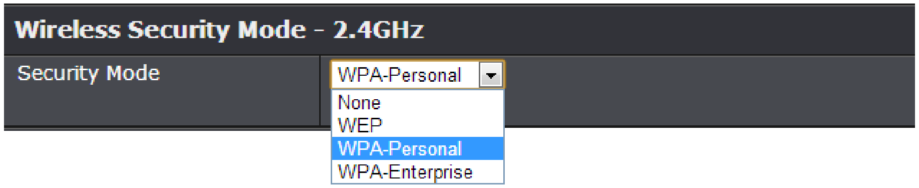
Preset Wireless Settings

Wi-Fi Name/SSID
XXXXXXXXXXXX

Wi-Fi Key
XXXXXXXXXXXX

Management Login
http://tew-752dru
username: admin
password: 01234567

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Wireless**, and click on **Basic**.
3. Under **Wireless Security Mode (2.4GHz or 5GHz)**, click on the **Security Mode** drop-down list to select your wireless security type.

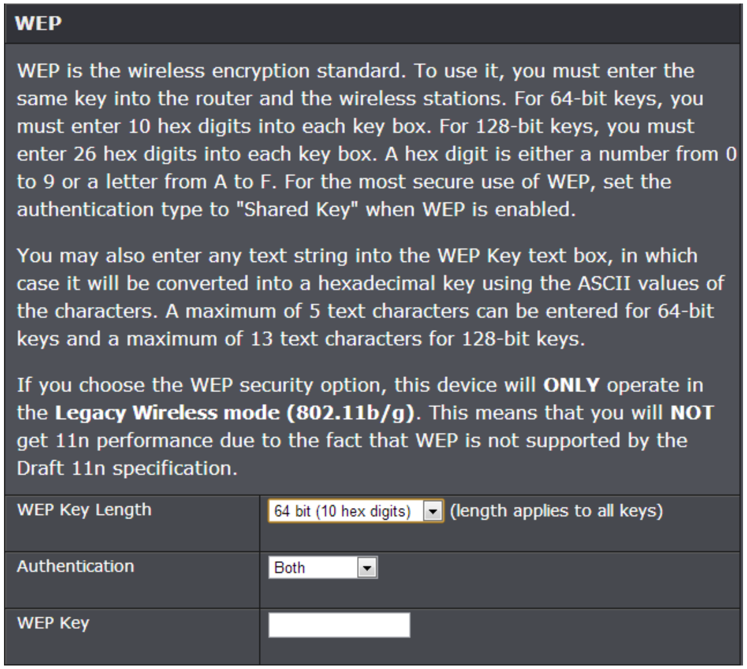


Wireless Security Mode - 2.4GHz

Security Mode: WPA-Personal

Selecting WEP:

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



WEP

WEP is the wireless encryption standard. To use it, you must enter the same key into the router and the wireless stations. For 64-bit keys, you must enter 10 hex digits into each key box. For 128-bit keys, you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP, set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into the WEP Key text box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys and a maximum of 13 text characters for 128-bit keys.

If you choose the WEP security option, this device will **ONLY** operate in the **Legacy Wireless mode (802.11b/g)**. This means that you will **NOT** get 11n performance due to the fact that WEP is not supported by the Draft 11n specification.

WEP Key Length: 64 bit (10 hex digits) (length applies to all keys)

Authentication: Both

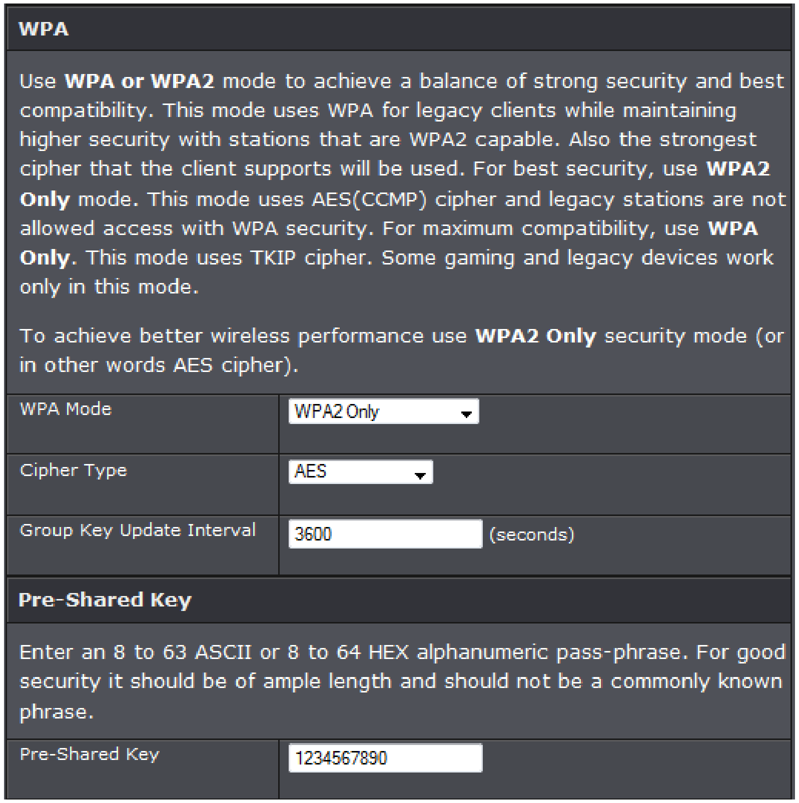
WEP Key:

- **WEP Key Length:** 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.*
- **Authentication:** Choose **Both** or **Shared.**
  Note: *It is recommended to use Both which includes both Open and Shared. Open is known to be more secure than Shared Key.*
- **WEP Key:** Enter the WEP key. This is the password or key that is used to connect your computer to this router wirelessly.

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

Selecting WPA-Personal with Auto (WPA or WPA2)/WPA Only/WPA2 Only (WPA2 Only recommended):

In the **Security Mode** drop-down list, select **WPA-Personal.** Please review the WPA-Personal settings to configure and click **Save Settings** to save the changes.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

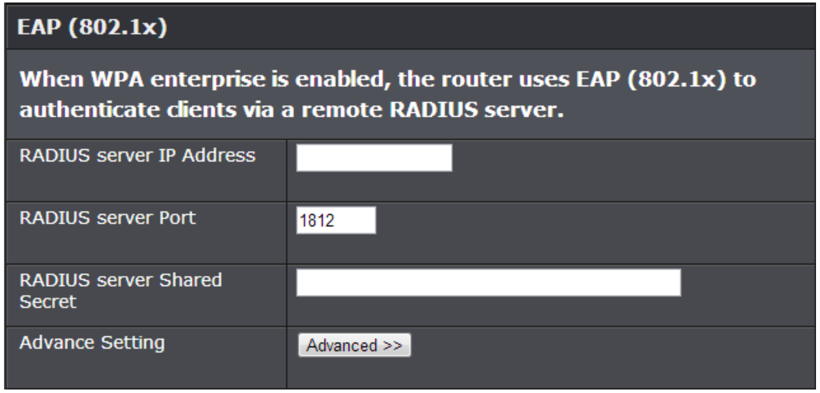
WPA Mode	WPA2 Only
Cipher Type	AES
Group Key Update Interval	3600 (seconds)

Pre-Shared Key

Enter an 8 to 63 ASCII or 8 to 64 HEX alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key	1234567890

Selecting WPA-Enterprise with Auto (WPA or WPA2)/WPA Only/WPA2 Only (WPA2 Only recommended):



EAP (802.1x)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address	
RADIUS server Port	1812
RADIUS server Shared Secret	
Advance Setting	Advanced >>

The following section outlines options when selecting **WPA-Enterprise** (EAP or RADIUS). This security type is also known as EAP (Extensible Authentication Protocol) or Remote Authentication Dial-In User Service or RADIUS.

Note: *This security type requires an external RADIUS server, Pre-Shared Key only requires you to create a passphrase.*

- **RADIUS Server Address:** Enter the IP address of the RADIUS server. (e.g. *192.168.10.250)*
- **RADIUS Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
  Note: *It is recommended to use port 1812 which is typical default RADIUS port.*
- **RADIUS Server Shared Secret:** Enter the shared secret used to authorize your router with your RADIUS server.
- **Advance Setting** – Click this option to set up an additional backup RADIUS server.

Connect wireless devices to your router

A variety of wireless network devices can connect to your wireless network such as:

- Gaming Consoles
- Internet enabled TVs
- Network media players
- Smart Phones
- Wireless Laptop computers
- Wireless IP cameras

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this router's wireless network.

See the "Appendix" on page 53 for general information on connecting to a wireless network.

Connect wireless devices using WPS

WPS (Wi-Fi Protected Setup) is a feature that makes it easy to connect devices to your wireless network. If your wireless devices support WPS, you can use this feature to easily add wireless devices to your network.

***Note:** You will not be able to use WPS if you set the SSID Broadcast setting to Disabled or if you are using WEP security.*

There are two methods the WPS feature can easily connect your wireless devices to your network.

- Push Button Configuration (PBC) method
  - (RECOMMENDED) Hardware Push Button method–with an external button located physically on your router and on your client device
  - WPS Software/Virtual Push Button - located in router management page
- PIN (Personal Identification Number) Method - located in router management page

  ***Note:** Refer to your wireless device documentation for details on the operation of WPS.*

Recommended Hardware Push Button (PBC) Method

- ***Note:*** It is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. By default your router is preconfigured with a wireless encryption key. If no wireless key is defined when connecting via PBC, the router will automatically create an encryption key that is 64 characters long. This 64 character key will then have to be used if one has to connect computers to the router using the traditional connection method.

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. The WPS LED will blink to indicate WPS has been activated on your router. (See "Product Hardware Features" on page 5)

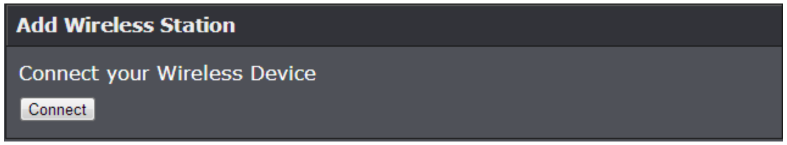
For connecting additional WPS supported devices, repeat this process for each additional device.

PBC (Software/Virtual Push Button)

Wireless > Wi-Fi Protected Setup

In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

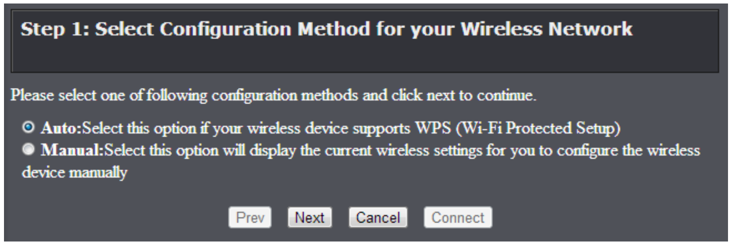
1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Wireless**, and click on **Wi-Fi Protected Setup**.
3. To add a wireless device to your network, click the **Connect** button in the router management page.



Add Wireless Station

Connect your Wireless Device

4. Make sure **Auto** is selected and click **Next**.

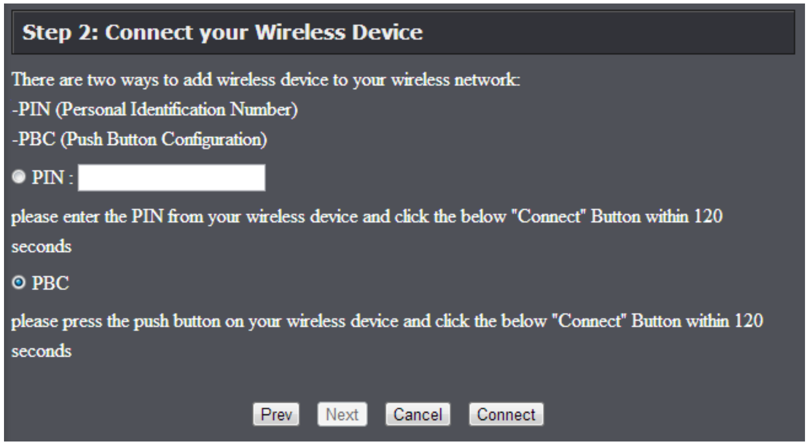


Step 1: Select Configuration Method for your Wireless Network

Please select one of following configuration methods and click next to continue.

◉ **Auto:**Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)
○ **Manual:**Select this option will display the current wireless settings for you to configure the wireless device manually

5. Select **PBC** and click **Connect**. Then push the WPS button on the wireless device (consult wireless device's User's Guide for length of time) you are connecting.



Step 2: Connect your Wireless Device

There are two ways to add wireless device to your wireless network:
-PIN (Personal Identification Number)
-PBC (Push Button Configuration)

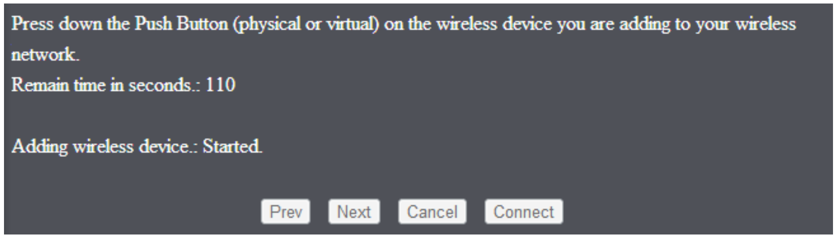
○ PIN :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

◉ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

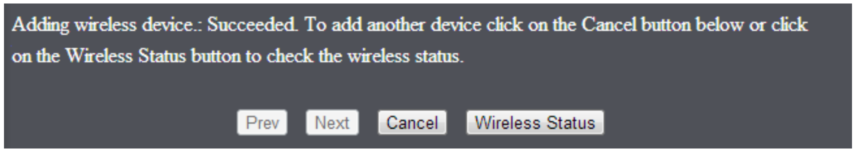
6. Wait for your router to finsh the WPS process.



Press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network.
Remain time in seconds.: 110

Adding wireless device.: Started.

7. If successful, you will receive the message below. Click on **Wireless Status** to view the information about the current wireless client devices connected to your router.



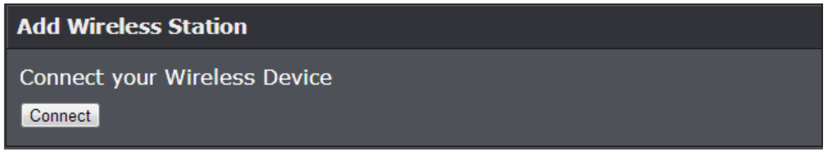
Adding wireless device.: Succeeded. To add another device click on the Cancel button below or click on the Wireless Status button to check the wireless status.

PIN (Personal Identification Number)

Wireless > Wi-Fi Protected Setup

If your wireless device has WPS PIN (typically an 8-digit code printed on the wireless device product label or located in the wireless device wireless software utility), you can use this method.

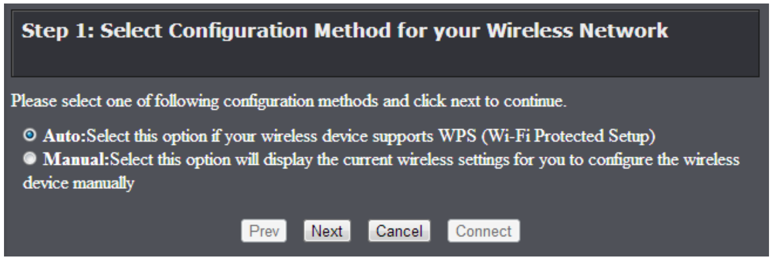
1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Wireless**, and click on **Wi-Fi Protected Setup**.
3. To add a wireless device to your network, click the **Connect** button in the router management page.



Add Wireless Station

Connect your Wireless Device

4. Make sure **Auto** is selected and click **Next**.



Step 1: Select Configuration Method for your Wireless Network

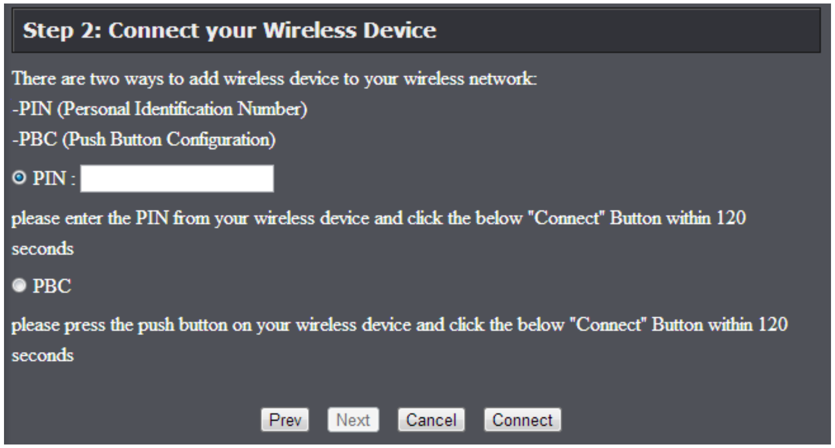
Please select one of following configuration methods and click next to continue.

● **Auto:**Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

○ **Manual:**Select this option will display the current wireless settings for you to configure the wireless device manually

5. Select **PIN** and enter the 8-digit numeric PIN number of the wireless client device and click **Connect**.

Note: *You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.*



Step 2: Connect your Wireless Device

There are two ways to add wireless device to your wireless network:

-PIN (Personal Identification Number)

-PBC (Push Button Configuration)

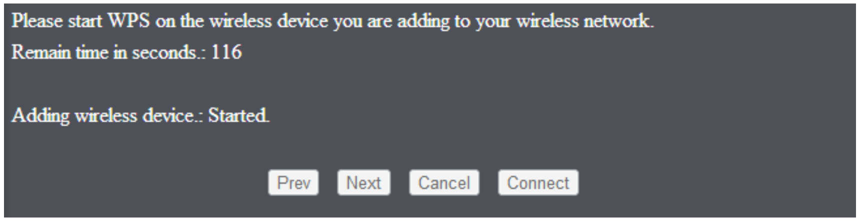
● PIN :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

○ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

6. Wait for your router to finsh the WPS process.

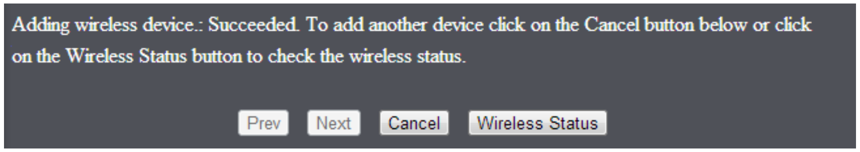


Please start WPS on the wireless device you are adding to your wireless network.

Remain time in seconds.: 116

Adding wireless device.: Started.

7. If successful, you will receive the message below. Click on **Wireless Status** to view the information about the current wireless client devices connected to your router.



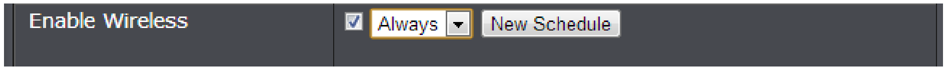
Adding wireless device.: Succeeded. To add another device click on the Cancel button below or click on the Wireless Status button to check the wireless status.

Basic wireless settings

Wireless > Basic

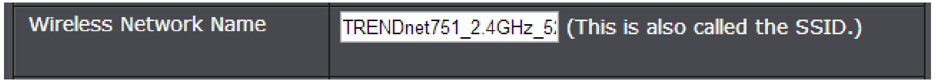
This section outlines available management options under basic wireless sub tab for both 2.4GHz and 5GHz wireless sections.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Wireless** and click on **Basic** scroll down to **Wireless Network Settings** (2.4GHz or 5GHz)
3. To save changes to this section, click **Save Settings** when finished.
   - **Enable Wireless:** Check the option to enable the wireless or uncheck to disable. ***Note:*** *It is recommended to leave this setting checked.*
     - **New Schedule:** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **New Schedule** and refer to page 35. After you have created a new schedule, click the drop-down list and the new schedule will be available for selection.



Enable Wireless ☑ Always New Schedule

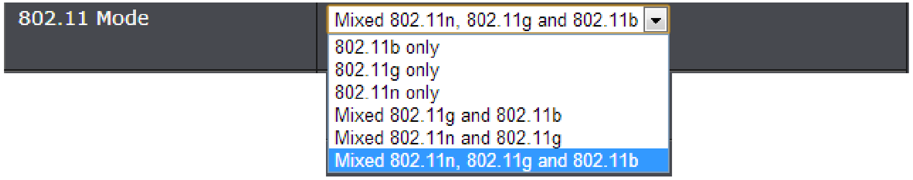
   - **Wireless Network Name (SSID):** Enter the wireless name (SSID) for your wireless network. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.



Wireless Network Name TRENDnet751_2.4GHz_5: (This is also called the SSID.)

When applying the 802.11 Mode setting, please keep in mind the following:

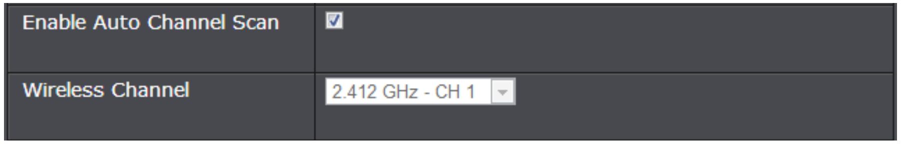
- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.



802.11 Mode Mixed 802.11n, 802.11g and 802.11b

802.11b only
802.11g only
802.11n only
Mixed 802.11g and 802.11b
Mixed 802.11n and 802.11g
Mixed 802.11n, 802.11g and 802.11b

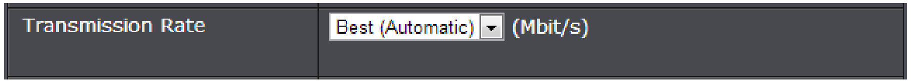
- **Enable Auto Channel Scan:** Check this option to set your router to scan for which wireless channels to use automatically.
- **Wireless Channel:** Unchecking the **Enable Auto Channel Scan** option will you to manually set the channel on which the router will broadcast. Click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.



Enable Auto Channel Scan ☑

Wireless Channel 2.412 GHz - CH 1

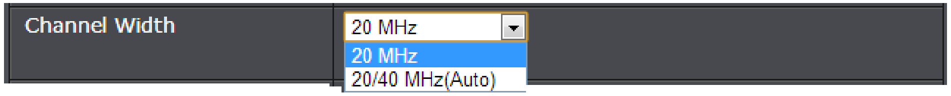
- **Transmission Rate –** Allows you to lock down the wireless transmission rate. ***Note:*** *This feature is only available when using 802.11 n only mode.*



Transmission Rate Best (Automatic) (Mbit/s)

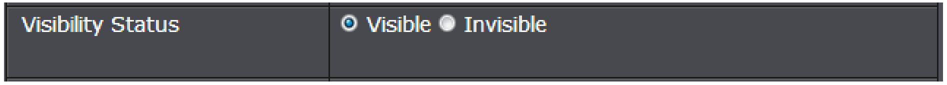
- **Channel Width:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n. For greater 802.11n performance, select **20/40MHz (Auto)** (Options: 20MHz or 20/40MHz (Auto)). It is recommended to use the default channel bandwidth settings.
  Note: *Please note that this setting may provide more stability than the higher channel bandwidth settings such as* 20/40MHz (Auto) *for connectivity in busy wireless environments where there are several wireless networks in the area.*
  - **20 MHz:** This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than 20/40MHz (Auto) for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.

- **20/40MHz (Auto):** When 20/40MHz (Auto) is active, this mode is capable of providing higher performance only if the wireless devices support the channel bandwidth settings. Enabling 20/40MHz (Auto) typically results in substantial performance increases when connecting an 802.11n client.



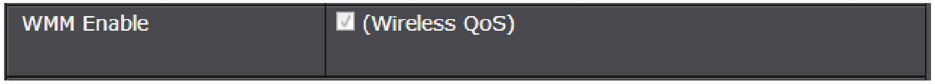
Channel Width	20 MHz ▾ 20 MHz 20/40 MHz(Auto)

- **Visibility Status**
  - **Visible:** **A**llows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
  - **Invisible:** Turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network. Disabling this setting will disable WPS functionality.



Visibility Status	● Visible ○ Invisible

  - **WMM:** Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your router. ***Note:*** *This feature can only be disabled in 802.11b/g modes.*



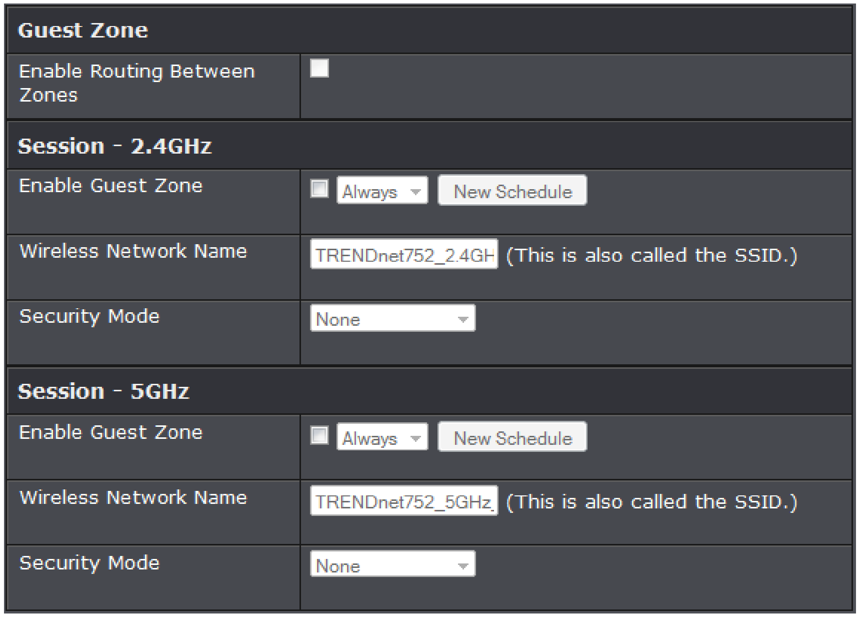
WMM Enable	☑ (Wireless QoS)

Guest Network

Access > Guest Zone

Creating an isolated and separate wireless guest network (2.4GHz or 5GHz) allows wireless clients to connect to your network for Internet access only and keep your local LAN network safe by restricting guest access to your LAN network resources such as shared documents and media files on your computers, network storage, and printers.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access** and click on **Guest Zone**.
3. Review the Guest Zone settings, click **Save Settings** when finished.



Guest Zone	
Enable Routing Between Zones	□
Session - 2.4GHz	
Enable Guest Zone	□ Always ▾ New Schedule
Wireless Network Name	TRENDnet752_2.4GH (This is also called the SSID.)
Security Mode	None ▾
Session - 5GHz	
Enable Guest Zone	□ Always ▾ New Schedule
Wireless Network Name	TRENDnet752_5GHz_ (This is also called the SSID.)
Security Mode	None ▾

- **Enable Routing Between Zones:** If checked, allows wireless clients connected to the guest network access to your private LAN network.

Choose which band to enable the Guest Network (Wireless – 2.4GHz or 5GHz):

- **Enable Guest Zone:** Check the option to enable the guest network.
- **New Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).
  Note: *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 34 to configure Time Settings and see page 35 to create a schedule.*
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. It is recommended to use a different name from your primary wireless network to a name that you can easily identify and differentiate from the primary. You can reference your guests to access this network instead of the primary.
- **Security Mode:** Select the wireless security to use for the guest network.

4. Under Security Mode, you can apply a different wireless security type and key to the guest network. Please refer to page 12 to find out about different security types and page 13 for wireless security configuration.

Steps to improve wireless connectivity

There are a number of factors that can impact the range of wireless devices. Follow these tips to help improve your wireless connectivity:

1. 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.
    a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
    b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
    c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
    d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
    e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.

2. 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.
3. 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.
4. 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.

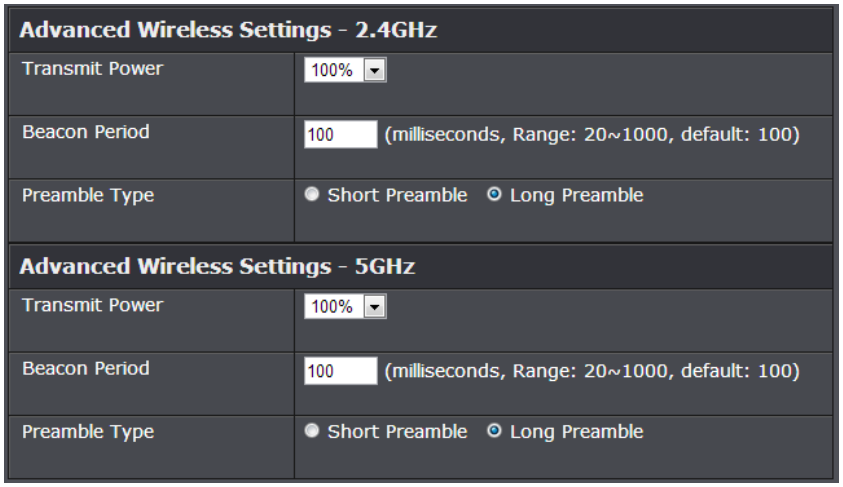
If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n or 802.11ac. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal consider repositioning the wireless devices, installing additional access points or wireless extenders.

Advanced wireless settings

Wireless > Advanced

These settings are advanced options that can be configured to change advanced wireless broadcast specifications. It is recommended that these settings remain set to their default values unless you are knowledgeable about the effects of changing these values. Changing these settings incorrectly can degrade performance.

- **Transmit Power:** This setting allows you to adjust the wireless transmit power to a lower setting. In busy wireless environments, lowering the transmit power may improve better performance and connectivity and decrease interference with neighboring wireless networks.
- **Beacon Period:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.
  Default Value: 100 milliseconds (range: 20-1000)
- **Preamble Type:** Select the option that works best for your installation. It may be best to keep this option at its default setting.
  - **Short Preamble:** Using a short guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections.
  - **Long Preamble:** Using a long preamble can help to decrease the error rate in wireless data transmission and receiving.



Advanced Wireless Settings - 2.4GHz	
Transmit Power	100%
Beacon Period	100 (milliseconds, Range: 20~1000, default: 100)
Preamble Type	○ Short Preamble ● Long Preamble

Advanced Wireless Settings - 5GHz	
Transmit Power	100%
Beacon Period	100 (milliseconds, Range: 20~1000, default: 100)
Preamble Type	○ Short Preamble ● Long Preamble

Access Control Filters

Access control basics

MAC Address Filters

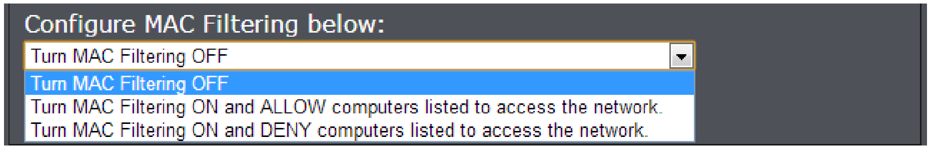
Access > MAC Filters

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this router's wired or wireless network. You can enter up to 24 MAC address entries.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access**, click on **MAC Filters.**
3. Review the MAC Filter options, click **Save Settings** to save settings.

Click the **Configuring MAC Filtering below** drop-down list to choose the MAC filter function.

- **Turn MAC Filtering OFF:** disables the MAC address filter.
- **Turn MAC Filtering ON and ALLOW computers listed to access the network** Only **Allow** computers/devices with MAC addresses listed to access the router management page and the Internet. Deny all others. **Turn MAC Filtering ON and DENY computers listed to access the network**
  Only **Deny** computers/devices with MAC addresses listed to access to the router management page and the Internet. Allow all others.



Configure MAC Filtering below:

Turn MAC Filtering OFF

Turn MAC Filtering OFF
Turn MAC Filtering ON and ALLOW computers listed to access the network.
Turn MAC Filtering ON and DENY computers listed to access the network.

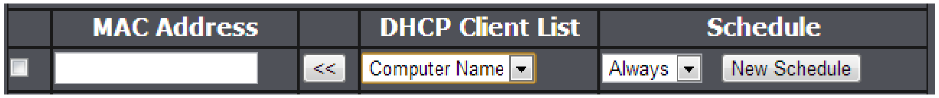
***Note:** MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access.*

Before saving settings, add the MAC addresses to the MAC Table and configure the options first.

- **MAC Address:** Check the box next to the entry to enable and in the empty field, enter the MAC address of the devices you would like to filter.

  (e.g. 00:11:22:AA:BB:CC)
- **DHCP Client List:** Click the drop-down list to select from the list of client devices connected to your router. Once selected, click **<<** to copy the MAC address of the selected device to MAC Address field.
- **New Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).

  Note: *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 34 to configure Time Settings and see page 35 to create a schedule.*



	MAC Address		DHCP Client List	Schedule
☐		<<	Computer Name ▾	Always ▾ New Schedule

Note: *If you device is not listed, please refer to your computer or device documentation to find the MAC address.*

Parental Control

Access > Parental Control

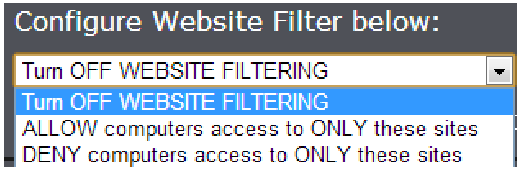
You may want to block computers or devices on your network access to specific websites (e.g. *www.xxxxxxxx.com, etc.)*, also called domains or URLs (Uniform Resource Locators). You may also enter a keyword (e.g. instead of complete URL to generally block computers or devices access to websites that may contain the keyword in the URL or on the web page. You may also apply a schedule when these websites are allowed or denied. You can enter up to 40 parental control entries.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access**, click on **Parental Control.**
3. Review the settings under **Parental Control** section. Click **Save Settings** to save settings.

Click the **Configuring MAC Filtering below** drop-down list to choose the MAC filter function.

- **Turn OFF WEBSITE FILTERING:** disables the website filtering.
- **ALLOW computers access to ONLY these sites:** Only **Allow** computers/devices access to the listed websites/keywords and deny access to others.
- **DENY computers access to ONLY these sites**

  Only **Deny** computers/devices access to the listed websites/keywords and allow access to others.



Configure Website Filter below:

Turn OFF WEBSITE FILTERING ▾

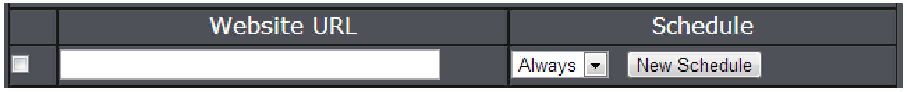
Turn OFF WEBSITE FILTERING
ALLOW computers access to ONLY these sites
DENY computers access to ONLY these sites

Before saving settings, enter the website URLs/domains/keywords and configure the options first.

- **Website URL:** Check the box next to the entry to enable and in the empty field, enter the website URL/domain/keyword you would like to filter.

  (e.g. *www.xxxxxxxx.com, xxxxxxxx)*
- **New Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).

  Note: *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 34 to configure Time Settings and see page 35 to create a schedule.*



	Website URL	Schedule
☐		Always ▾ New Schedule

Firewall Rules

Access > Firewall & DMZ

You may want specify inbound or outbound access control to allow/deny sources (or Internet IP addresses) to your network from the Internet or from computers or devices on your network to the Internet. Firewall rules may allow for more granular control of specific inbound and outbound access between your network and the Internet. It is recommended that these settings remain set to default unless you are knowledgeable about the effects of changing the firewall rule configuration. It is possible to have undesirable functionality from your router if these settings are improperly modified. You can enter up to 32 firewall rule entries.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, click on **Firewall & DMZ.**

3. Review the settings under **Firewall Rules** section. Click **Save Settings** to save settings.

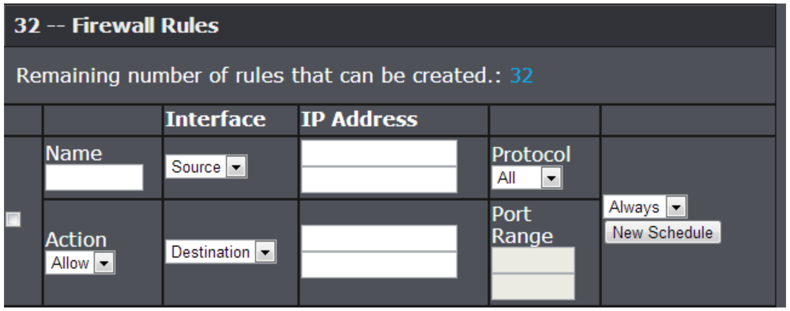
Check the box next to the firewall rule entry to enable it. Uncheck the option to disable the firewall rule entry.

- **Name:** Enter a name for the firewall rule.
- **Action:** Select **Allow** will allow access and selecting **Deny** will block or deny access.
- **Interface (Source):** Click the drop-down list and select **LAN** (from your network) or **WAN** (from the Internet) depending on where the traffic will be coming from.
- **IP Address (Source):** Enter the IP address or IP address range to apply the protocol (e.g. *192.168.1.20-192.168.1.20* or *192.168.1.20-192.168.1.30)*. To specify all IP address, enter an asterisk ***** .

  Note: *The filter will not be applied to IP addresses outside of the range specified.*

- **Interface (Destination):** Click the drop-down list and select **LAN** (your network) or **WAN** (Internet) depending on where the traffic will be coming from.
- **IP Address (Destination):** Enter the IP address or IP address range to apply the protocol (e.g. *192.168.10.20-192.168.10.20* or *192.168.10.20-192.168.10.30)*. To specify all IP address, enter an asterisk ***** .
- **Protocol:** Select the protocol type to filter. **TCP, UDP, ICMP**, or **All**.
- **Port Range:** If selecting **TCP** or **UDP** protocol, enter the port number or range of port numbers to apply in the firewall rule. (e.g. *80-80* or *20-21*). For all ports, use the port range 1 - *65535.*
- **New Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).

Note: *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 34 to configure Time Settings and see page 34 to Create Schedule.*



32 -- Firewall Rules

Remaining number of rules that can be created.: 32

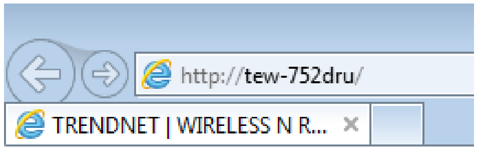
		Interface	IP Address		
☐	Name	Source		Protocol All	Always New Schedule
	Action Allow	Destination		Port Range	

Advanced Router Setup

Access your router management page

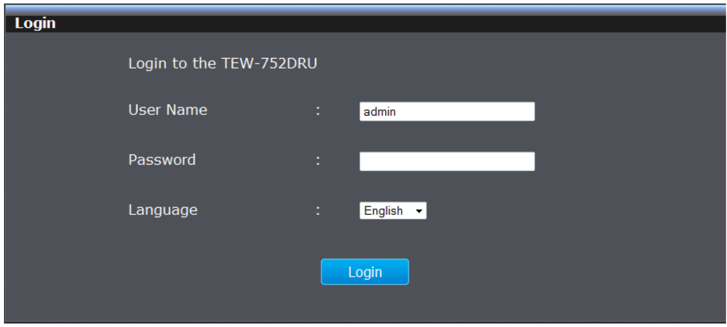
Note: *Your router management page URL/domain name http://tew-752dru or IP address http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.*

1. Open your web browser and go to URL/domain name http://tew-752dru or IP address http://192.168.10.1. Your router will prompt you for a user name and password.



2. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router. Enter your **Username** and **Password**, select your preferred language, then click **Login**.

User Name: **admin**
Password: **(xxxxxxxx)**
Note: *User Name and Password are case sensitive.*

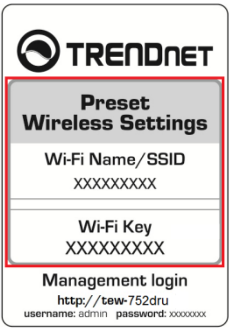

Login

Login to the TEW-752DRU

User Name : admin

Password :

Language : English



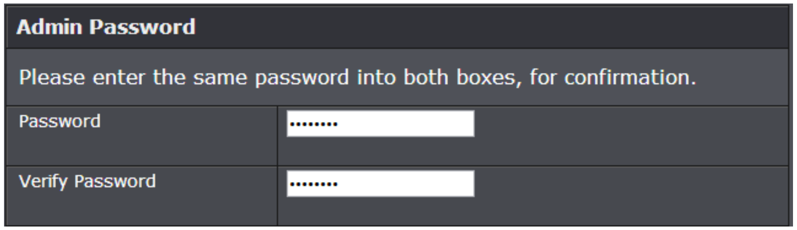
Change your router login password

Main > Password

1. Log into your router management page (see "[Access your router management page](#)" on page 25).

2. Click on **Main**, and click on **Password**.

3. Under the **Admin Password** section, in the **Password** field, enter the new password and enter the password again in the **Verify Password** field to confirm.


Admin Password

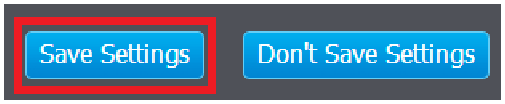
Please enter the same password into both boxes, for confirmation.

Password ••••••••

Verify Password ••••••••

3. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click **Don't Save Settings.***



Note: *If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the predefined default password. If you reset the device to defaults, you will need to access the router management page use the predefined settings on the side or bottom labels.*

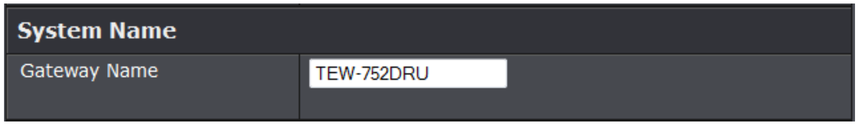
Change your device name

Main > Password

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **Password**.

3. Under the **System Name** section, in the **Gateway Name** field, enter the new device name to display on your network to identify the router.

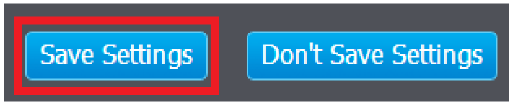


System Name

Gateway Name: TEW-752DRU

3. To save changes, click **Save Settings**.

Note:** If you would like to discard the changes, click **Don't Save Settings.



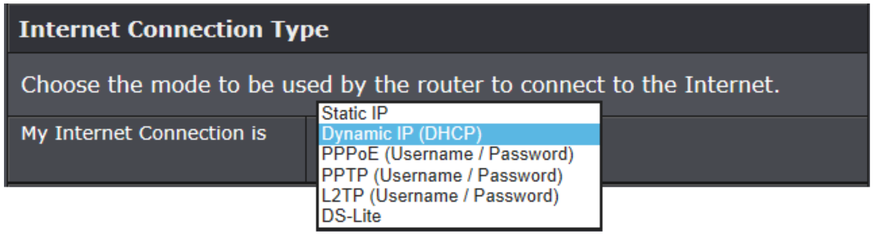
Manually configure your Internet connection

Main > WAN

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **WAN**.

3. Under **Internet Connection Type** in drop-down list, select the type of Internet connection provided by your Internet Service Provider (ISP).



Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is: Dynamic IP (DHCP)

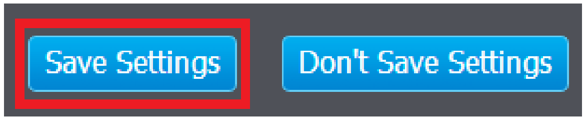
Static IP
Dynamic IP (DHCP)
PPPoE (Username / Password)
PPTP (Username / Password)
L2TP (Username / Password)
DS-Lite

4. Complete the fields required by your ISP.

5. Complete the optional settings only if required by your ISP.

6. To save changes, click **Save Settings**.

Note:** If you would like to discard the changes, click **Don't Save Settings.



***Note:** If you are unsure which Internet connection type you are using, please contact your ISP.*

IPv6 Connection Settings

Main > IPv6

IPv6 (Internet Protocol Version 6) is a new protocol that significantly increases the number of available Internet public IP addresses due to the 128-bit IP address structure versus IPv4 32-bit address structure. In addition, there are several integrated enhancements compared to the most commonly used and well known IPv4 (Internet Protocol Version 4) such as:

- Integrated IPsec: Better Security
- Integrated Quality of Service (QoS): Lower latency for real-time applications
- Higher Efficiency of Routing: Less transmission overhead and smaller routing tables
- Easier configuration of addressing

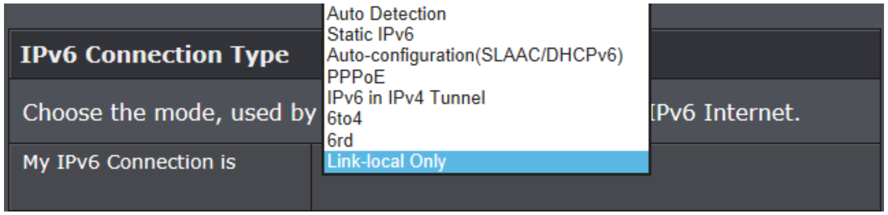
Note: *In order to use IPv6 Internet connection settings, it is required that your ISP provide you with the IPv6 service. Please contact your ISP for availability and more information about the IPv6 service.*

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **IPv6**.

3. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP. Click **Save Settings** to save changes.

Note: *Please contact your ISP for IPv6 service availability.*



Select the IPv6 connection type provided by your ISP.Auto Detection

- Static IPv6
- Auto-configuration (SLAAC/DHCPv6)
- PPPoE
- IPv6 in IPv4 Tunnel
- 6to4
- 6rd
- Link-Local Only

Clone a MAC address

Main > WAN

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and to prevent the re-provisioning and registration process of a new MAC address with your ISP, then you can clone the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from the previous device (computer or old router that directly connected to the modem, you should first determine the MAC address of the device or computer and manually enter it into your router using the clone MAC address feature.

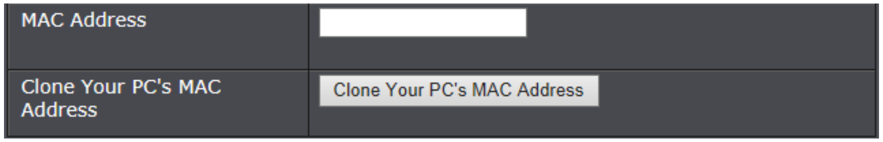
Note: *For many ISPs that provide dynamic IP addresses automatically, typically, the stored MAC address in the modem is reset each time you restart the modem. If you are installing this router for the first time, turn your modem before connecting the router to your modem. To clear your modem stored MAC address, typically the procedure is to disconnect power from the modem for approximately one minute, then reconnect the power. For more details on this procedure, refer to your modem's User Guide/Manual or contact your ISP.*

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **WAN**.

3. Next to MAC Address field, click **Clone Your PC's MAC Address** to copy your computer's MAC address in the **MAC Address** field.

Note: *You can also check the DHCP Client List for the MAC addresses of the devices on your network, see page 29 or refer to your computer or device documentation to find the MAC address.*



MAC Address

Clone Your PC's MAC Address: Clone Your PC's MAC Address

3. To save changes, click **Save Settings**.

Change your router IP address

Main > LAN

In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

Note: *If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.*

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

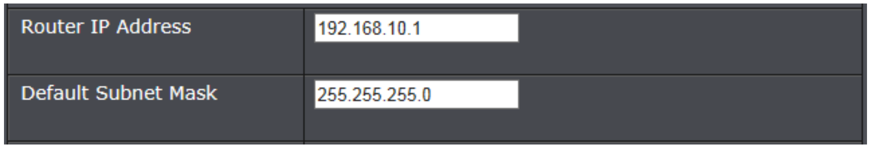
1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **LAN Setting**.

3. In **LAN Interface Setting** section, Enter the router IP address settings.

- **Router IP Address:** Enter the new router IP address. (e.g. *192.168.200.1*)
- **Default Subnet Mask:** Enter the new router subnet mask. (e.g. *255.255.255.0*)

  Note: *The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.*



Router IP Address: 192.168.10.1

Default Subnet Mask: 255.255.255.0

4. To save changes, click **Save Settings**.

Note: *You will need to access your router management page using your new router IP address. (e.g. Instead of using the default http://192.168.10.1 your new router IP address will use the following format using your new IP address http://(new.ipaddress.here) to access your router management page. You can also use the default login URL http://tew-752dru*

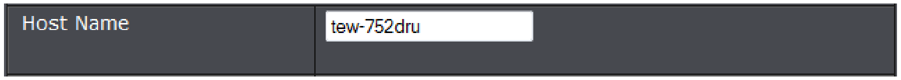
Change your device URL

Main > LAN

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **LAN**.

3. Next to **Host Name**, enter the new name used to access your router management page. (*e.g. "myrouter" will use http://myrouter to access the router management page.)*



Host Name: tew-752dru

Note: *Even if the LAN IP address of the router is changed, the device URL will still allow to use the name as reference to log into the router management page.*

4. To save changes, click **Save Settings**.

Enable DNS relay on your router

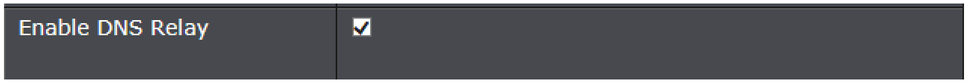
Network > LAN Setting

DNS (Domain Name System) is protocol used for resolving IP addresses to domain names such as www.trendnet.com. In order for computers to be able to access domain names, your computer requires a DNS server or directory IP addresses to domain names. Your router can be used as a DNS relay server to an actual DNS server available on the Internet. This can improve the speed in which your computer is able to resolve these domain names by acting as a relay instead of your computer having to communicate directly with an Internet DNS server. Your router uses the WAN DNS servers issues or assigned by your ISP as the outside DNS server. It is recommended to leave this setting enabled.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **LAN**.

3. Next to **Enable DNS Relay**, check the option to enable or uncheck to disable.



Enable DNS Relay	☑

4. To save changes, click **Save Settings**.

Change your local domain name

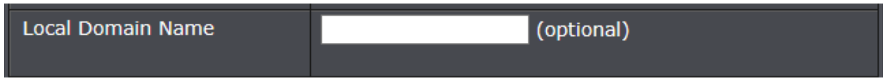
Main > LAN

DNS (Domain Name System) is protocol used for resolving IP addresses to domain names such as www.trendnet.com. In order for computers to be able to access domain names, your computer requires a DNS server or directory IP addresses to domain names. Your router can be to provide your LAN computers with local domain information such as trendnet.com. This is an optional setting and is not required to be configured for basic operation.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Main**, and click on **LAN**.

3. Next to **Local Domain Name (Optional)**, enter the domain name you would like to assign to your local LAN computers.



Local Domain Name	(optional)

4. To save changes, click **Save Settings**.

Set up the DHCP server on your router

Main > LAN

Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you can disable this setting. It is recommended to leave this setting enabled.

1. Log into your router management page (see "Access your router management page" on page 25).

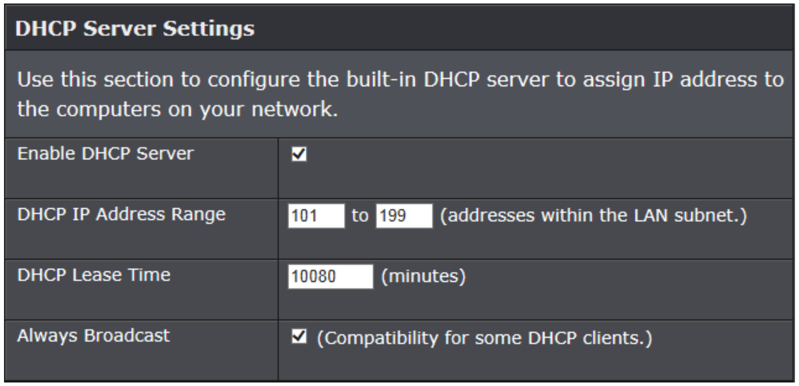
2. Click on **Main**, and click on **LAN**.

3. Review the DHCP Server settings. Click **Save Settings** to save settings.

- **Enable DHCP Server:** Enable or Disable the DHCP server.
- **DHCP IP Address Range:** Changes the starting address and ending address for the DHCP server range. (e.g.*192.168.10.20 to 192.168.10.30)*

  Note: *The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*
- **DHCP Lease Time:** Enter the DHCP lease time in minutes.

  Note: *The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.*

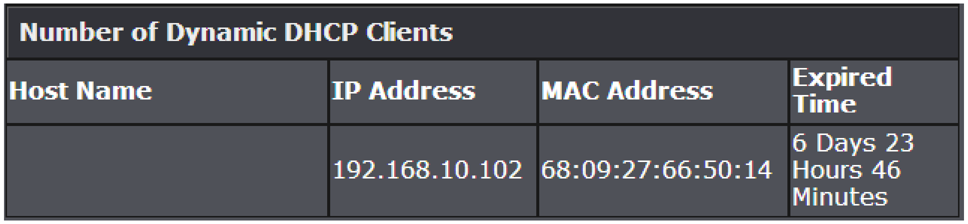


DHCP Server Settings

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server	☑
DHCP IP Address Range	101 to 199 (addresses within the LAN subnet.)
DHCP Lease Time	10080 (minutes)
Always Broadcast	☑ (Compatibility for some DHCP clients.)

You can also view the current DHCP clients in the **Number of Dynamic DHCP Clients** list.



Number of Dynamic DHCP Clients

Host Name	IP Address	MAC Address	Expired Time
	192.168.10.102	68:09:27:66:50:14	6 Days 23 Hours 46 Minutes

Set up DHCP reservation

Main > LAN

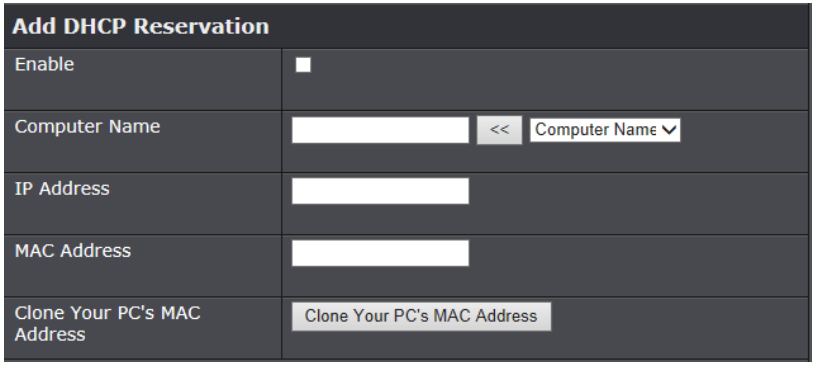
DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see "Virtual Server" on page 35) or special applications (also called port triggering, see "Special Applications" on page 37).

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Main**, and click on **LAN**.
3. Review the DHCP reservation settings.

- **Enable:** Enable or Disable the DHCP reservation.
- **Computer Name:** Enter a name of the device you will assign the DHCP reservation. ***Note:*** *You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.*
- **IP Address:** Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)

  Note: *You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.*
- **MAC Address:** Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC)*

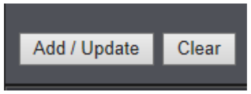
  Note: *You can click Clone your PC's MAC Address to copy the current computer's MAC address into the MAC address field.*



Add DHCP Reservation

Enable	□
Computer Name	[ ] << Computer Name ▾
IP Address	[ ]
MAC Address	[ ]
Clone Your PC's MAC Address	Clone Your PC's MAC Address

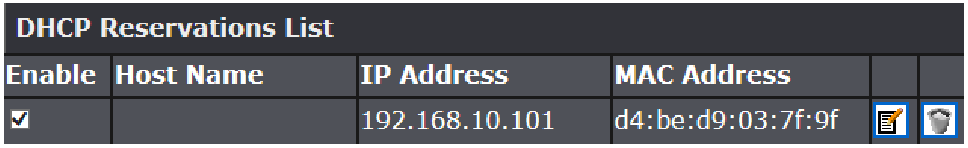
Click **Add/Update** - Saves the reservation.
Note: *Click Clear discards and erases the current information.*



You will see the new reservation added to the DHCP Reservation List.

You can check the **Enable** option to enable the reservation or uncheck to disable.

You can click the 📝 icon to edit the reservation or 🗑 to delete the reservation.



DHCP Reservations List

Enable	Host Name	IP Address	MAC Address		
☑		192.168.10.101	d4:be:d9:03:7f:9f	📝	🗑

To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click* ***Don't Save Settings.***

Enable/disable UPnP on your router

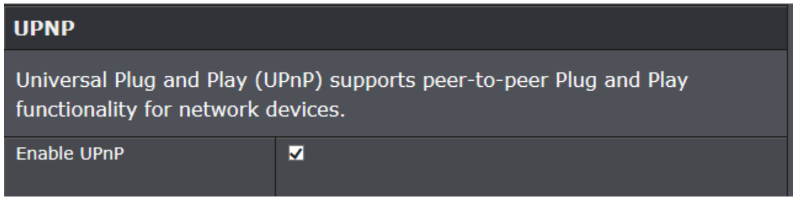
Access > Advanced Network

UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP is enabled on your router by default to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Advanced Network**.

3. Under the **UPnP** section , check the option to enable UPnP or uncheck to disable UPnP.



UPNP

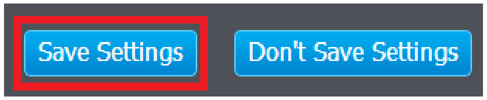
Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP	☑

Note: *It is recommended to leave this setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.*

4. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click **Don't Save Settings.***



Enable/disable Application Layer Gateways (ALG)

Access > Firewall & DMZ

You may want to configure your router to allow computers the use of specific high layer applications or service sessions to pass through. Application Layer Gateways (ALG) allows you to easily enable or disable these applications to pass through your router.

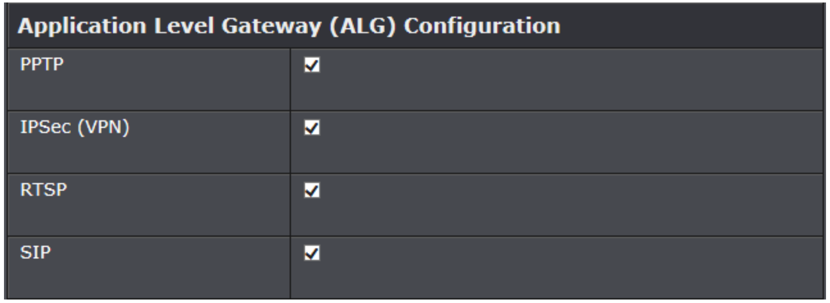
Note: *It is recommended to leave these settings enabled.*

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Firewall & DMZ**.

3. Review the applications to enable or disable. Click **Save Settings** to save the changes.

- **PPTP:** Allows PPTP VPN client connections through your router.
- **IPsec (VPN):** Allows IPsec VPN client connections through your router.
- **RTSP:** Allows RTSP video protocol through your router typically video/audio conferencing calling.
- **SIP:** Allows SIP protocol through your router typically used in VoIP applications



Application Level Gateway (ALG) Configuration

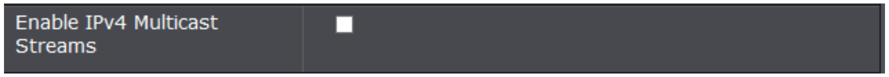
PPTP	☑
IPSec (VPN)	☑
RTSP	☑
SIP	☑

Allow/deny multicast streaming

Access > Advanced Network

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access**, and click on **Advanced Network**.
3. Next to **Enable IPv4 Multicast Streams**, check the option to enable or uncheck to disable.



Enable IPv4 Multicast Streams □

4. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click* ***Don't Save Settings.***

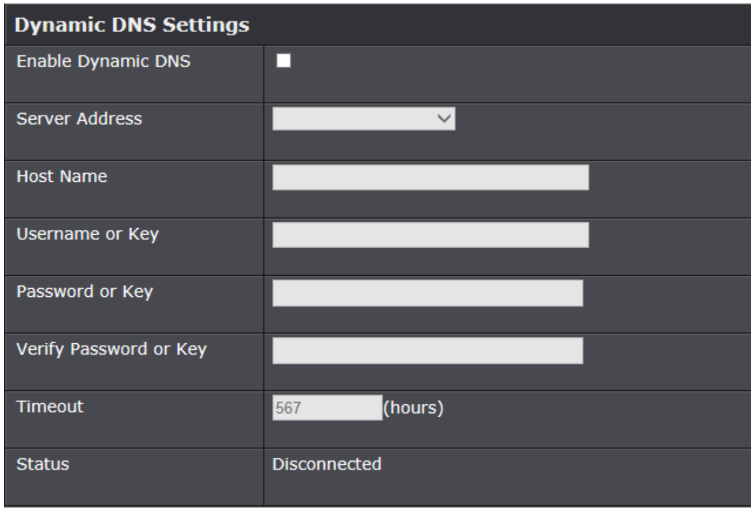
Identify your network on the Internet

Main > Dynamic DNS

Since most ISPs constantly change your home IP address, providing access to devices on your home or small office Local Area Network (such as IP Cameras) from the Internet requires setting up a Dynamic DNS service and entering the parameters into this management area. Dynamic DNS services allow your router to confirm its location to the given Dynamic DNS service, thereby providing the Dynamic DNS service with the ability to provide a virtual fixed IP address for your network. This means that even though your ISP is always changing your IP address, the Dynamic DNS service will be able to identify your network using a fixed address—one that can be used to view home IP Camera and other devices on your local area network.

> ***Note:*** *First, you will need to sign up for one of the DDNS service providers listed in the* ***Server Address*** *drop-down list.*

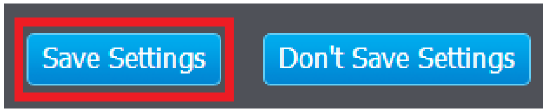
1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *dyndns.com*, etc.)
2. Log into your router management page (see "Access your router management page" on page 25).
3. Click on **Main** and click on **Dynamic DNS**.
4. Review the **DDNS Settings** section. Click **Save Settings** to save settings.
   - **Enable Dynamic DNS:** Check the option to enable the DDNS feature or uncheck the option to disable.
   - **Server Address:** Click the drop-down list Select your DDNS service.
   - **Host Name:** Personal URL provided to you by your Dynamic DNS service provider (e.g. www.trendnet.dyndns.biz)
   - **User Name or Key:** The user name needed to log in to your Dynamic DNS service account
   - **Password or Key:** This is the password to gain access to Dynamic DNS service for which you have signed up to. (NOT your router or wireless network password)
   - **Timeout:** The timeout period or interval assigned when your router will send an update to your DDNS service provider about the router's Internet IP address information.
   - **Status:** The status will display whether your router has success fully connected to your DDNS service.



Dynamic DNS Settings	
Enable Dynamic DNS	□
Server Address	
Host Name	
Username or Key	
Password or Key	
Verify Password or Key	
Timeout	567 (hours)
Status	Disconnected

5. To save changes, click **Save Settings**.

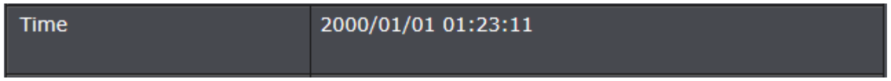
Note: *If you would like to discard the changes, click **Don't Save Settings.***



Set your router date and time

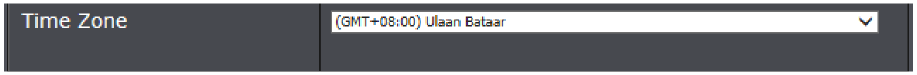
Main > Time

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Main**, and click on **Time**.
3. Review the Time settings. Click **Save Settings** to save settings.
    - **Time:** Displays the current device time and date information.



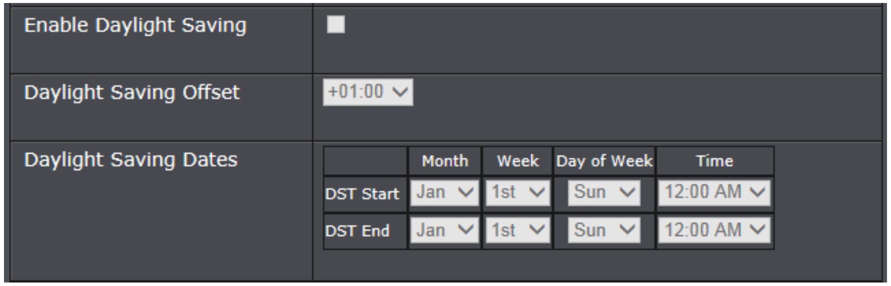
Time	2000/01/01 01:23:11

- **Time Zone –** Click the drop-down list and select your time zone.



Time Zone	(GMT+08:00) Ulaan Bataar

- **Enable Daylight Saving:** Check the option to enable daylight savings time and set the annual range when daylight saving is activated.

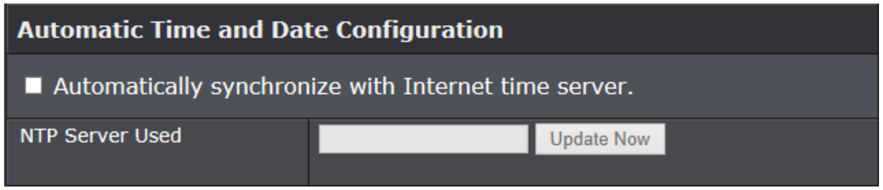


Enable Daylight Saving	□
Daylight Saving Offset	+01:00
Daylight Saving Dates	

	Month	Week	Day of Week	Time
DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

- **Automatically synchronize with Internet Time Server –** Check the **optionerver** option to set your router date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to Default NTP server, (e.g. pool.ntp.org). Click the **Time Zone** drop-down list to select the appropriate zone and you can optionally change your NTP Sync period.

  Note: *NTP servers are used for computers and other network devices to synchronize time across an entire network.*

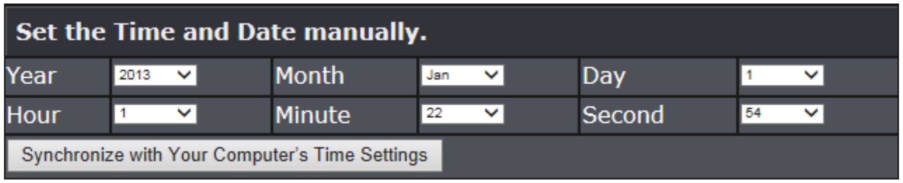


Automatic Time and Date Configuration

□ Automatically synchronize with Internet time server.

NTP Server Used	Update Now

- **Manually set time –** Set your router date and time manually in the Date and Time Settings section. ***Note:*** *Time is specified in 24-hour format. In addition, you can click Synchronize with Your Computer's Time Settings to copy the time and date settings from your computer.*



Set the Time and Date manually.

Year	2013	Month	Jan	Day	1
Hour	1	Minute	22	Second	54

Create schedules

Tools > Schedules

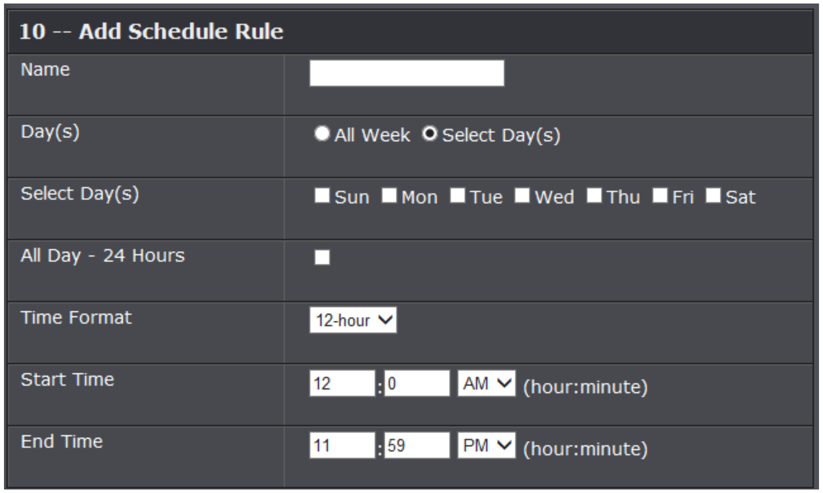
For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly.

Note: *You can apply a predefined schedule to the following features:*

- *Wireless (2.4GHz and 5GHz)*
- *Wireless Guest Zone*
- *MAC Filters*
- *Virtual Server*
- *Firewall Rules*
- *Application Rules*
- *Parental Control (Website Filtering)*

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Tools** and click on **Schedules**.
3. Review the Schedule settings. Click **Save Settings** to save settings.
   - **Name:** Enter a name for the schedule you would like to apply.
   - **Day(s)/Select Day(s):** Check **Select Day(s)** to select the days in the **Select Day(s)** section or select **All Week** to set the schedule for all days.
   - **All Day – 24 Hours:** Check the option to set the schedule to 24 hours or define the schedule under **Start Time** and **End Time.**
   - **Start/End Time:** Select the start and end time you would like the schedule to follow.

Note: *The schedule defined will define the time/day the feature will be activated.*



10 -- Add Schedule Rule

Name	
Day(s)	● All Week ○ Select Day(s)
Select Day(s)	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day - 24 Hours	□
Time Format	12-hour
Start Time	12 : 0 AM (hour:minute)
End Time	11 : 59 PM (hour:minute)

Open a device on your network to the Internet

This router can provide access to devices on your local area network to the Internet using the Virtual Server, Special Application, method (DMZ NOT recommended).

DMZ

Access > Firewall & DMZ

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is a very **insecure** technology and will open local area network to greater threats from Internet attacks.

It is strongly recommended to use **Virtual Server** (also called port forwarding, see "Virtual Server" on page 35) to allow access to your computers or network devices from the Internet.

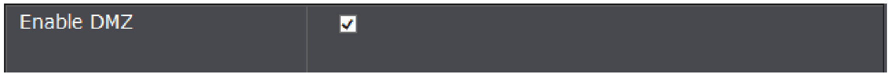
1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address. Signing up for a Dynamic DNS service (outlined in Identify Your

Network section page 32) will provide identification of the router's network from the Internet.

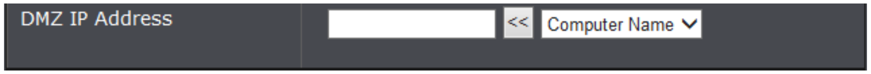
2. Log into your router management page (see "Access your router management page" on page 25).

3. Click on **Access**, and click on **Firewall & DMZ**.

4. Select Enable in the **DMZ Host** section.


Enable DMZ ☑

5. Enter the IP address you assigned to the computer or network device to expose to the Internet. ***Note:*** *You can also click the **Computer Name** drop-down list to select a computer from your DHCP client list and click << to copy information into the field.*


DMZ IP Address

6. To save changes, click **Save Settings**.

Virtual Server

Access > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "DMZ" on page 34) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet. To open several ports please refer to "Port Forwarding" section on page 36.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (outlined in Identify Your Network section page 32).

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Virtual Server**.

3. Review the virtual server settings. Click **Save Settings** to save settings.

Check the option to the left most of the entry to enable and uncheck to disable.

- **Name:** Enter a name for the virtual server.

  Note: *You can also click the **Application Name** drop-down list to select from a predefined list of applications and click **<<** to copy the information into the fields.*

- **IP Address:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101).*

  Note: *You can also click the **Computer Name** drop-down list to select a computer from the DHCP client list and click **<<** to copy the information into the field.*

- **Public Port:** Enter the port number used to access the device from the Internet.

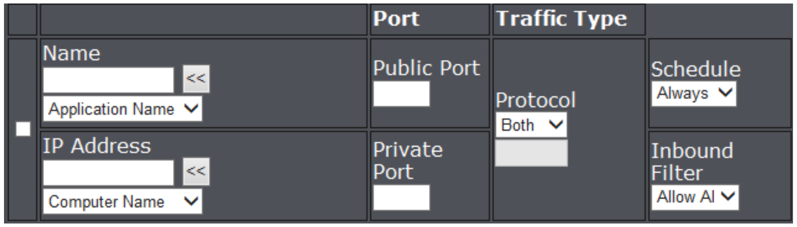
- **Private Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.

- **Protocol**: Select the protocol required for your device. **TCP**, **UDP, Both** (TCP and UDP), or **Other** to define a non-listed protocol.

  Note: *The Public Port can be assigned a different port number than the Private Port (also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required.It is recommended to assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.*

- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).

- **Inbound Filter:** Select the defined IP address range to allow access. (see "Inbound Filter" section on page 37).



		Port	Traffic Type	
□	Name << Application Name	Public Port	Protocol Both	Schedule Always
	IP Address << Computer Name	Private Port		Inbound Filter Allow Al

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see Identify Your Network section page 32).

2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)
3. Make sure to configure your network/IP camera to use a static IP address.

***Note:** You may need to reference your camera documentation on configuring a static IP address.*

4. Log into your router management page (see "Access your router management page" on page 25).
5. Click on **Access**, and click on **Virtual Server**.
6. Check the option next to the virtual server entry to enable.
7. Under **Name**, click the **Application Name** drop-down list and select the predefined **HTTP** entry, then click **<<** to copy the application information to the fields.
8. Next to **IP Address**, enter the IP address assigned to the camera. (e.g. *192.168.10.101*)
9. Next to **Protocol**, make sure **TCP** is selected in the drop-down list.
10. The **Private Port** and **Public Port**, make sure port number **80** is configured for both settings.
11. To save the changes, click **Save Settings.**

Port Forwarding

Access > Port Forwarding

Port Forwarding allows you to define a range of multiple public ports (used or required by a specific application or game) and forward them to a single IP address (a computer or device) on your network on a specific port. Using this feature is more secure compared to using DMZ (see "DMZ" on page 34) in which DMZ forwards all ports instead of only specific ports used by an application. Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (see "Identify your network over the Internet" section on page 32).

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access**, and click on **Port Forwarding**.
3. Review the port forwarding settings. Click **Save Settings** to save settings.

Check the option to the left most of the entry to enable and uncheck to disable.

- **Name:** Enter a name for the virtual server.

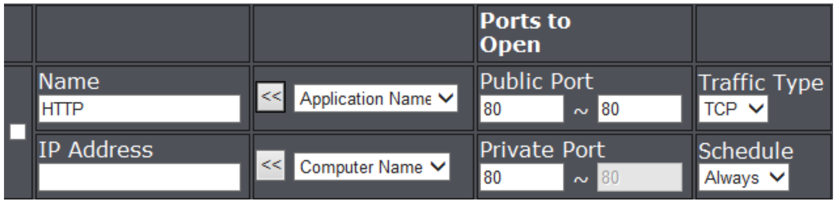
  ***Note:** You can also click the **Application Name** drop-down list to select from a predefined list of applications and click **<<** to copy the information into the fields.*

- **IP Address:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101).*

  ***Note:** You can also click the **Computer Name** drop-down list to select a computer from the DHCP client list and click **<<** to copy the information into the field.*

- **Public Port:** Enter the port range used to access the device from the Internet.
- **Private Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Traffic Type**: Select the protocol required for your device. **TCP** or **UDP**.

  ***Note:** Please refer to the device documentation to determine which ports and protocols are required.* You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.



			Ports to Open	
□	Name HTTP	<< Application Name	Public Port 80 ~ 80	Traffic Type TCP
	IP Address	<< Computer Name	Private Port 80 ~ 80	Schedule Always

Application Rules

Access > Application Rules

Application rules (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on page 31.

***Note:** Please refer to the device documentation to determine if your device supports UPnP first, before configuring this feature.*

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Application Rules**.

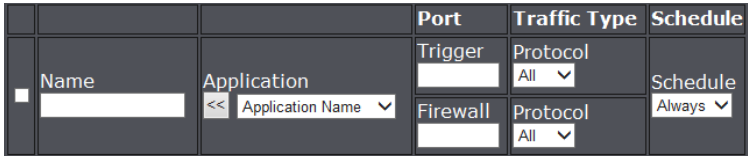
3. Review the application rule settings. Click **Save Settings** to save settings.

Check the option to the left most of the entry to enable and uncheck to disable.

- **Name:** Enter a name for the application.

  ***Note:** You can also click the **Application Name** drop-down list to select from a predefined list of applications and click **<<** to copy the information into the fields.*
- **Trigger:** Enter the port requested by the device. (e.g. *554-554 or 6112-6112).*
- **Firewall:** Enter the ports or port range to be forwarded to the device. (e.g. *2000-2038,2200-2210).*
- **Protocol (Trigger):** Select the trigger port protocol requested by the device. **TCP** or **UDP.**
- **Protocol (Firewall):** Select the firewall ports or port range protocol to be forwarded to the device. **TCP** or **UDP.**

  ***Note:** Please refer to the device documentation to determine which ports and protocols are required.*
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).



			Port	Traffic Type	Schedule
□	Name	Application << Application Name	Trigger	Protocol All	Schedule Always
			Firewall	Protocol All	

Inbound Filter

Access > Inbound Filter

Inbound Filters allows you to allow or deny a specific range of IP addresses. You can create a predefined range of IP addresses to apply to a specific feature.

***Note:** You can apply a predefined inbound filter to the following features:*

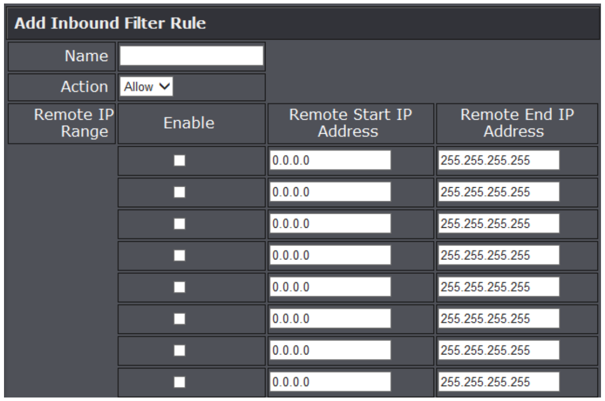
- *Remote Management*
- *Virtual Server*

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Inbound Filter**.

3. Review the inbound filter settings.

- **Enable:** Check the option to enable the IP address range.
- **Action:** Select **Allow** to allow the specified IP address range or **Deny** to deny the specified IP address range.
- **Name:**– Enter a name for the IP address range.
- **Remote Start IP Address/End IP Address:** Enter the IP address or IP address range of the filter (e.g. *192.168.1.20-192.168.1.20* or *192.168.1.20-192.168.1.30).*



Add Inbound Filter Rule

Name			
Action	Allow		
Remote IP Range	Enable	Remote Start IP Address	Remote End IP Address
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255
	□	0.0.0.0	255.255.255.255

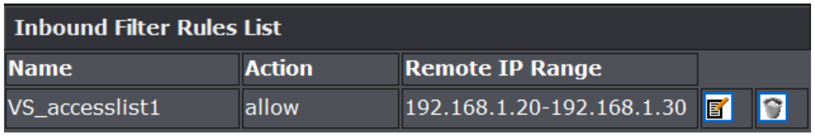
Click **Add** to save the inbound filter.

***Note:** Clicking Cancel discards and erases the current information.*

You will see the new reservation added to the Inbound Filter Rules List.

You can check the **Enable** option to enable the filter or uncheck to disable.

You can click the 📝 icon to edit the rule or 🗑 to delete the rule.



Inbound Filter Rules List

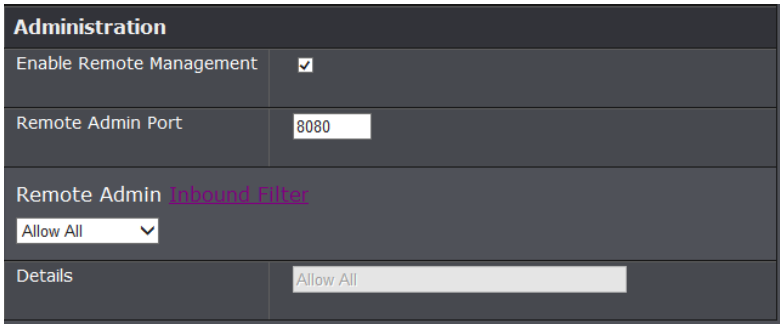
Name	Action	Remote IP Range		
VS_accesslist1	allow	192.168.1.20-192.168.1.30	📝	🗑

Allow remote access to your router management page

Main > Password

You may want to make changes to your router from a remote location such at your office or another location while away from your home.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Main**, and click on **Password**.
3. Review the setting on the **Administration** section. Click **Save Settings** to save settings
   - **Enable Remote Management:** Check the option to enable the feature to uncheck to disable.
   - **Remote Admin Port:** Enter the port to assign remote access to the router. It is recommended to leave this setting as 8080.
     ***Note:** If you have configured port 8080 for another configuration section such as virtual server or special application, please change the port to use. (Recommended port range 1024-65534)*
   - **Remote Admin:** Select the defined inbound filter you would like to apply. (see "Inbound Filter " section on page 37). You can click the Inbound Filter link to go to the **Inbound Filter** section and create an Inbound Filter rule. Once the inbound rule is selected here, the name of the filter rule will appear in the Details field.



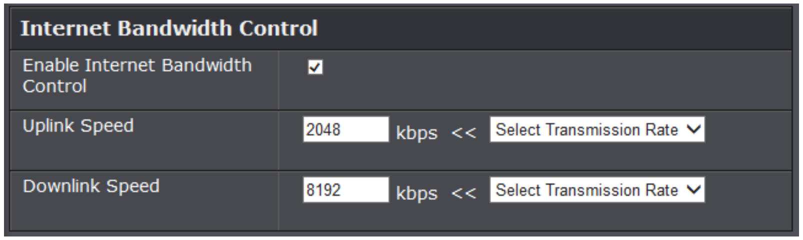
Administration	
Enable Remote Management	☑
Remote Admin Port	8080
Remote Admin Inbound Filter Allow All	
Details	Allow All

Set Internet bandwidth

Access > Internet Bandwidth Control

You may want to set the maximum upload and download limits for your Internet connection.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Access**, and click on **Internet Bandwidth Control**.
3. Review the Internet Bandwidth Control settings. Click **Save Settings** to save settings.
   - **Enable Internet Bandwidth Control:** Check the option to enable Internet Bandwidth Control and uncheck to disable.
   - **Uplink Speed:** Manually enter the maximum upload speed provided by your ISP (Internet Service Provider).
     ***Note:** You can also click the Select Transmission Rate drop-down list to select a predefined speed closest to the one provided by your ISP.*
   - **Downlink Speed:** Manually enter the maximum download speed provided by your ISP (Internet Service Provider).
     ***Note:** You can also click the Select Transmission Rate drop-down list to select a predefined speed closest to the one provided by your ISP.*



Internet Bandwidth Control	
Enable Internet Bandwidth Control	☑
Uplink Speed	2048 kbps << Select Transmission Rate
Downlink Speed	8192 kbps << Select Transmission Rate

4. To save changes, click **Save Settings**.

Add static routes to your router

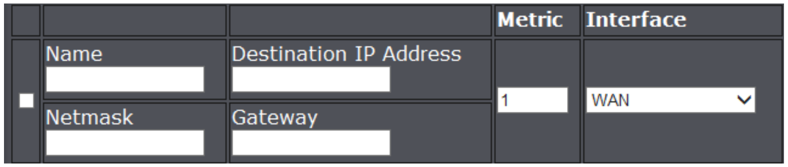
Routing > Static

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate between the two separate networks, static routing needs to be configured. Below is an example diagram where routing is needed for devices and computers on your network to access the other network.

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

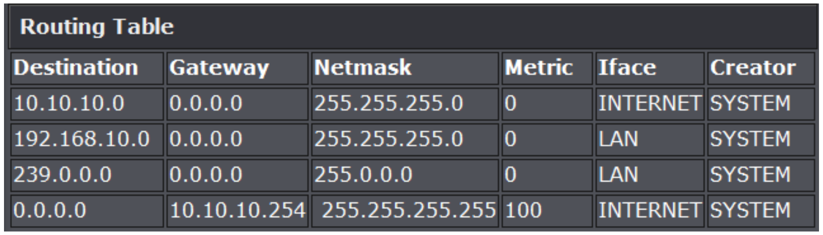
1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Routing**, and click on **Static**.
3. Review the Routing section. Click **Save Settings** to save settings.

- **Name –** Enter a name for the static route.
- **Destination IP Address:** Enter the IP network address of the destination network for the route. (e.g. *192.168.20.0*)
- **Subnet Mask:** Enter the subnet mask of the destination network for the route.(e.g. *255.255.255.0*)
- **Gateway:** Enter the gateway to the destination network for the route. (e.g. *192.168.10.2*)
- **Metric:** Enter the metric or priority of the route. The metric range is *1-16*, the lowest number *1* being the highest priority. (e.g. *1*)
- **Interface** – Select the interface to assign the route.



			Metric	Interface
☐	Name	Destination IP Address	1	WAN
	Netmask	Gateway		

You can also view the routing table under Routing > Routing Table.



Routing Table

Destination	Gateway	Netmask	Metric	Iface	Creator
10.10.10.0	0.0.0.0	255.255.255.0	0	INTERNET	SYSTEM
192.168.10.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN	SYSTEM
0.0.0.0	10.10.10.254	255.255.255.255	100	INTERNET	SYSTEM

Using External USB Storage

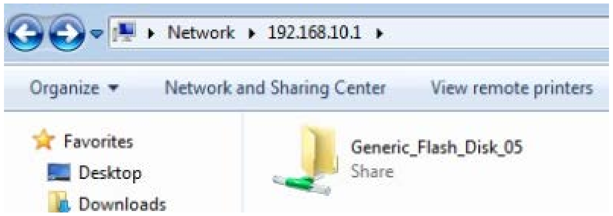
Your router's USB port can be used to share files through the network when a USB storage device is connected on the back USB port. The router supports SAMBA (SMB) filing sharing protocols.

Samba Network File Server

Administrator > File Sharing

Samba is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router. You can access these files under your network map or by typing \\routerIPaddress on your File Explorer address bar. Please follow the below steps.

1. Open your File Explore window.
2. Type \\routerIPaddress on the address bar



3. Your USB storage device will appear on the file explore window.

Router Maintenance & Monitoring

Reset your router to factory defaults

Tools > Restart

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on page 44.

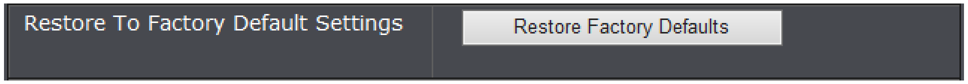
There are two methods that can be used to reset your router to factory defaults.

- **Reset Button** – Located on the side panel of your router, see "Product Hardware Features" on page 5. Use this method if you are encountering difficulties with accessing your router management page.

  OR

- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Tools** and click on **Restart**.
3. Next to **Restore to Factory Default Settings**, click **Restore to Factory Defaults**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer to sticker or device label
Router Default URL	*http://tew-752dru*
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless 2.4GHz & 5GHz	Enabled
Wireless 2.4GHz Network Name/Encryption	Please refer to sticker or device label
Wireless 2.4GHz & 5GHz Guest Network	Disabled

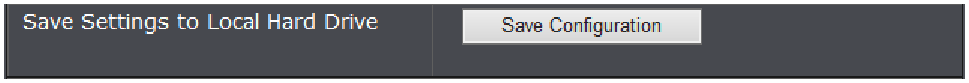
Backup and restore your router configuration settings

Tools > Restart

You may have added many customized settings to your router and in the case that you need to reset your router to default, all your customized settings would be lost and would require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

To backup your router configuration:

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Tools** and click on **Restart**.
3. Next to **Save Settings to Local Hard Drive** section, click **Save Configuration**.



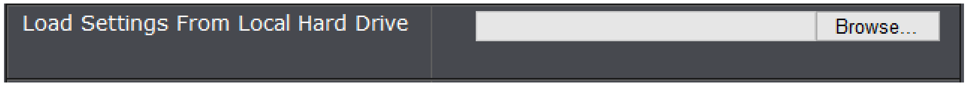
4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *config.bin)*

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Tools** and click on **Restart**.

3. Next to **Load Settings From Local Hard Drive,** depending on your web browser, click on **Browse** or **Choose File**.



4. A separate file navigation window should open.

5. Select the router configuration file to restore and click **Import**. (Default Filename: *config.bin*). If prompted, click **Yes** or **OK**.

6. Wait for the router to restore settings.

Reboot your router

Tools > Restart

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

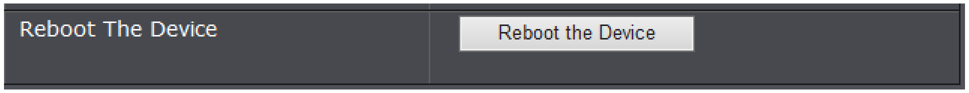
There are two methods that can be used to restart your router.

- **Turn the router** off for 10 seconds using the router On/Off switch located on the rear panel of your router or disconnecting the power port, see "Product Hardware Features" on page 5.
  Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.
  OR
- **Router Management Page** – This is also known as a soft reboot or restart.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Tools** and click on **Restart**.

3. Next to **Reboot The Device**, click **Reboot the device**.



4. Wait for the device to reboot.

Upgrade your router firmware

Tools > Firmware

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet router model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. http://www.trendnet.com/downloads/

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, click on the Administrator section and then on the Status. The firmware used by the router is listed at the top of this page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.

2. Unzip the file to a folder on your computer.

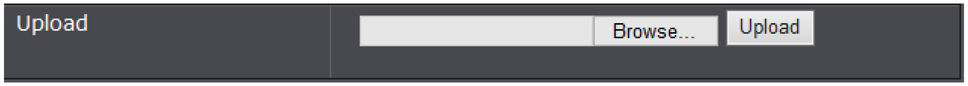
Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your router.

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Tools** and click on **Firmware**.

3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.



4. Navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.

5. Click **Upload**. If prompted, click **Yes** or **OK**.

Allow/deny ping requests to your router from the Internet

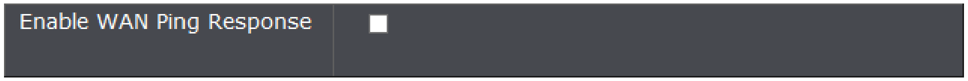
Access > Advanced Network

To provide additional security, you may want to disable your router from responding to ping or ICMP (Internet Control Message Protocol) requests from the Internet. A ping is network communication test to check if a device with IP address is alive or exists on the network. By disabling this feature, you can conceal your router's IP address and existence on the Internet by denying responses to ping requests from the Internet. You can additionally use this feature as a tool for troubleshooting purposes

1. Log into your router management page (see "Access your router management page" on page 25).

2. Click on **Access**, and click on **Advanced Network**.

3. Next to **Enable WAN Ping Response**, check the option to allow your router to respond to ping requests from the Internet.



Enable WAN Ping Response □

4. To save changes, click **Save Settings**.

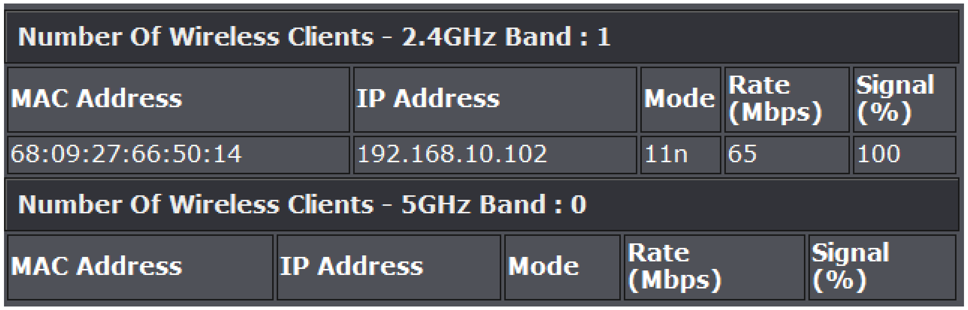
Note:** If you would like to discard the changes, click **Don't Save Settings.

Wireless Client List

Status > Wireless

You can view the list of active wireless devices currently connected to your router.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Status**, and click on **Wireless.**



Number Of Wireless Clients - 2.4GHz Band : 1				
MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)
68:09:27:66:50:14	192.168.10.102	11n	65	100

Number Of Wireless Clients - 5GHz Band : 0				
MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)

- **MAC Address:** Displays the current MAC address of your wireless client.
- **IP Address:** Displays the current IP address of your wireless client.
- **Mode:** Displays the current mode your wireless client is connected (11a/b/g/n)
- **Rate:** Displays the current rate your wireless client has established.
- **Signal:** Displays the signal strength of your wireless client.

Check the router system information

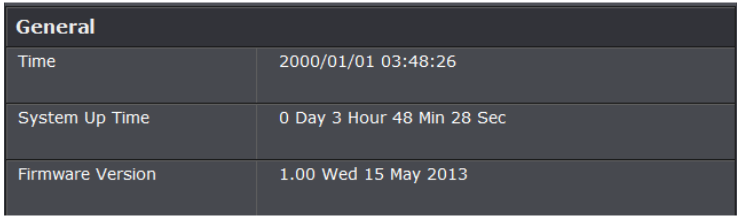
Status > Device Information

You may want to check the system information of your router such as WAN (Internet) connectivity, wireless and wired network settings, router MAC address, and firmware version.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Status** and click on **Device Information**.

System Information

- **Time:** The current time set on your router.
- **System Up Time** – The duration your router has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Firmware Version** – The current firmware version your router is running.

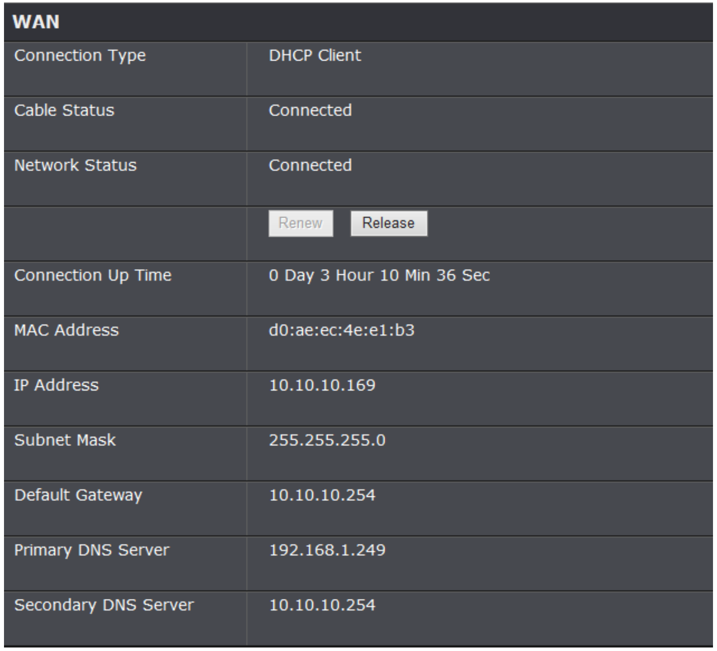


General	
Time	2000/01/01 03:48:26
System Up Time	0 Day 3 Hour 48 Min 28 Sec
Firmware Version	1.00 Wed 15 May 2013

WAN Information

- **Connection Type:** Displays the current WAN connection type applied.
- **Cable Status:** Displays the physical link status of the WAN port
- **Network Status:** Displays the current WAN connection status.
  - **Renew (DHCP WAN Type):** Click this option to renew your WAN IP address.
  - **Release (DHCP WAN Type):** Click this option to release the WAN IP address of your router.
  - **Connect (PPPoE WAN Type):** Click this option to connect to your DSL ISP
  - **Disconnect (PPPoE WAN Type):** Click this option to disconnect from your DSL ISP.
- **Connection Uptime:** Displays the amount of time the WAN connection has been up and running without any disconnects.

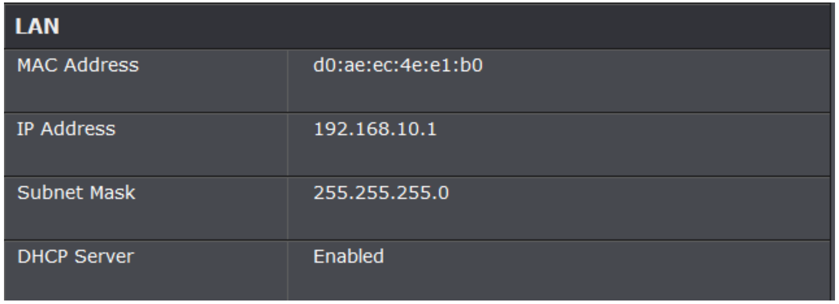
- **MAC Address:** Displays the current WAN MAC address.
- **IP Address** – The current IP address assigned to your router WAN port or interface configuration.
- **Subnet Mask** - The current subnet mask assigned to your router WAN port or interface configuration.
- **Default Gateway** – The current gateway assigned to your router WAN port or interface configuration.
- **Primary/Secondary DNS (Domain Name System) Server** – The current DNS address(es) assigned to your router port or interface configuration.



WAN	
Connection Type	DHCP Client
Cable Status	Connected
Network Status	Connected
Connection Up Time	0 Day 3 Hour 10 Min 36 Sec
MAC Address	d0:ae:ec:4e:e1:b3
IP Address	10.10.10.169
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.254
Primary DNS Server	192.168.1.249
Secondary DNS Server	10.10.10.254

LAN Information

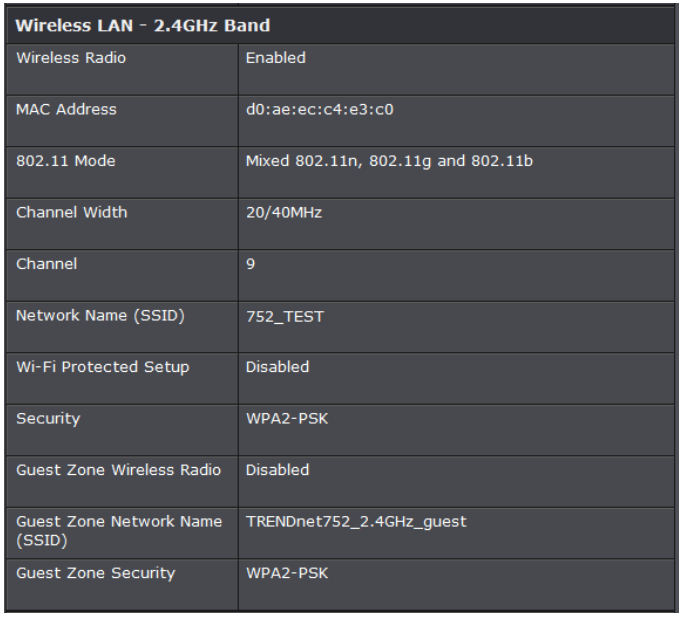
- **MAC Address** – The current MAC address of your router's wireless or interface configuration.
- **IP Address** - Displays your router's current IP address.
- **Subnet Mask** – Displays your router's current subnet mask.
- **DHCP Server –** Displays the current status of the LAN DHCP server.



LAN	
MAC Address	d0:ae:ec:4e:e1:b0
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

2.4GHz Wireless LAN

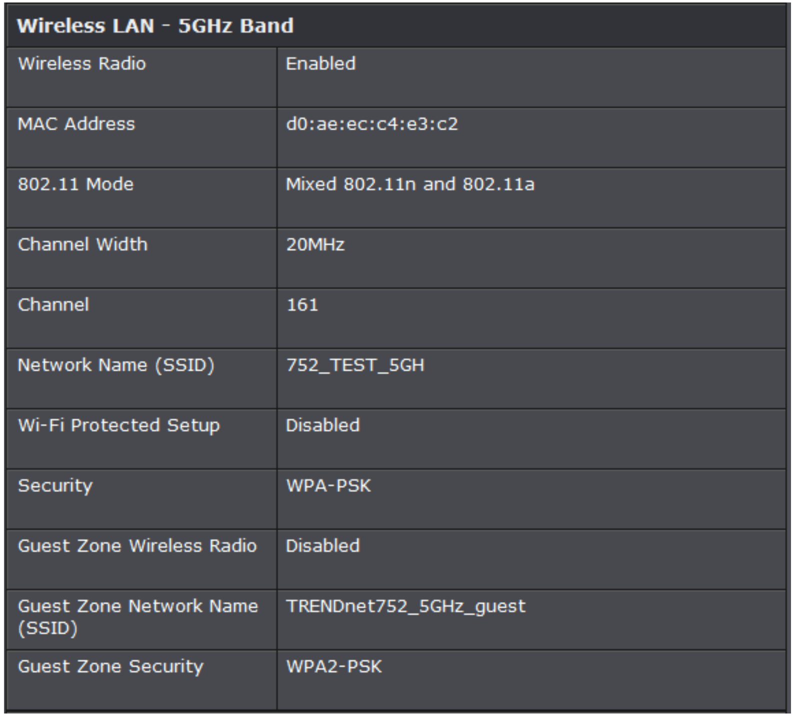
- **Wireless Radio:** Displays if the current status if the 2.4GHz radio is enabled or disabled.
- **MAC Address:** The MAC address of your router's 2.4GHz wireless LAN or interface configuration.
- **802.11 mode:** Displays the current 802.11 Mode of the 2.4GHz radio.
- **Channel Width**– Displays the current channel width configuration of the 2.4GHz radio.
- **Channel** – Displays the current 2.4GHz wireless channel your router is operating.
- **Network Name (SSID):** Displays the current 2.4GHz wireless network name assigned to your router.
- **Wi-Fi Protected Setup:** Displays the current 2.4GHz WPS status.
- **Security:** Displays the wireless security type applied to 2.4GHz primary SSID.
- **Guest Zone Wireless Radio**: Displays the current status of the 2.4GHz wireless guest zone.
- **Guest Zone Network Name (SSID):** Displays the current 2.4GHz wireless guest network name assigned to your router.
- **Guest Zone Security:** Displays the wireless security type applied to the 2.4GHz wireless guest network.



Wireless LAN - 2.4GHz Band	
Wireless Radio	Enabled
MAC Address	d0:ae:ec:c4:e3:c0
802.11 Mode	Mixed 802.11n, 802.11g and 802.11b
Channel Width	20/40MHz
Channel	9
Network Name (SSID)	752_TEST
Wi-Fi Protected Setup	Disabled
Security	WPA2-PSK
Guest Zone Wireless Radio	Disabled
Guest Zone Network Name (SSID)	TRENDnet752_2.4GHz_guest
Guest Zone Security	WPA2-PSK

5GHz Wireless LAN

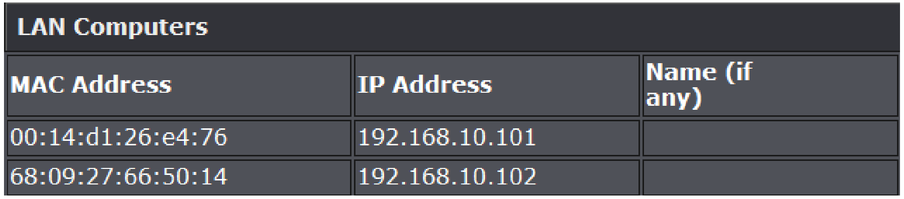
- **Wireless Radio:** Displays if the current status if the 5GHz radio is enabled or disabled.
- **MAC Address:** The MAC address of your router's 5GHz wireless LAN or interface configuration.
- **802.11 mode:** Displays the current 802.11 Mode of the 5GHz radio.
- **Channel Width**– Displays the current channel width configuration of the 5GHz radio.
- **Channel** – Displays the current 5GHz wireless channel your router is operating.
- **Network Name (SSID):** Displays the current 5GHz wireless network name assigned to your router.
- **Wi-Fi Protected Setup:** Displays the current 5GHz WPS status.
- **Security:** Displays the wireless security type applied to 5GHz primary SSID.
- **Guest Zone Wireless Radio**: Displays the current status of the 5GHz wireless guest zone.
- **Guest Zone Network Name (SSID):** Displays the current 5GHz wireless guest network name assigned to your router.
- **Guest Zone Security:** Displays the wireless security type applied to the 5GHz wireless guest network.



Wireless LAN - 5GHz Band	
Wireless Radio	Enabled
MAC Address	d0:ae:ec:c4:e3:c2
802.11 Mode	Mixed 802.11n and 802.11a
Channel Width	20MHz
Channel	161
Network Name (SSID)	752_TEST_5GH
Wi-Fi Protected Setup	Disabled
Security	WPA-PSK
Guest Zone Wireless Radio	Disabled
Guest Zone Network Name (SSID)	TRENDnet752_5GHz_guest
Guest Zone Security	WPA2-PSK

LAN Computers

- **MAC Address:** Displays if the MAC address of the LAN client device.
- **IP Address:** Displays the current IP address of the LAN client device.
- **Name:** Displays the host name of the LAN client device.



LAN Computers

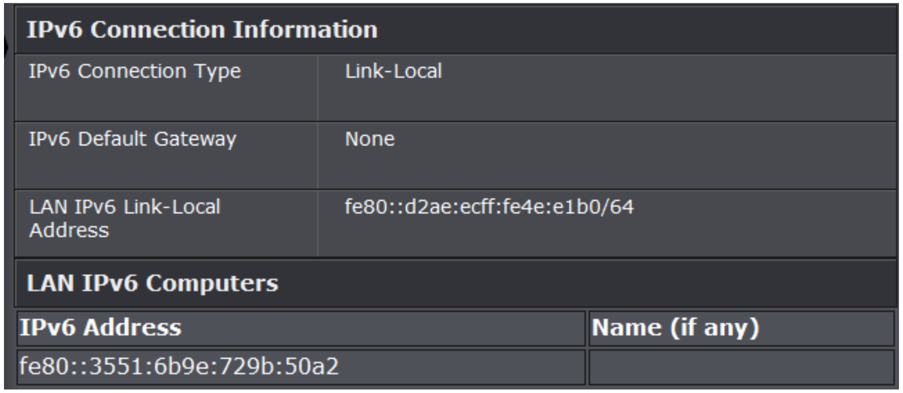
MAC Address	IP Address	Name (if any)
00:14:d1:26:e4:76	192.168.10.101	
68:09:27:66:50:14	192.168.10.102	

IPv6 Status

Status > IPv6

You can view the current IPv6 status on your router.

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Administrator**, and click on **IPv6 Status**
   - **IPv6 Connection Type:** The type of IPv6 being used on your router.
   - **IPv6 Default Gateway:** Displays the IPv6 default gateway.
   - **LAN IPv6 Link-Local Address:** Displays the link-local address.
   - **LAN IPv6 Computer:** Lists the current IPv6 devices connected to your router.



IPv6 Connection Information

IPv6 Connection Type	Link-Local
IPv6 Default Gateway	None
LAN IPv6 Link-Local Address	fe80::d2ae:ecff:fe4e:e1b0/64

LAN IPv6 Computers

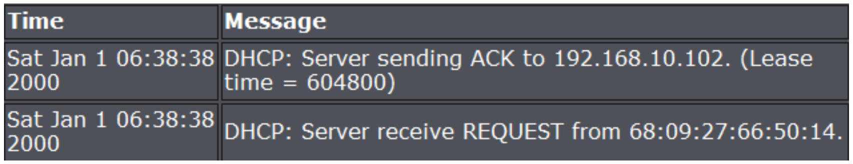
IPv6 Address	Name (if any)
fe80::3551:6b9e:729b:50a2	

View your router log

Status > Log

Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

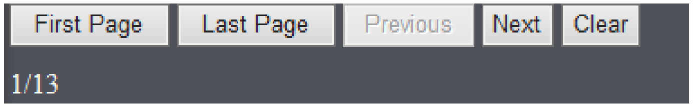
1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Status**, and click on **Log**.
   - **Time:** Displays the time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly. (See "Set your router date and time" on page 34)
   - **Message:** Displays the log message.



Time	Message
Sat Jan 1 06:38:38 2000	DHCP: Server sending ACK to 192.168.10.102. (Lease time = 604800)
Sat Jan 1 06:38:38 2000	DHCP: Server receive REQUEST from 68:09:27:66:50:14.

Router Log Navigation

- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous:** Display the log page previous to the current.
- **Next:** Displays the log page next to the current.
- **Clear:** - Clears all logging



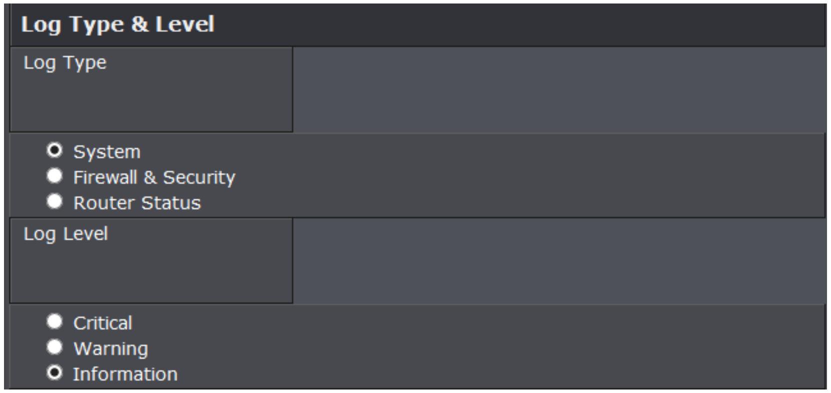
Configure your router log

Status > Log

You may want to only see specific categories of logging for troubleshooting purposes.

Set the types or categories to include in logging

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Status** and click on **Log**.
3. Next to **Log Type & Level**, check the types or categories to include in logging.



Log Type & Level

Log Type

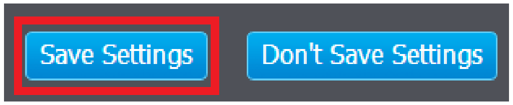
● System
○ Firewall & Security
○ Router Status

Log Level

○ Critical
○ Warning
● Information

4. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click* ***Don't Save Settings.***



Save your router log

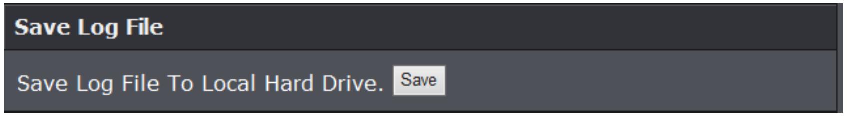
You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to save the router logging to a local text file for troubleshooting purposes.

Save router logs to your hard drive

Status > Log

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Status** and click on **Log.**
3. Next **Save Log File to Local Hard Drive**, click **Save.** (Default Filename: log.txt)

Note: *Browse for a location on your local hard drive to save the log file.*



Save Log File

Save Log File To Local Hard Drive. Save

Send router logs to your e-mail address

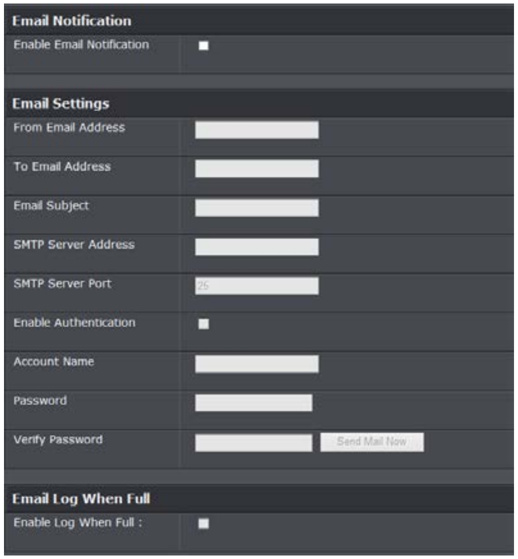
Tools > Email Settings

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Tools** and click on **Email Settings.**
3. Review the e-mail log settings.
   - **Enable Email Notification –** Check the option to enable email log notification.
   - **From Email Address** – Enter a sender e-mail address. (e.g. *router@trendnet.com*)

     Note: *This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.*
   - **To Email Address** – Enter your e-mail address.
   - **Email Subject** – Enter the subject for your email.
   - **SMTP Server Address** – Enter the IP address (e.g. *10.10.10.10*) or domain name (e.g. *mail.trendnet.com*) of your e-mail server.

- **SMTP Server Port** – Enter the port used by your e-mail service. (e.g. *Default SMTP Server Port: 25*)
- **Enable Authentication** – Check this option if your e-mail service requires authentication. If not, leave this settings disabled (unchecked)

  Note: *If you are unsure of this setting check with your e-mail service provider if authentication is required.*
- **Account Name**– Enter your account user name for your e-mail service.
- **Password** – Enter your password for your e-mail service.
- **Send Mail Now** – Click this option to send an e-mail with the current router log using your email settings.
- **Email Logs When Fulll –** The router log will be e-mailed to your e-mail address when router internal log is full.



Email Notification

Enable Email Notification ☐

Email Settings

From Email Address

To Email Address

Email Subject

SMTP Server Address

SMTP Server Port 25

Enable Authentication ☐

Account Name

Password

Verify Password

Email Log When Full

Enable Log When Full : ☐

4. To save changes, click **Save Settings**.

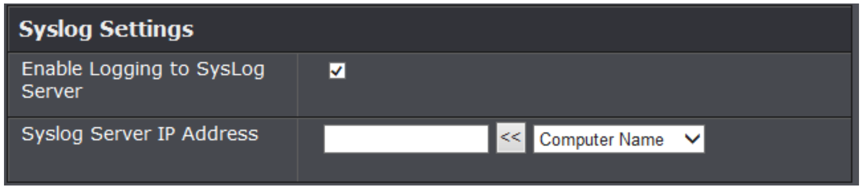
Note: *If you would like to discard the changes, click* ***Don't Save Settings.***

Send router logs to an external log server

Tools > Syslog

1. Log into your router management page (see "Access your router management page" on page 25).
2. Click on **Tools** and click on **Syslog.**
3. Next to **Enable Logging to Syslog Server**, check the option to enable Syslog. Enter the IP address of the local syslog server to forward the logs.

Note: *You can also click the* ***Computer Name*** *drop-down list and select from the DHCP server list. Click* ***<<*** *to copy the IP address information to the* ***Syslog Server IP Address*** *field.*



Syslog Settings

Enable Logging to SysLog Server ☑

Syslog Server IP Address

4. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click* ***Don't Save Settings.***

Router Management Page Structure

Main

- Wizard
- LAN
  - DHCP Server Setting
  - DHCP Reservation
- WAN
- Password
  - Remote Management
- Time
- Dynamic DNS
- IPv6

Wireless

- Basic
  - 2.4GHz Settings & Security
  - 5GHz Settings & Security
- Advanced
- WPS (Wi-Fi Protected Setup)IPv6 Setting

Status

- Device Information
- Log
- Statistic
- Active Sessions
- Wireless
- IPv6

Routing

- Static
- Routing Table

Access

- MAC Filters
- Inbound Filter
- Virtual Server
- Firewall & DMZ
  - ALG
- Port Forwarding
- Application Rules
- Internet Bandwidth Control
- Guest Zone
- Advanced Network
  - UPnP
- Parental Control (Domain/URL Filters)

Tools

- Restart
  - Backup Configuration
  - Restore Configuration
  - Restore to Factory Defaults
  - Reboot Device
- Firmware
  - Upgrade Firmware
- Ping Test
- Email Settings
- Syslog
- Schedules

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T) Wireless: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, 802.11a
Internet Protocol	IPv4 and IPv6
LAN	4 x 10/100/1000 Mbps Auto-MDIX
WAN	1 x 10/100/1000 Mbps Auto-MDIX
USB	1 x USB 2.0 Type-A (Storage)
WPS Button	Wi-Fi Protected Setup (WPS) connects with other WPS compliant devices
Reset Button	Reset unit back to factory default (press and hold for 10 seconds)
Network Protocols / Features	Static routing, UPnP, DHCP, server, Dynamic DNS (DynDNS.com), NTP, VPN/RTSP/SIP pass through, IPv6
Quality of Service	WMM and Internet Bandwidth Control (Configurable Upload / Download)
Internet Connection Type	Static routing, UPnP, DHCP, server, Dynamic DNS (DynDNS.com), NTP, VPN/RTSP/SIP pass through, IPv6
Firewall	NAT, SPI, DMZ host, virtual server, port forwarding MAC, IP and URL filter, Schedules (wireless, MAC filter, virtual server, port forwarding, firewall rule, application rule, guest network, and URL filter), Inbound IP filter (virtual server)
Management / Monitoring	Local / remote configuration, upgrade firmware, backup / restore configuration via web browser, internal system log (Categories: System, Firewall & Security, Router Status / Filter: Critical, Warning, Information), syslog, email log, active sessions,
Supported Web Browser	Internet Explorer 8.0 or above, Firefox, Chrome, Opera, Safari
LED Indicator	Power, WAN (Internet), Wireless, WPS, USB
Power Adapter	Input: 100 ~ 240 V, 50~60 Hz, 0.5 A Output: 12 V DC, 1.25 A external power adapter
Power Consumption	14.7 watts (max.)
Dimension (L x W x H)	45 x 118 x 164 mm (1.8 x 4.6 x 6.5 in.)
Weight	255 g (9 oz)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F)
Humidity	Max. 95% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.4 GHz: 2.412~2.462 (FCC) and 2.412~2.472 (ETSI) 5 GHz: 5.15 ~ 5.35 / 5.725~5.825 GHz (FCC) and 5.15 ~ 5.35 / 5.47 ~ 5.725 GHz (ETSI)
Antenna	2.4 GHz: 2 x 2 dBi printed 5 GHz: 2 x 5.4 dBi PIFA internal
Modulation	CCK, DQPSK, DBPSK, OFDM, BPSK, QPSK, 16/64-QAM
Data Rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps (for both 2.4 & 5 GHz)
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
Guest network	1 per wireless band, access control between 2.4GHz and 5GHz guest zones
Output Power	802.11a: 15 dBm (typical)

	802.11b: 18 dBm (typical) 802.11g: 15 dBm (typical) 802.11n: 18 dBm (typical) (for 2.4 & 5GHz)
Receiving Sensitivity	802.11a: -65 dBm (typical) @ 54 Mbps 802.11b: -76 dBm (typical) @ 11 Mpbs 802.11g: -65 dBm (typical) @ 54 Mbps 802.11n: -79 dBm (typical) @ 300 Mbps (for 2.4 & 5 GHz)
Channels	2.4 GHz: 1~11 (FCC), 1~13 (ETSI) 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161, 165 (FCC) 36, 40, 44, 48 (ETSI)

*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.

Troubleshooting

Q: I typed *http://tew-752dru* in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?
Answer:
Access the router using the default IP address 192.168.10.1.
http://192.168.10.1

Q: I typed http://192.168.10.1 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?
Answer:
1. Check your hardware settings again. See "Router Installation" on page 8.
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Obtain an IP address automatically* or *DHCP* (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?
Answer:
Contact your Internet Service Provider (ISP) for the correct information.

Q: The Wizard does not appear when I access the router. What should I do?
Answer:
1. Click on Wizard on the left hand side.
2. Near the top of the browser, "Pop-up blocked" message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser's pop up blocker.

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?
Answer:
1. Verify that you can get onto the Internet with a direct connection into your modem (meaning plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Q: I cannot connect wirelessly to the router. What should I do?
Answer:
1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(*model_number)*.
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see "Steps to improve wireless connectivity" on page 20 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Command Prompt Method

Windows 2000/XP/Vista/7

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.

2. In the dialog box, type ***cmd*** to bring up the command prompt.

3. In the command prompt, type ***ipconfig /all*** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.

2. Double-click on **Terminal** to launch the command prompt.

3. In the command prompt, type ***ipconfig getifaddr <en0 or en1>*** to display the wired or wireless IP address settings.

Note: en0 *is typically the wired Ethernet and* ***en1*** *is typically the wireless Airport interface.*

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to configure your network settings to obtain an IP address automatically or use DHCP?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Obtain an IP address automatically** and click **OK**.

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.
b. Click the **Network** icon.
c. From the **Location** drop-down list, select **Automatic**.
d. Select and view your Ethernet connection.
In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use DHCP.
In MAC 10.4, from the Configure IPv4, drop-down list, select Using **DHCP** and click the **Apply Now** button.
In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7,

Your computer MAC addresses are also displayed in this window, however, you can type ***getmac –v*** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**

2. From the **Show** menu, select **Built-in Ethernet**.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**

2. Select **Ethernet** from the list on the left.

3. Click the **Advanced** button.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

How to connect to a wireless network using the built-in Windows utility?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for connecting to a wireless network using the built-in utility.*

Windows 7

1. Open Connect to a Network by clicking the network icon (📶 or 🖧) in the notification area.

2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**. ⊞ and then click **Connect To.**

2. In the **Show** list, click **Wireless**.

3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.

2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.

3. You may be prompted to enter a security key in order to connect to the network.

4. Enter in the security key corresponding to the wireless network, and click **Connect**.

Federal Communication Commission Interference Statement

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

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

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

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.

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.

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC.

Regulation (EC) No. 1275/2008
Regulation (EC No. 278/2009
EN60950-1 : 2006 + A11 : 2009 + A1: 2010 + A12: 2011

Safety of Information Technology Equipment

EN 50385 : 2002
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) Class B
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
EN 301 489-1 V1.9.2 : (2011-09)
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 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems
EN 301 893 V1.6.1 : (2011-11)
Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN;Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
This device is a 2.4/5G 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.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-752DRU je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-752DRU overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-752DRU in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-752DRU vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, TRENDnet, declares that this TEW-752DRU is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-752DRU cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, 2009/125/CE y.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑTRENDnet ΔΗΛΩΝΕΙ ΟΤΙTEW-752DRUΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ, 2006/95/ΕΚ, 2009/125/ΕΚ και.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-752DRU est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.
it Italiano[Italian]	Con la presente TRENDnet dichiara che questo TEW-752DRU è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-752DRU atbilstDirektīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-752DRU atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-752DRU in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-752DRU jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-752DRUmegfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-752DRU jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
pt Português [Portuguese]	TRENDnet declara que este TEW-752DRU está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-752DRU v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES in 2009/125/ES.
Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TEW-752DRUspĺňazákladnépožiadavky a všetkypríslušnéustanoveniaSmernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-752DRU tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-752DRU står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2006/95/EG och 2009/125/EG.

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-752DRU – 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, NEGLECT, 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 2013/09/12

TRENDnet®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA