



## Contents

<b>Product Overview .....</b>	<b>1</b>
Package Contents .....	1
Features .....	1
Rear Panel View .....	2
Front Panel View .....	3
Side Panel View .....	4
Application Diagram .....	4
<b>Basic Router Setup .....</b>	<b>5</b>
Creating a Home Network .....	5
Before you Install .....	6
Installation.....	7
Setup Wizard .....	8
How to connect additional wired devices to your network .....	11
<b>Advanced Router Setup.....</b>	<b>12</b>
How to access your router management page .....	12
How to manually configure your Internet connection.....	12
How to clone a MAC address .....	13
How to set your router date and time .....	14
How to change your router login password .....	15
How to change your router IP address .....	16
How to set up the DHCP server on your router .....	17
How to set up DHCP reservation.....	18
How to enable/disable UPnP on your router.....	19
How to allow/deny VPN connections through your router .....	19
How to allow/deny multicast streaming .....	20
How to identify your network on the Internet .....	20
How to allow remote access to your router management page.....	21

How to expose a device on your network to the Internet.....	21
How to add static routes to your router .....	22
How to enable dynamic routing on your router .....	23
<b>Wireless Networking.....</b>	<b>24</b>
How to choose the type of security for your wireless network.....	24
How to secure your wireless network .....	25
How to connect wireless devices using WPS.....	27

## Product Overview



**TEW-711BR**

### Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5m / 5ft)
- Power adapter (5V DC, 1A)

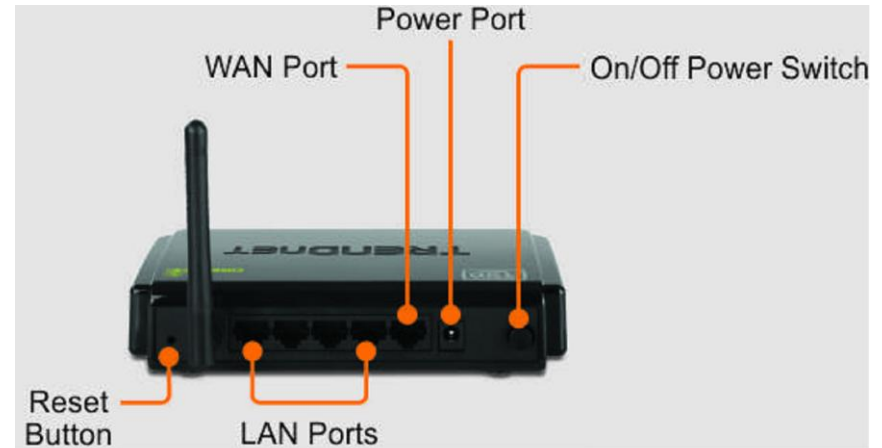
If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor that the item was purchased.

### Features

The 150Mbps Wireless N Home Router delivers the highest level of security with 6x the speed and 3x the coverage of wireless g products. Quickly install the router and use it with TRENDnet wireless n adapters to receive the full benefits of wireless n speed and coverage.

The latest in wireless encryption and a secure firewall protect your valuable data. Router setup is fast and intuitive. Wireless Protected Setup (WPS) integrates other WPS supported wireless adapters at the touch of a button. Seamlessly stream HD media, download files and surf online with wireless n speed.

- 6x the speed and 3x the coverage of wireless g
- Seamlessly stream video, download files, talk online and play games
- Advanced wireless encryption protects your valuable data
- Intuitive installation process

**Rear Panel View**

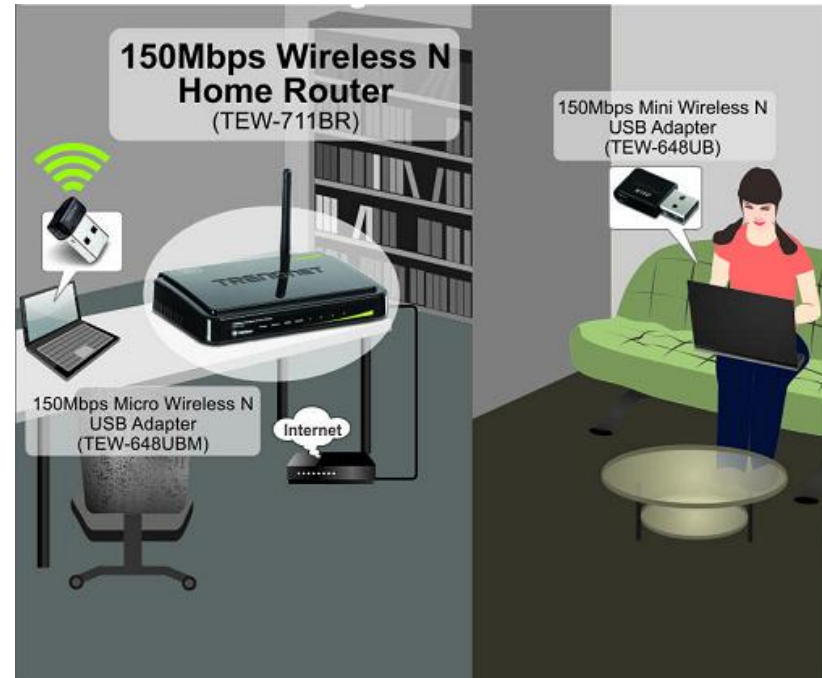
- **Reset Button** – Use an item such as a paperclip to push and hold this button for 15 seconds and release to reset your router to its factory defaults.
- **LAN Ports** – Connect Ethernet cables (also called network cables) from your router LAN ports and to your wired network devices.
- **WAN Port** - Connect an Ethernet cable (also called network cable) from your router WAN port and to your xDSL/Cable modem.
- **Power Port** – Connect the included power adapter from your router power port and to an available power outlet.  
**Caution:** Use only the adapter that came with your router.
- **On/Off Power Switch** – Push your router On/Off push button power switch to turn your router “On” (Inner position) or “Off” (Outer position).

**Front Panel View**

- **Power** - This LED indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router.
- **Status** - This LED indicator is blinking green when your router is ready and working successfully. If this LED indicator is solid green on or off, your router is not receiving power or not working properly.
- **WAN (Link/Activity)** – This LED indicator is solid green when your router WAN port is physically connected to the xDSL/Cable modem Ethernet port (also called network port) successfully with an Ethernet cable (also called network cable). The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router.
- **WLAN (Link/Activity)** – This LED indicator is blinking green when the wireless is “On” and functioning properly on your router. This LED indicator will be blinking green rapidly while data is transmitted or received by your wireless clients or wireless network devices connected to your router.
- **LAN 1-4 (Link/Activity)** – These LED indicators are solid green when the LAN ports are physically connected to your wired network devices successfully with an Ethernet cable (also called network cable). These LED indicators will be blinking green while data is transmitted or received through your router LAN ports.
- **Antenna** – The antenna broadcasts wireless signals to allow your wireless clients and wireless network devices to connect to your router.

*Side Panel View*

- **WPS (Wi-Fi Protected Setup)** – Push and hold this button for 3 seconds to activate WPS. The button LED is blinking blue when WPS is activated.

*Application Diagram*

The router is installed in the room where the xDSL/Cable modem (typically supplied by your ISP “Internet Service Provider”) is located in order to physically connect an Ethernet cable (also called network cable) from the router WAN port to the modem network port which connects to the Internet. Wireless signals from the router are broadcasted to allow wireless clients such as laptops with wireless capability to discover and connect to the router providing wireless access to the local network and the Internet.

## 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 web cameras.

- **Modem** – Connects a computer or router to the Internet or ISP (Internet Service Provider).
- **Router** – Connects your wireless and wired network devices to each other and to the modem.
- **Switch** – Allows you to 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 your computers and devices and also connects to the modem.

2. Make sure that your modem is working. Your ISP can help you set up your modem and verify that it's working correctly.
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 "How to connect additional wired devices to your network" on [page 11](#).
5. To set up wireless networking on your router, see "Wireless Networking" on [page 24](#).

#### How to setup your router

The easiest way and fastest way to follow the included Quick Installation Guide or continue to the next section "Before you Install" on [page 6](#), and complete the remaining sections of "Basic Router Setup".

#### Where to find more help

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

- <http://www.trendnet.com/support> (documentation, downloads, FAQs, how to contact technical support)
- Internet service to your home, provided by an ISP (Internet Service Provider)
- Autorun CD (Quick Installation Guide)

## Before you Install

It is recommended, that you verify your Internet connection type with your ISP (Internet Service Provider) and ensure you have all the information for one of the following connection types below before proceeding with the router installation.

### 1. Obtain IP Address Automatically (DHCP)

Host Name (Optional)

Clone Mac Address (Optional)

### 2. Fixed IP address

WAN IP Address: \_\_\_\_\_

(e.g. 215.24.24.129)

WAN Subnet Mask: \_\_\_\_\_

WAN Gateway IP Address: \_\_\_\_\_

DNS Server Address 1: \_\_\_\_\_

DNS Server Address 2: \_\_\_\_\_

### 3. PPPoE to obtain IP automatically

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

### 4. PPPoE with a fixed IP address

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)

### 5. PPTP or Russian PPTP

Type (Dynamic IP or Static IP )

My IP Address: \_\_\_\_\_

(e.g. 215.24.24.129)

Subnet Mask: \_\_\_\_\_

Gateway: \_\_\_\_\_

Server IP: \_\_\_\_\_

PPTP Account: \_\_\_\_\_

PPTP Password: \_\_\_\_\_

Retype Password: \_\_\_\_\_

### 6. L2TP or Russia L2TP

Type (Dynamic IP or Static IP)

My IP Address: \_\_\_\_\_

(e.g. 215.24.24.129)

Subnet Mask: \_\_\_\_\_

Gateway: \_\_\_\_\_

Server IP: \_\_\_\_\_

L2TP Account: \_\_\_\_\_

L2TP Password: \_\_\_\_\_

Retype Password: \_\_\_\_\_

### 7. Russia PPPoE

Type (Dynamic IP or Static IP)

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

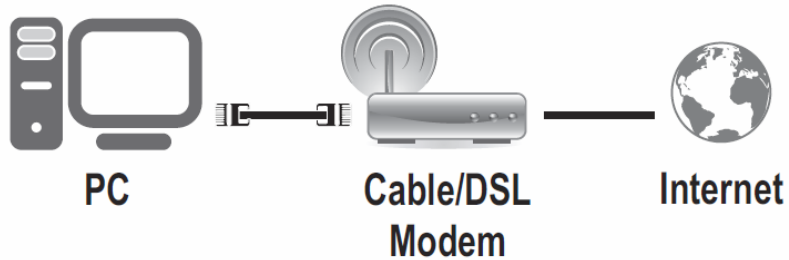
Verify Password: \_\_\_\_\_

IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)



## Installation

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

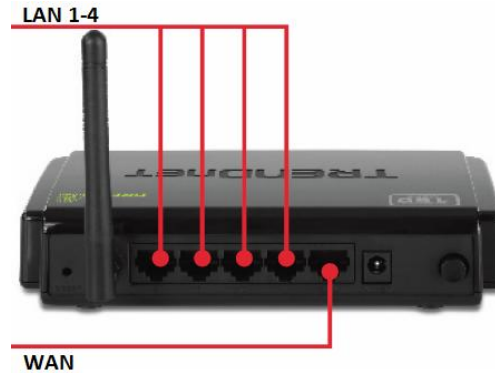


2. Turn off your xDSL/Cable modem.

3. Disconnect the Ethernet cable (also called network cable) from your xDSL/Cable modem and your computer.

4. Connect one end of a network cable to one of your router LAN ports (1-4). Connect the other end of the network cable to the computer Ethernet port (also called network port).

5. Connect one end of a network cable to your router WAN port. Connect the other end of the network cable to your xDSL/Cable modem network port.



6. Connect the included power adapter to your router Power Port and then to an available power outlet. Push the On/Off Power Switch on your router to the "On" (inner) position.



7. Turn on your xDSL/Cable modem.

8. Verify that the following front panel LED indicators on your router: Power (Solid Green), Status (Blinking Green), LAN 1, 2, 3, or 4 (Solid/Blinking Green), WAN (Solid/Blinking Green), and WLAN (Blinking Green)

## Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Next to Language, click the drop-down list to select your preferred language. Enter the default user name and password and then click **Login**.

Default User Name: **admin**

Default Password: **admin**

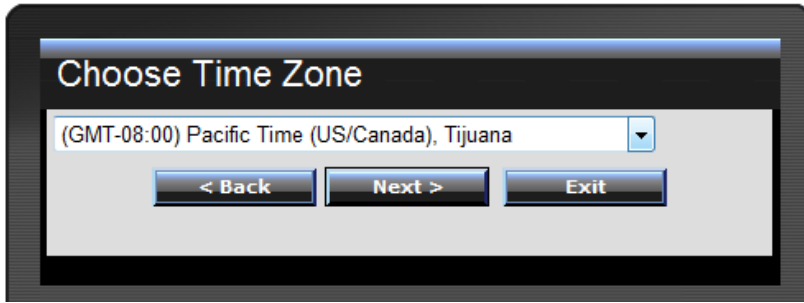
3. The Setup Wizard will automatically appear. Click **Next**.

**Note:** If the Setup Wizard does not automatically appear, click **Wizard**.

4. Enter a new login password for your router and enter it again next to “Verify Password” to confirm. This will change the password required to log into your router. Click **Next**.

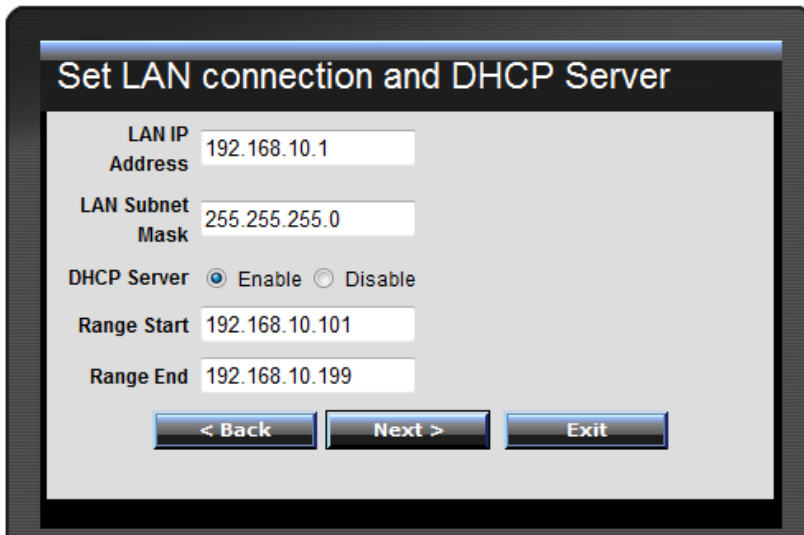
**Note:** Once you change the login password, it will be required every time you log into your router.

5. Select the Time Zone for your router and click **Next**.



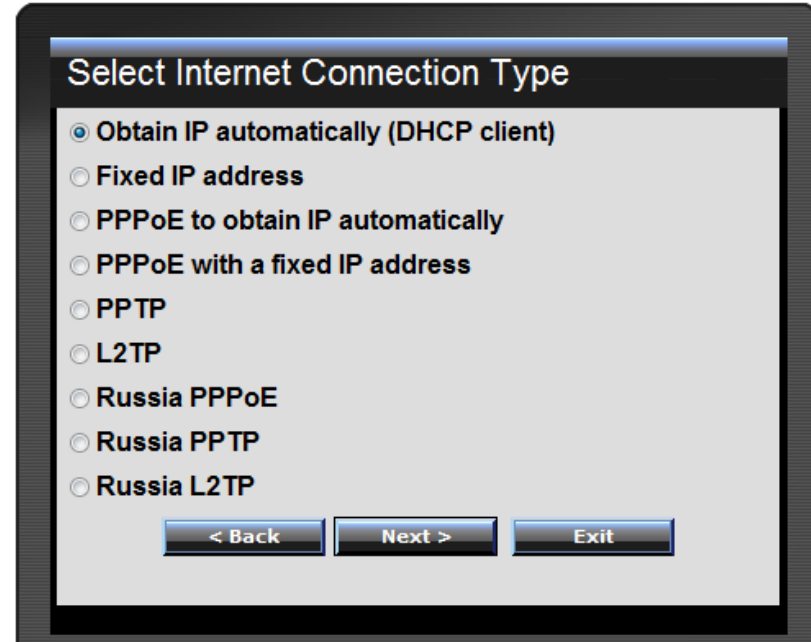
6. Click **Next** at the Set LAN connection and DHCP Server window.

**Note:** If you are an advanced user, you can make LAN IP address interface and DHCP IP address range changes here.



7. Configure the settings based on information provided by your ISP (Internet Service Provider). Follow the Wizard instructions to complete your configuration.

**Note:** Each Internet connection type may have different options.

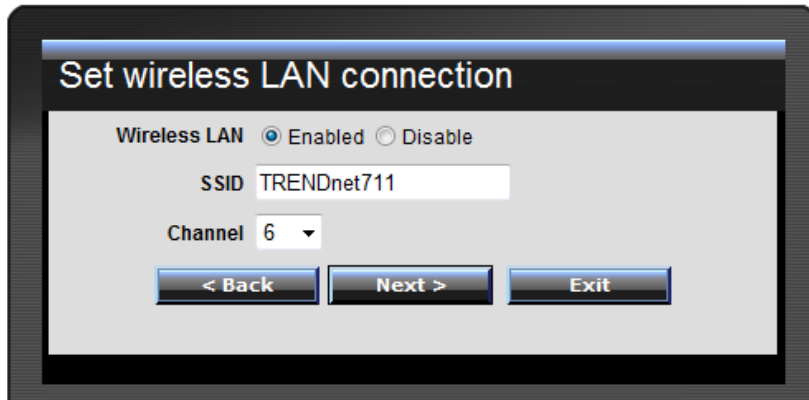


8. **Wireless LAN:** Select Enable for Wireless LAN.

**Note:** Selecting Disable will disable the wireless functionality of the router and will not allow wireless clients to connect.

9. **SSID:** Enter a unique SSID (Wireless Network Name). Choose something that you would easily identify when searching for available wireless networks (using laptops, smart phones, etc.)

Click **Next**.

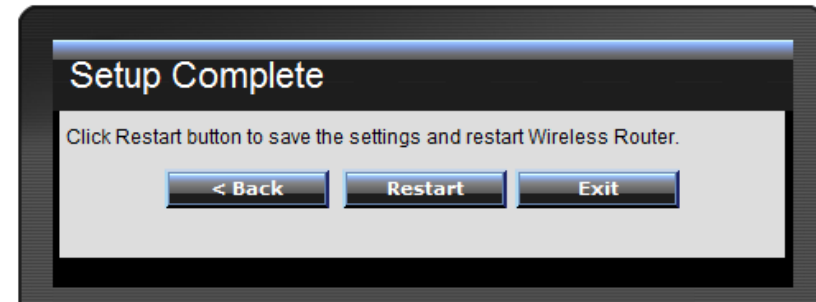


**Note:**

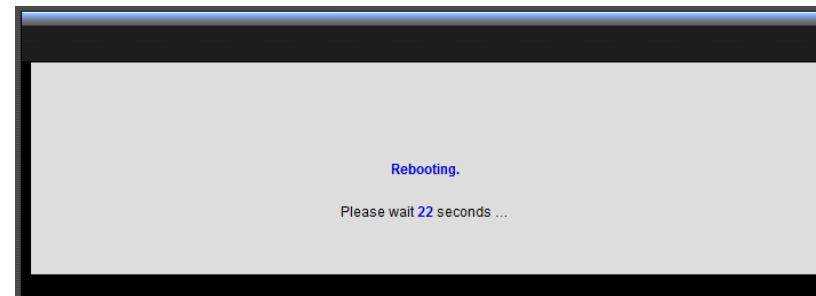
1. To protect your network from unauthorized access, it is recommended to enable wireless encryption. See "How to secure your wireless network" on [page 24](#)) for information on configuring wireless security.

2. Once wireless security is enabled on your router, each wireless device connecting to your router must be configured with the same wireless security type and key.

10. Click **Restart** and wait for your router to reboot.



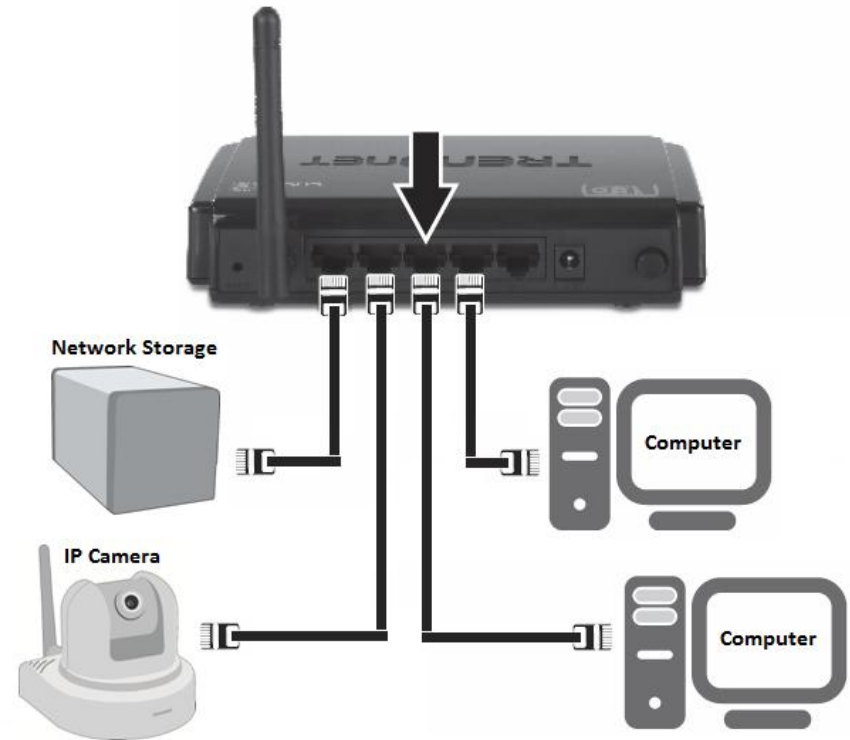
11. Wait for your router to reboot.



## How to connect additional wired devices to your network

You can connect an additional computer or device to your network by connecting one end of an Ethernet cable (also called network cable) from your computer or device Ethernet port (also called network port) to one of the available 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.

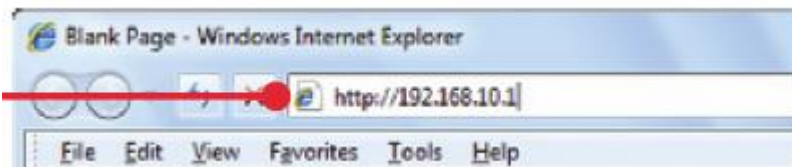


## Advanced Router Setup

### How to access your router management page

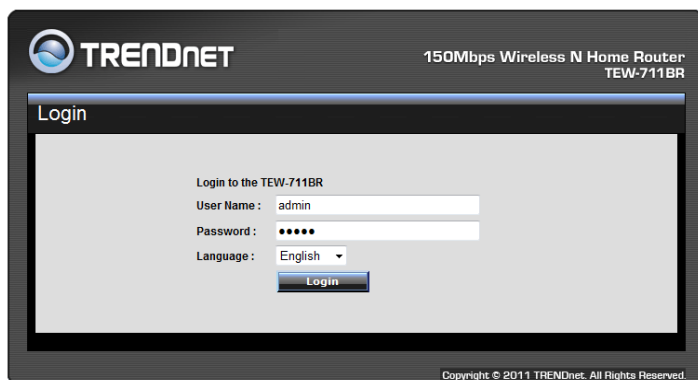
**Note:** Your router management page <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Next to Language, click the drop-down list to select your preferred language. Enter the default user name and password and then click **Login**.

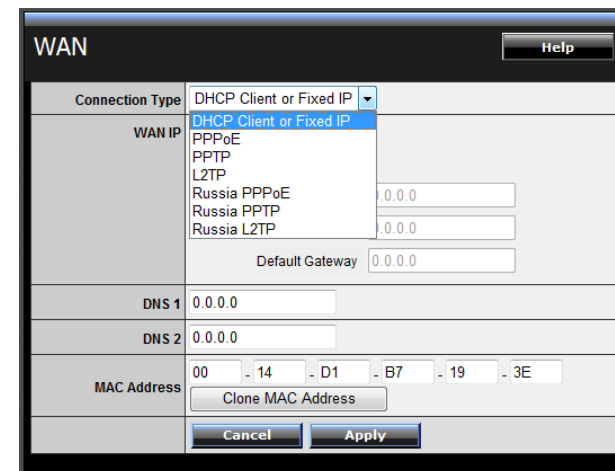
Default User Name: **admin**    Default Password: **admin**



### How to manually configure your Internet connection

Main > WAN

1. Log into your router management page (see "How to access your router management page" on [page 11](#)).
2. Click on **Main**, and click on **WAN**.
3. In the **Connection Type** drop-down list, click the type of Internet connection provided by your ISP (Internet Service Provider).
4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Apply**.



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

**Note:** If your ISP requires a host name to be specified, you can specify it under *Main > LAN & DHCP Server*, in the **Host Name** field. To save changes, click **Apply** at bottom of the page.

## How to clone a MAC address

Main > WAN

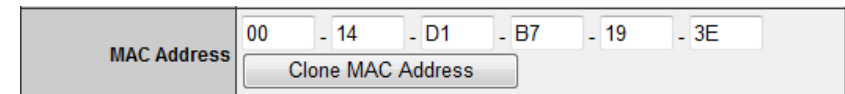
On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs (Internet Service Providers) register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and 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 "How to access your router management page" on [page 11](#)).

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

3. Under your Internet connection settings, find the **MAC Address** section shown below.



MAC Address	00	-	14	-	D1	-	B7	-	19	-	3E
<input type="button" value="Clone MAC Address"/>											

4. Click either **Clone MAC Address** to clone the MAC address of the computer you are currently using or manually enter the 12-digit MAC address of your old router.

5. To save changes, click **Apply**.



<input type="button" value="Cancel"/>	<input type="button" value="Apply"/>
---------------------------------------	--------------------------------------

## How to set your router date and time

Main > Time

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).
  2. Click on **Main**, and click on **Time**.
  3. Next to **Time Zone**, click the drop-down list to select your **Time Zone**.
  4. Next to **Synchronize the clock with**, you can choose one of the following options:
    - **Manual** – Set your router date and time manually in the **Set Time** section. To save changes, click **Apply**.  
**Note:** Time is specified in 24-hour format.  
 OR
    - **Automatic** – 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). Next to **Daylight Saving**, set the annual range when daylight saving is activated. To save changes, click **Apply**.
- Note:** NTP servers are used for computers and other network devices to synchronize time across network.

5. You can verify the time/date settings next to **Local Time** at the top of the page. **Local Time** displays the current date and time set on your router.

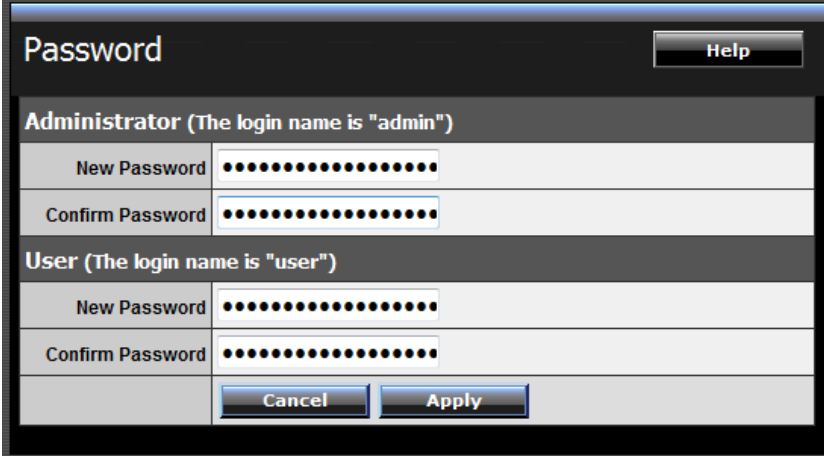
The screenshot shows the 'Time' configuration page. At the top right is a 'Help' button. The 'Local Time' field displays 'Sep/2/2010 1:42:48'. The 'Time Zone' is set to '(GMT-08:00) Pacific Time (US/Canada), Tijuana'. The 'Synchronize the clock with' dropdown is set to 'Manual'. The 'Default NTP server' field is empty. The 'Set Time' section shows 'Year 2011', 'Month Aug', 'Day 12', 'Hour 11', 'Minute 17', and 'Second 21', with a 'Set Time' button. The 'Daylight Saving' section has 'Enabled' and 'Disabled' radio buttons, with 'Disabled' selected. The 'Start' is set to 'Jan 1st Sun' and the 'End' is set to 'Jan 1st Sun'. At the bottom are 'Cancel' and 'Apply' buttons.



## How to change your router login password

Main > Password

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).
2. Click on **Main**, and click on **Password**.
3. Under the **Administrator** section, in the **New Password** field, enter the new password, and in the **Confirm Password** field, retype the new password again to confirm.
4. To save changes, click **Apply**.



The screenshot shows a web-based configuration interface for a router. The main heading is "Password" with a "Help" button to its right. Below this, there are two distinct sections for password configuration. The first section is for the "Administrator" (login name "admin") and includes "New Password" and "Confirm Password" fields, both masked with dots. The second section is for a "User" (login name "user") and also includes "New Password" and "Confirm Password" fields, both masked with dots. At the bottom of the form, there are "Cancel" and "Apply" buttons.

**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 default password “admin”.

**User (Optional):** The User account is an additional account used for viewing the settings on the router management page only. Accessing the router management page using the User account will restrict access to viewing only and will not allow any settings to be changed.

Default User Name: user

Default Password: user

## How to change your router IP address

Main > LAN & DHCP Server

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 “How to access your router management page” on [page 11](#)).

2. Click on **Main**, and click on **LAN & DHCP Server**.

3. Enter the router IP address settings.

IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

- **IP Address** – Enter the new router IP address.  
(e.g. 192.168.200.1)
- **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.

4. To save changes, click **Apply**.

**Note:** You will need to access your router management page using your new router IP address to access the router management page. (e.g Instead of using the default <http://192.168.10.1> using your new router IP address will use the following format using your new router IP address [http://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access your router management page.

## How to set up the DHCP server on your router

Main > LAN & DHCP Server

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 "How to access your router management page" on [page 11](#)).
2. Click on **Main**, and click on **LAN & DHCP Server**.
3. Review the DHCP Server settings.
  - **DHCP Server** – Enable or Disable the DHCP server.
  - **Start IP** – Changes the starting address for the DHCP server range. (e.g. *192.168.10.20*)
  - **End IP** – Changes the last address for the DHCP server range. (e.g. *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.

- **Domain Name (Optional)** – Specifies a domain name to assign to computers or devices. (e.g. *trendnet.com*)
- **Lease Time** – Click the drop-down list to select the lease time.

**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.

4. To save changes, click **Apply**.

DHCP Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Start IP	192.168.10.101
End IP	192.168.10.199
Domain Name	
Lease Time	1 Week ▼

**Dynamic DHCP List** – You can view the list of active lease entries for computers or devices that have been assigned IP addresses automatically from the DHCP server on your router.

Dynamic DHCP List		
Host Name	IP Address	MAC Address
	192.168.10.101	48:5B:39:2C:FB:36

## How to set up DHCP reservation

Main > LAN & DHCP Server

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 “How to allow access using virtual server” on [page 31](#)) or special applications (also called port triggering, see “How to allow access using special applications” on [page 33](#)).

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).

2. Click on **Main**, and click on **LAN & DHCP Server**.

3. Review the DHCP reservation settings.

- **Static DHCP**– Enable or Disable the DHCP reservation feature.
- **Name** – Enter a name for the reservation.
- **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)

**Note:** You cannot assign IP addresses outside of the DHCP range. The IP address is required to be within the DHCP IP address range (Start IP & End IP).

- **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)
- **Add** - Saves the reservation.

Static DHCP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	<input type="button" value="Cancel"/> <input type="button" value="Apply"/>
Name	trendnet1
IP Address	192.168.10.101
MAC Address	48:5B:39:2C:FB:36
	<input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>

**Static DHCP List** – You can view the list of reservations for computers or devices that have been created in this list.

Static DHCP List		
Host Name	IP Address	MAC Address
trendnet1	192.168.10.101	48:5B:39:2C:FB:36

To modify an existing reservation, click on the entry in the Static DHCP list. When selected, the entry will be highlighted.

trendnet1	192.168.10.101	48:5B:39:2C:FB:36
-----------	----------------	-------------------

- **Update** – Saves changes to an existing reservation.
- **Delete** – Removes an existing reservation.
- **Cancel** – Discards changes to existing reservation.

## How to enable/disable UPnP on your router

Management > Remote Management

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 “How to access your router management page” on [page 11](#)).

2. Click on **Management**, and click on **Remote Management**.

3. Next to **UPnP**, click **Enabled** or **Disabled** to turn the feature on or off on your router.

**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 **Apply**.

UPnP  Enabled  Disabled

## How to allow/deny VPN connections through your router

Management > Remote Management

VPN (Virtual Private) Network) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work their remote office/home office, or while traveling.

If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically does not require any additional configuration changes.

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).

2. Click on **Management**, and click on **Remote Management**.

3. Next to **PPTP**, **L2TP**, or **IPsec** (depending the VPN protocol your corporation requires) click **Enabled** or **Disabled** to turn the VPN pass through feature on or off on your router.

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

PPTP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
L2TP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPSec	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

4. To save changes, click **Apply**.



## How to allow remote access to your router management page

Management > Remote Management

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

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).
2. Click on **Management**, and click on **Remote Management**.
3. Under the **HTTP** section, click **Enabled**.
  - **Port**– 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 IP Range** – It is recommended to leave this setting as \*, to allow remote access from anywhere on the Internet.  
**Note:** You can enter a specific range of Internet IP addresses that are allowed to access your router management page, all others will be denied.

<b>HTTP</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Port: <input type="text" value="8080"/> Remote IP Range: From <input type="text" value="*"/> To <input type="text"/>
-------------	---

4. To save changes, click **Apply**.

## How to expose a device on your network to the Internet

Access > 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 also very **insecure** method.

It is strongly recommended to use **virtual server** (also called port forwarding, see “How to allow access using virtual server” on [page 31](#)) instead, to allow access to your computers or network devices from the Internet.

1. Make sure to configure your computer or network device to use a static IP address or you can use the DHCP reservation feature (see “How to setup DHCP reservation” on [page 17](#)).
2. Log into your router management page (see “How to access your router management page” on [page 11](#)).
3. Click on **Access**, and click on **DMZ**.
4. Next to **DMZ Enable**, click **Enabled**.
5. Next to **DMZ Host IP**, enter the IP address you assigned to the computer or network device to expose to the Internet.

<b>DMZ Enable</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>DMZ Host IP</b>	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/>	

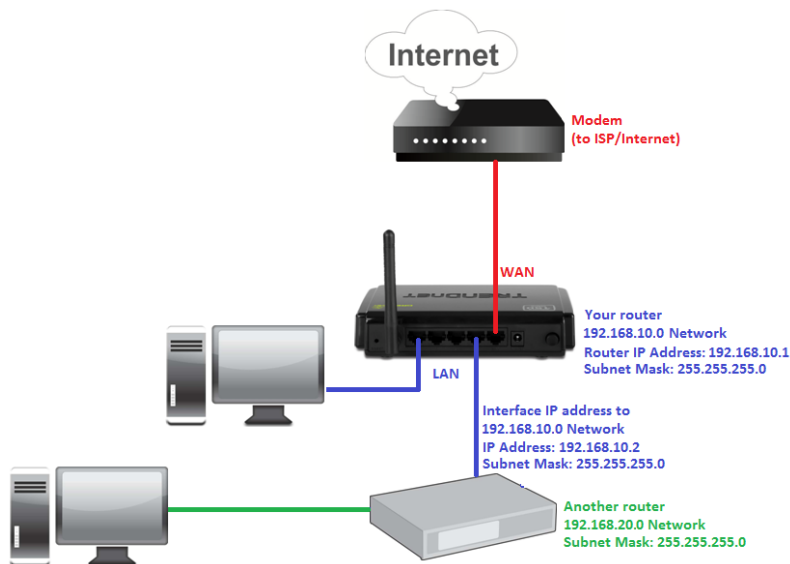
6. To save changes, click **Apply**.

## How to 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, 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 “How to access your router management page” on [page 11](#)).

2. Click on **Routing**, and click on **Static**.

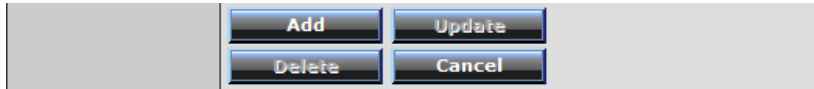
3. Review the static route settings.

- **Network Address** – Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
- **Network Mask** – Enter the subnet mask of the destination network for the route. (e.g. 255.255.255.0)
- **Gateway Address** – Enter the gateway to the destination network for the route. (e.g. 192.168.10.2)
- **Interface** – Click the drop-down list and select the Interface on your router where the route is active. (e.g. LAN)
- **Metric** – Enter the metric or priority of the route. The metric range is 1-15, the lowest number 1 being the highest priority. (e.g. 1)

Network Address	<input type="text"/>
Network Mask	<input type="text"/>
Gateway Address	<input type="text"/>
Interface	LAN ▾
Metric	<input type="text"/>



- **Add** – Saves the static route.



To modify an existing reservation, click on the entry in the static route list. When selected, the entry will be highlighted.

192.168.20.0	255.255.255.0	192.168.10.2	LAN	1
--------------	---------------	--------------	-----	---

- **Update** – Saves changes to an existing static route.
- **Delete** – Removes an existing static route.
- **Cancel** – Discards changes to existing static route.

## How to enable dynamic routing on your router

*Routing > Dynamic*

You may want set up your router to route computers or devices on your network to other local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other routers to exchange information about the network.

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

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).
2. Click on **Routing**, and click on **Dynamic**.
3. Select the appropriate dynamic routing protocol and version communicate with other routers.

- **Transmit** – Allows your router to send out network information to other routers so other routers can dynamically build routes to your network.
  - **Disabled** – Disable sending routing information from your router to other routers.
  - **RIP 1** - Sends out routing information to other routers using the RIP version 1 protocol.
  - **RIP 2** – Sends out routing information to other routers using the RIP version 2 protocol.
- **Receive** - Allows your router to receive network information from other router so your router can build routes to other networks.
  - **Disabled** – Disable receiving routing information from other routers to your router.
  - **RIP 1** - Receive routing information from other routers using the RIP version 1 protocol.
  - **RIP 2** – Receive routing information from other routers using the RIP version 2 protocol.

Transmit	<input checked="" type="radio"/> Disabled <input type="radio"/> RIP 1 <input type="radio"/> RIP 2
Receive	<input checked="" type="radio"/> Disabled <input type="radio"/> RIP 1 <input type="radio"/> RIP 2

4. Click **Apply** to save the changes or click **Cancel** to discard the changes.



## Wireless Networking

### How to choose the type of security for your wireless network

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.

- **WEP:** Legacy encryption method supported by most 802.11b/g hardware. Older hardware may only support up to WEP encryption.
- **WPA:** Legacy encryption method supported in most 802.11g hardware.
- **WPA2:** Currently the most secure method of wireless security and required for 802.11n performance.

**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 Comparison	WEP	WPA	WPA2
Wireless Standard	IEEE 802.11a/b/g	IEEE 802.11a/b/g	IEEE 802.11a/b/g/n
Performance	Up to 54Mbps	Up to 54Mbps	Up to 450Mbps*
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

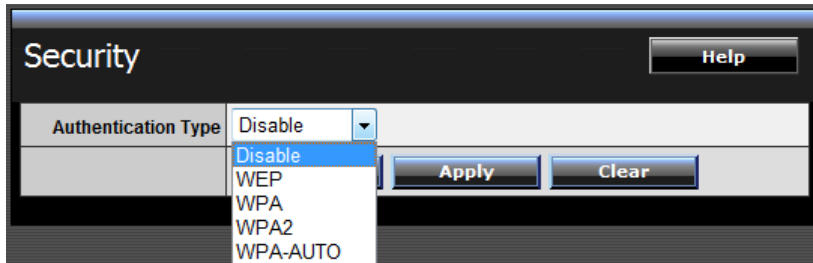
\*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 450Mbps)

## How to secure your wireless network

Wireless > Security

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 22](#)), you can set up wireless security.

1. Log into your router management page (see “How to access your router management page” on [page 11](#)).
2. Click on **Wireless**, and click on **Security**.
3. Click on the **Authentication Type** drop-down list to select your wireless security type.



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

Authentication Type	WEP
WEP	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key
Mode	HEX
WEP Key	64-bit
Key 1	<input checked="" type="radio"/> 0000000000
Key 2	<input type="radio"/> 0000000000
Key 3	<input type="radio"/> 0000000000
Key 4	<input type="radio"/> 0000000000
<input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Clear"/>	

- **WEP**– Choose **Open System** or **Shared Key**.

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

- **Mode** – Choose **HEX** or **ASCII**.

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

- **WEP Key** – 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.

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

- **Key 1-4** – Choose a key index 1,2,3, or 4 and enter the key.

**Note:** The Key Index # must also match when configuring wireless devices to connect to your wireless network.

If selecting **WPA** or **WPA2** (Wi-Fi Protected Access) **PSK** (Preshared Key), please review the **WPA** or **WPA2 PSK** settings to configure and click **Apply** to save the changes.

**Note:** It is recommended to choose the specific security type **WPA** or **WPA2**, instead of choosing **WPA-AUTO**.

Authentication Type	WPA
PSK / EAP	<input checked="" type="radio"/> PSK <input type="radio"/> EAP
Cipher Type	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> Auto
Passphrase :	●●●●●●●●
Confirmed Passphrase :	●●●●●●●●
<input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Clear"/>	

- **PSK/EAP**– Choose **PSK** (Preshared Key) or **EAP** (Extensive Authentication Protocol, also called RADIUS) Remote Authentication Dial-In User Service).

**Note:** It is recommended to use PSK because it is easier to setup and simply requires you to create a passphrase compared to EAP which requires you to connect an external RADIUS server and requires more configuration.

- **Cipher Type** – Choose **TKIP**, **AES**, or **Auto**.

**Note:** For best the wireless performance and compatibility with wireless devices:

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA2** security, it is recommended to use **AES**.
- It is recommended to configure the specific cipher type instead of choosing **Auto**.
- **Passphrase** – Enter the passphrase.
- **Confirmed Passphrase** – Re-enter the passphrase.

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

For advanced users, if selecting **WPA** or **WPA2** (Wi-Fi Protected Access) **EAP** (Extensible Authentication Protocol, also called RADIUS, Remote Authentication Dial-In User Service), please review the WPA or WPA2 EAP settings to configure and click **Apply** to save the changes.

Authentication Type	WPA
PSK / EAP	<input type="radio"/> PSK <input checked="" type="radio"/> EAP
Cipher Type	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> Auto
Radius Server 1	IP: 0.0.0.0
	Port: 1812
	Shared Secret: ●●●●●●●●
Radius Server 2 (optional)	IP: 0.0.0.0
	Port: 1812
	Shared Secret: ●●●●●●●●
<input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Clear"/>	

- **RADIUS Server 1/2** - Configure the RADIUS server settings.

**Note:** RADIUS Server 2 is optional and can be configured as a backup if there are any issues with RADIUS Server 1.

- **IP** – Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
- **Port** – Enter the port your RADIUS server is configured to use for RADIUS authentication.  
**Note:** It is recommended to use port 1812.
- **Shared Secret** – Enter the shared secret used to authorize your router with your RADIUS server.

## ***How to 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.

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

- PBC (Push Button Configuration) Method
  - Hardware Push Button - located physically on your router
  - 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.

### **PBC (Hardware Push Button)**

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting, then push and hold the WPS button located on your router for 3 seconds and release it. A blue LED on your router WPS button will flash indicating that the WPS setup process has been activated on your router. (See "Side Panel View" on [page 4](#))

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