

User's Guide



N300 Wireless Gigabit Router

TEW-639GR

Table of contents

Product Overview	4
Package Contents	4
Features	4
Product Hardware Features.....	5
Application Diagram	7
Wireless Performance Considerations	7
Basic Router Setup	8
Creating a Home Network	8
Router Installation	9
Connect additional wired devices to your network.....	13
Wireless Networking and Security	14
How to choose the type of security for your wireless network	14
Secure your wireless network	15
Connect wireless devices to your router	17
Connect wireless devices using WPS	17
Basic wireless settings	18
Steps to improve wireless connectivity	20
Advanced wireless settings.....	21
Wireless Distribution System (WDS).....	22
Access Control Filters	22
Access control basics	22
Port Range and Service Block.....	22
MAC Filters	23
Advanced Router Setup.....	23

Access your router management page.....	23
Using the Configuration Menu	23
Change your router login password	24
Change your router device name	24
Manually configure your Internet connection	25
Clone a MAC address.....	25
Change your router IP address	26
Set up the DHCP server on your router	26
Set up DHCP reservation	27
Set your router date and time.....	27
Set schedules	28
QoS (Quality of Service).....	28
Open a device on your network to the Internet.....	28
DMZ.....	28
Virtual Server	29
Special Applications	30
Gaming.....	31
Inbound Filter.....	32
Add static routes to your router.....	32
Enable dynamic routing on your router	33
Enable Application Level Gateway (ALG).....	33
Enable/disable UPnP on your router	34
Identify your network on the Internet	34
Allow remote access to your router management page	35
Router Maintenance & Monitoring	35
Reset your router to factory defaults.....	35
Router Default Settings	36

Backup and restore your router configuration settings 36

Reboot your router 37

Upgrade your router firmware 37

Remotely check router status..... 38

View your router log 38

Router Status 38

 Check the router system information..... 38

 Dynamic DHCP List..... 40

 Wireless Station List 40

Management Page Structure 41

Technical Specifications..... 42

Troubleshooting 43

Appendix 44

Product Overview



Package Contents

In addition to the access point, the package includes:

- TEW-639GR N300 Wireless Gigabit Router
- CD-ROM (Utility and User's Guide)
- Multi-Language Quick Installation Guide
- Network cable Ethernet Cable (1.5m / 5ft.)
- Power Adapter (12V, 1A)

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

The TEW-639GR 2.4GHz 300Mbps Wireless N Gigabit Router is an high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the TEW-639GR provides data transfers at up to 300Mbps when using 11n connection. This router is also back compatible with 802.11g or 11b devices. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 11n's speed when you mix 11n and 11b/g devices, but you will not lose the ability to communicate when you incorporate the 11n standard into your 11b/g network. You may choose to slowly change your network by gradually replacing the 11b/g devices with 11n devices.

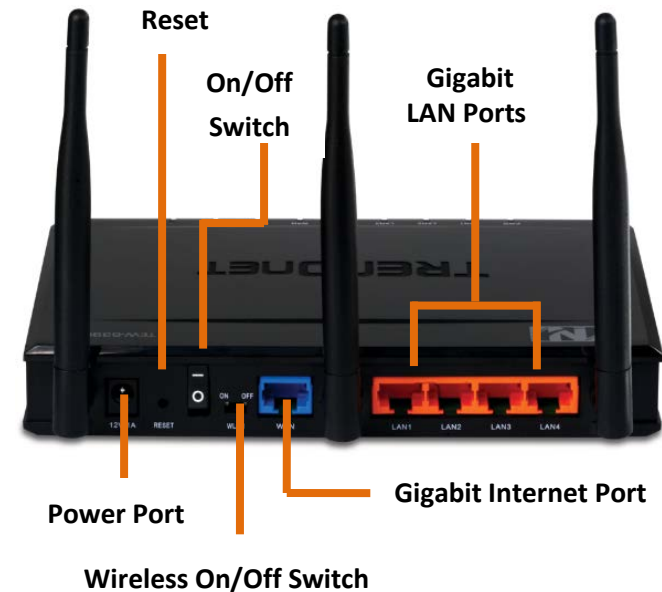
- 4 x 10/100/1000Mbps Auto-MDIX LAN ports
- 1 x 10/100/1000Mbps WAN port (Internet)
- 1 x external wireless radio on/off switch (turn off your wireless network when away)
- 1 x external Wi-Fi Protected Setup (WPS) button
- One-touch wireless security setup using the Wi-Fi Protected Setup (WPS) button when connecting to a WPS adapter
- Wireless Distribution System (WDS) support
- Compatible with most popular cable/DSL Internet service providers using Dynamic/Static IP, PPPoE, PPTP and L2TP
- High-speed wireless data rates up to 300Mbps using an IEEE 802.11n connection
- 3 external antennas provide high-speed performance and expansive wireless coverage
- Advanced Firewall protection with Network Address Translation (NAT) and Stateful Packet Inspection (SPI)
- Access restriction with Internet Access Control; time scheduling and MAC filtering
- Built-in pre-configured virtual servers and Application Level Gateway services for special Internet applications
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications

- Multiple pass-through sessions for popular VPN applications (IPSec, L2TP and PPTP)
- WMM quality of service support
- Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, Safari, and Chrome
- 3- year limited warranty

*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



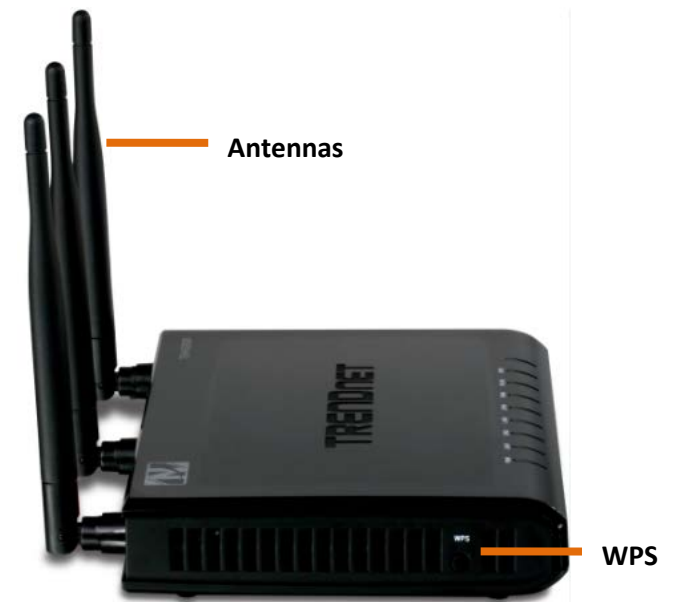
- **Power port:** Connect the included power adapter from your router power port and to an available power outlet.
- **Reset:** Press and hold this button for 10 seconds to reset your router to default settings
- **On/Off power switch (EU version):** Switch to the on position to power on the device.
- **Wireless On/Off Switch:** Switch to the on or off position to turn on your wireless router's wireless network or off your wireless network.
- **Internet port:** 1x 10/100/1000Mbps Auto-MDIX port. Connect an Ethernet cable from your router WAN port to your modem.
- **GigabitLAN ports:** 4x 10/100/1000Mbps Auto-MDIX ports. Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.

Front View



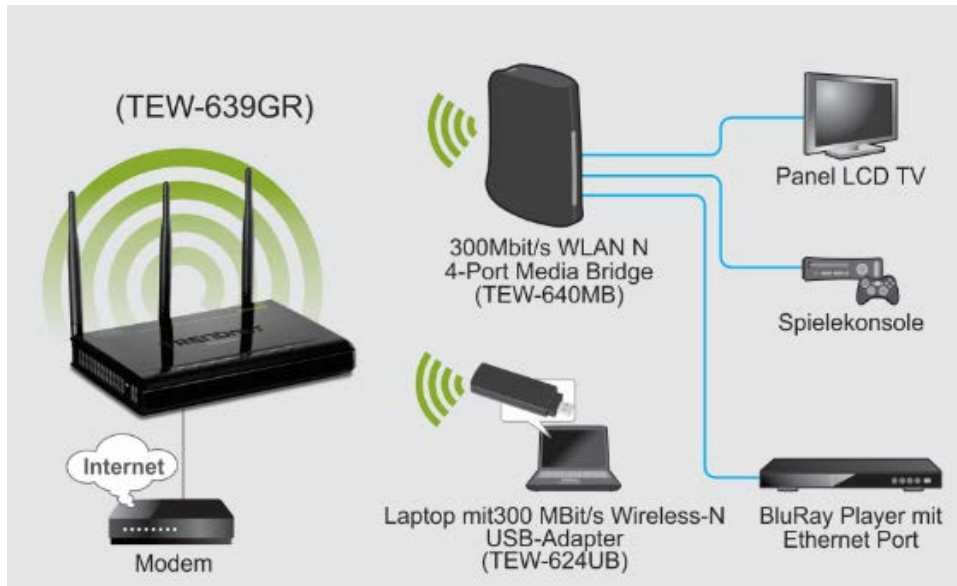
- **Power LED** -This LED indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router.
- **WAN (Link/Activity) LED** – This LED indicator is solid green when your router WAN port is physically connected to the modem Network port (also called network port) successfully with a Network cable. The LED indicator will be
- **LAN 1-4 (Link/Activity) LEDs** – These LED indicators are solid green when the LAN ports are successfully connected to your wired network devices (which are turned on). These LED indicators will blink green while data is transmitted or received through your router's LAN ports.
- **2.4GHz WLAN (Link/Activity) LED** – 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.
- **WPS LED** - The button LED is blinking when WPS is activated.

Side View



- **Antenna:** Fixed antennas to transmit wireless signals.
- **WPS (Wi-Fi Protected Setup)** – Push and hold this button for 5 seconds to activate WPS.

Application Diagram



The router is installed near the modem connected to its Gigabit Internet port of the router which connects to the Internet. Wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) thereby providing Internet access.

Wireless Performance Considerations

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

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

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

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 13.
5. To set up wireless networking on your router, see "[Wireless Networking and Security](#)" on page 14.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "[Router Installation](#)" on page 9 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 (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: _____

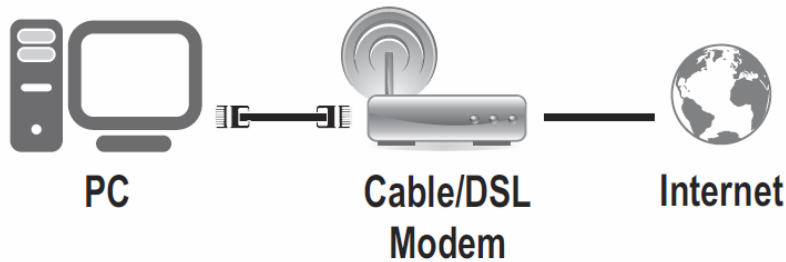
Password: _____

Verify Password: _____

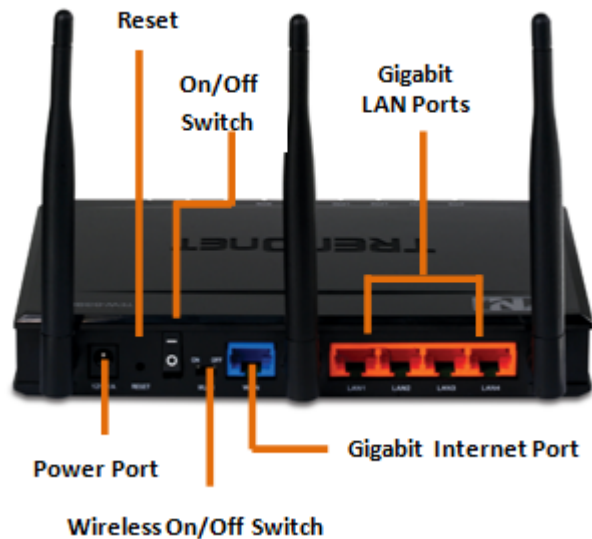
IP Address: _____ (e.g. 215.24.24.129)

Hardware Installation

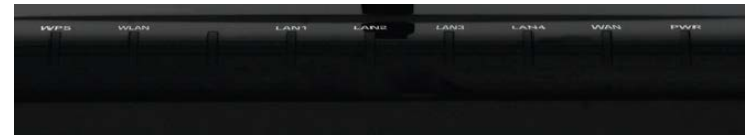
1. Verify that you have an Internet connection when connecting your computer directly to your modem.



2. Turn off your modem.
3. Disconnect the Network cable from your computer to your modem.



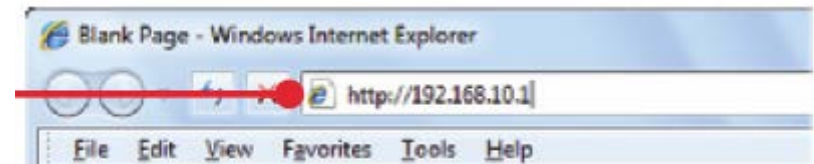
4. Using a Network cable, connect the Gigabit Internet port on the router to your modem.
5. Using another Network cable, connect your computer to one of the four Gigabit ports on the router.
6. Plug in the power adapter, connect it to the router's power port, and then push the On/Off Power Switch to the "On" position (pushed in).
7. Turn on your 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 for ports for which devices are connected), 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.



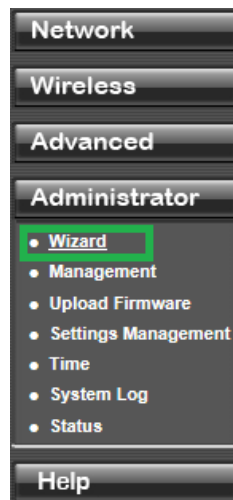
2. Enter the default user name and password and then click Login.

Default User Name: **admin**

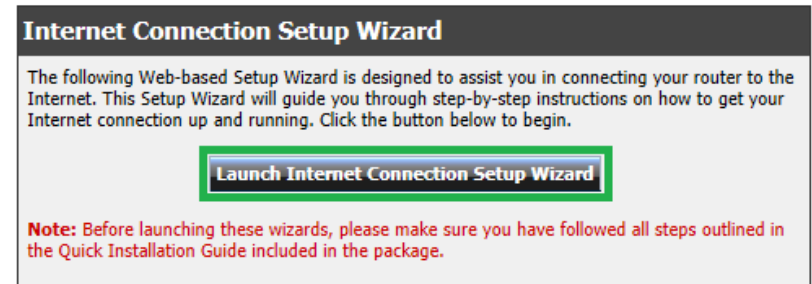
Default Password: **admin**



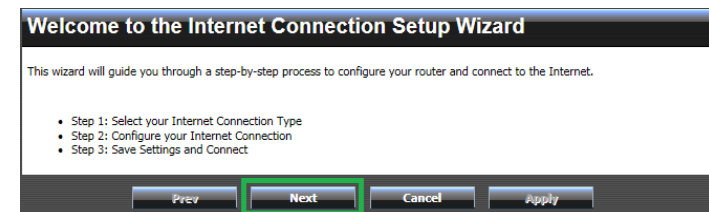
3. Click on the Administrator button and then Wizard button on the left side.



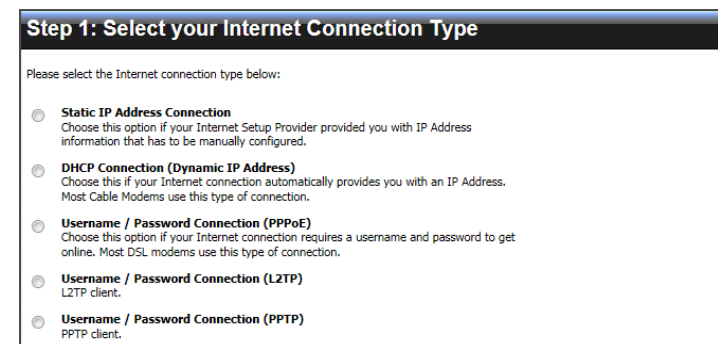
4. Click “Launch Internet Connection Setup Wizard” to setup your Internet connection on the router.



5. Click Next to begin the wizard



7. Select your Internet connection type and click Next to continue. Note: The most common Internet connection used is DHCP.



8. Some ISP (Internet Service Providers) requires their customer to clone MAC address of their computer into the router. Click “Clone Your PC’s MAC Address” if your ISP requires this step. Click Next to continue.

Step 2: DHCP Connection (Dynamic IP Address)

To set up DHCP connection, please make sure that you are connected to the router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the router.

To set up DHCP connection, you may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

MAC Address : (optional)

Host Name : (optional)

9. Verify if your settings are correct and click Apply to complete the Internet Setup Wizard.

Step 3: Setup Complete!

The Internet Connection Setup Wizard has completed. Click the Apply button to save and apply your settings.

Internet Connection Type : DHCP

Host Name :

10. Click OK to apply your settings.

Save and apply the changes?

11. The router will reboot once the process is completed. Click the Wizard button again to run the Wireless Setup Wizard.

Network

Wireless

Advanced

Administrator

- Wizard
- Management
- Upload Firmware
- Settings Management
- Time
- Status

Help

12. Click “Launch Wireless Security Setup Wizard”.

Wireless Security Setup Wizard

The following Web-based Setup Wizard is designed to assist you in your wireless network setup. This Setup Wizard will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the router.

13. Click Next to begin

Welcome to the Wireless Security Setup Wizard

This wizard will guide you through a step-by-step process to set up your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

14. Configure the Wireless Network Name (SSID) of the router. This name will be used when connecting to your wireless network. Click Next to continue

Step 1: Name your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID):

15. Select the type of wireless security to use. Click Next to continue. It is recommended to use wireless security to protect your wireless network from any intruders.

Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are two levels of wireless security -Good Security and Best Security. The level you choose depends on the security features your wireless adapters support.

BEST Select this option if your wireless adapters SUPPORT WPA2

BETTER Select this option if your wireless adapters SUPPORT WPA

GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA

NONE Select this option if you do not want to activate any security features

16. Enter the password or encryption key. Click Next to continue.
17. Verify your wireless settings are correct and click Apply.

Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

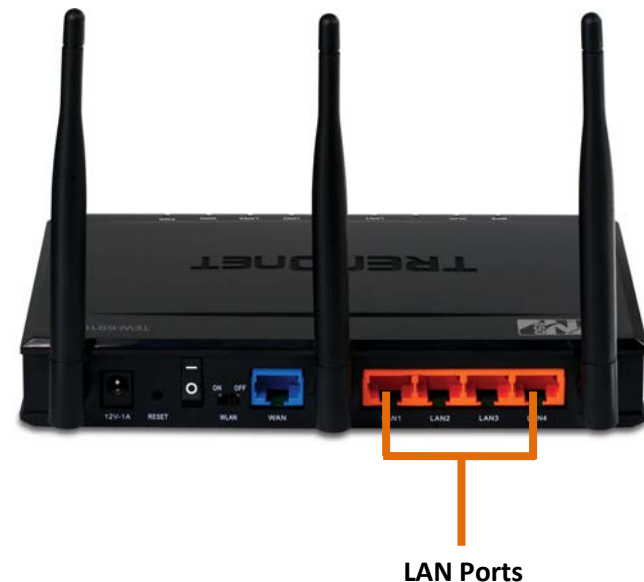
Wireless Network Name (SSID):	TRENDnet639
Encryption:	WPA2-PSK/AES (also known as WPA2 Personal)
Pre-Shared Key:	1234567890

Note: Save your wireless settings in a location you can find easily in case you forget the applied wireless settings.

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 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 unsecured 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

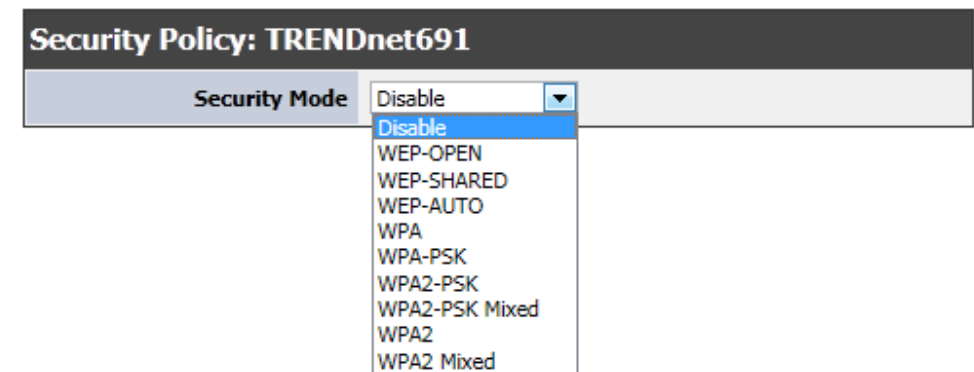
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps)

Secure your wireless network

Wireless > 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 14), you can set up wireless security.

1. Log into your router management page (see "[Access your router management page](#)" on page 24).
2. Click on Wireless band you would like to configure either **Wireless** and click on **Security**.
3. Click on the **Security Mode** drop-down list to select your wireless security type.



Selecting WEP:

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

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

Selecting WPA-PSK, WPA2-PSK, or WPA2-PSK Mixed (WPA2-PSK recommended):

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

- Select a Cipher Type. When selecting **WPA-PSK** security, it is recommended to use **TKIP**.
- When selecting **WPA2-PSK Mixed** security, it is recommended to use **AES**.
- When selecting **WPA2-PSK** security, it is recommended to use **AES**.

Create your Wireless security Pres-Shared Key (password or key):

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

- **Passphrase** – Enter the passphrase.
 - This is the password or key that is used to connect your computer to this router wirelessly
- **Confirmed Passphrase** – Re-enter the passphrase.
Note: 8-63 alphanumeric characters (a,b,C,?,,/,1,2, etc.)*

Selecting WPA, WPA2, or WPA2Mixed:

The following section outlines options when selecting **EAP** (Extensive Authentication Protocol), **EAP** (Extensible Authentication Protocol) is also called Remote Authentication Dial-In User Service or **RADIUS**.

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

- **Cipher Type**
 - When selecting **WPA** security, it is recommended to use **TKIP**.
 - When selecting **WPA-Auto** security, it is recommended to use **AES**.
 - When selecting **WPA2** security, it is recommended to use **AES**.
- **Key Renewal Interval**
 - Set the renewal key interval based on seconds.
- **PMK Cache Period**
 - Set the cache period based on minutes
- **Pre-Authentication**
 - Enable or disable pre-authentication of your wireless encryption
- **RADIUS Server** - Configure the RADIUS server settings.
 - **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.

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 48 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.

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. 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. A blue LED on your router WPS button will flash indicating that the WPS setup process 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 > WiFi Protected Setup*

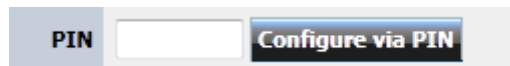
In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 24).
2. Click on **Wireless** and click on **WPS**.
3. To add a wireless device to your network, simply the push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are connecting, then in your router management page next to **Push Button Configuration**, click **Configure via PBC**.

**PIN (Personal Identification Number)***Wireless > WiFi 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 23).
2. Click on **Wireless** and click on **WPS**.
3. Next to **PIN**, enter the WPS PIN of the wireless device you are connecting and click **Configure via PIN**.

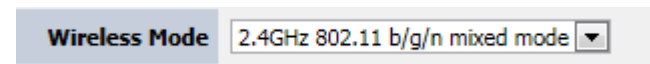


Note: You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.

Basic wireless settings*Wireless > Basic*

This section outlines available management options under the Basic Wireless sub tab.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Wireless** and click on **Basic**.
3. To save changes to this section, click **Apply** when finished.



- **Wireless Mode:** Select the appropriate mode for your network.
 - **2.4GHz 802.11b/g/n mixed mode** – Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
 - **2.4GHz 802.11b/g mixed mode** – This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
 - **2.4GHz 802.11n only mode** – This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if you have older 802.11g wireless clients, they will no longer be able to connect to this router.
 - **2.4GHz 802.11g only mode** – This mode only allows devices to connect to the router using older and slow 802.11g technology (typically not recommended).
 - **2.4GHz 802.11b only mode** – This mode only allows devices to connect to the router using older and slow 802.11b technology (typically not recommended).
- Note:** Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (2.4GHz 802.11b/g/n mixed mode) for the best compatibility.

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.

Wireless Name(SSID)	TRENDnet639
----------------------------	-------------

- **Wireless 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. By default, the router broadcast TRENDnet639 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember.

Multiple SSID1	<input type="text"/>
Multiple SSID2	<input type="text"/>
Multiple SSID3	<input type="text"/>

- **Multiple SSID:** This router support additional SSID, you can set an additional of 3 SSSID for your wireless network.

Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
--------------------------------------	---

- **Broadcast Network Name (SSID):**
 - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
 - **Disabled** 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.

Note: Setting this option to **Disabled**, will disable WPS functionality.

Frequency (Channel)	AutoSelect
----------------------------	------------

- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.

WDS	Enable
AP MAC Address	<input type="text"/>

- **WDS:** This acronym stands for Wireless Distribution System and when enabled it creates a wireless bridge connection between your wireless router and an access point that supports WDS.
 - **AP MAC Address:** Enter the MAC address of the access point you would like the router to WDS to. You will also have to enter the MAC address of the router into the access point to establish the WDS or bridge connection. This wireless router supports up to 3 WDS connections.

Channel BandWidth	<input checked="" type="radio"/> 20MHz <input type="radio"/> Auto 20/40MHz
--------------------------	--

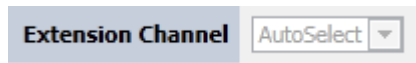
- **Channel Width:** This setting only applies to wireless devices connecting at 802.11n. Select the appropriate channel width for your wireless network.
 - **20 MHz** – This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n. This setting may provide more stability than Auto 20/40 MHz for connectivity in busy wireless environments where there are several wireless networks in the area.
 - **Auto 20/40 MHz** – This mode can automatically switch between using a single 20MHz channel or 40MHz (two 20MHz channels). When 40MHz is active, this mode is capable of providing higher performance only if the wireless devices support the 40MHz channel width. Enabling 20/40MHz typically results in substantial performance increases when connecting to an 802.11n client.

Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
-----------------------	--

- **Guard Interval:** The purpose of the guard interval is to introduce immunity propagation delays, echoes and reflections to which digital data is normally sensitive to
 - **Long: Guard interval of 800nsec.**
 - **Auto: Router automatically set the interval**



- **MCS:** Modulation and Coding Scheme is the value that determines the modulation, coding number of spatial channels.



- **Extension Channel:** Extension channel is used when Channel Bandwidth is set to "Auto 20/40MHz" and the channel being used is statically assigned. This allows you to statically assign the extended channel to use in 40MHz.



- **HT Physical Mode:** Use these settings to allow enhance your wireless router channel bandwidth.
 - **Channel Bandwidth:** Select Auto 20/40MHz to allow your wireless router to to channel bond and increase your wireless performance.
 - **Control Sideband:** Select which section of the channels to channel bond.

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. 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 or installing additional access points.

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.

Advanced Wireless	
Beacon Interval:	100 (20-1024 ms)
Data Beacon Rate (DTIM):	1 (1-255)
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Protection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
MPDU Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
WLAN Partition:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
STBC:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
20/40MHz Coexist:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%

- **Beacon Interval:** 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: 25-1000)

- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **RTS Threshold** – The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2346 (range: 256-2346)
- **IAPP(Inter-Access Point Protocol):** IEEE 802.11F or Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
- **Protection:** These protection mechanisms ensure that a STA that is a potential interferer defers any transmission for a known period of time. These mechanisms are used to ensure that non-ERP STAs do not interfere with frame exchanges using ERP PPDU between ERP STAs and that non-HT STAs do not interfere with frame exchanges using HT PPDU between HT STAs, thereby allowing non-ERP and/or non-HT STAs to coexist with ERP and/or HT STAs.
- **20/40MHz CoExist:** Enable this option to allow legacy wireless adapters (802.11b/g) to connect to your wireless router.
- **RF Output Power:** Select the output power you would like the wireless router to operate in.

Multicast-to-Unicast Enable Disable

- **Multicast-to-Unicast:** Some 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. Enable this feature when using application that requires multicast traffic.

Wireless Distribution System (WDS)

Wireless > Basic

WDS or Wireless Distribution System allows your router to establish a wireless bridge connection to another access point. To use this feature the access point you want to connect has to also support WDS mode.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Select Enable in the Wireless Distribution System section.

Wireless Distribution System(WDS)

WDS

AP MAC Address

AP MAC Address

AP MAC Address

AP MAC Address

3. Enter the MAC address of the access point you want to establish a wireless bridge connection with.
4. Log into your access point and enter the MAC address of your router. Please see the access point's user manual for more information on how to configure WDS mode.
5. To save changes to this section, click **Apply** when finished.

Access Control Filters

Access control basics

Advanced > Access Control

Port Range and Service Block

Advanced > Access Control

You may want to block computers or devices on your network access to specific ports (used or required by a specific application) to the Internet.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advance**, click on **Access Control**.

Access Control Function

Access Control

Apply

3. Select **Enable** to enable all access controls

Add Port Range and Service Block Rule

Policy Enable

Policy Name

Schedule

Client IP Address ~

Rule Define Special Service User Define

Service Name	Description	Enabled
WWW	HTTP, TCP Port 80, 8080	<input type="checkbox"/>
Email Sending	SMTP, TCP Port 25	<input type="checkbox"/>
Email Receiving	POP3, TCP Port 110	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
DNS Query	UDP Port 53	<input type="checkbox"/>
TCP Protocol	All TCP Port	<input type="checkbox"/>
UDP Protocol	All UDP Port	<input type="checkbox"/>

Add **Cancel**

4. Review the settings under **Port Range and Service Block Rule** section
 - **Enabled:** Selecting **Enable** turns on the filter
 - **Policy Name:** Enter a name for the Protocol/IP Filter.
 - **Schedule:** Select the defined schedule you would like to have the rule to be applied. (see "[Set Schedule](#)" section on page 31).
 - **IP Range** – Enter the IP address or IP address range to apply the protocol/IP filter. (e.g. *192.168.10.20-192.168.10.20* or *192.168.10.20-192.168.10.30*).

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

- **Rule Define:** Select a predefined rule you would like to apply or click User Define to manually set the rule.

5. Click **Add** to save settings and **Save Status** on the top of the page to apply settings.

MAC Filters

Wireless > Security

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 wireless network.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Wireless**, click on **Security**.

Wireless MAC Filter	
Filter Mode	Allow ▼
MAC Address	<input type="text"/> (Ex: 00:11:22:33:44:55)

3. Review the MAC Filter options.

- **Filter Mode:** Select the mode applied to t listed MAC addresses.
 - **Allow** computers/devices with MAC addresses listed below to access the local network, web management, and the Internet.
 - **Deny** computers/devices with MAC addresses listed below to access the local network, web management, and the Internet

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.

4. Click **Apply** to save settings

Advanced Router Setup

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. Enter the default user name and password and then click **Login**.

Default User Name: **admin**

Default Password: **admin**

Using the Configuration Menu

Whenever you want to configure your TEW-639GR, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the TEW-639GR.

- Open the Web browser.
- Type in the current **IP Address** of the AP (i.e. <http://192.168.10.1>)
- Type **admin** in the **User Name** field.
- The **Password** is **admin**.
- Click **Login In**.



When you log into the unit the initial screen you will see is the status page that provides system information and network configurations.

Status

The device status.

System Info	
Firmware Version	v3.1.3.0, 24-Aug-2012
System Time	Fri Aug 24 13:02:23 2012
System Up Time	00:04:08

Internet Configurations	
Connected Type	DHCP Client
WAN IP Address	192.168.231.31
Subnet Mask	255.255.255.0
Default Gateway	192.168.231.254
Primary Domain Name Server	192.168.231.254
Secondary Domain Name Server	

LAN	
MAC Address	00:14:D1:9B:70:A8
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

Wireless LAN	
Wireless Radio	Radio On
MAC Address	00:14:D1:9B:70:A8
Network Name (SSID)	TRENDnet639
Channel	9
Security Mode	WPA2

Change your router login password

Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Administrator**, and click on **Management**.

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password"/> (Max Length: 16 characters)
Idle Timeout	<input type="text" value="300"/> (120-3600 seconds)

3. Under the **Administrator Settings** section, in the **Password** field, enter the new password
4. Enter the idle timeout time (in seconds) of when you would want to have log in prompt to appear.
5. To save changes, click **Apply**.

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".

Change your router device name

Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Administrator**, and click on **Management**.

- Under the **Device Name Settings** section, in the **Device Name** field, enter the new device name to show up on your network as reference to the router.
- To save changes, click **Apply**.

Manually configure your Internet connection

Network > WAN Setting

- Log into your router management page (see "[Access your router management page](#)" on page 23).
- Click on **Network**, and click on **WAN Setting**.

- In the **Connection Type** drop-down list, click the type of Internet connection provided by your Internet Service Provider (ISP).
- Complete the fields required by your ISP.
- Complete the optional settings only if required by your ISP.
- To save changes, click **Apply**.

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

Clone a MAC address

Network > WAN Setting

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.

- Log into your router management page (see "[Access your router management page](#)" on page 23).
- Click on **Main**, and click on **WAN**.
- Under your Internet connection settings, find the **MAC Address** section shown below.

- Select **Enabled** in the pull down menu and manually enter the 12-digit MAC address of your old router.
- To save changes, click **Apply**.

Change your router IP address

Network > LAN Setting

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 23).
2. Click on **Network**, and click on **LAN Setting**.

LAN Interface Setting	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
MAC Address	00:0C:43:28:80:DF

3. In **LAN Interface Setting** section enter the router IP address settings.
 - **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)
 - **MAC Address:** The MAC address of your router
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.

Set up the DHCP server on your router

Network > LAN Setting

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 23).
2. Click on **Network**, and click on **LAN Setting**.

DHCP Server Setting	
DHCP Server	Enable ▾
DHCP Start IP	192.168.10.100
DHCP End IP	192.168.10.200
DHCP Lease Time	604800 (seconds)

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.
 - **DHCP 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**.

Set up DHCP reservation

Network > LAN Setting

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 33) or special applications (also called port triggering, see "[Special Applications](#)" on page 34).

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Network**, and click on **LAN Setting**.

3. Under **Add DHCP Reservation** section, review the DHCP reservation settings.

- **Enable:** Enable or Disable the DHCP reservation feature.
- **Computer 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.
- **Edit** – Saves changes to an existing reservation.
- **Delete** – Removes an existing reservation.

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

DHCP Reservations List					
Enable	Computer Name	IP Address	MAC Address	Edit	Delete

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

Set your router date and time

Main > Time

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Administrator**, and click on **Time**.

3. Select **Enable NTP Server**, to use a NTP server for the time settings. Or you can manually set the time settings by not selecting **NTP Server** option.

4. To manually set the time settings. Select from the pull down menu the year, month day and time you would like to apply on the router.

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

Set schedules

Advanced > Schedule

Your router has features Virtual Server rules and Access Controls that can turn on or off through schedules.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Administrator**, and click on **Time**.

3. Review the Schedule settings.
 - **Rule Name:** Enter a name for the virtual server.
 - **Days:** Select the days you would like the rule to be applied or select **All Week** to enable the rule all week.
 - **All Day:** Select if you would like the rule to be applied through the day of the select days.
 - **Start/End Time:** Select the start and end time you would like the schedule to follow.
 - **Delete:** Removes an existing schedule.
 - **Edit:** Modifies an existing schedule.
4. To save changes, click **Add**.

QoS (Quality of Service)

Network > QoS

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Network**, and click on **QoS**.
3. Review the DHCP reservation settings.

- **Quality of Service:** Enable or Disable the Quality DHCP reservation feature.
- **Bandwidth:** Select from the pull down menu Limit bandwidth of upload manually with 'User Defined' or set the bandwidth limit via drop-down menu (between 64Mbits ~ 230Mbits) per device on network.
- **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)

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

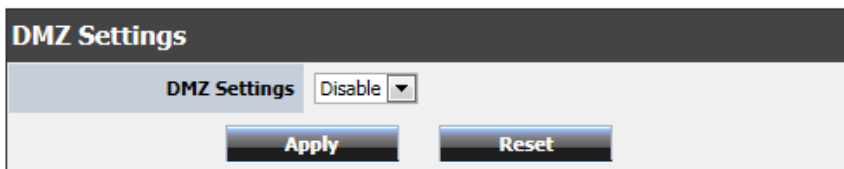
Advanced > DMZ

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 29) 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 (or you can use the DHCP reservation feature to ensure the device has a fixed IP address) see "[Set up DHCP reservation](#)" on page 27. Signing up for a Dynamic DNS service (outlined in the DDNS section) 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 23).
3. Click on **Advanced**, and click on **DMZ**.



3. Select **Enable** in the **DMZ Settings** section.
4. Enter the IP address you assigned to the computer or network device to expose to the Internet.
5. To save changes, click **Apply**.

Virtual Server

Advanced > 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 28) 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 "[Gaming](#)" section on page 31.

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 DynDNS section).

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **Virtual Server**.

3. Review the virtual server settings.
 - **Rule Enabled:** Selecting **Enabled** turns on the virtual server and selecting **Disabled** turns off the virtual server.
 - **Rule Name:** Enter a name for the virtual server.
 - **IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).
 - **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).

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.
 - **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.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "[Set Schedule](#)" section on page 28).

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.

- **Add:** Saves a new virtual server entry.
- **Clear:** Discard changes to an existing virtual server.
- **Edit:** Modifies an existing virtual server.
- **Delete:** Removes an existing virtual server.

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (See DynDNS section).
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 or you can use the DHCP reservation feature (see "[Set up DHCP reservation](#)" on page 28).

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 23).
5. Click on **Advanced**, and click on **Virtual Server**.
6. Click **Enabled** to turn on this virtual server.
7. Next to **Name**, you can enter another name for the virtual server, otherwise, leave the default name.
8. Next to **LAN Server**, 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 **Add**.

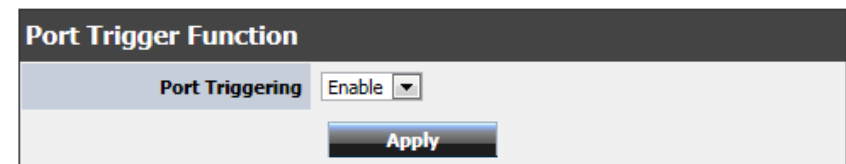
Special Applications

Advanced > Special Application

Special applications (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 34.

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 23).
2. Click on **Advanced**, and click on **Special Application**.



3. Select **Enable** under **Port Triggering Function**.

4. Review the special application settings.

- **Rule Enable:** Selecting **Enabled** turns on the special application.
- **Rule Name:** Enter a name for the special application.
- **Match Protocol:** Select the protocol to be forwarded to the device. **TCP**, **UDP**, or you can select **Both** to choose both TCP and **UDP**.
- **Match Port:** Enter the ports or port range to be forwarded to the device. (e.g. 2000-2038,2069,2081,2200-2210).
- **Trigger Protocol:** Select the protocol requested by the device. **TCP**, **UDP**, or you can select **Both** to choose both TCP and **UDP**.
- **Trigger Port:** Enter the ports or port range requested by the device. (e.g. 554-554 or 6112-6112).

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 "[Set Schedule](#)" section on page 28).
- **Add:** Saves a new special application.
- **Delete:** Removes an existing special application.
- **Edit:** Modifies an existing special application.
- **Cancel:** Discard changes to an existing special application.

Gaming

Advanced > Gaming

Gaming allows you to define multiple 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. Using this feature is more secure compared to using DMZ (see "[DMZ](#)" on page 28) 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 34).

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **Gaming**.

3. Review the virtual server settings.

- **Rule Enabled:** Selecting **Enabled** turns on the virtual server
- **Rule Name:** Enter a name for the virtual server or select predefined rules in the pull down menu.
- **IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).
- **TCP Ports to Open:** Enter the TCP port you would like to set.
- **UDP Ports to Open:** Enter the UDP port you would like to set.

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.

- **Inbound Filter:** Select the inbound filter you have applied to reflect on the applied rule.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "[Set Schedule](#)" section on page 28).
- **Add:** Saves a new virtual server entry.
- **Clear:** Discard changes to an existing virtual server.
- **Edit:** Modifies an existing virtual server.
- **Delete:** Removes an existing virtual server.

Inbound Filter

Advanced > Inbound Filter

Inbound filters allow you to control data going through your router from the Internet. The feature allows you to control devices from your network through IP address.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **Inbound Filter**.

3. Review the inbound filter settings.
 - **Rule Enabled:** Selecting **Enabled** turns on the virtual server
 - **Action:** Select which rule you would like to apply, Allow or Deny data.
 - **IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).

Add static routes to your router

Advanced > Routing

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 23).
2. Click on **Advanced**, and click on **Routing**.

3. Review the static route settings.
 - **Destination IP Address:** Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
 - **Destination IP Netmask:** 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 1-15, the lowest number 1 being the highest priority. (e.g. 1)
- **Interface:** Click the drop-down list and select the Interface on your router where the route is active. (e.g. LAN)
- **Add:** Saves the static route.

Enable dynamic routing on your router

Advanced > Routing

You may want to setup 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 "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **Routing**.

Add Static Route	
Destination IP Address :	<input type="text" value="0.0.0.0"/>
Destination IP Netmask :	<input type="text" value="0.0.0.0"/>
Gateway :	<input type="text" value="0.0.0.0"/>
Metric :	<input type="text" value="1"/>
Interface :	<input type="text" value="LAN/WLAN"/>
<input type="button" value="Add"/> <input type="button" value="Clear"/>	

3. Review the settings under **Add Static Route** section and click **Add** to save settings.
 - **Destination IP:** The IP address of packets that will take this route.
 - **Gateway:** Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN.

- **Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.
- **Interface:** Specifies the interface -- LAN or WAN -- that the IP packet must use to transit out of the router, when this route is used.
- **Clear:** Re-initialize this area of the screen, discarding any changes you have made.
- **Routes List:** The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Route" section is activated for editing. Click the Enable checkbox at the left to directly activate or de-activate the entry.

Enable Application Level Gateway (ALG)

Advanced > ALG

You may want to setup your router to allow computers to use certain protocols or services on your network. Application Level Gateway or ALG allows you to simply enable or disables these services.

Note: Default all services are enabled.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **ALG**.
3. View and select which service you would like to enable or disable.

Application Level Gateway (ALG) Configuration		
Service Name	Description	Enable
Email Receiving	Post Office Protocol - Version 3 (POP3)	<input checked="" type="checkbox"/>
Email Receiving	Simple Mail Transfer Protocol(SMTP)	<input checked="" type="checkbox"/>
Streaming Media	Real Time Transport Protocol (RTP)	<input checked="" type="checkbox"/>
Streaming Media	Real Time Streaming Protocol (RTSP)	<input checked="" type="checkbox"/>
Streaming Media	Microsoft Media Server protocol(WMP/MMS)	<input checked="" type="checkbox"/>
Streaming Media-VoIP	Session Initiation Protocol(SIP)	<input checked="" type="checkbox"/>
Streaming Media-VoIP	NetMeeting (H.323)	<input checked="" type="checkbox"/>
File transfer	File Transfer Protocol (FTP)	<input checked="" type="checkbox"/>
File transfer	Trivial File Transfer Protocol (TFTP)	<input checked="" type="checkbox"/>
Remote control	Telnet	<input checked="" type="checkbox"/>
Instant messaging	MSN messenger	<input checked="" type="checkbox"/>
IPSec		<input checked="" type="checkbox"/>

- **RIP mode:** Allows your router to send out network information to other routers so other routers can dynamically build routes to your network.
- **Email Receiving (POP3):** Allows POP3 protocol to be used through your router
- **Email Receiving (SMTP):** Allows SMTP protocol to be used through your router
- **Streaming Video (RTP):** Allows RTP video protocol to be used through your router
- **Streaming Media (RTSP):** Allows STMP video protocol to be used through your router
- **Streaming Media (WMP/MMS):** Allows WMP/MMS protocol to be used through your router
- **Streaming Media-VoIP (SIP):** Allows SIP protocol to be used through your router
- **Streaming Media-VoIP (H.323):** Allows H.323 protocol to be used through your router
- **File Transfer (FTP):** Allows FTP protocol to be used through your router
- **File Transfer (TFTP):** Allows TFTP protocol to be used through your router
- **Remote control (Telnet):** Allows Telnet protocol to be used through your router
- **Instant messaging (MSN):** Allows MSN instant messaging protocols to be used through your router

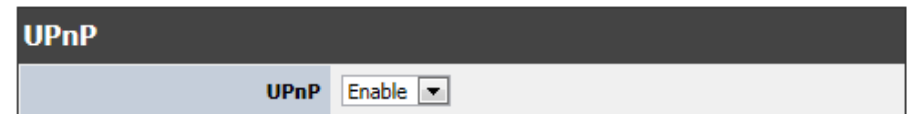
- **IPSec:** Allows IPSec VPN passthrough to be used through your router

Enable/disable UPnP on your router

Advanced > 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 23).
2. Click on **Advanced**, and click on **Advanced Network**.



3. Next to **UPnP**, select **Enable** or **Disable** on the pull down menu 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**.

Identify your network on the Internet

Administrator > Management

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 23).
3. Click on **Administrator** and click on **Management**.

4. In the Dynamic DNS Provider drop-down list, select the provider you selected, and enter your information in the fields.
 - Host Name: Personal URL provided to you by your Dynamic DNS service provider (e.g. *www.trendnet.dyndns.biz*)
 - User Name: The user name needed to log in to your Dynamic DNS service account
 - Password: This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.
5. To save changes, click **Apply**.

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 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 23).
2. Click on **Administrator**, and click on **Management**.

3. On the Remote Management section, select **Enabled** in the **Remote Control** setting.
 - **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)
4. To save changes, click **Apply**.

Router Maintenance & Monitoring

Reset your router to factory defaults

Administrator > Settings Management

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 36.

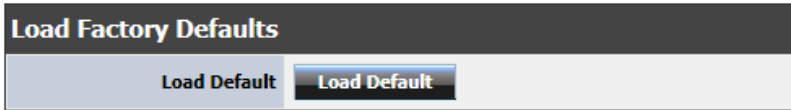
There are two methods that can be used to reset your router to factory defaults.

- **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 23).
2. Click on **Administrator** and click on **Settings Management**.



3. Under **Load Factory Default**, click **Load Default**. When prompted to confirm this action, click **OK**.

Router Default Settings

Administrator User Name	admin
Administrator Password	admin
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	Enabled

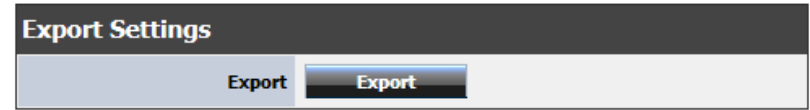
Backup and restore your router configuration settings

Administrator > Settings Management

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 23).
2. Click on **Administrator** and click on **Settings Management**.



3. Under **Export Settings** section, click **Export**.
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: *cfg.bin*)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Administrator** and click on **Settings Management**.



3. Under **Import Settings**, next to **Settings file location**, depending on your web browser, click on **Browse** or **Choose File**.
5. A separate file navigation window should open.
6. Select the router configuration file to restore and click **Load**. (Default Filename: *cfg.bin*). If prompted, click **Yes** or **OK**.
7. Wait for the router to restore settings.

Reboot your router

Administrator > Settings Management

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.

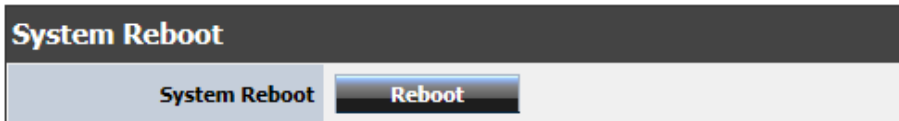
- **Turn the router off** for 10 seconds using the router On/Off switch located on the rear panel of your router, see "[Product Hardware Features](#)" on page 5.

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 23).
2. Click on **Administrator** and click on **Settings Management**.



3. Under **System Reboot** section, click **Reboot**.

Upgrade your router firmware

Administrator > Settings Management

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 23).
2. Click on **Administrator** and click on **Upload Firmware**.



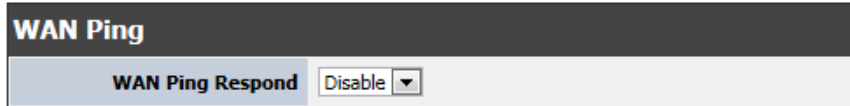
3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.
5. Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.
6. Click **Upgrade**. If prompted, click **Yes** or **OK**.

Remotely check router status

Advanced > Advanced Network

For remote troubleshooting purposes, you may want to check your routers connectivity in a remote location. You can disable or enable your router to respond to ping request through the Internet.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Advanced**, and click on **Advanced Network**.



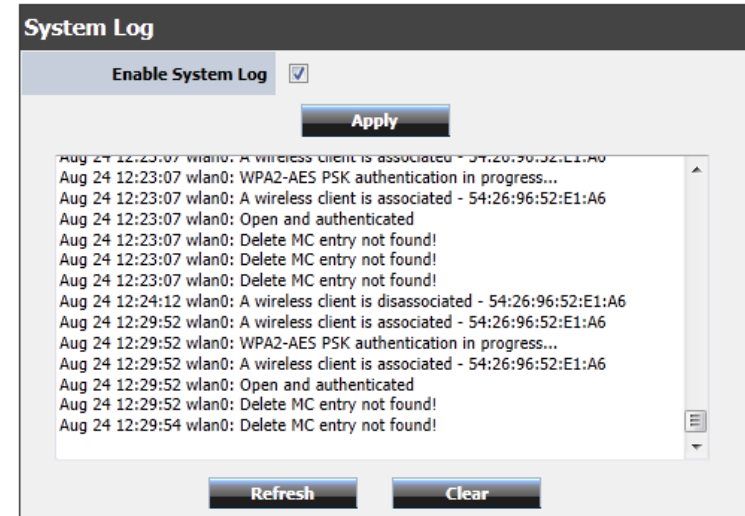
3. Next to **WAN Ping Respond**, select **Enable** or **Disable** on the pull down menu to turn the feature on or off on your router.

View your router log

Toolbox > View 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 23).
2. Click on **Administrator**, and click on **System Log**.
3. Select **Enable System Log**.



Router Status

Check the router system information

Administrator > Status

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 23).
2. Click on **Administrator** and click on **Status**.

System Info

System Info	
Firmware Version	v3.1.3.0, 24-Aug-2012
System Time	Fri Aug 24 13:33:22 2012
System Up Time	00:35:07

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

Internet Configurations

Internet Configurations	
Connected Type	DHCP Client
WAN IP Address	192.168.231.31
Subnet Mask	255.255.255.0
Default Gateway	192.168.231.254
Primary Domain Name Server	192.168.231.254
Secondary Domain Name Server	

- **Connected Type:** The WAN connection type applied on your router.
- **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.

- **DNS (Domain Name System)** – The current DNS address(es) assigned to your router port or interface configuration.
- **Renew:** Click this option to renew your WAN IP address.
- **Release:** Click this option to release the WAN IP address of your router.

LAN Information

LAN	
MAC Address	00:0C:43:28:80:DF
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

- **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.

Wireless LAN

Wireless LAN	
Wireless Radio	Radio On
MAC Address	00:14:D1:9B:70:A8
Network Name (SSID)	TRENDnet639
Channel	9
Security Mode	WPA2

- **Wireless Radio:** The current state of your router's wireless signal.
- **MAC Address:** The MAC address of your router's wireless LAN or interface configuration.
- **Channel** – Displays the current wireless channel your router is operating.
- **Network Name (SSID)/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID

Dynamic DHCP List

Network > DHCP Client 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.

1. Log into your router management page (see "[Access your router management page](#)" on page 23).
2. Click on **Network**, and click on **DHCP Client List**.

DHCP Clients		
MAC Address	IP Address	Expires in

Wireless Station List

Wireless > Station List

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 23).
2. Click on **Wireless**, and click on **Station List**

Wireless Network			
MAC Address	Mode	Rate	Singal

Management Page Structure

Network

- WAN Setting
 - Clone MAC Address
- LAN Setting
 - DHCP Reservation
- QoS
- DHCP Client List

Wireless

- Basic
 - WDS
- Advanced
- Security
 - MAC Filter
- WPS
- Station List

Advanced

- DMZ
- Virtual Server
- Routing
- Access Control
- Application Level Gateway (ALG)
- Special Applications
- Gaming
- Inbound Filter
- Schedule

- Advanced Network
 - UPnP
 - WAN Ping
 - Ping tool

Administrator

- Wizard
 - Internet Setup Wizard
 - Wireless Setup Wizard
- Management
 - Password
 - DDNS
 - Remote Management
- Upload Firmware
- Settings Management
 - Export Settings
 - Import Settings
 - Load Factory Defaults
 - Reboot
- Time
- System Log
- Status

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX) and IEEE 802.3ab (1000BaseT) Wireless: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
WAN	1 x 10/100/1000Mbps Auto-MDIX port (Internet)
LAN	4 x 10/100/1000Mbps Auto-MDIX port
Wireless On/Off Switch	Turn on/off wireless LAN
On/Off Power Switch	Electrical power on/off switch
WPS Button	Wi-Fi Protected Setup (WPS) automated wireless connection push button
Reset Button	Reset button to Factory Default
Connection Type	Dynamic IP, Static (fixed) IP, PPPoE, PPTP, L2TP
NAT Firewall	3K configurable NAT entries; restricted NAT IP ranges, port ranges and schedule Port triggering for 24 special applications ALG support (enable/disable support) –RTP/RTSP, AOL, FTP, ICMP, WMP/MMS, NetMeeting, SIP
WDS	Enable/disable Wireless Distribution System support
UPnP	UPnP IGD 1.0 compliant
DMZ	DMZ host, 24 configurable Virtual Servers and Game Servers
DNS	Static or WAN assigned DNS servers; 4 verified services for DDNS
Internet Access Control	Time based Internet access; port range/service filtering; Internet domain restriction; 32 user defined schedules, 24 MAC address filter entries
LED Indicator	Power, LAN1~LAN4, WAN, WLAN, WPS

Power Switch	On/Off power switch
Power Adapter	12V DC, 1A external power adapter
Power Consumption	779mA
Dimension (L x W x H)	150 x 163 x 26 mm (5.9 x 6.4 x 1.0 in)
Weight	350g (0.8 lb)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F); Storage: -20°~ 60°C (-4°F~140 °F)
Humidity	Max. 90% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.412 ~ 2.472 GHz
Antenna	3 x 4dBi fixed dipole antenna
Modulation	DBPSK/DQPSK/CCK/OFDM (BPSK/QPSK/16-QAM/64-QAM)
Data Rate	802.11b: up to 11Mbps 802.11g: up to 54Mbps 802.11n: up to 300Mbps
Security	WEP(HEX/ASCII): 64/128-bit WPA(AES/TKIP): WPA/WPA2-Radius, WPA-PSK/WPA2-PSK
Output Power	802.11b: 18dBm (typical) 802.11g: 15dBm (typical) 802.11n: 12dBm (typical)
Receiving Sensitivity	802.11b: -84dBm (typical) @ 11Mbps 802.11g: -72dBm (typical) @ 54 Mbps 802.11n: -65dBm (typical) @ 300Mbps
Channels	1~ 11 (FCC), 1~13 (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://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 9](#).
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 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.

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.

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

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

RoHS

This product is RoHS compliant.

**Europe – EU Declaration of Conformity**

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



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

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

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-639GR – 3 Years Warranty

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

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

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

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

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

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

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

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

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

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

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

PWP05202009v2

2012/11/30



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