



## User's Guide

**TEW-692GR**

1.01

## Statement

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

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Operations of this device in 5.15~5.25GHz frequency range are restricted for indoor use only.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

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

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

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

## Europe – EU Declaration of Conformity

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



- **EN60950-1:2006+A11: 2009**  
Safety of Information Technology Equipment
- **EN 62311:2008**
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
- **EN 300 328 V1.7.1: (2006-10)**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 489-1 V1.8.1: (2008-04)**
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 V2.1.1:( 2009-05)**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems
- 










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

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

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



 Český [Czech]	TRENDnet tímto prohlašuje, že tento <i>TEW-692GR</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr <i>TEW-692GR</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät <i>TEW-692GR</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme <i>TEW-692GR</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this <i>TEW-692GR</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el <i>TEW-692GR</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΩΝΕΙ ΟΤΙ <i>TEW-692GR</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente TRENDnet déclare que l'appareil <i>TEW-692GR</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo <i>TEW-692GR</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
 Latviski [Latvian]	Ar šo TRENDnet deklarē, ka <i>TEW-692GR</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis <i>TEW-692GR</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

 Nederlands [Dutch]	Hierbij verklaart <i>TRENDnet</i> dat het toestel <i>TEW-692GR</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>TRENDnet</i> , jiddikjara li dan <i>TEW-692GR</i> jikkonforma mal-ħtigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>TRENDnet</i> nyilatkozom, hogy a <i>TEW-692GR</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>TRENDnet</i> oświadcza, że <i>TEW-692GR</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>TRENDnet</i> declara que este <i>TEW-692GR</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>TRENDnet</i> izjavlja, da je ta <i>TEW-692GR</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
 Slovensky [Slovak]	<i>TRENDnet</i> týmto vyhlasuje, že <i>TEW-692GR</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>TRENDnet</i> vakuuttaa täten että <i>TEW-692GR</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>TRENDnet</i> att denna <i>TEW-692GR</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

## European Union Notice:

Radio products with the CE marking comply with the R&TTE Directive (1999/5/EC), the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms:

- EN 60950 Product Safety
- EN 300 328 Technical requirement for radio equipment
- EN 301 489-1/-17 General EMC requirements for radio equipment

## Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

# Contents

Getting Started.....	8
Package Contents .....	8
Minimum System Requirements.....	8
Introduction .....	9
Features .....	9
Overview .....	10
Network Diagram:.....	10
Front Panel LEDs .....	10
Rear panel.....	10
Wireless Performance Considerations .....	11
Using the Configuration Menu.....	12
Setup Wizard .....	13
Network.....	14
WAN Setting .....	14
LAN Setting .....	17
QoS .....	18
DHCP Client List.....	19
Wireless 2.4GHz .....	20
Basic.....	20
Advanced .....	23
Security .....	24
WPS .....	26
Station List.....	27
Wireless 5GHz .....	28
Basic.....	28
Advanced .....	31
Security .....	32
WPS .....	34
Station List.....	35
Advanced .....	36
DMZ.....	36
Virtual Server.....	38
Routing.....	39
Access Control .....	40
ALG .....	41
Special Applications .....	42
Gaming.....	43
Inbound Filter .....	44
Schedule .....	45
Advanced Network .....	46
Administrator.....	47
Management .....	47
Upload Firmware .....	48
Setting Management .....	49
Time .....	50
Status .....	51
Help .....	52
Appendix.....	53

Wireless LAN Networking.....	53
Glossary .....	55
Specification.....	59
Limited Warranty .....	60

# Getting Started

Congratulations on purchasing the TEW-692GR. This manual provides information for setting up and configuring the TEW-692GR. This manual is intended for both home users and professionals.

The following conventions are used in this manual:

## PACKAGE CONTENTS

- TEW-692GR
- CD-ROM (User's Guide)
- Multi-Language Quick Installation Guide
- Network cable
- Stand
- Power Adapter (12V, 1A)

Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product. If any item is found missing or damaged, please contact your local reseller for replacement.

## MINIMUM SYSTEM REQUIREMENTS

- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter and CD-ROM Drive
- Internet Explorer Version 6.0 or Netscape Navigator Version 7.0 and Above



# Introduction

TRENDnet's 450Mbps Concurrent Dual Band Wireless N Router, model TEW-692GR, is the first router to support 450Mbps speeds on both the 2.4GHz and 5GHz bands at the same time. This router's raw horsepower redefines wireless networking as we know it, to easily stream HD video through the home. Gigabit Wide Area Network and Local Area Network ports transfer wired data fast. Embedded GREENnet technology reduces port-based power consumption by up to 70%.

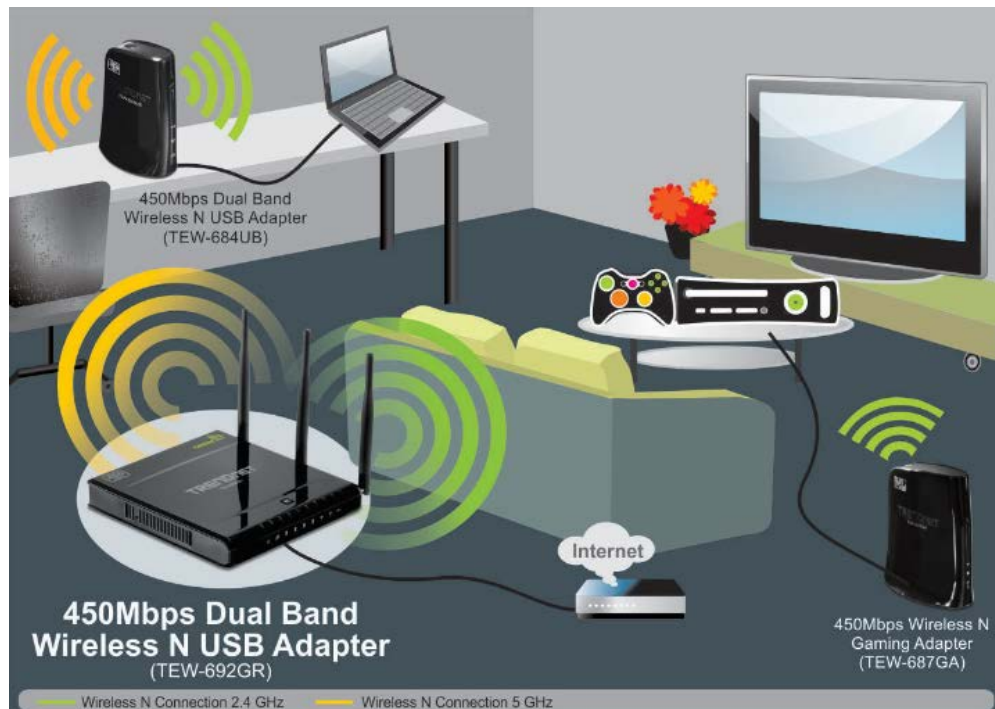
Advanced Multiple Input Multiple Output (MIMO) antenna technology reduces wireless dead spots. Wi-Fi Protected Setup (WPS) connects other WPS supported wireless adapters at the touch of a button. WMM® Quality of Service (QoS) technology prioritizes gaming, Internet calls, and video streams. Assign up to four virtual networks on each wireless band and manage access control for IP addresses, website URLs, and data protocols.

## FEATURES

- 4 x 10/100/1000Mbps Auto-MDIX LAN ports
- 1 x 10/100/1000Mbps WAN port (Internet)
- Wi-Fi Protected Setup (WPS) button
- On/off power switch (EU Version)
- LED status indicators
- Compliant with IEEE 802.11n/b/g/a standards
- High-speed data rates of up to 450 Mbps using both 2.4 GHz and 5 GHz bands
- Compatible with most popular cable/DSL Internet Service Providers using Dynamic/Static IP, PPPoE, L2TP, and PPTP connection
- Advanced firewall protection with Network Address Translation (NAT) support
- Advanced wireless security of up to WPA2-RADIUS
- DMZ support
- Wi-Fi Multimedia (WMM) Quality of Service (QoS) data prioritization
- Support for up to four virtual wireless networks (SSIDs) per wireless band
- Gaming Port Controls: supports opening multiple ports or a range of ports
- Internet Access Control with MAC, URL, Service Type, and IP Range filtering
- Internet Access Control Rule Scheduling: schedule access to websites, online video games, Internet cameras and more for specific times through the week
- One touch wireless connection to wireless clients using the WPS button
- Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, Safari, and Chrome
- Virtual server and Application Level Gateway (ALG) services for special Internet applications
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications
- Coverage up to 100 meters (330 ft.) indoor and 300 meters (980 ft.) outdoor (depends on the environment)
- 3- year limited warranty

# Overview

## NETWORK DIAGRAM:



## FRONT PANEL LEDS

- PWR
- WAN
- LAN1
- LAN2
- LAN3
- LAN4
- Wireless
- Wireless
- WPS
- Reserve



## REAR PANEL

- DC-IN
- POWER SWITCH( EU)
- WAN
- LAN1
- LAN2
- LAN3
- LAN4



# 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.

limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- 1 Keep the number of walls and ceilings between the TEW-639GR and other network devices to a minimum - each wall or ceiling can reduce your wireless products range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2 Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 3 Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- 4 Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.

# Using the Configuration Menu

Whenever you want to configure your TEW-692GR, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the TEW-692GR. The TEW-692GR's default IP Address is `http://192.168.10.1`

- Open the Web browser.
- Type in the IP Address of the Router (`http://192.168.10.1` )



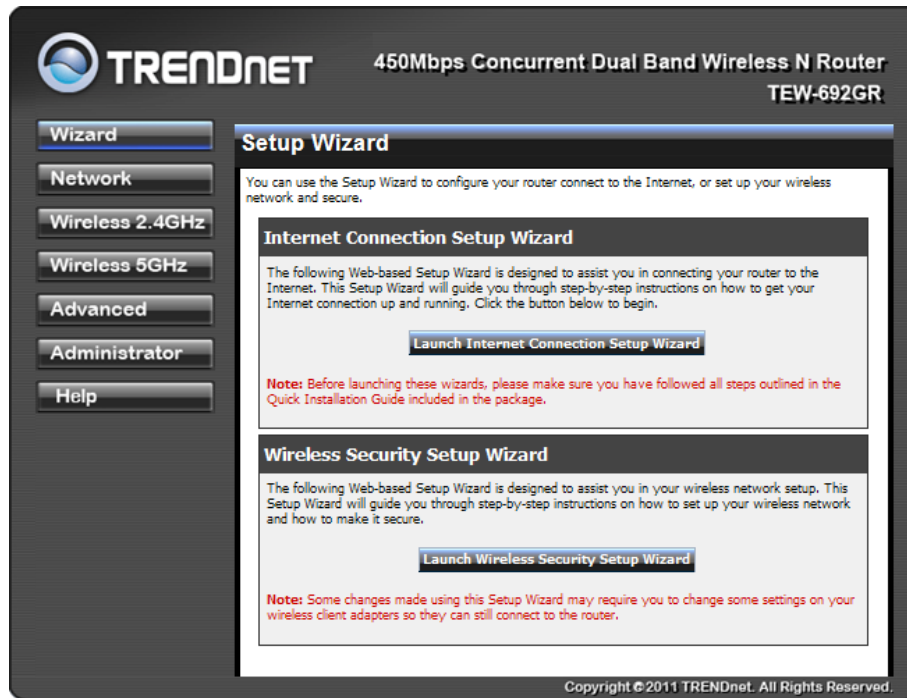
## NOTE

If you have changed the default IP Address assigned to the TEW-692GR, make sure to enter the correct IP Address.

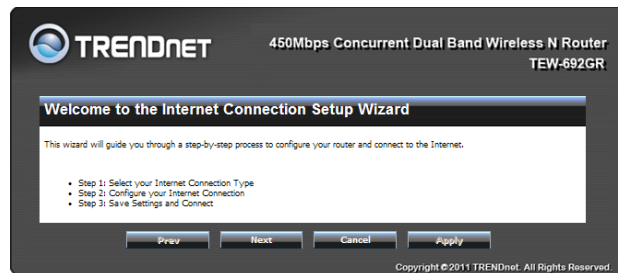
- Select admin in the User Name field.
- Default password is admin.
- Click OK.

# Setup Wizard

Setup Wizard is an easy way to set up the TEW-692GR step by step. The Wizard will guide user's to set up the TEW-692GR in just few steps.



To setup the router's internet connection settings, click 'Launch Internet Connection Setup Wizard' and follow Wizard to complete your setting.



Once the internet connection setup is completed, click "Launch Wireless Security Setup Wizard" to configure the router's wireless settings.



# Network

## WAN SETTING

There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and Russia PPTP. If you are unsure of your connection method, please contact your Internet Service Provider.

### WAN Connection Type

There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and Russia PPTP. If you are unsure of your connection method, please contact your Internet Service Provider.

**Static:** Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the IP address, Subnet Mask, Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all of this information.

**DHCP:** A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. **Host Name:** Some ISP's may check your computer's Host Name. The Host Name identifies your system to the ISP's server.

**PPPoE:** Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

**Reconnect Mode:** Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are:

**Always on:** A connection to the Internet is always maintained.

**On demand:** A connection to the Internet is made as needed.

**Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.

**Maximum Idle Time:** Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

**L2TP:**L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet.

**L2TP Server IP Address:** The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.

**Reconnect Mode:** Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are:

**Always on:** A connection to the Internet is always maintained.

**On demand:** A connection to the Internet is made as needed.

**Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.

**Maximum Idle Time:** Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

#### **WAN Interface IP Type**

**Static:** If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields for **WAN Interface IP Setting: IP Address, Subnet Mask, Default Gateway.**

**Dynamic:** If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.

**PPTP:** PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

**PPTP Server IP Address:** The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.

**Reconnect Mode:** Typically PPPoE connections are not always on. The router allows you to set the reconnection mode. The settings are:

**Always on:** A connection to the Internet is always maintained.

**On demand:** A connection to the Internet is made as needed.

**Manual:** You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.

**Maximum Idle Time:** Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

### **WAN Interface IP Type**

**Static:** If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields for **WAN Interface IP Setting: IP Address, Subnet Mask, Default Gateway**, and optional for **DNS Server**

**Dynamic:** If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.

**Russia PPTP:** The Russia PPTP can configure IP address on the WAN interface and establish PPTP to get IP address, subnet mask, default gateway and DNS for ANOTHER logical IP interface on WAN port. So the physical WAN port will have 2 logical IP interfaces and can communicate with internal ISP's network resources and also communicate with Internet through PPTP tunnel. It is specified by Russia Cobrina ISP, user can configure it the same as the normal PPTP and PPTP server IP Address can use the domain name string.

**WAN MTU Setting:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer. t modes.

**MAC Address Clone:** Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's may check your computer's MAC address. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. This router has a different MAC address than the computer or router that initially connected to the ISP. If you need to change the MAC address of the router's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the **Clone Your PC's**



**MAC Address** button. The WAN interface will then use the MAC address of the network adapter in your computer.

## LAN SETTING

**IP Address:**The IP address of the this device on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN.

**Subnet Mask:** The subnet mask of the local area network.

**DHCP Server Settings:** DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

**Enable DHCP Server:** Once your router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically". When you set **Enable DHCP Server**, the following options are displayed.

**DHCP IP Address Range:** These two IP values (Start and End) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved, so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

Your router, by default, has a static IP address of 192.168.10.1. This means that addresses 192.168.10.2 to 192.168.10.254 can be made available for allocation by the DHCP Server.

**Subnet Mask:** The subnet mask of the local area network.

**Gateway:** The IP address of the router on the local area network. For example, 192.168.10.1.

**DHCP Lease Time:** The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

**Add/Edit DHCP Reservation:** This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP

Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

**Computer Name:** You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way. Example: **Game Server**.

**IP Address:** The LAN address that you want to reserve.

**MAC Address:** To input the MAC address of your system, enter it in manually or connect to the router's Web-Management interface from the system and click the **Copy Your PC's MAC Address** button.

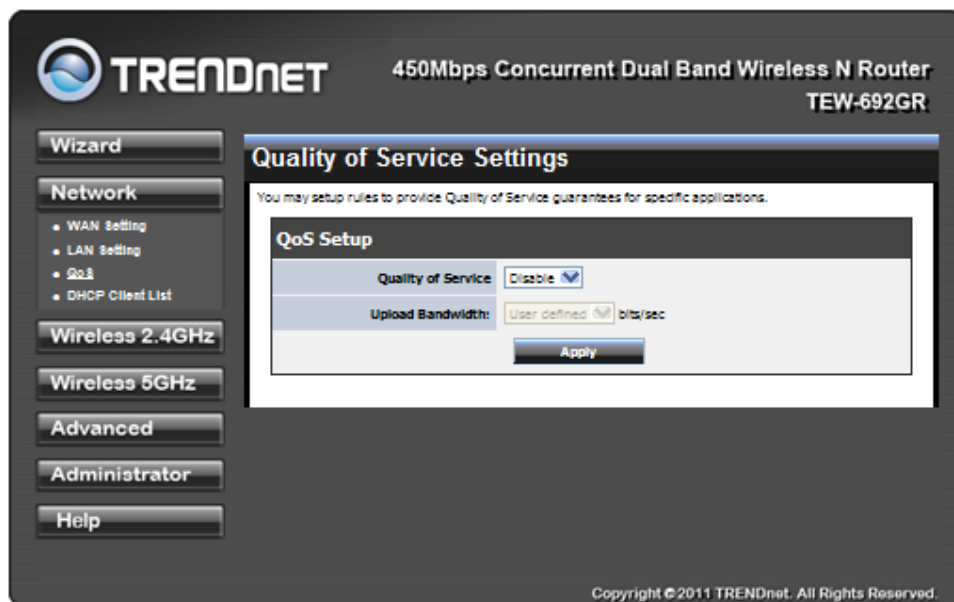
A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22. If your network device is a computer and the network card is already located inside the computer, you can connect to the router from the computer and click the **Copy Your PC's MAC Address** button to enter the MAC address.

**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

**DHCP Reservations List:** This shows clients that you have specified to reserve DHCP addresses. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry 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 DHCP Reservation" section is activated for editing.

## QOS

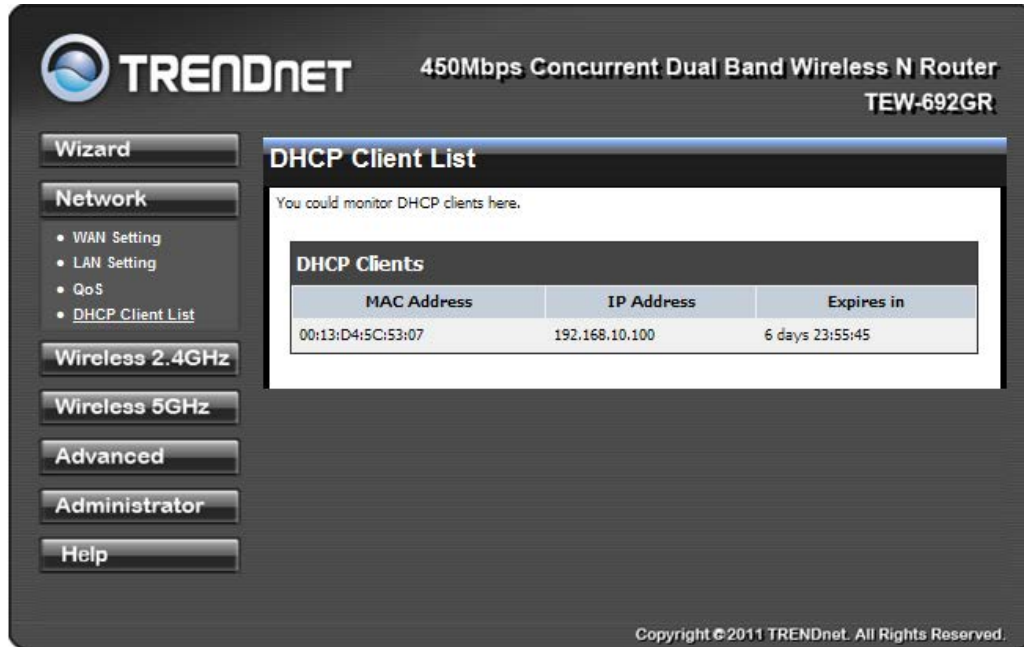
QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications.



**Upload Bandwidth:** Limit bandwidth of upload manually with 'User Defined' or set the bandwidth limit via drop-down menu (between 64Mbits ~ 230Mbits) per device on network.

## DHCP CLIENT LIST

This section displays all connected LAN devices currently receiving IP address from the router.



The screenshot shows the Trendnet web interface for a 450Mbps Concurrent Dual Band Wireless N Router (TEW-692GR). The left sidebar contains navigation buttons for Wizard, Network, Wireless 2.4GHz, Wireless 5GHz, Advanced, Administrator, and Help. The Network section is expanded, showing sub-options for WAN Setting, LAN Setting, QoS, and DHCP Client List. The main content area is titled "DHCP Client List" and contains a table of active DHCP clients.

MAC Address	IP Address	Expires in
00:13:D4:5C:53:07	192.168.10.100	6 days 23:55:45

Copyright ©2011 TRENDnet. All Rights Reserved.

# Wireless 2.4GHz

## BASIC

**TRENDnet** 450Mbps Concurrent Dual Band Wireless N Router  
TEW-692GR

Wizard  
Network  
Wireless 2.4GHz  
• Basic  
• Advanced  
• Security  
• WPS  
• Station List  
Wireless 5GHz  
Advanced  
Administrator  
Help

### Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

#### Wireless Network

Radio On/Off	<input type="radio"/> RADIO OFF
Wireless Mode	2.4GHz 802.11 b/g/n mixed mode
Wireless Name (SSID)	TRENDnet692_2.4GHz
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Frequency (Channel)	AutoSelect

#### Wireless Distribution System(WDS)

WDS	Disable
-----	---------

#### HT Physical Mode

Channel Bandwidth	<input checked="" type="radio"/> 20MHz <input type="radio"/> Auto 20/40MHz
20/40 Coexistence	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto
Extension Channel	AutoSelect

Apply Cancel

Copyright © 2011 TRENDnet. All Rights Reserved.

**Radio On/Off:** This indicates the wireless operating status. When the radio is on, the following parameters are in effect.

**Wireless Mode:** If all of the wireless devices you want to connect with this router can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate wireless mode. If you have some devices that use a different transmission mode, choose the appropriate wireless mode. The TEW-692GR supports 2.4GHz wireless networks. There are many different configuration options available to choose from. Use the drop down list to select the wireless mode. Note: One wireless mode can be selected can select at any one time. This means that you can only select one of the operating frequency at a time.

**Wireless Mode options: 2.4GHz 802.11b/g mixed mode** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access the

TEW-692GRat 11Mbps for wireless b, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.

**2.4GHz 802.11 n only** – This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless n client devices to connect and access the TEW-692GRup to 450Mbps\*. Although the wireless n operates in the 2.4GHz frequency, this mode will only permit wireless n client devices to work and will exclude any other wireless mode and devices that are not wireless n only.

**2.4 GHz 802.11b/g/n mixed mode** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access the TEW-692GRat 11Mbps for wireless b, 54Mbps for wireless g and up to 450Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.

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

**Wireless Network Name (SSID):** When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Add up to three additional SSIDs to create virtual wireless networks from one wireless Router Access Point device.

**Add Additional Wireless Network Name (SSID):** To add additional wireless Network Names simply add the name to the Multiple SSID field and click on apply at the bottom of the page. When finished, go to the Security section in this Users Guide for wireless security configuration.

**Frequency (Channel):** A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

**Wireless Distribution System (WDS):** When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel.

(Note that WDS security is incompatible with mixed mode, like WPAPSK+WPA2PSK mixed, WEP AUTO and 802.1x, both feature cannot be used at the same time).

**Configuring WDS with TEW-692GR:** Enable the option for WDS and input the MAC Address of the wireless device that also supports WDS in to the blank fields. You can add up to four additional devices in the spaces provided. Click on apply at the bottom of the page, to apply your setting changes. Enable the security seeing in security page, each WDS APs need to use same security setting.

(Note: WDS supports wireless g/n modes. The use multiple Access Point will reduce the overall network throughput to ½ the WRT-893L.

**HT Physical Mode:** In HT (High Throughput) Physical mode setting allow for control of the 802.11n wireless environment.

**Channel BandWidth:**

Set channel width of wireless radio.

20 Channel Width = 20 MHz

20/40 Channel Width = Enables the router to operate on both 20/40 MHz

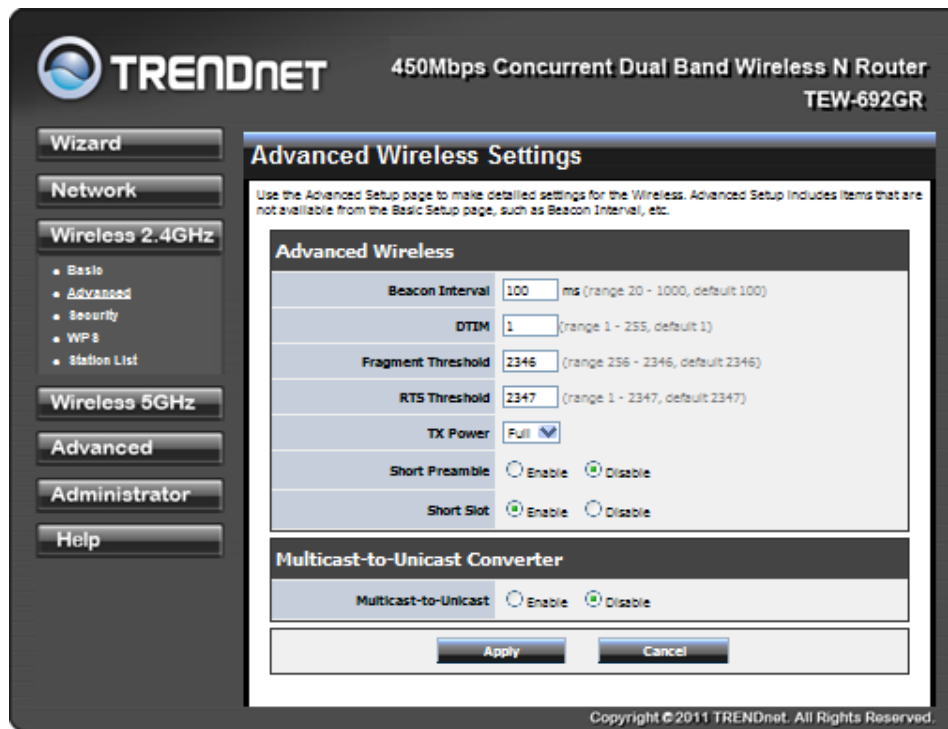
**Guard Interval:** Support Short/Long GI, the purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive.

Long Guard Interval, 800 nsec

Short Guard Interval, 400 nsec

**MCS:** Fix MCS rate for HT rate (0-15). The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels.

## ADVANCED



**Beacon Interval:** Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

**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.

**Fragmentation 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:** When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.

**Short Preamble and Slot:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

**TX Power:** Allows the wireless Router to deliver better throughput in the same period and environment in order to increase speed. Higher power output delivers better throughput

## SECURITY

**TRENDNET** 450Mbps Concurrent Dual Band Wireless N Router  
TEW-692GR

Wizard  
Network  
Wireless 2.4GHz

- Basic
- Advanced
- Security**
- WPA
- Station List

Wireless 5GHz  
Advanced  
Administrator  
Help

### Wireless Security Setting

Setting wireless security.

**Select SSID**

SSID choice: TRENDnet692\_2.4GHz

**Security Policy: TRENDnet692\_2.4GHz**

Security Mode: WEP-OPEN

**WEP**

Default Key: Key 1

WEP Key 1: 12345 ASCII

WEP Key 2: ASCII

WEP Key 3: ASCII

WEP Key 4: ASCII

**Wireless MAC Filter**

Filter Mode: Disable

MAC Address: (Ex: 00:11:22:33:44:55)

Apply Cancel

Copyright © 2011 TRENDnet. All Rights Reserved.

### Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

**WEP:** A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is



easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

**WPA-Personal and WPA-Enterprise:** Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

**Group Key Update Interval:** The amount of time before the group key used for broadcast and multicast data is changed.

**WPA-Personal:** This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

**Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

**WPA-Enterprise:** This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

**Authentication Timeout:** Amount of time before a client will be required to re-authenticate.

**RADIUS Server IP Address:** The IP address of the authentication server.

**RADIUS Server Port:** The port number used to connect to the authentication server.

**RADIUS Server Shared Secret:** A pass-phrase that must match with the authentication server.

**WPA/WPA2 mixed environment:** For those WPA2 stations, they will use AES for unicast. For those WPA stations, they will use TKIP for unicast. But for multicast all WPA and WPA2 stations have to use the same key, and that will be TKIP, because WPA station only knows about TKIP, WPA2 is new standard, so it is defined to backward support TKIP on multicast.

**Wireless MAC Filtering:** Choose the type of MAC filtering needed.

**Turn MAC Filtering Disable:** When "Disable" is selected, MAC addresses are not used to control network access.

**Add MAC Filtering Rule:** Use this section to add MAC addresses to the list below.

**MAC Address:** Enter the MAC address of a computer that you want to control with MAC filtering. Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu.

*The rule of thumb: In mixed mode, multicast key has to be TKIP, but unicast key can be different per stations. In WPA or WPA2 only mode, unicast and multicast key can be only AES for WPA2, and TKIP for WPA. (AES means the unicast and multicast key are all AES. TKIP/AES means multicast is TKIP. But unicast can be AES or TKIP, which depends on the peer.)*

## WPS

The screenshot displays the 'Wi-Fi Protected Setup' configuration page on a Trendnet router. The page is titled '450Mbps Concurrent Dual Band Wireless N Router TEW-692GR'. The left sidebar contains navigation options: Wizard, Network, Wireless 2.4GHz (selected), Wireless 5GHz, Advanced, Administrator, and Help. The main content area is divided into three sections:

- WPS Config:** A dropdown menu for 'WPS' is set to 'Enable', with an 'Apply' button below it.
- WPS Summary:** A table showing the current configuration:

WPS Current Status	Idle
WPS Configured	Yes
WPS SSID	TRENDnet692_2.4GHz
WPS Security Mode	Open
WPS Encrypt Type	WEP
WPS Default Key Index	1
WPS Key(Hex value)	3132333435
AP PIN	37036164
- WPS Action:** Instructions to click the Wireless Client Card and Router's WPS button. It includes two buttons: 'Configure via PIN' (with a PIN input field) and 'Configure via PBC'.

Copyright © 2011 TRENDnet. All Rights Reserved.

**Enable:** Enable the WPS feature.

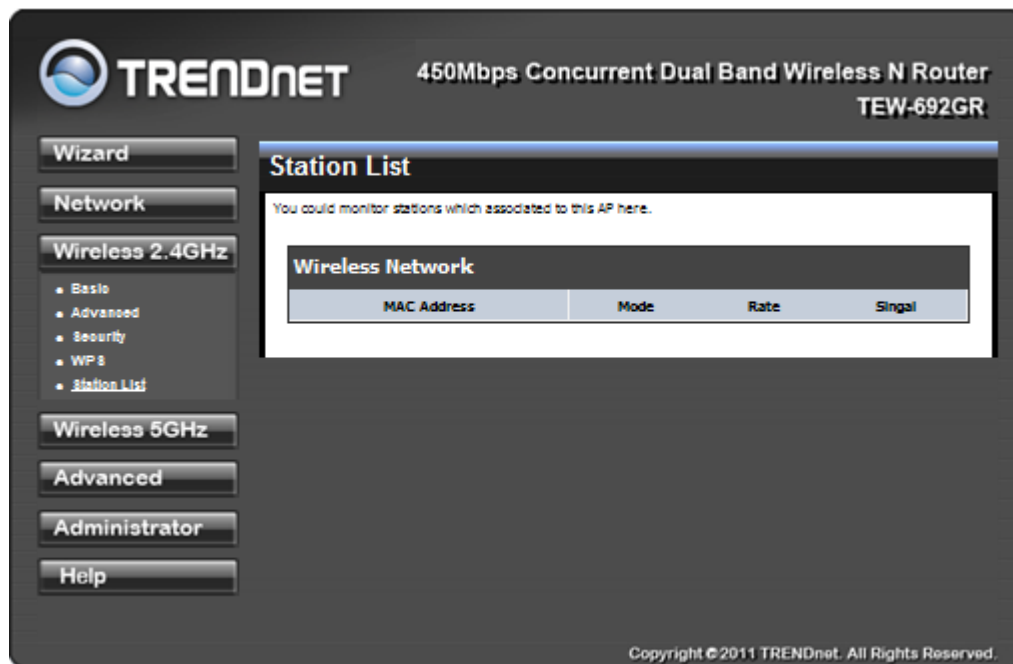
**Current PIN:** Shows the current value of the router's PIN.

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network.

**PBC Settings:** The push button method can be used to allow wireless clients to connect to the router without entering/remember any encryption keys. The user can use the PBC method by pressing the WPS button on the side of the router or select the PBC option under Wireless/WPS settings page and hit Apply.

## STATION LIST

All the wireless clients connecting to the router will be shown here, you could monitor your network and prevent any unauthorized wireless connection easily.



# Wireless 5GHz

## BASIC

The screenshot displays the 'Basic Wireless Settings' page for a TRENDnet 450Mbps Concurrent Dual Band Wireless N Router (TEW-692GR). The interface includes a sidebar with navigation options: Wizard, Network, Wireless 2.4GHz, Wireless 5GHz (selected), Advanced, Administrator, and Help. The main content area is titled 'Basic Wireless Settings' and contains the following sections:

- Wireless Network:** Radio On/Off (RADIO OFF), Wireless Mode (5GHz 802.11 a/n mixed mode), Wireless Name (SSID) (TRENDnet592\_5GHz), Multiple SSID1, Multiple SSID2, Multiple SSID3, Broadcast Network Name (SSID) (Enable/Disable), and Frequency (Channel) (5180MHz (Channel 36)).
- Wireless Distribution System (WDS):** WDS (Disable).
- HT Physical Mode:** Channel BandWidth (20MHz/Auto 20/40MHz), 20/40 Coexistence (Disable/Enable), Guard Interval (Long/Auto), MCS (Auto), and Extension Channel (5200MHz (Channel 40)).

Buttons for 'Apply' and 'Cancel' are located at the bottom of the settings area. The footer of the page reads 'Copyright © 2011 TRENDnet. All Rights Reserved.'

**Radio On/Off:** This indicates the wireless operating status. The wireless can be turned on or off by the slide switch. When the radio is on, the following parameters are in effect.

**Wireless Mode:** If all of the wireless devices you want to connect with this router can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate wireless mode. If you have some devices that use a different transmission mode, choose the appropriate wireless mode. The TEW-692GR supports 5GHz wireless networks. There are many different configuration options available to choose from. Use the drop down list to select the wireless mode. Note: One wireless mode can be selected can select at any one time. This means that you can only select one of the operating frequencies at a time.

## **Wireless Mode options:**

**5GHz 802.11a only mode** - This wireless mode works in the 5GHz frequency range and will allow wireless a client to connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router at 54Mbps for wireless a only mode. Although the wireless a operates in the 5GHz frequency, this mode will only permit wireless a client devices to work and will exclude any other wireless mode and devices that are not wireless a only.

**5GHz 802.11a/n mixed mode** - This wireless mode works in the 5GHz frequency range and will only allow the use of wireless a/n dual band client devices to connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router up to 450Mbps\*. Dual band wireless client devices that support both wireless a/n can connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router up to 450Mbps. Wireless a client devices can connect and access the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router but, will only connect up to 54Mbps, (this due to the legacy limitation of wireless a technology for that standard). Although the wireless a/n operate in the same 5GHz frequency, this mode will only permit wireless a/n client devices to work and will exclude any other wireless mode and devices that are not wireless a/n. (note: wireless b/g/n will not be able to connect at the same time to the TEW-692GR450Mbps Concurrent Wireless N Gigabit Router with 5GHz wireless a/n mode enable).

**Wireless Network Name (SSID):** When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Add up to three additional SSIDs to create virtual wireless networks from one wireless Router Access Point device.

**Wireless Network Name (SSID):** When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Add up to three additional SSIDs to create virtual wireless networks from one wireless Router Access Point device.

**Add Additional Wireless Network Name (SSID):** To add additional wireless Network Names simply add the name to the Multiple SSID field and click on apply at the bottom of the page. When finished, go to the Security section in this Users Guide for wireless security configuration.

**Frequency (Channel):** A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

**Wireless Distribution System (WDS):** When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. A WDS link is bidirectional;

so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel.

(Note that WDS security is incompatible with mixed mode, like WPAPSK+WPA2PSK mixed, WEP AUTO and 802.1x, both feature cannot be used at the same time).

**Configuring WDS with TEW-692GR:** Enable the option for WDS and input the MAC Address of the wireless device that also supports WDS in to the blank fields. You can add up to four additional devices in the spaces provided. Click on apply at the bottom of the page, to apply your setting changes.

Enable the security seeing in security page, each WDS APs need to use same security setting.

(Note: WDS supports wireless g/n modes. The use multiple Access Point will reduces the overall network throughput to ½ the WRT-893L.

**HT Physical Mode:** In HT (High Throughput) Physical mode setting allow for control of the 802.11n wireless environment.

**Channel BandWidth:** Set channel width of wireless radio.

20 Channel Width = 20 MHz

20/40 Channel Width = Enables the router to operate on both 20/40 MHz

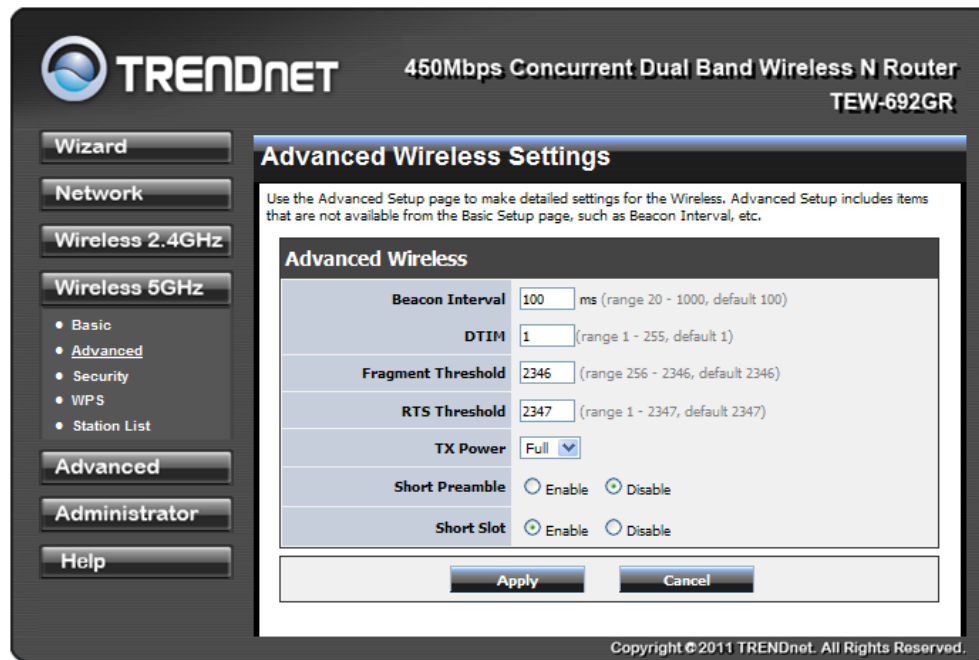
**Guard Interval:** Support Short/Long GI, the purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive.

Long Guard Interval, 800 nsec

Short Guard Interval, 400 nsec

**MCS:** Fix MCS rate for HT rate. The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels.

## ADVANCED



**Beacon Interval:** Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

**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.

**Fragmentation 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:** When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.

**TX Burst:** Allows the wireless Router to deliver better throughput in the same period and environment in order to increase speed.

**Short Preamble and Slot:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

## SECURITY

The screenshot displays the 'Wireless Security Setting' page for a TRENDnet 450Mbps Concurrent Dual Band Wireless N Router (TEW-692GR). The left sidebar contains navigation options: Wizard, Network, Wireless 2.4GHz, Wireless 5GHz (with sub-options: Basic, Advanced, Security, WPS, Station List), Advanced, Administrator, and Help. The main content area is titled 'Setting wireless security.' and includes the following sections:

- Select SSID:** SSID choice is set to 'TRENDnet692\_5GHz'.
- Security Policy: TRENDnet692\_5GHz:** Security Mode is set to 'WEP-OPEN'.
- WEP:** Default Key is 'Key 1'. WEP Key 1 is '12345' with an ASCII dropdown. WEP Key 2, 3, and 4 are empty with ASCII dropdowns.
- Wireless MAC Filter:** Filter Mode is 'Disable'. MAC Address is empty, with an example '(Ex: 00:11:22:33:44:55)'.

Buttons for 'Apply' and 'Cancel' are at the bottom. Copyright © 2011 TRENDnet. All Rights Reserved.

### Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

**WEP:** A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering a string in HEX



(hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

**WPA-Personal and WPA-Enterprise:** Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

**Group Key Update Interval:**

The amount of time before the group key used for broadcast and multicast data is changed.

**WPA-Personal:** This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

**WPA-Enterprise:** This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

**WPA/WPA2 mixed environment:** For those WPA2 stations, they will use AES for unicast. For those WPA stations, they will use TKIP for unicast. But for multicast all WPA and WPA2 stations have to use the same key, and that will be TKIP, because WPA station only knows about TKIP, WPA2 is new standard, so it is defined to backward support TKIP on multicast.

**Wireless MAC Filtering:** Choose the type of MAC filtering needed.

**Turn MAC Filtering Disable:** When "Disable" is selected, MAC addresses are not used to control network access.

**Add MAC Filtering Rule:** Use this section to add MAC addresses to the list below.

**MAC Address:** Enter the MAC address of a computer that you want to control with MAC filtering. Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu.

*The rule of thumb: In mixed mode, multicast key has to be TKIP, but unicast key can be different per stations. In WPA or WPA2 only mode, unicast and multicast key can be only AES for WPA2, and TKIP for WPA. (AES means the unicast and multicast key are all AES. TKIP/AES means multicast is TKIP. But unicast can be AES or TKIP, which depends on the peer.)*

## WPS

**TRENDNET** 450Mbps Concurrent Dual Band Wireless N Router TEW-692GR

**Wi-Fi Protected Setup**

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

**WPS Config**

WPS

**WPS Summary**

WPS Current Status	Idle
WPS Configured	Yes
WPS SSID	TRENDnet692_5GHz
WPS Security Mode	Open
WPS Encrypt Type	WEP
WPS Default Key Index	1
WPS Key(Hex value)	3132333435
AP PIN	35110569

**WPS Action**

Please click Wireless Client Card and Router's WPS button in 120 seconds to complete this setting.

PIN

PBC

Copyright © 2011 TRENDnet. All Rights Reserved.

**Enable:** Enable the WPS feature.

**Lock Wireless Security Settings:** Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using WPS.

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

**Current PIN:** Shows the current value of the router's PIN.

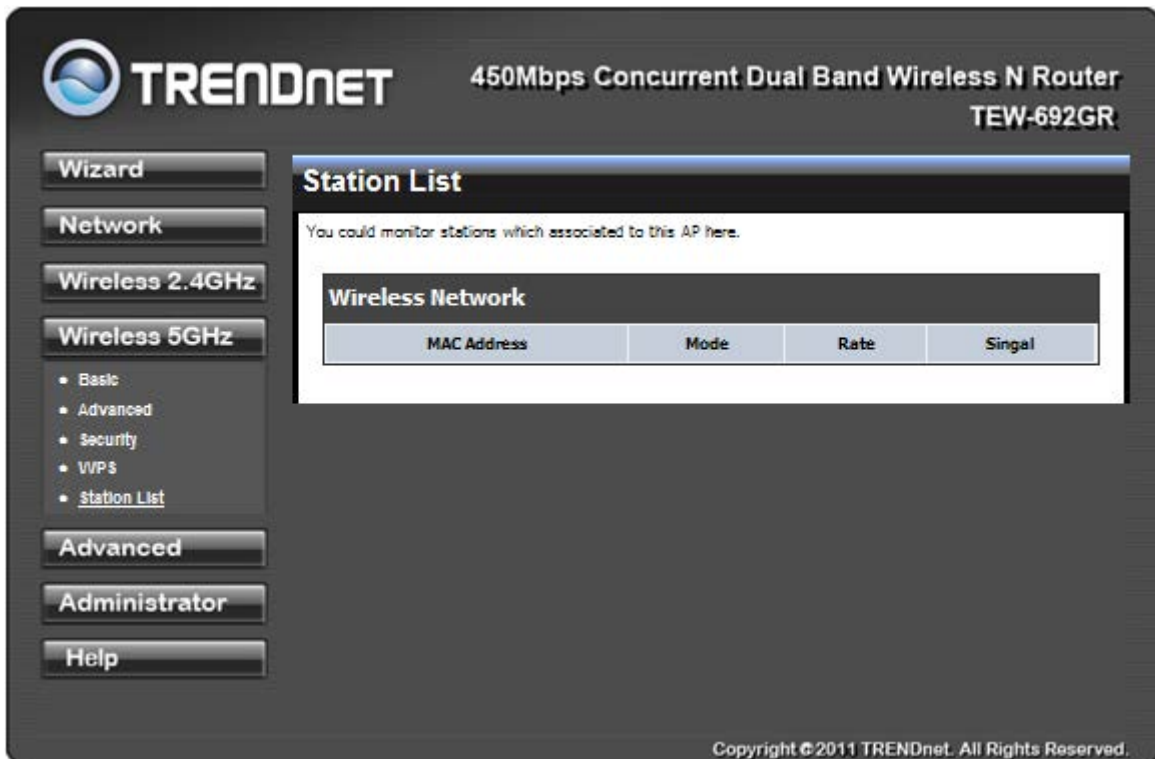
**Reset To WPS Default:** Restore the default PIN of the router.

**Generate New PIN:** Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.

**PBC Settings:** The push button method can be used to allow wireless clients to connect to the router without entering/remember any encryption keys. The user can use the PBC method by pressing the WPS button on the side of the router or select the PBC option under Wireless/WPS settings page and hit Apply.

## STATION LIST

All the wireless clients connecting to the router will be shown here, you could monitor your network and prevent any unauthorized wireless connection easily.



**TRENDNET** 450Mbps Concurrent Dual Band Wireless N Router  
TEW-692GR

Wizard  
Network  
Wireless 2.4GHz  
Wireless 5GHz  
• Basic  
• Advanced  
• Security  
• WPS  
• Station List  
Advanced  
Administrator  
Help

### Station List

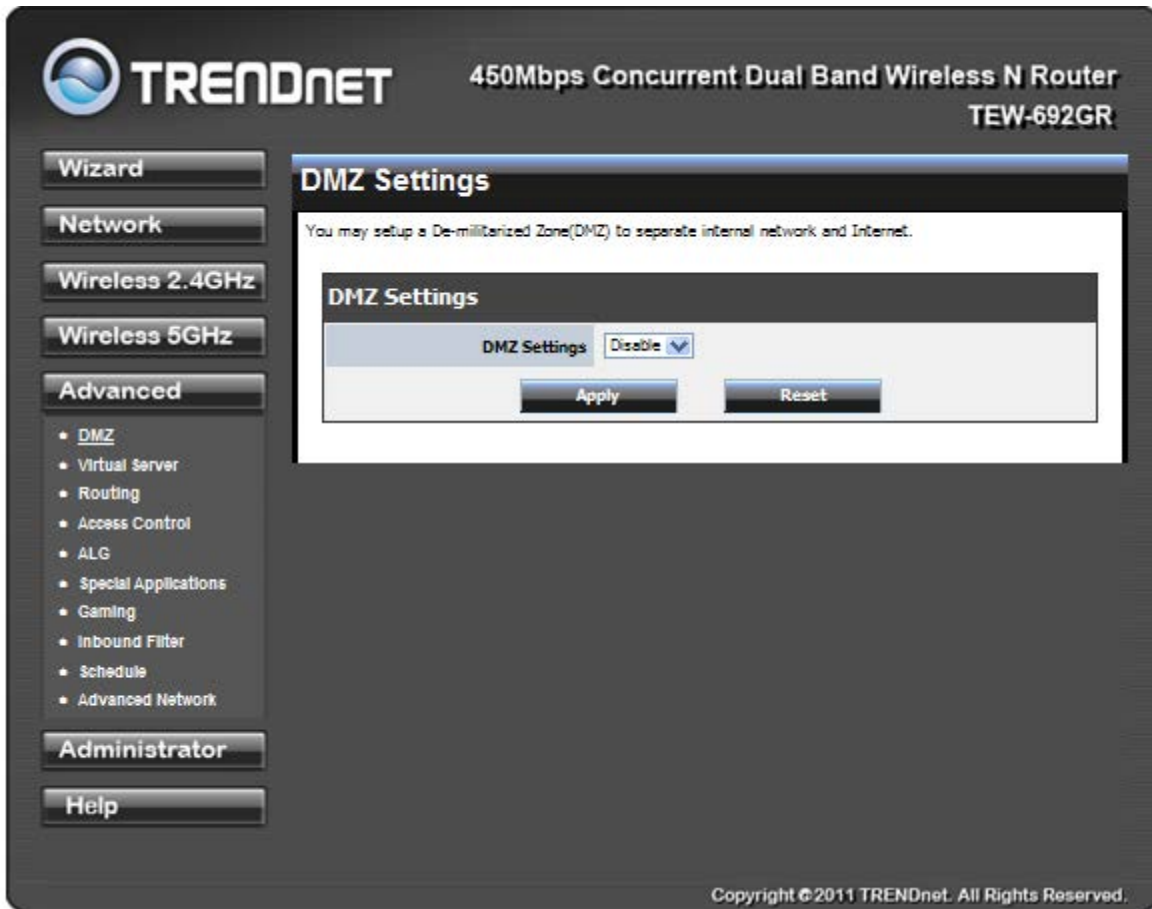
You could monitor stations which associated to this AP here.

Wireless Network			
MAC Address	Mode	Rate	Singal

Copyright © 2011 TRENDnet. All Rights Reserved.

# Advanced

## DMZ



### DMZ Setting

DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

When a LAN host is configured as a DMZ host, it becomes the destination for all incoming packets that do not match some other incoming session or rule. If any other ingress rule is in place, that will be used instead of sending packets to the DMZ host; so, an active session, virtual server, active port trigger, or port forwarding rule will take priority over sending a packet to the DMZ host. (The DMZ policy resembles a default port forwarding rule that forwards every port that is not specifically sent anywhere else.)

The router provides only limited firewall protection for the DMZ host. The router does not forward a TCP packet that does not match an active DMZ session, unless it is a connection establishment packet (SYN). Except for this limited protection, the DMZ host is effectively "outside the firewall". Anyone considering using a DMZ host should also consider running a firewall on that DMZ host system to provide additional protection.

Packets received by the DMZ host have their IP addresses translated from the WAN-side IP address of the router to the LAN-side IP address of the DMZ host. However, port numbers are not translated; so applications on the DMZ host can depend on specific port numbers.

The DMZ capability is just one of several means for allowing incoming requests that might appear unsolicited to the NAT. In general, the DMZ host should be used only if there are no other alternatives, because it is much more exposed to cyberattacks than any other system on the LAN. Thought should be given to using other configurations instead: a virtual server, a port forwarding rule, or a port trigger. Virtual servers open one port for incoming sessions bound for a specific application (and also allow port redirection and the use of ALGs).

Port forwarding is rather like a selective DMZ, where incoming traffic targeted at one or more ports is forwarded to a specific LAN host (thereby not exposing as many ports as a DMZ host). Port triggering is a special form of port forwarding, which is activated by outgoing traffic, and for which ports are only forwarded while the trigger is active.

Few applications truly require the use of the DMZ host. Following are examples of when a

**DMZ host might be required:**

- A host needs to support several applications that might use overlapping ingress ports such that two port forwarding rules cannot be used because they would potentially be in conflict.
- To handle incoming connections that use a protocol other than ICMP, TCP, UDP, and IGMP (also GRE and ESP, when these protocols are enabled by the PPTP and IPsec)

**Enable DMZ**

Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

**DMZ IP Address**

Specify the LAN IP address of the LAN computer that you want to have unrestricted Internet communication.

# VIRTUAL SERVER

The screenshot shows the Trendnet web interface for configuring a Virtual Server. The page title is 'Virtual Server' and the router model is '450Mbps Concurrent Dual Band Wireless N Router TEW-692GR'. The sidebar on the left contains navigation buttons for 'Wizard', 'Network', 'Wireless 2.4GHz', 'Wireless 5GHz', 'Advanced' (with sub-menu items: DMZ, Virtual Server, Routing, Access Control, ALG, Special Applications, Gaming, Inbound Filter, Schedule, Advanced Network), 'Administrator', and 'Help'. The main content area is titled 'Virtual Server' and includes a description: 'The Virtual Server can define a single public port for redirection to an internal IP and port.' Below this is the 'Add Virtual Server' form with the following fields: 'Rule Enable' (checkbox), 'Rule Name' (text input), 'IP Address' (text input), 'Protocol' (dropdown menu set to 'TCP'), 'Public Port' (text input), 'Private Port' (text input), 'Inbound Filter' (dropdown menu set to 'Allow All'), and 'Schedule' (dropdown menu set to 'Always'). There are 'Add' and 'Clear' buttons at the bottom of the form. Below the form is a 'Virtual Server List' table with the following columns: 'Enable', 'Rule Name', 'IP Address', 'Protocol, Public Port/Private Port', 'Inbound Filter', 'Schedule', 'Edit', and 'Delete'. The footer of the page reads 'Copyright © 2011 TRENDnet. All Rights Reserved.'

**Enable:** Specifies whether the entry will be active or inactive.

**Name:** Assign a meaningful name to the virtual server, for example **Web Server**. Several well-known types of virtual server are available from the "Application Name" drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

**IP Address:** The IP address of the system on your internal network that will provide the virtual service, for example **192.168.10.50**. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

**Protocol:** Select the protocol used by the service. The common choices -- UDP, TCP, and both UDP and TCP -- can be selected from the drop-down menu. To specify any other protocol, select "Other" from the list, then enter the corresponding protocol number (as assigned by the IANA) in the **Protocol** box.

**Private Port:** The port that will be used on your internal network.

**Public Port:** The port that will be accessed from the Internet.

**Schedule:** Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules.

**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

# ROUTING

**Static Routing Settings**

The Static Routing option allows you to define fixed routes to specific destinations.

**Add Static Route**

Destination IP Address : 0.0.0.0  
Destination IP Netmask : 0.0.0.0  
Gateway : 0.0.0.0  
Metric : 1  
Interface : WAN

**Static Route List**

No.	IP	Netmask	Gateway	Metric	Interface
Delete					

**RIP**

Enable RIP: Disable

**Routing Table**

IP	Netmask	Gateway	Metric	Interface
255.255.255.255	255.255.255.255	0.0.0.0	0	LAN/WLAN
239.255.255.250	255.255.255.255	0.0.0.0	0	LAN/WLAN
10.4.3.0	255.255.255.0	0.0.0.0	0	WAN
192.168.10.0	255.255.255.0	0.0.0.0	0	LAN/WLAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN/WLAN
224.0.0.0	240.0.0.0	0.0.0.0	0	LAN/WLAN
0.0.0.0	0.0.0.0	10.4.3.1	0	WAN

Copyright © 2011 TRENDnet. All Rights Reserved.

**Add/Edit Route:** Adds a new route to the IP routing table or edits an existing route.

**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.

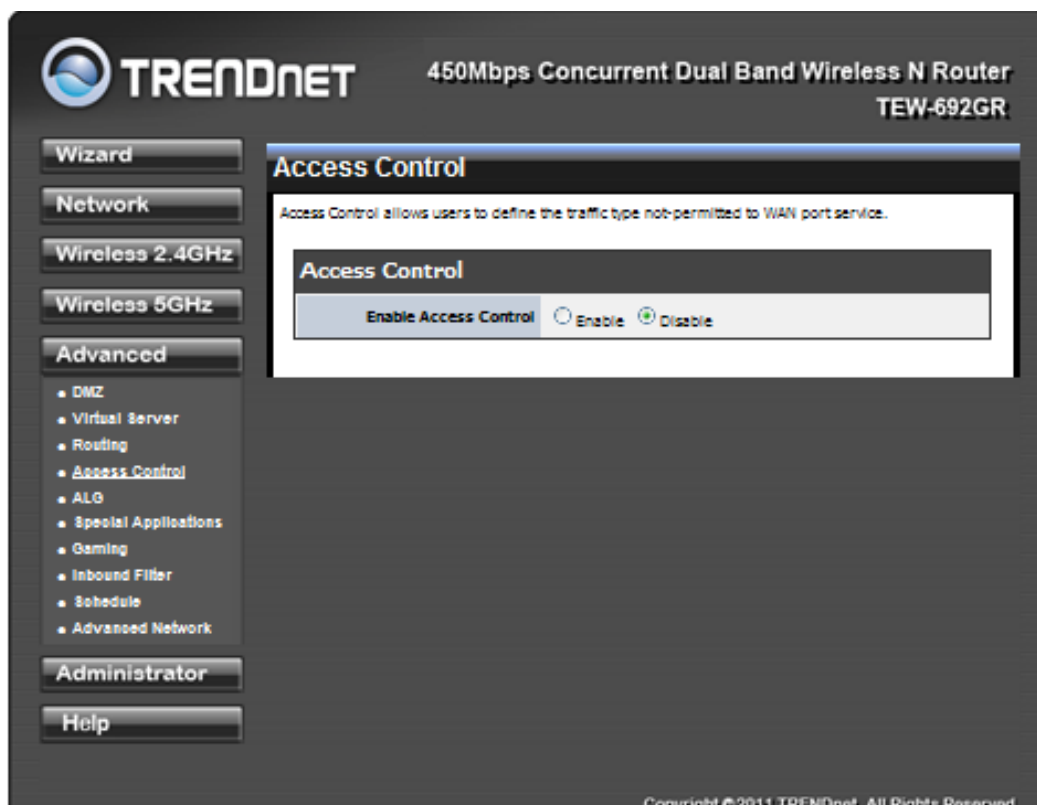
**Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network 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.

## ACCESS CONTROL

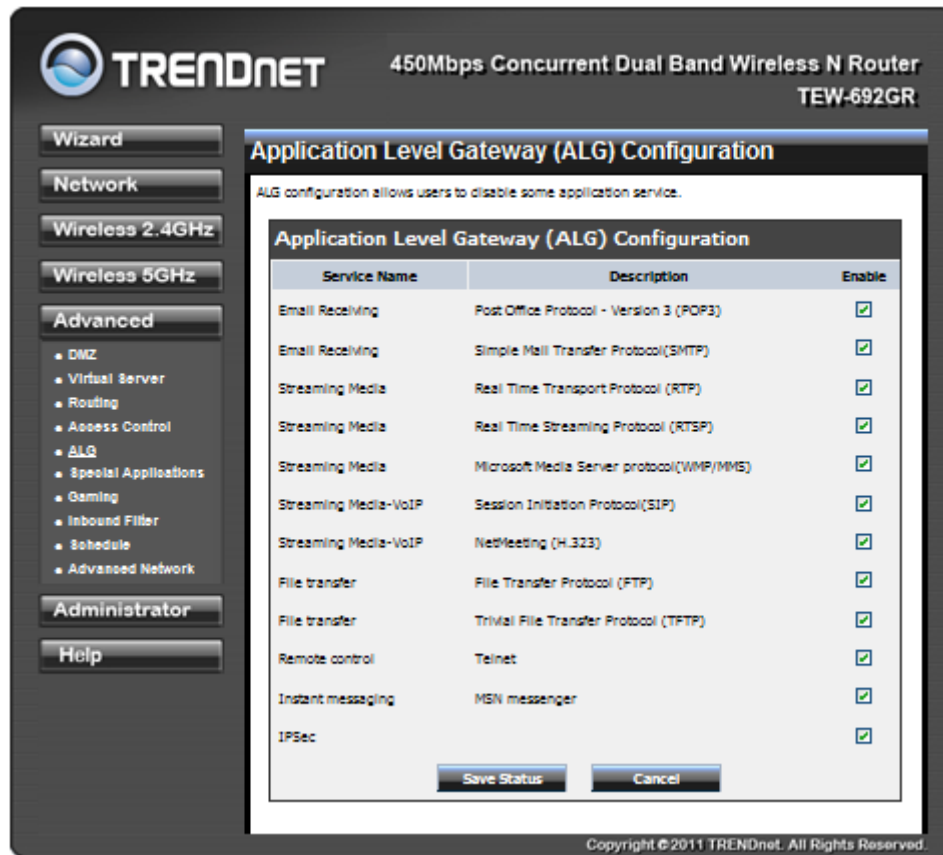


**Enable:** By default, the Access Control feature is disabled. If you need Access Control, check this option.

**Note:** When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.



# ALG



**ALG (Application level gateway):** It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, SIP, RTSP, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

# SPECIAL APPLICATIONS



## Add/Edit Port Trigger Rule

**Enable:** Specifies whether the entry will be active or inactive.

**Name:** Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. Alternatively, you can select from the **Application** list of common applications.

**Protocol:** Select the protocol used by the service. The common choices -- UDP, TCP, and both UDP and TCP -- can be selected from the drop-down menu.

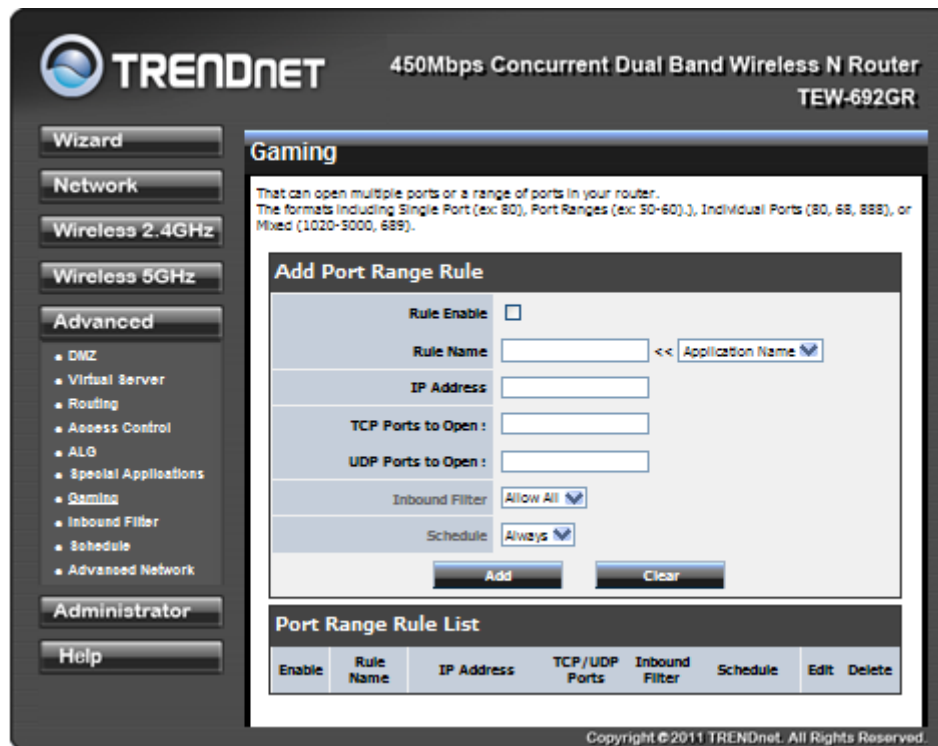
**Trigger Port:** Enter the outgoing port range used by your application (for example **6500-6700**).

**Schedule:** Select a schedule for when this rule is in effect.

**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

**Port Trigger Rule List:** This is a list of the defined application rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon.

# GAMING



**Add/Edit Port Range Rule:** Use this section to add a Port Range Rule to the following list or to edit a rule already in the list.

**Rule Enable:** Specifies whether the entry will be active or inactive.

**Rule Name:** Give the rule a name that is meaningful to you, for example **Game Server**. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.

**IP Address:** Enter the local network IP address of the system hosting the server, for example **192.168.10.50**. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

**TCP Ports to Open:** Enter the TCP ports to open (for example **6159-6180, 99**).

**UDP Ports to Open:** Enter the UDP ports to open (for example **6159-6180, 99**).

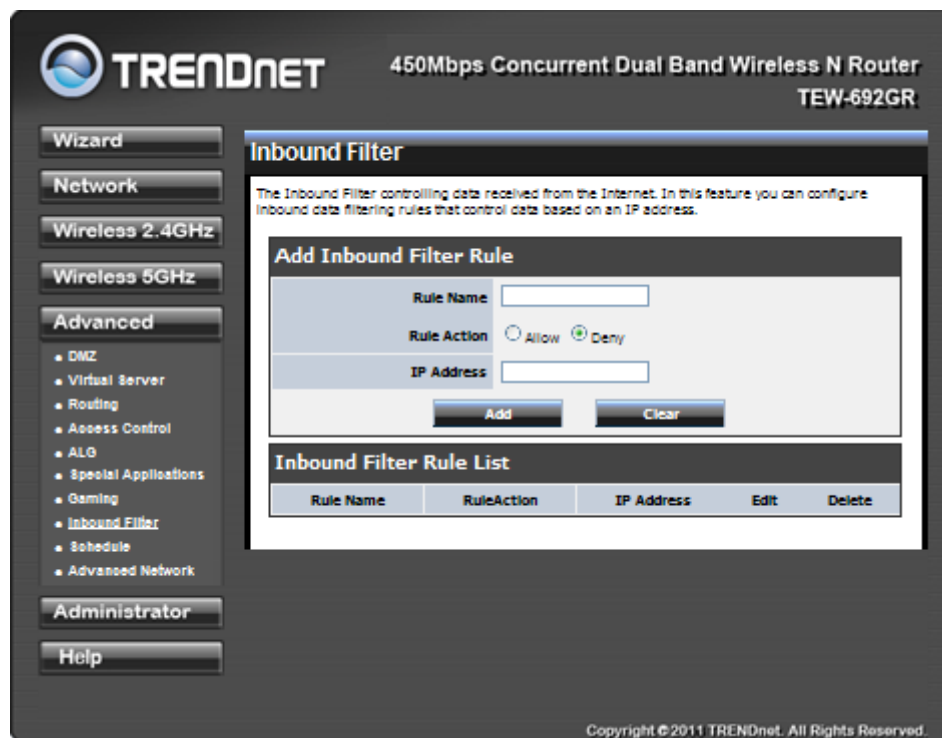
**Inbound Filter:** Select a filter that controls access as needed for this rule.

**Schedule:** Select a schedule for the times when this rule is in effect.

**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

**Port Range Rule List:** This is a list of the defined Port Range Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry 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 Port Forwarding Rule" section is activated for editing.

# INBOUND FILTER



**Add/Edit Inbound Filter Rule:** Here you can add entries to the Inbound Filter Rules List below, or edit existing entries.

**Name:** Enter a name for the rule that is meaningful to you.

**Action:** The rule can either Allow or Deny messages.

**Remote IP Range:** Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the **Start** and **End** boxes. Up to eight ranges can be entered. The **Enable** checkbox allows you to turn on or off specific entries in the list of ranges.

**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

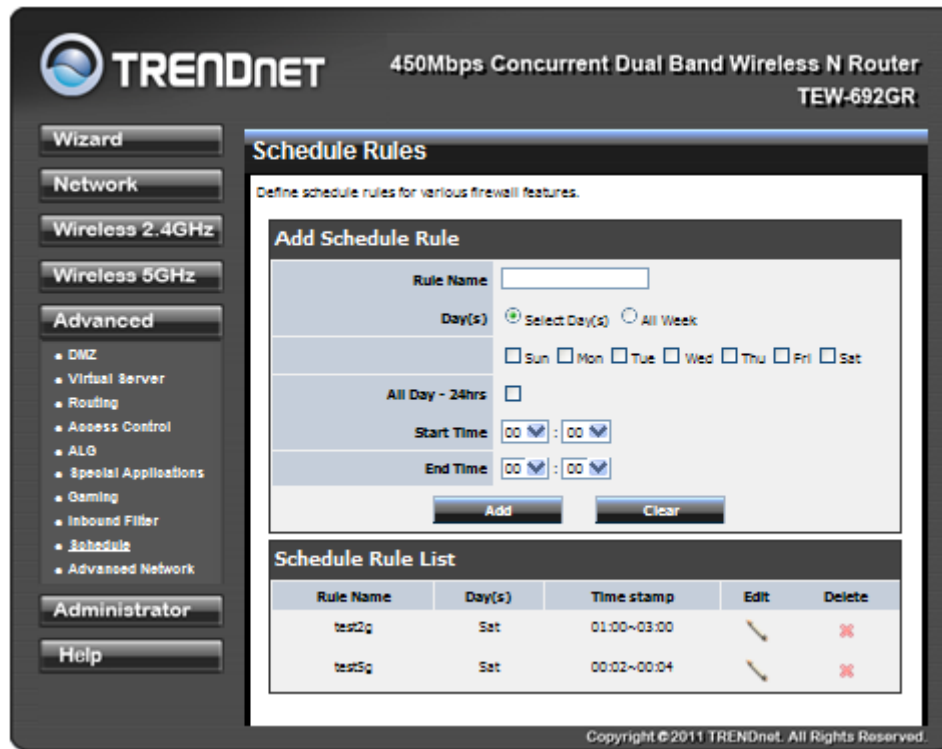
**Inbound Filter Rules List:** The section lists the current Inbound Filter Rules. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Inbound Filter Rule" section is activated for editing.

In addition to the filters listed here, two predefined filters are available wherever inbound filters can be applied:

**Allow All:** Permit any WAN user to access the related capability.

**Deny All:** Prevent all WAN users from accessing the related capability. (LAN users are not affected by Inbound Filter Rules.)

# SCHEDULE



**Add/Edit Schedule Rule:** In this section you can add entries to the Schedule Rules List below or edit existing entries.

**Name:** Give the schedule a name that is meaningful to you, such as "Weekday rule".

**Day(s):** Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

**All Day - 24 hrs:** Select this option if you want this schedule in effect all day for the selected day(s).

**Start Time:** If you don't use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are normally triggered only by the start time. End Time

The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not normally used for email events.

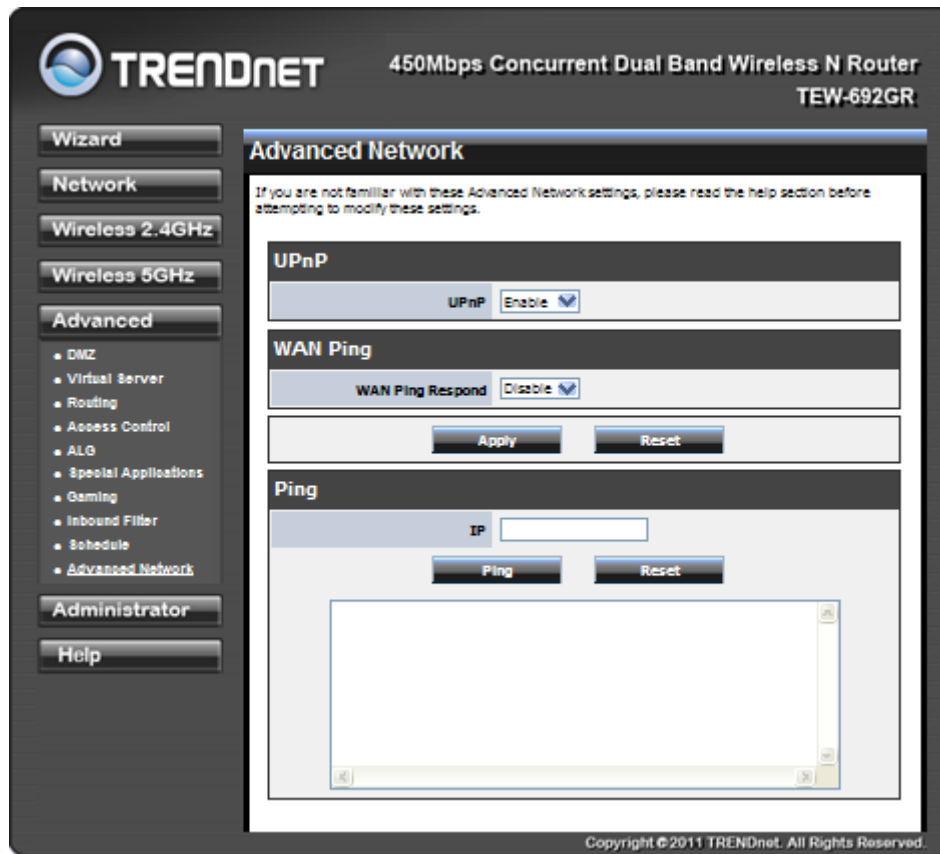
**Clear:** Re-initialize this area of the screen, discarding any changes you have made.

**Schedule Rules List:** This section shows the currently defined Schedule Rules. An entry 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 Schedule Rule" section is activated for editing.

Clear Re-initialize this area of the screen, discarding any changes you have made.

**Schedule Rules List :** This section shows the currently defined Schedule Rules. An entry 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 Schedule Rule" section is activated for editing.

# ADVANCED NETWORK



**UPnP:** By default, the UPnP feature is enabled. Universal Plug and Play (UPnP) is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

**WAN Ping:** By default, the WAN Ping Respond feature is disabled. Enable WAN Ping Respond will reply information of router to outside network.

# Administrator

## MANAGEMENT

The screenshot displays the 'System Management' page of a Trendnet router. The page title is '450Mbps Concurrent Dual Band Wireless N Router TEW-692GR'. The left sidebar contains navigation options: Wizard, Network, Wireless 2.4GHz, Wireless 5GHz, Advanced, Administrator (selected), and Help. The main content area is titled 'System Management' and includes a sub-header 'You may configure administrator account and password.' Below this are five sections: 1. Administrator Settings: Account (admin), Password (empty, with a note '(Max Length: 16 characters)'), Idle Timeout (300 seconds). 2. Device Name Settings: Device Name (TEW-692GR). 3. Device URL Settings: Device URL (trendnet.com). 4. DDNS Settings: Dynamic DNS Provider (None), Host Name (empty), Account (empty), Password (empty). 5. Remote Management: Remote Control (via WAN) (Disable), Remote Port (8080). Each section has 'Apply' and 'Cancel' buttons. A copyright notice 'Copyright © 2011 TRENDnet. All Rights Reserved.' is at the bottom right.

**Admin Password:** Enter a password for the user "admin", who will have full access to the Web-based management interface.

**Device Name:** The name of the router can be changed here.

**Enable Dynamic DNS:** Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following parameters are displayed when the option is enabled.

**Dynamic DNS Provider:** Select a dynamic DNS service provider from the pull-down list.

**Host Name:** Enter your host name, fully qualified; for example: **myhost.mydomain.net**.

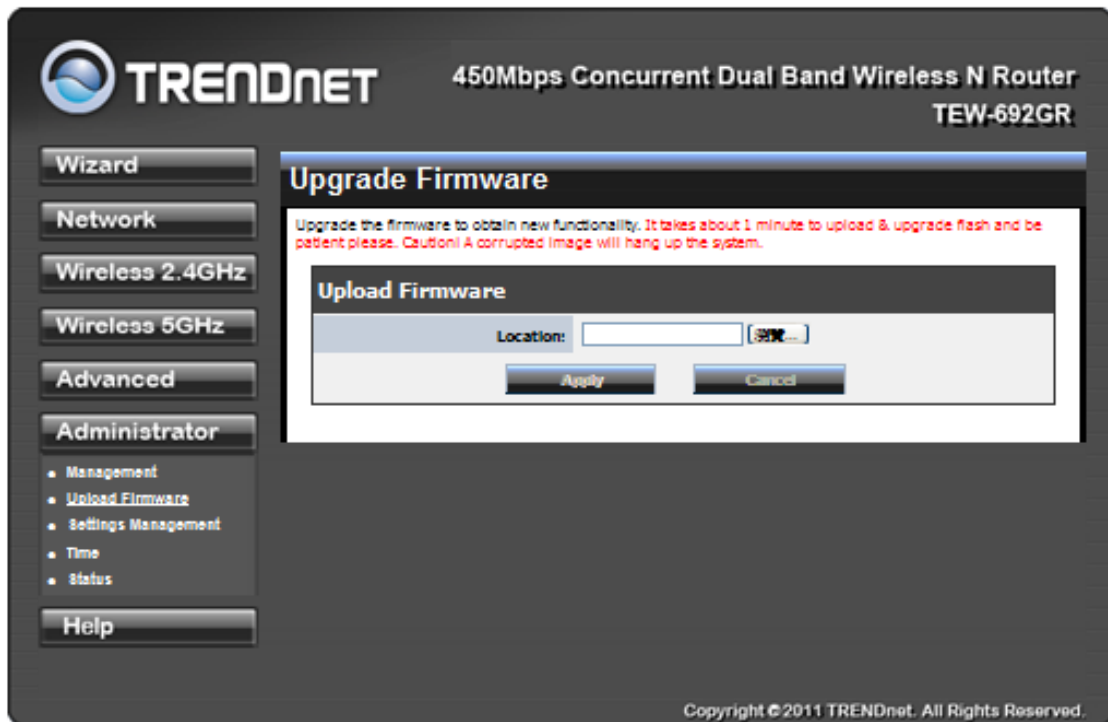
**Account:** Enter the account provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

**Password:** Enter the password provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields. Enter your host name, fully qualified; for example: **myhost.mydomain.net**.

**Account:** Enter the account provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

**Password:** Enter the password provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

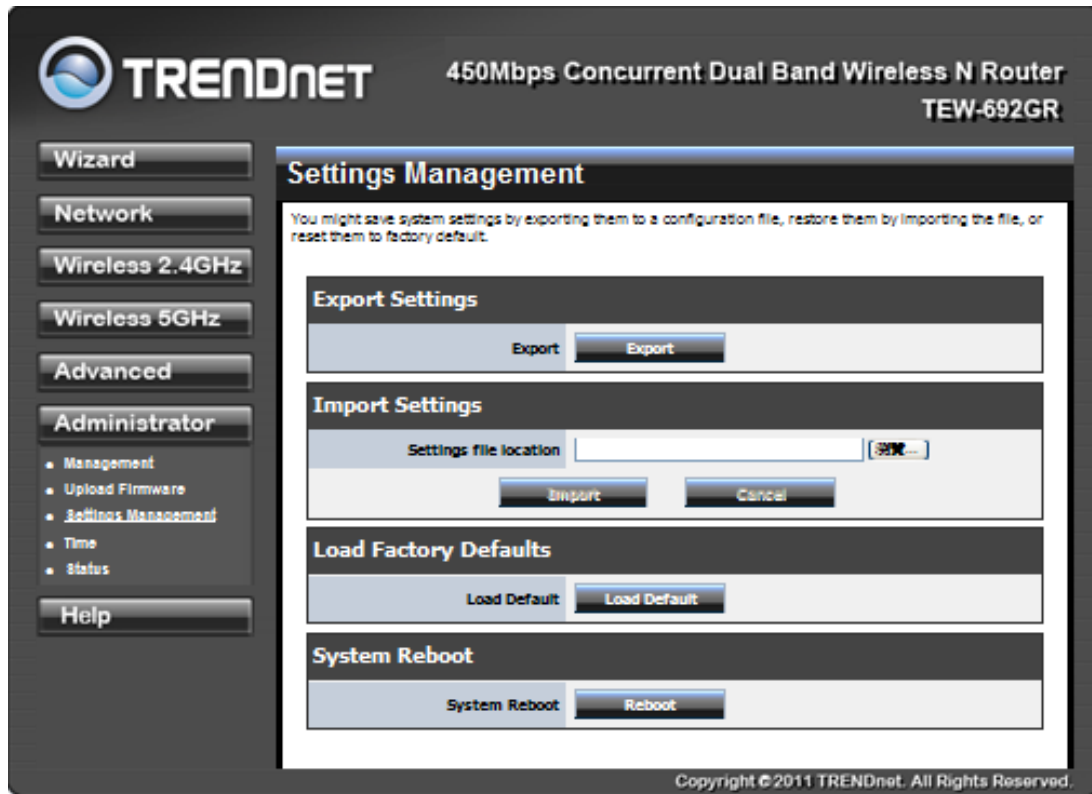
## UPLOAD FIRMWARE



Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the router.



# SETTING MANAGEMENT



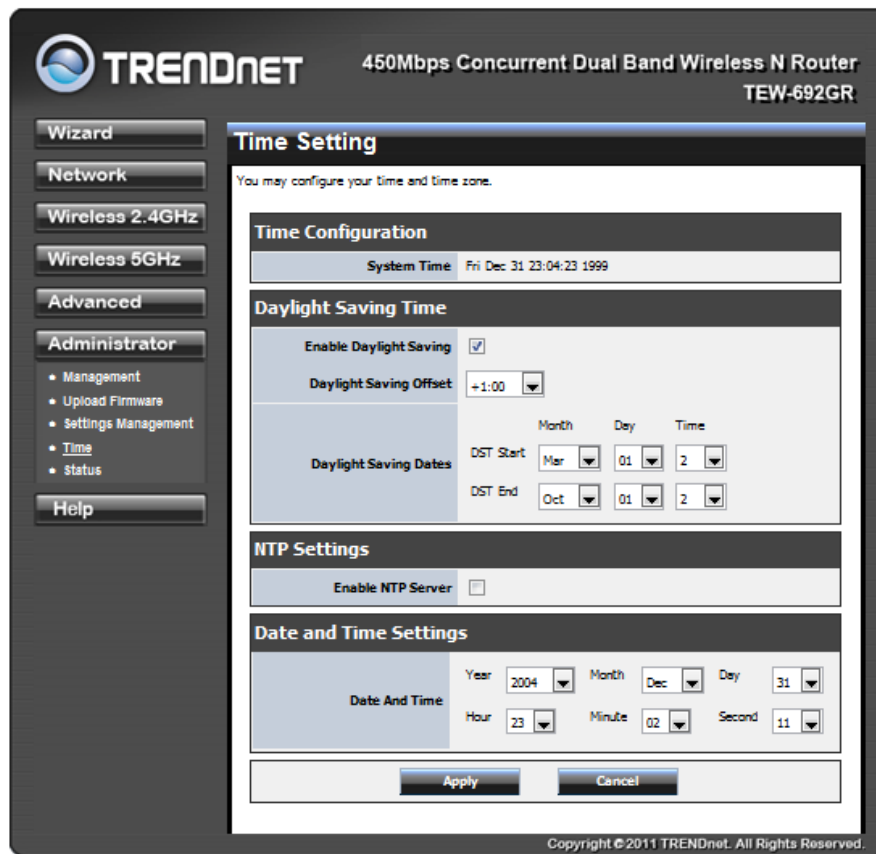
**Export Settings:** This option allows you to export and then save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

**Import Settings:** Use this option to restore previously saved router configuration settings.

**Load Factory Defaults:** This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your router configuration settings, use the **Export Settings** option above.

**System Reboot:** This restarts the router. It is useful for restarting when you are not near the device.

# TIME



## Time Configuration

**Current Router Time:** Displays the time currently maintained by the router. If this is not correct, use the following options to configure the time correctly.

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

**Enable NTP Server:** Select this option if you want to synchronize the router's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate. Note that, even when NTP Server is enabled, you must still choose a time zone and set the daylight saving parameters.

**NTP Server Used:** Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

**Set the Date and Time Manually:** If you do not have the NTP Server option in effect, you can either manually set the time for your router here.

# STATUS

The section displays the current status of the router.

The screenshot shows the 'Status' page of a TrendNet 450Mbps Concurrent Dual Band Wireless N Router (TEW-692GR). The page is divided into several sections: System Info, Internet Configurations, LAN, Wireless LAN, and Wireless2 LAN. A sidebar on the left contains navigation buttons for Wizard, Network, Wireless 2.4GHz, Wireless 5GHz, Advanced, Administrator, and Help. The Administrator section is expanded to show Management, Upload Firmware, Settings Management, Time, Status, and Help.

**TRENDNET** 450Mbps Concurrent Dual Band Wireless N Router  
TEW-692GR

**Status**

The status status.

### System Info

Firmware Version	0.0.0.42, 21-Apr-2011
System Time	Sat Jan 1 00:48:09 2000
System Up Time	00:48:10

### Internet Configurations

Connected Type	Static IP
WAN IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary Domain Name Server	0.0.0.0
Secondary Domain Name Server	0.0.0.0

### LAN

MAC Address	00:0C:42:25:92:10
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

### Wireless LAN

MAC Address	00:0C:42:25:92:40
Channel	1
Network Name (SSID) / Security Mode	TRENDnet92_2.4GHz / WEP-OPEN
Multiple SSID 1 / Security Mode	
Multiple SSID 2 / Security Mode	
Multiple SSID 3 / Security Mode	

### Wireless2 LAN

MAC Address	00:0C:42:25:92:10
Channel	20
Network Name (SSID) / Security Mode	TRENDnet92_5GHz / WEP-OPEN
Multiple SSID 1 / Security Mode	
Multiple SSID 2 / Security Mode	
Multiple SSID 3 / Security Mode	

Copyright © 2011 TRENDnet, All Rights Reserved.

# Help

Help section provides web-based explanations on each configurable field.

**TRENDNET** 450Mbps Concurrent Dual Band Wireless N Router  
TEW-692GR

Wizard  
Network  
Wireless 2.4GHz  
Wireless 5GHz  
Advanced  
Administrator  
Help

- Menu
- Network
- Wireless
- Advanced
- Administrator

### Help menu

- Network
- Wireless
- Advanced
- Administrator

#### Network Help

- WAN Setting
- LAN Setting
- QoS Setting
- DHCP Client List

[TOP](#)

#### Wireless Help

- Basic
- Advanced
- Security
- WPS
- Station List

[TOP](#)

#### Advanced Help

- DMZ
- Virtual Server
- Routing
- Access Control
- AIG
- Special Applications
- Gaming
- Inbound Filter
- Schedule
- Advanced Network

[TOP](#)

#### Administrator Help

- Management
- Upload Firmware
- Setting Management
- Time
- Status

[TOP](#)

Copyright © 2011 TRENDnet. All Rights Reserved.

# Appendix

## WIRELESS LAN NETWORKING

This section provides background information on wireless LAN networking technology. Consult the **Glossary** for definitions of the terminology used in this section.

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

### Transmission Rate (Transfer Rate)

---

The TEW-692GR provides various transmission (data) rate options for you to select. In most networking scenarios, the factory default Best (automatic) setting proves the most efficient. This setting allows your TEW-692GR to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the TEW-692GR automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the TEW-692GR gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

### Types of Wireless Networks

---

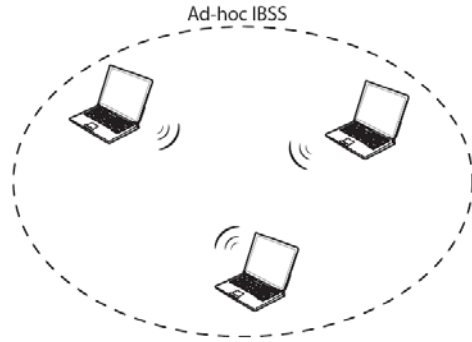
Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

#### **AD-HOC (IBSS) NETWORK**

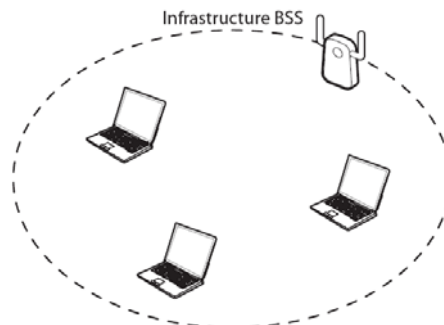
Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each station.



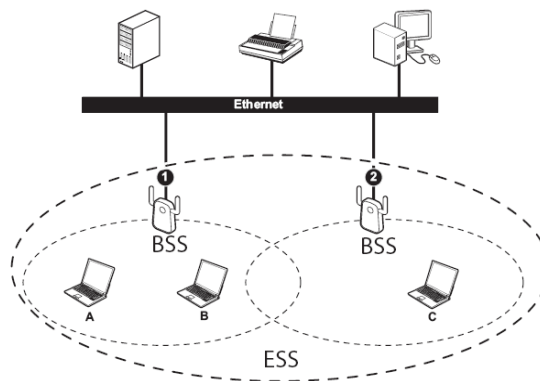
Ad-hoc (peer-to-peer) network diagram

When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).



Infrastructure (BSS) network diagram

In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



Infrastructure (ESS) network diagram

In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the WLAN client devices automatically switches to the channel used in BSS (2).

# GLOSSARY

802.11 - A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. also used to expand the range of a wireless network.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.

Bandwidth - The transmission capacity of a given device or network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

Daisy Chain - A method used to connect devices in a series, one after the other.

DDNS (Dynamic Domain Name System) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access.

Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

FTP (File Transfer Protocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (MegaBits Per Second) - One million bits per second; a unit of measurement for data transmission.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet Internet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard mail server commonly used on the Internet.



Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power over Ethernet (PoE) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

RADIUS (Remote Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

SPI (Stateful Packet Inspection) Firewall - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (Service Set Identifier) - Wireless network's name.

Static IP Address - A fixed assigned address to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (Transmission Control Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (Temporal Key Integrity Protocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network)- The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (Wi-Fi Protected Access) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

xDSL - A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Yagi antenna - A directional antenna used to concentrate wireless signals on a specific location

# Specification

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T) Wireless: IEEE 802.11n, 802.11g, 802.11b, 802.11a
LAN	4 x 10/100/1000Mbps Auto-MDIX port
WAN	1 x 10/100/1000Mbps Auto-MDIX port
WPS Button	Wi-Fi Protected Setup (WPS) connects with other WPS compliant devices
LED Indicator	Power, LAN 1-4, WAN, 2.4 GHz Wireless, 5 GHz Wireless, WPS
Power Adapter	12V DC, 1.5A external power adapter
Power Consumption	9.6 watts (max)
Dimension (L x W x H)	163 x 156 x 26 mm (6.4 x 6.1 x 1 in.)
Weight	175 g
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	FCC: 2.412~2.462 GHz, 5.180~5.240 GHz, 5.725~5.850 GHz ETSI: 2.412~2.472 GHz, 5.150~5.250 GHz
Antenna	2.4GHz: 2dBi (internal), 5GHz: 3dBi (external fixed)
Modulation	OFDM: BPSK, QPSK, 16-QAM, 64-QAM, DBPSK, DQPSK, CCK
Data Rate	802.11a: up to 54Mbps 802.11b: up to 11Mbps 802.11g: up to 54Mbps 802.11n: up to 450Mbps (for both 2.4 & 5GHz)
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
Output Power	802.11a: 14dBm (typical) 802.11b: 18dBm (typical) 802.11g: 15dBm (typical) 802.11n: 15dBm +/- 1 dBm (typical) (for 2.4 & 5GHz)
Receiving Sensitivity	802.11a: -72dBm (typical) @ 54Mbps 802.11b: -84dBm (typical) @ 11Mbps 802.11g: -73dBm (typical) @ 54Mbps 802.11n: -66dBm +/- 1 dBm (typical) @ 450Mbps (for 2.4 & 5GHz)
Channels	2.4GHz: 1~11 (FCC), 1~13 (ETSI) 5GHz: 36, 40, 44, 48, 149, 153, 157, 161 and 165 (FCC) / 36, 40, 44, and 48 (ETSI)

# Limited Warranty

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

## TEW-692GR – 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.



**TRENDnet<sup>®</sup>**

## Product Warranty Registration

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