User's Guide

TRENDnet®

AC750 Wireless VDSL2/ADSL2+ Modem Router

TEW-816DRM

Contents

Product Overview

TEW-816DRM

Package Contents

In addition to your router, the package includes:

- TEW-816DRM
- Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5 m/5 ft.)
- RJ11 telephone cable (1 m/3 ft.)
- Power adapter (12 V DC, 1.5 A)

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

Features

TRENDnet's AC750 Wireless VDSL2/ADSL2+ Modem Router, model TEW-816DRM, offers a combination high performance modem for internet access and a powerful wireless AC750 router. The built-in modem supports the latest ADSL2+ and VDSL2 standards for downstream speeds of up to 200 Mbps*. Wireless AC750 produces concurrent high speed 433 Mbps Wireless AC and 300 Mbps Wireless N networks. Use the two USB and four Ethernet ports to share content and devices across the network.

Features

Easy Setup

Get up and running quickly with the intuitive guided setup

VDSL Internet Service

Compatible with VDSL2 internet service provider networks (Profile 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a support) for downstream throughput of up to 200 Mbps*

ADSL Internet Service

Compatible with ADSL 2/2+ internet service provider networks (ADSL 2/2+ and Annex A, B, I, J, L, and M support)*

Wireless AC750

Concurrent high speed 433 Mbps Wireless AC + 300 Mbps Wireless N bands

Pre-Encrypted Wireless

For your convenience the wireless network arrives pre-encrypted with its own unique password

One Touch Connection

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

Ethernet Ports

Four Ethernet ports to connect wired devices

USB Share Ports

Plug in flash or storage drives to the two high speed USB ports to share content across the network

Parental Controls

Control access to specific websites and manage which devices can access the router

Remote Management

Remote management and troubleshooting support with TR-069

3G WAN Backup

3G WAN backup support

IPv6

IPv6 network support

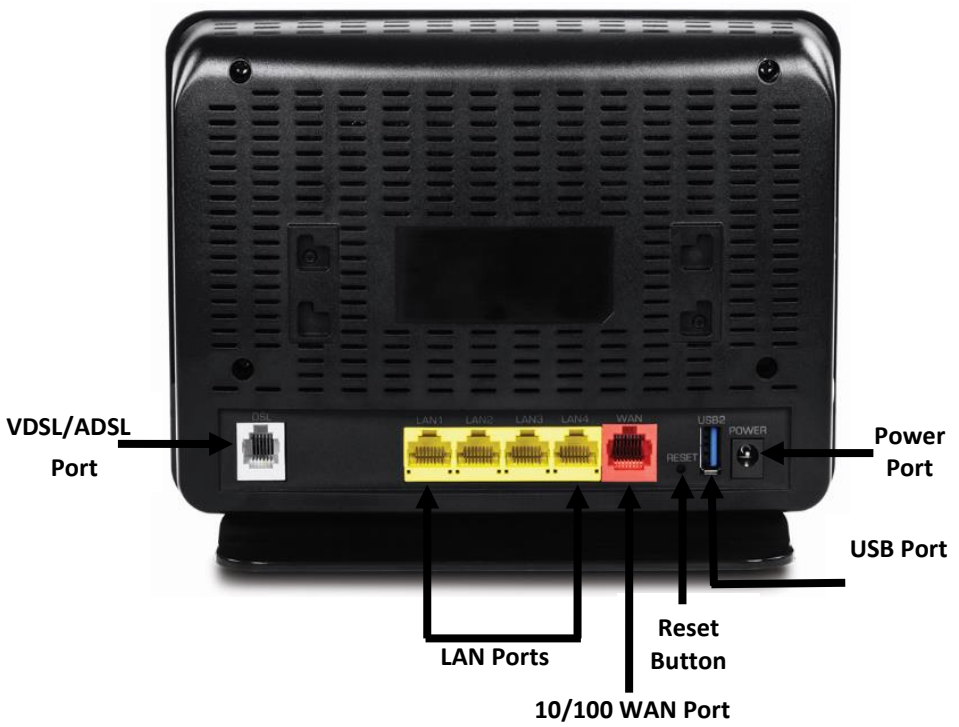
On/Off Power Button

Convenient on/off power button

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

Product Hardware Features

Rear View



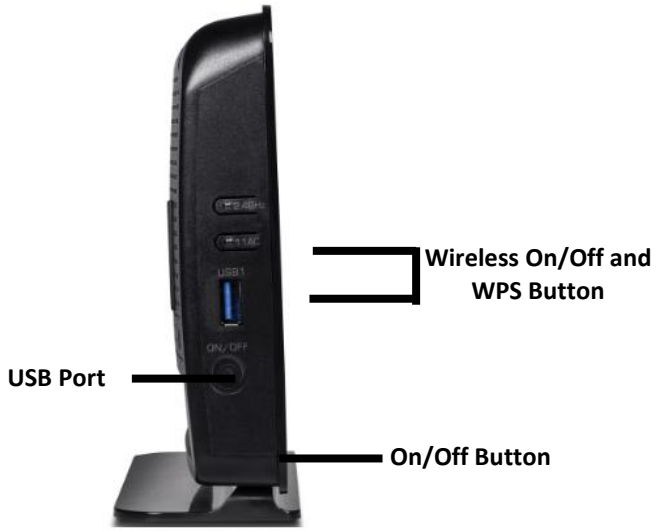
- **VDSL/ADSL Port:** Connect an RJ-11 telephone cable from your modem router ADSL WAN port to your telephone jack/DSL line.
- **LAN Ports:** Connect Network cables (also called network cables) from your modem router LAN ports to your wired network devices.
- **10/100 WAN Port:** Connect an RJ-45 cable when not using VDSL/ADSL WAN connection.
- **Reset Button**: Push and hold this button for **10** seconds and release to reset your router to its factory defaults.
- **USB Port:** Connect a USB device to share files within your network
- **Power Port:** Connect the included power adapter from your modem router power port and to an available power outlet.

Front View

- **Power LED:** This LED indicator is blinks green when properly connected to a power supply. When the device is malfunctioned LED indicator will be red.
- **Internet LED:** This LED indicator is blinking green when the ADSL status of the modem router is ready to establish connection to your ISP. The LED indicator will turn solid green when the modem router has been properly configured with the settings provided by your ISP and successful ADSL connection has been made to your ISP. This LED indicator will be blink while data is transmitted or received through the ADSL port of your modem router.
- **WAN LED**: This LED Indicator is solid green with valid internet connection. The LD indicator blinks green during data transmission. If the indicator is red, this indicates invalid internet connection.
- **LAN 1-4 (Link/Activity) LEDs** – These LED indicators are solid green when the LAN ports are successfully connected to your wired network devices (which are turned on). These LED indicators will blink green while data is transmitted or received through your modem router's LAN ports.
- **2.4GHz Wireless LED:** This LED indicator is solid green when the wireless is "On" and functioning properly on your modem router. This LED indicator will be blinking while data is transmitted or received by your wireless clients or wireless network devices connected to your modem router. This LED indicator will be off when the wireless functionality of your modem router is disabled.
- **5GHz Wireless LED:** This LED indicator is solid green when the wireless is "On" and functioning properly on your modem router. This LED indicator will be blinking while data is transmitted or received by your wireless clients or wireless network devices connected to your modem router. This LED indicator will be off when the wireless functionality of your modem router is disabled.
- **WPS LED:** This LED indicator blinks green when WPS is activated. The LED will stop blinking and remain solid when WPS is completed. When the indicator blinks red it indicates there was no WPS device connected.
- **USB1/2:** This LED indicator blinks green when a device is connected to the USB port.

Side View

v



- **Wireless On/Off and WPS Button:** Push button and hold the button down to **10** seconds to turn off the wireless radio. To turn on the wireless radio push and hold down the button for another **10** seconds. To activate WPS to activate WPS (WiFi Protected Setup) push and hold the button for **3** seconds and release to activate WPS. Within 2 minutes, push and hold the WPS button on your wireless client device.
- **USB Port:** Connect a USB device to share files within your network
- **On/Off Button:** Press to on or off the device.

Basic Router Setup

Creating a Home Network

What is a network?

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

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

- **Modem:** Connects a computer or router to the Internet or ISP (Internet Service Provider).
  Note: *The TEW-816DRM is a combination DSL modem and router, therefore, you do not require a separate DSL modem from your ISP when setting up this product.*
- **Router:** Connects multiple devices to the Internet.
- **Switch:** Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Network ports on your router, you will need an additional switch to add more wired connections.

How to set up a home network

1. For a network that includes Internet access, you'll need:
   - Computers/devices with a Network port or wireless networking capabilities.
   - A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
   - A router to connect multiple devices to the Internet.
2. Set up your router. See "How to setup your router" below.
3. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 11.
4. To set up wireless networking on your router, see "Wireless Networking and Security" on page 10.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on page 6 for more detailed installation instructions.

Where to find more help

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

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

Router Installation

Before you Install

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

General ADSL Parameters
VCI: ____
VPI: ____
MTU: _____
Data Encapsulation (LLC/VCMux) : _____
Schedule Type (UBR/CBR/VBR/GFR): _____
VLAN Tag (If required by your ISP): _____

ADSL Connection Types:
1. Ethernet over ATM (RFC 1483 Bridged) with NAT

- **1a. Obtain IP Address Automatically (Dynamic IP Address)**

Host Name (Optional) _____
ISP registered Mac Address or Clone MAC address (Optional)___:___:___:___:___:___

- **1b. Fixed IP address (Static IP Address)**

WAN IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
WAN Subnet Mask: _____. _____._____._____
WAN Gateway IP Address: _____. _____._____._____
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Server Address: _____. _____._____._____

2. IP over ATM (RFC 1483 Routed)

- **2a. Obtain IP Address Automatically (Dynamic IP Address)**

Host Name (Optional) _____
ISP registered Mac Address or Clone MAC address (Optional)___:___:___:___:___:___

- **2b . Fixed IP address (Static IP Address)**

WAN IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
WAN Subnet Mask: _____. _____._____._____
WAN Gateway IP Address: _____. _____._____._____
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Server Address: _____. _____._____._____

3. PPP over ATM (PPPoE)

- **3a. PPPoE to obtain IP automatically**

Account/User Name: _____
Password: _____

- **3b. PPPoE with a fixed IP address**

User Name: _____
Password: _____
Verify Password: _____
IP Address: ____. _____._____._____ (e.g. 215.24.24.129)
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Server Address: _____. _____._____._____

4. PPP over Ethernet (PPPoA)

- **4a. PPPoA to obtain IP automatically**

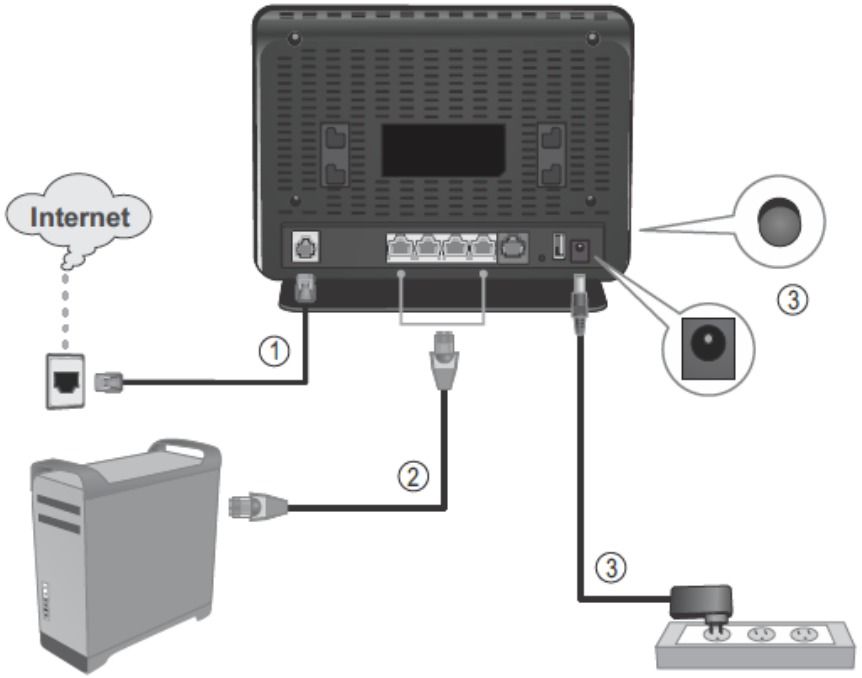
Account/User Name: _____
Password: _____

- **4b. PPPoA with a fixed IP address**

User Name: _____
Password: _____
Verify Password: _____
IP Address: ____. _____._____._____ (e.g. 215.24.24.129)
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Server Address: _____. _____._____._____

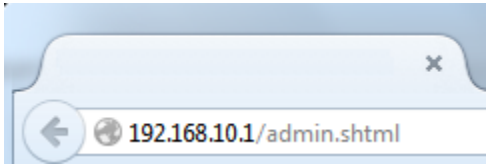
Hardware Installation

1. Connect the detachable antenna to your modem router.
2. Connect one end of the RJ-11 telephone cable to the modem router ADSL port. Connect the other end of the RJ-11 telephone cable to the telephone jack/DSL line.
3. Using the Network cable, connect your computer to one of the four LAN ports on the modem router.
4. Connect the power adapter to the modem router and then to a power outlet.
5. Verify that the status LED indicators on the front of the modem to confirm the device is fully functional: Status (Green), ADSL (Green), WLAN (Green) and the LAN port (1,2,3,4) (Green) your computer is connected.

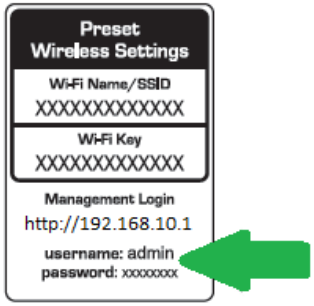


Setup Wizard

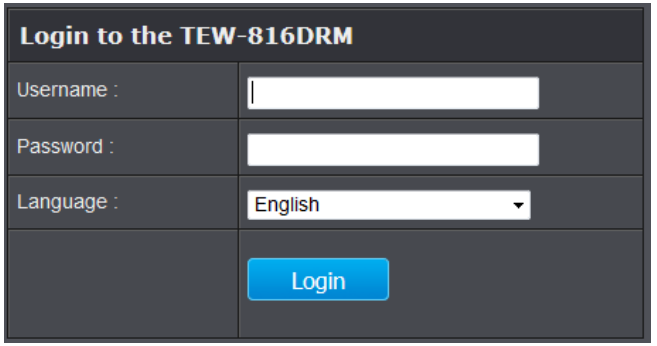
1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1. Your router will prompt you for a user name and password.



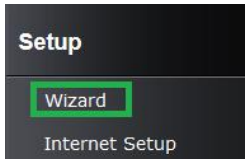
2. Your router will prompt you for a user name and password. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router.



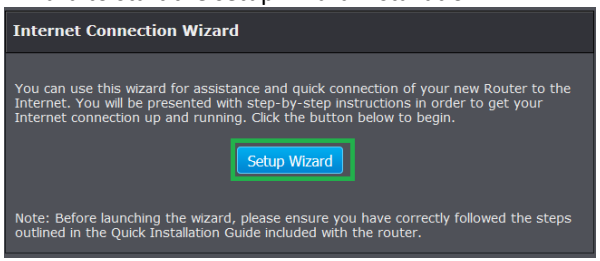
3. Enter your **Username** and **Password**, select your preferred language, and then click ***Login***.



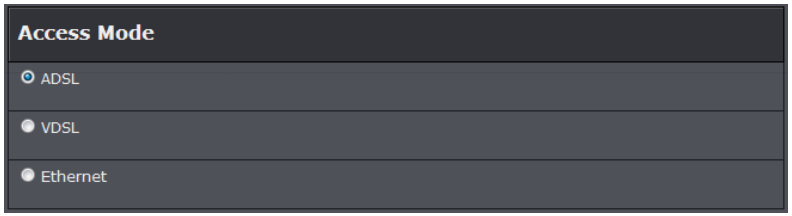
3. Once logged into the router's user interface click Setup Wizard under Setup section on the left side of the interface.



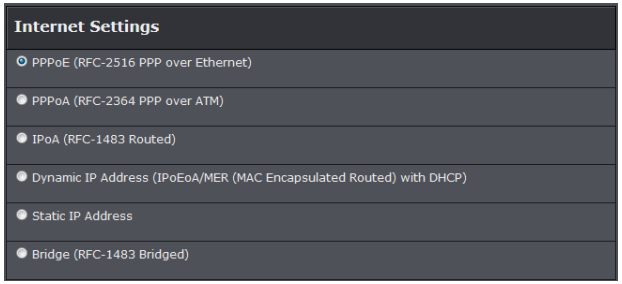
4. Click on Setup Wizard to start the setup wizard installation.



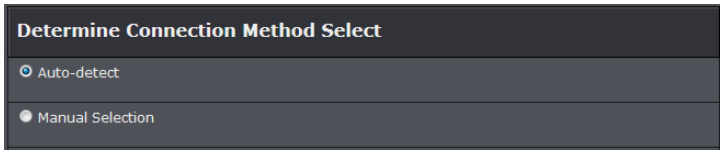
5. Select the mode provided by your ISP (Internet Service Provider) and click Next to continue. The example below is based on PPPoE type with an ADSL connection type. Please contact your ISP (Internet Service Provider) if you uncertain your connection type. l



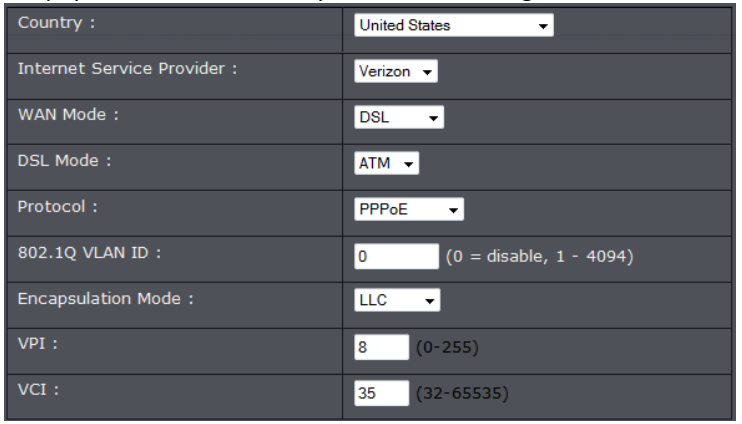
6. Select your connection mode and click **Next**.



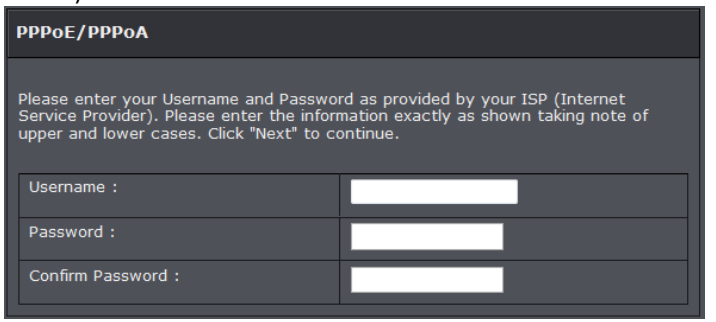
7. Select **Auto**-detect to have the router automatically detect your encapsulation information. Or simply select **Manual Selection** option to manually enter your VPI/VCI settings. Click Next to continue.



9. Once the router detects your **VPI/VCI** settings, select your country and ISP services. If your ISP services it not listed, select **Other**. If you selected Manual Selection on the previous step, you will need to enter your VPI/VCI settings on this section.



10. Enter your assigned Username and Password information from your ISP (Internet Service Provider). Click Next to continue.



11. Verify your settings, and click Finish to completer the setup wizard.

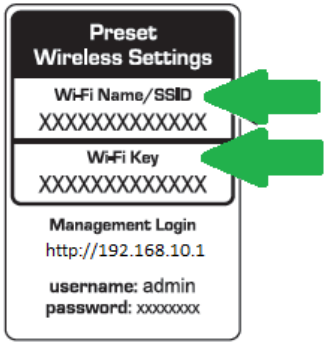
Setup Summary

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

Time Settings :	0
NTP Server 1 :	ntp.trendnet.com
NTP Server 2 :	N/A
Time Zone :	PST
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
802.1Q VLAN ID :	0
Priority :	0
Username :	
Password :	
SSID (2.4G):	816DRM
Visibility Status :	Visible
Encryption :	WPA/WPA2 Mixed
Pre-Shared Key :	1234567890
WEP Key :	N/A
SSID (5G) :	TRENDnet816_5GHz
Visibility Status (5G) :	Visible
Encryption (5G) :	WPA/WPA2 Mixed
Pre-Shared Key (5G) :	123456789
WEP Key (5G) :	N/A

Note: *If you cannot access the Internet, please verify your hardware connections and LED status and re-run the Setup Wizard to verify you have applied the correct settings.*

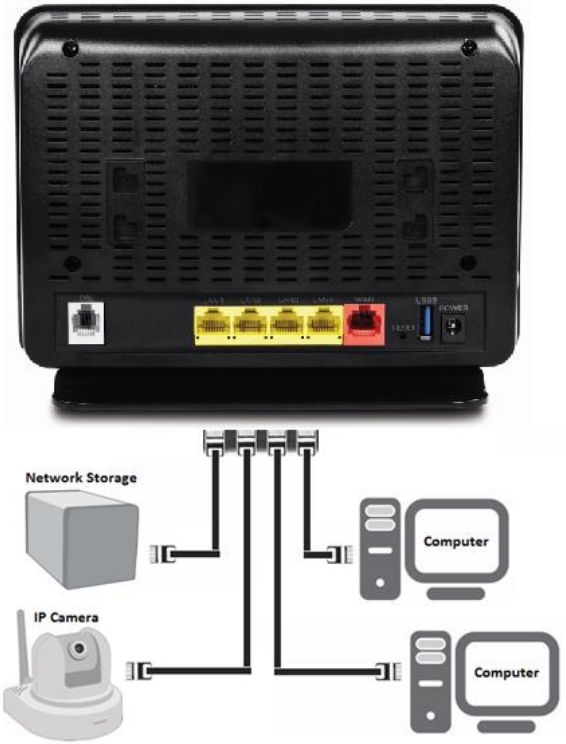
12. For added security, the router is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and pre-assigned network name (SSID) on a sticker on the front of the router and on a label on the bottom of the router. If you would like to change the wireless settings, continue to the next page to launch the wireless setup wizard.



Connect additional wired devices to your network

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

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



Wireless Networking and Security

How to choose the type of security for your wireless network

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

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

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

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

Wireless Encryption Types

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

  Note: *Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.*Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g/n (802.11n devices will operate at 802.11g speeds)	IEEE 802.11a/b/g/n (802.11n devices will operate at 802.11g speeds)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	**Up to 54Mbps**	**Up to 54Mbps**	**Up to 433 Mbps***
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

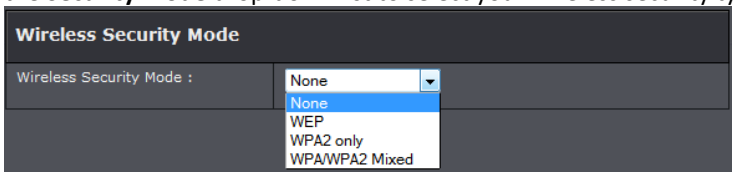
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 433Mbps)

Secure your wireless network

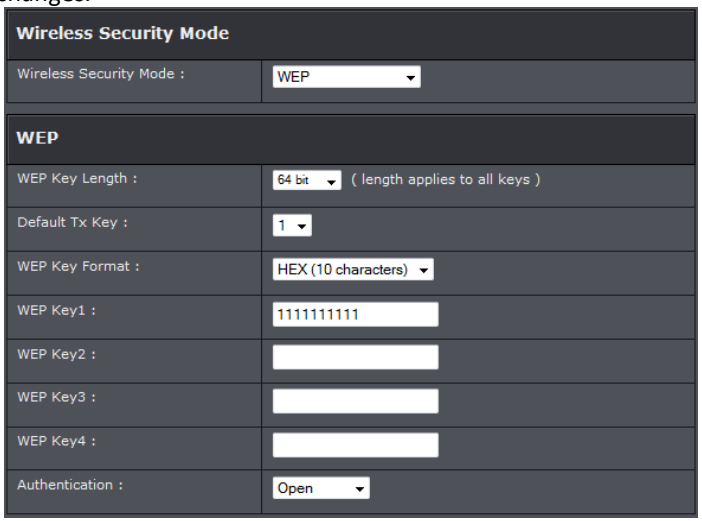
Setup > Wireless Settings

After you have determined which security type to use for your wireless network (see "How to choose the security type for your wireless network" on page 12), you can set up wireless security.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Wireless Settings**.
3. Click on the **Security Mode** drop-down list to select your wireless security type.



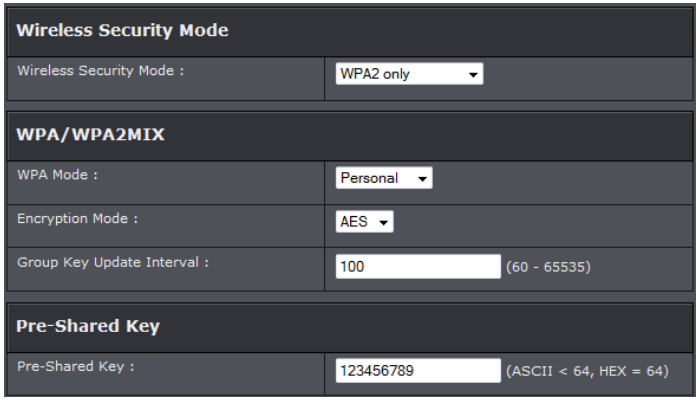
Selecting WEP:
WEP encryption is only available when **802.11b** and **802.11g** is selected in **802.11 Mode** section. Please note that 802.11n does not support **WEP** encryption. If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.



- **Authentication Type:** Choose **Open**, **Shared,** or **Auto**.
  Note: *It is recommended to use Open System because it is known to be more secure than Shared Key.*
- **WEP Key 1-4**
  - Choose **HEX** or **ASCII**.
    Note: *It is recommended to use ASCII because of the much larger character set that can be used to create the key.*
  - This is where you enter the password or key needed for a computer to connect to the router wirelessly
  - You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
  - Choose a key index 1, 2, 3, or 4 and enter the key.
  - When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

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

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



First, from the Security Mode drop-down list, select **WPA-PSK, WPA-PSK / WPA2-PSK,** or **WPA2-PSK.**

- Select the **Encryption** type. When selecting **WPA-PSK** security, it is recommended to use **TKIP.**
- When selecting **WPA-PSK / WPA2-PSK** security, it is recommended to use **AES.**
- When selecting **WPA2-PSK** security, it is recommended to use **AES**.

Create your Wireless security preshared key (password or key):

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

Then from the PSK/EAP row, select either **PSK or EAP**

- **PSK** stands for Preshared Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).
  Note: *EAP requires an external RADIUS server, PSK only requires you to create a passphrase.*

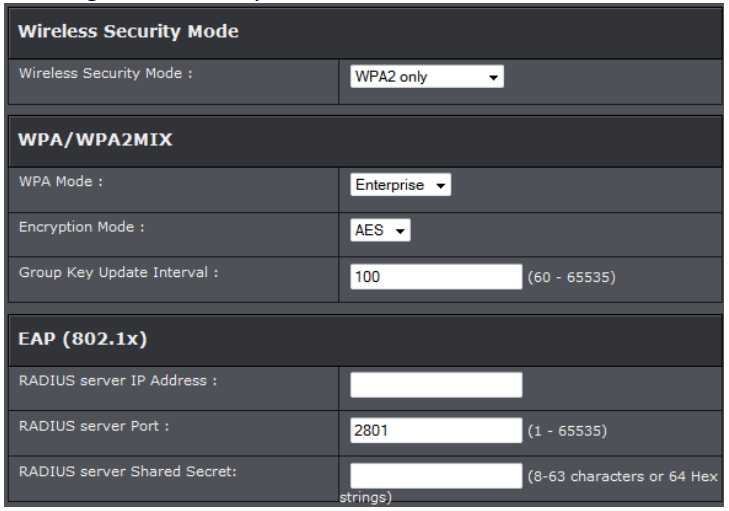
Selecting WPA, WPA / WPA2, or WPA2:

If selecting **WPA, WPA / WPA2, or WPA2 (Wi-Fi Protected Access Extensible Authentication Protocol)** please review the settings to configure and click **Apply** to save the changes.

EAP (Extensible Authentication Protocol) is also called Remote Authentication Dial-In User Service or RADIUS.

Select the **Encryption** Type

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



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

Connect wireless devices to your router

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

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

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this router's wireless network.
See the "Appendix" on page 59 for general information on connecting to a wireless network.

Connect wireless devices using WPS

Setup > Wireless Settings > WPS Setup

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

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

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

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

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

Recommended Hardware Push Button (PBC) Method

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

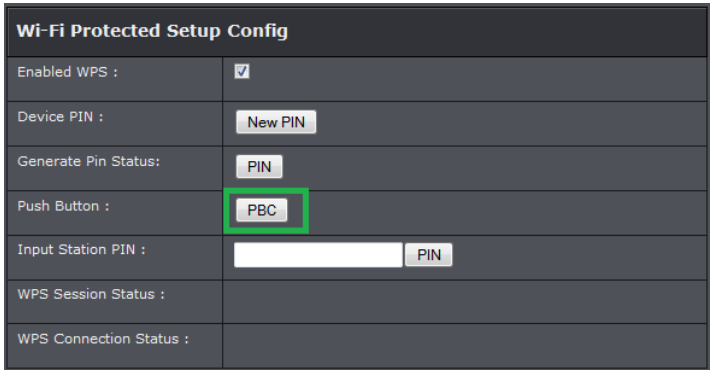
To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting(consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. The WLAN LED on your modem router will flash rapidly indicating that the WPS setup process has been activated. (See "Product Hardware Features" on page 2)
For connecting additional WPS supported devices, repeat this process for each additional device.

PBC (Software/Virtual Push Button)

Setup > Wireless Settings > WPS Setup

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup** and click **Wireless Settings,** then click on the **WPS Setup** button at the bottom of the page.
3. To add a wireless device to your network, simply the push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are connecting, then in your router management page, make sure the **Config Method** is set to **Push Button** (default setting) and click on the **Trigger** button at the bottom of the page.



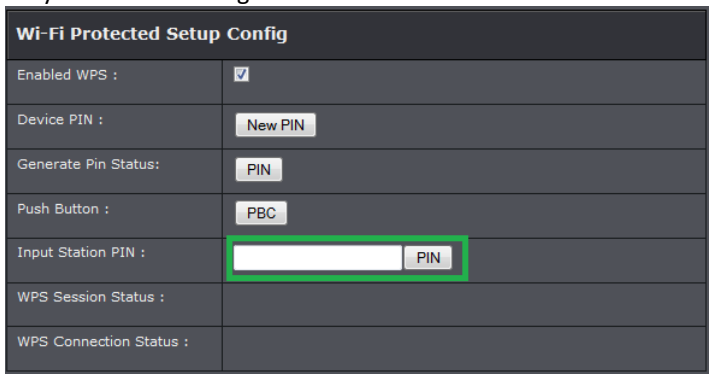
4. The **WPS Status** area will display status messages about the WPS process.
5. The **WPS Status** area will display "Configured" message to indicate that the wireless client device successfully connected using WPS.

PIN (Personal Identification Number)

Setup > Wireless Settings > WPS Setup

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click **WPS Setting** under the wireless band you would like to configure (2.4GHz or 5GHz).
3. In the empty field next to **Input Station PIN**, enter the 8-digit WPS PIN of the wireless client device you are connecting and click **PIN**.



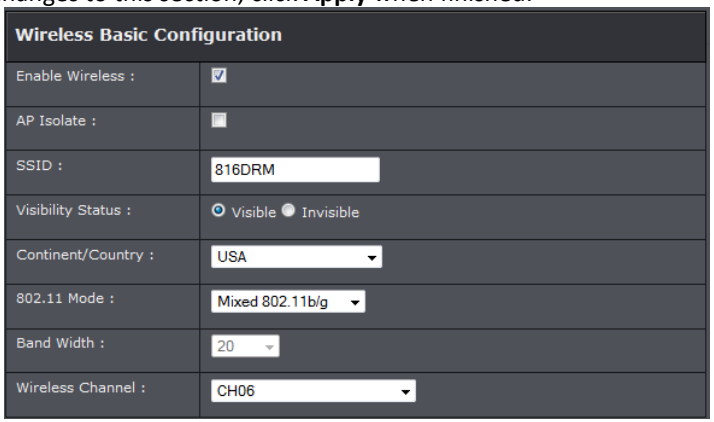
Note: *You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.*

Basic wireless settings

Setup > Wireless Settings

This section outlines available management options under the Wireless Settings tab.

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



- **Enable Wireless**
  - **Enable** turns on the wireless networking on your router (by default it is enabled).
  - **Disable** turns off wireless networking on your router.

    Note: *It is recommended to leave the wireless setting to* ***Enable*** *unless you do not plan on connecting any wireless computers or devices to your network.*
- **AP Isolate:** Check this option to isolate the wireless bands to see each other. .
- **SSID:** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router broadcast TRENDnet816 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember.
- **Visibility Status:**
  - **Visible** turns on broadcasting or your wireless network for clients to see.
  - **Invisible** turns off broadcasting of wireless networking on your router.
- **Continent / Country:** Select the country you the device is operating in.
- **Band Width:** Select the appropriate mode for your network.
  - **B/G/N mixed:** Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
  - **B/G mixed:** This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
  - **N only:** This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if

you have older 802.11g wireless clients, they will no longer be able to connect to this router.
  - **G only:** This mode only allows devices to connect to the router using older and slow 802.11g technology (typically not recommended).
  - **B only:** This mode only allows devices to connect to the router using older and slow 802.11b technology (typically not recommended).
  Note: *Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (B/G/N mixed) for the best compatibility.*

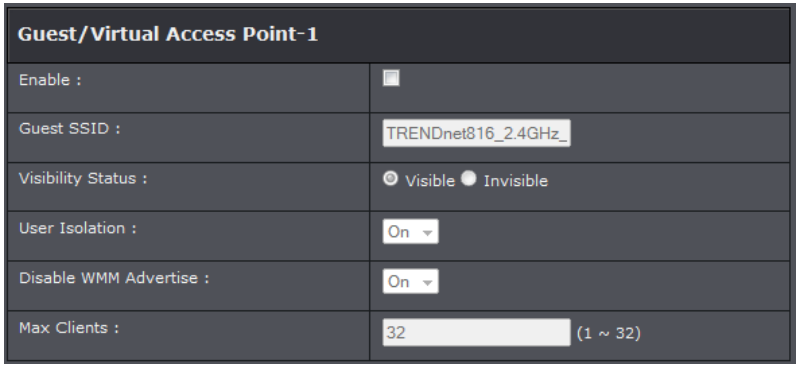
When applying the 802.11 mode setting, please keep in mind the following:
  - **Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.**
  - **Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.**
  - **Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.**
  - **Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.**
  - **Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.**
- **Wireless Channel:** In North America, this router can broadcast on 1 of 11 Channels (13 in Europe and other countries). Selecting the Auto option enables the router to automatically select the best Channel for wireless communication. To manually set the channel on which the router will broadcast, click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.

Guest Network

Setup > Wireless Settings

This section outlines available management options under the Wireless Settings tab.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup,** and click on **Guest Network**.
3. To save changes to this section, click **Apply** when finished.



- **Enable:** Select to enable wireless guest network.
- **Guest (SSID):** Enter the wireless name or SSID of your guest network.
- **Visibility Status:**
  - **Visible** turns on broadcasting or your wireless network for clients to see.
  - **Invisible** turns off broadcasting of wireless networking on your router.
- **User Isolation:** Select On to isolate all users connected to the guest network from each other.
- **Disable WMM Advertise:** Select this option to turn on or off WMM on the specified network.
- **Max Clients:** Enter the maximum wireless clients allowed to connect to the specified network.

Steps to improve wireless connectivity

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

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
   a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
   b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
   c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
   d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
   e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

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

Advanced wireless settings

Setup > Wireless Settings

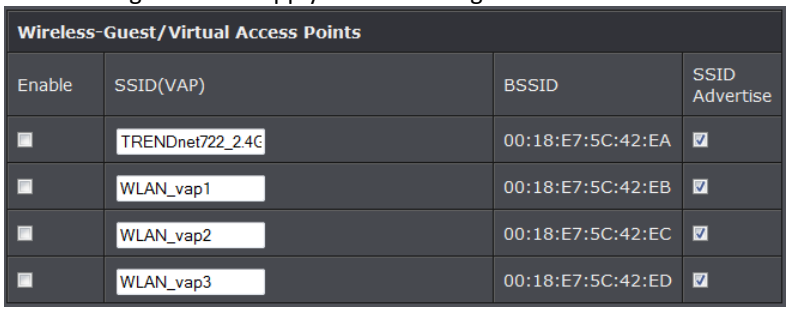
The advanced wireless features can provide you with additional options for setting up your wireless network such as multiple SSID, activate/deactivate wireless according to schedule, and operation modes such as WDS (Wireless Distribution System) bridging or wireless bridging.

Multiple SSID

Setup > Wireless Settings

The multiple SSID feature allows you to broadcast up to two additional SSIDs (or wireless network names). To wireless devices searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Since they appear as separate wireless networks, they are also referred to as virtual APs (Access Points). Each virtual AP can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private. In addition, the SSIDs can be mapped to a specified VLAN ID. See the VLAN section for instructions on assigning VLAN IDs to the SSIDs.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced,** and click on **MBSSID**.
3. Review the settings and click Apply to save settings.



Wireless-Guest/Virtual Access Points

Enable	SSID(VAP)	BSSID	SSID Advertise
☐	TRENDnet722_2.4G	00:18:E7:5C:42:EA	☑
☐	WLAN_vap1	00:18:E7:5C:42:EB	☑
☐	WLAN_vap2	00:18:E7:5C:42:EC	☑
☐	WLAN_vap3	00:18:E7:5C:42:ED	☑

- **Enable:** Check box to enable SSID
- **SSID (VAP):** Enter the SSID you would like to apply.

- **BSSID:** MAC address of the SSID
- **SSID Advertise:** Select to broadcast SSID.

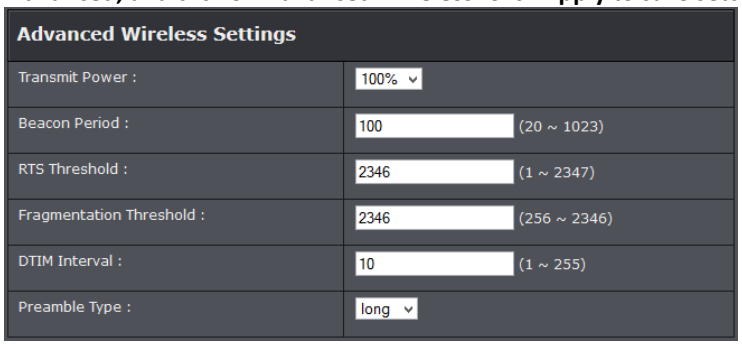
4. See section Secure your wireless network to configure wireless security settings.

Additional Wireless Settings

Advanced > Advanced Wireless

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced,** and click on **Advanced Wireless**. Click **Apply** to save settings.



- **Transmit Power:** The wireless transmit power can be modified to a lower setting such as 50%, 25%, and 12% if necessary. Lowering the wireless transmit may help to better stabilize the wireless connectivity and reduce the effects of wireless interference in areas where there are several 2.4GHz wireless devices. (Default: 100%)
- **Beacon Interval:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.
  Default Value: 100 milliseconds (range: 1-1000)
- **RTS Threshold:** The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
  Default Value: 2346 (range: 256-2346)
- **Fragment Threshold:** Fragmentation in wireless networks is the process of breaking down data communications into smaller data packets in order to improve data efficiency when transferring or receiving data between wireless devices. The fragmentation threshold defines the maximum size of the data packets that are broken down.
- **DTIM Interval:** Is the interval of when the access point informs the clients about the presence of buffered multicast/broadcast data.
- **Preamble Type:** Select long or short preamble.

Wireless bridging using WDS (Wireless Distribution System)

Advanced > Wireless (2.4GHz or 5GHz) > WDS

Wireless bridging using WDS allows the device to create a wireless bridge with other WDS supported wireless routers and access points configured in WDS mode to bridge groups of network devices together wirelessly. Simultaneously, the router will also function in access point mode allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect in order to access network resources from multiple groups of network devices as well as the Internet.

Note: *You can create up to four WDS bridge connections on each wireless band (2.4GHz and 5GHz). WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.*

By default, your router functions in Access Point mode to allow wireless client devices to connect and access your network resources and access the Internet.

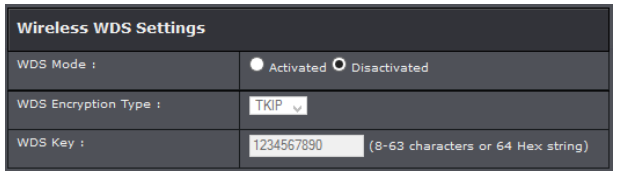
The diagram below shows your router in Access Point mode and clients connecting to your router.

Note: *Before configuring WDS, please ensure the following first:*

1. *Make sure different IP addresses are assigned to each WDS supported wireless device used for bridging. (ex. 192.168.10.1,192.168.10.2, 192.168.10.3) to avoid IP address conflict. See page 29 for changing the LAN IP address.*
2. *If you are using more than one WDS supported router, please make sure the LAN DHCP server is enabled on only one and disabled on all others to avoid IP address conflict. See page 29 for DHCP server options.*
3. *Configure the same wireless channel and use the same on all WDS supported wireless devices. See page 14for configuring basic wireless settings.*
4. *Configure the same wireless security and key on all WDS supported devices. See page 11 for configuring wireless security settings.*

To configure WDS bridging between TEW-816DRM routers:

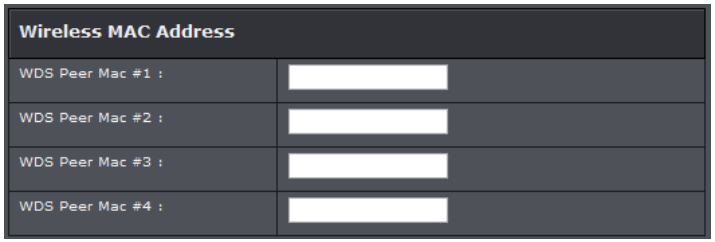
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **Wireless (2.4GHz** or **5GHz*)***, then click on **WDS**.
3. Click on Activate in the **WDS Mode** section**.**



4. Select and enter the encryption type to use.

   Note: *For added security WPA-PSK encryption type is only supported when using WDS feature.*

5. Next to **Wireless Distribution System (WDS)**, in an empty field, enter the MAC address of the other WDS supported wireless device you are bridging. (e.g. *00:11:22:AA:BB:CC)*

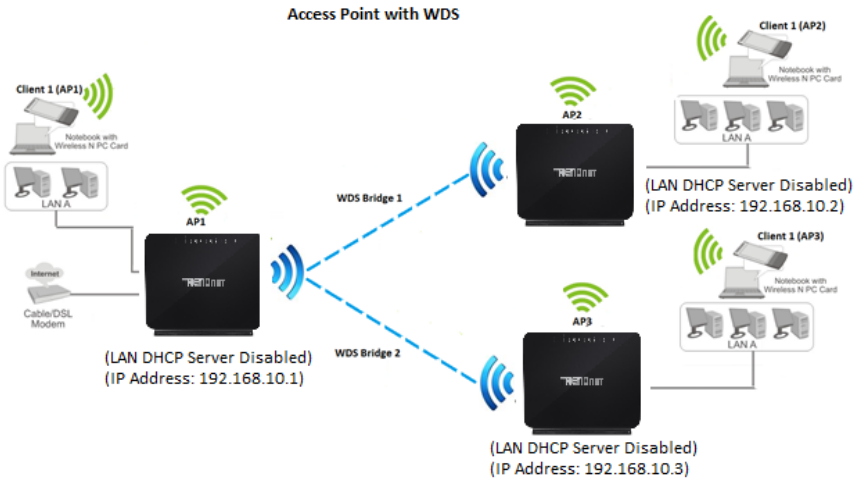


5. To save changes, click **Apply**.

Note: *If you would like to discard the changes, click* ***Cancel*** *before you click* ***Save****.*

For additional routers, make sure to disable the DHCP server first on all additional routers and configure the LAN IP address to be different on each router. You will connect devices to the LAN ports 1-4 only on all additional routers and the WAN port is not used. Then, repeat the steps for additional routers you are bridging.

In the diagram below, the blue color represents the WDS wireless bridged connections between the routers. The green color represents access point mode connections between wireless client devices and the routers.



.

Access Control Filters

Access control basics

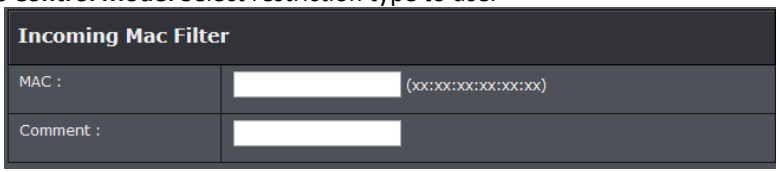
Wireless MAC address filters

Advanced > Advanced Wireless > Wireless MAC Filter

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using wireless MAC filters, you can allow or deny specific wireless clients using this router's wireless network.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Advanced Wireless**, and click on **MAC Filtering**.
3. Review the settings and click **Apply** to save settings and **Add** to enter MAC addresses.

- **Name (SSID):** Select the SSID or wireless network name you would like to apply the wireless MAC filter rule.
- **Access Control Mode:** Select restriction type to use.



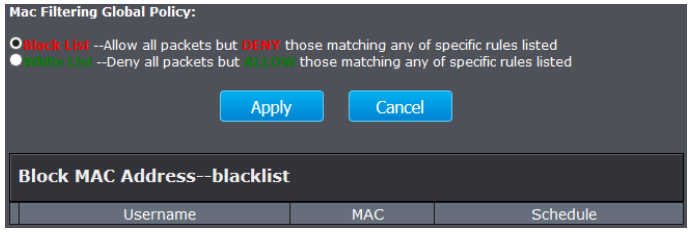
- **MAC:** Enter the MAC address to apply the rule. Click Add to add MAC address to select rule.
- **Comment:** Enter any notes you would like to help distinguish the device.

Note: *Any unspecified MAC/IP addresses or entries without the* ***Allow*** *option checked will be denied network access.*

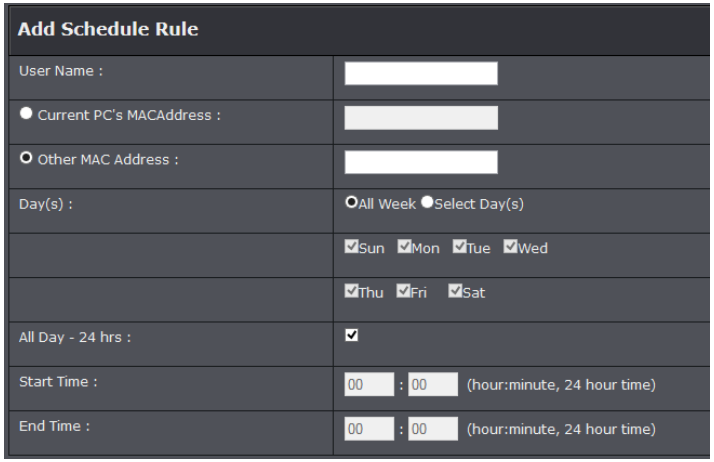
MAC address filters

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Parental Control**, and click on **MAC Filter**.
3. Select the type of Mac filtering option to enable.
   - **Black List:** Deny clients listed on the Mac address table to connect.
   - **White List:** Allows clients listed on the Mac Address table to connect.



4. Click Add to add Mac address to the rule selected.



- **User Name:** Enter the name of the device you are adding.
- **PC's MAC Address:** Select **Current PC's MAC Address** option to automatically enter the PC's Mac address. Or select **Other MAC Address** to manually enter the Mac address.
- **Days:** Select the days you would like the rule to apply on the assignedMac addres
- Start/End Time: Enter the time of when you would like the rule to apply on the assigned Mac address.

5. Click Apply to saving settings

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

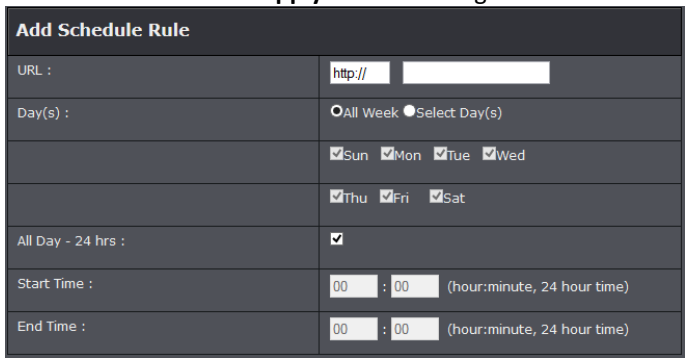
URL/Keyword Blocking

You may want to block computers or devices on your network access to websites using specific keywords (e.g. chat, messenger) or URLs (Uniform Resource Locators).

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Parental Control**, and click on **Website Filter**.
3. Select the mode you would like to apply on your network.

- **Deny:** Select this option to deny all URL listed
- **Allow:** Select this option to only allow URL listed.

4. Click **Add** to enter a URL and click **Apply** to save settings.

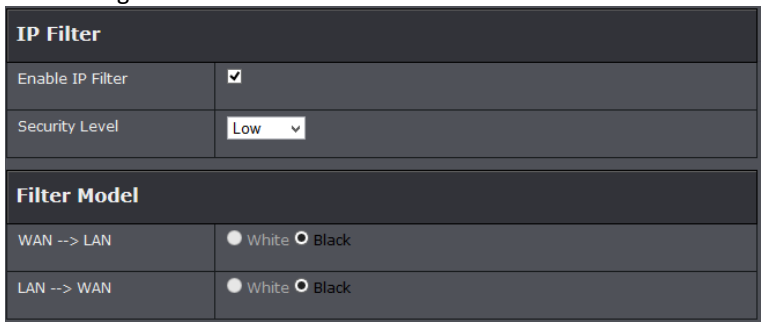


- **URL:** Enter the URL you are adding.
- **Days:** Select the days you would like the rule to apply on the assignedMac addres
- **Start/End Time:** Enter the time of when you would like the rule to apply on the assigned Mac address.

IP Filtering

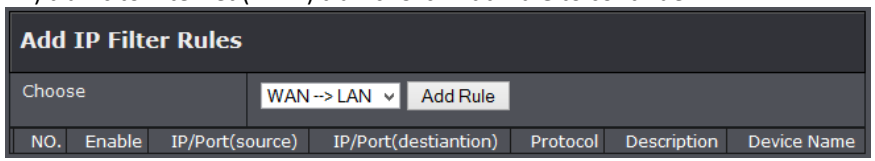
You may want to block computers or devices on your network access to your network using IP address. These steps are similar when using IPv4 or IPv6 IP filtering feature.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Filtering Options**, and click on **IPv4** or **IPv6**.
3. Review the settings and click **Submit** to save.

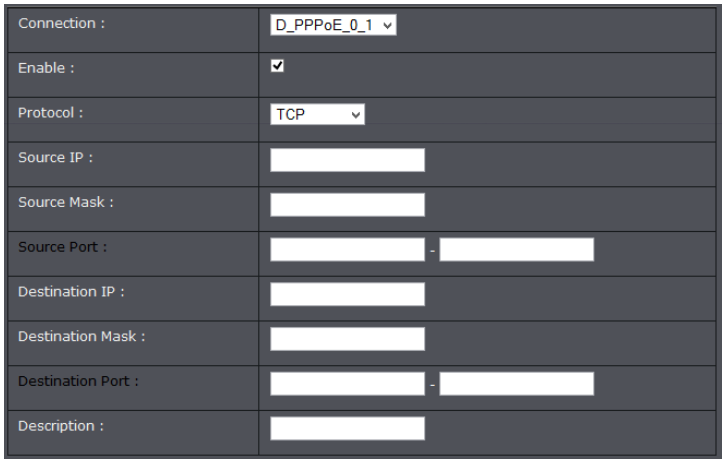


- **Enable:** Check to enable rule.
- **Security Level: Select the level of security to apply. You can refer to the filter model section on the level of security that will apply.**
  - **White:** Allows access
  - **Black:** Denies access
- **Start/End Destination IP Address:** Enter the starting and ending points of the source IP address to filer.

4. Once you have set the level of security, select the Filter you would like to apply. **WAN → LAN** filters Internet (WAN) traffic to Local (LAN) traffic or **LAN → WAN** filters Local (LAN) traffic to Internet (WAN) traffic. Click **Add Rule** to continue.



4. Review the settings below and click Submit to save settings.



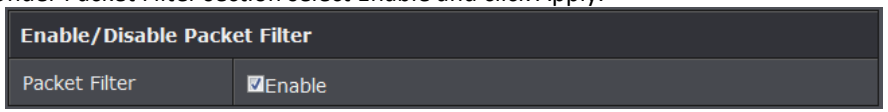
- **Connection:** Select the connection you are applying the filter to.
- **Enable:** Select to enable rule.
- **Protocol:** Select the protocol you would like to filter
- **Source/Destination IP:** Enter the starting and ending points of the source IP address to filer.
- **Source/Destination Port:** Enter the source and destination ports of the filter IP address.
- **Source/Destination Netmask:** Enter the network mask of your source
- **Description:** Enter a description of the rule.

Packet Filters

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

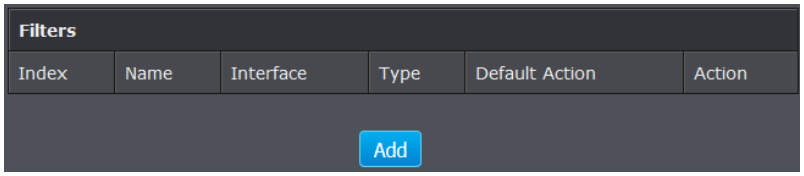
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **Packet Filter**.

3. Under Packet Filter section select Enable and click Apply.



Filter

1. To create a new filter rule. Click Add in the Filters section.

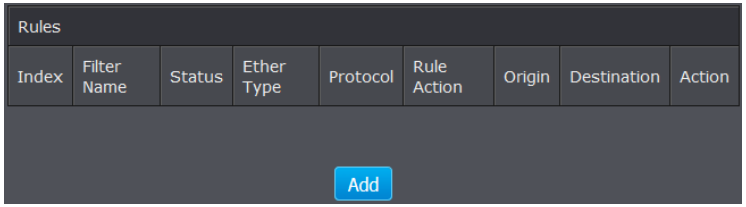


2. Review the settings and click Apply to save.

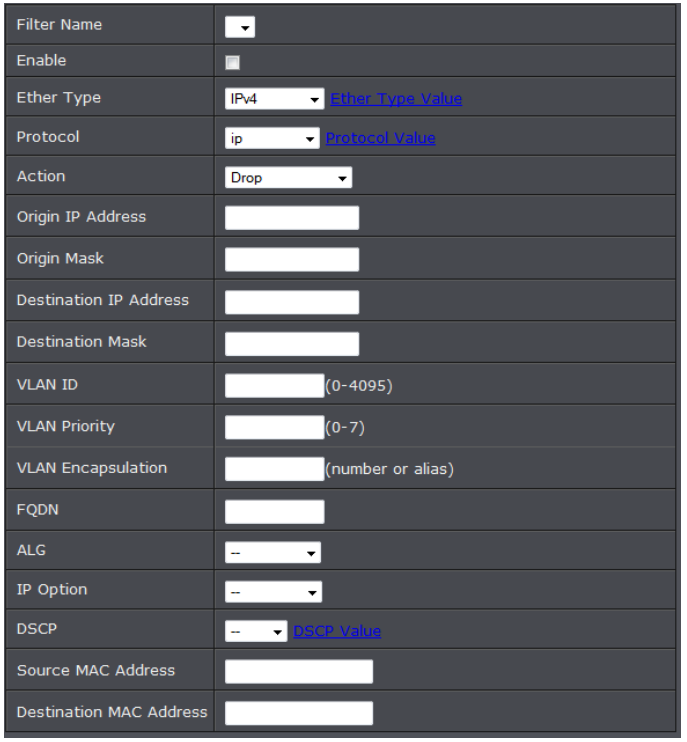
- **Name:** Enter the name of the filter.
- **Interface:**
- **Type:** Select the type of packets to filter. In for incoming packets and Out to filter outgoing packets Select the interface used for the filter..
- **Default Action:** Select to drop or allow the packets.

Rules

1. To create a new rule. Click Add in the Rules section.



2. Review the settings and click Apply to save.

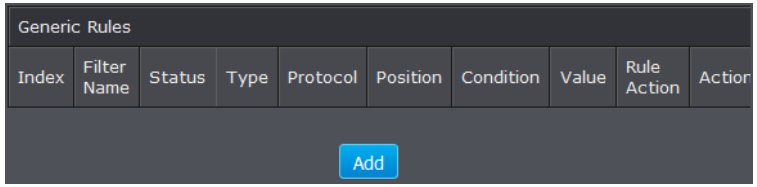


- **Filter Name:** Select the filter name to apply the rule. Enter the name of the filter.
- **Enable:** Check to enable rule
- **Ether Type:** Select the ether type to apply on the rule.
- **Protocol:** Select the protocol type to apply on the rule.
- **Action:** Select the action to take on the rule
- **Origin/Destination IP:** Enter the IP address of the packets origin and destination
- **Origin/Destination Mask:** Enter the Subnet mask of the packets origin and destination.
- **VLAN ID:** Enter the VLAN ID to apply on the rule
- **VLAN Priority:** Enter the VLAN priority of the packets
- **VLAN Encapsulation:** Enter the encapsulation type
- FQDN: Enter the domain name
- **ALG:** Select the ALG type
- **IP Option:** Select IP option type

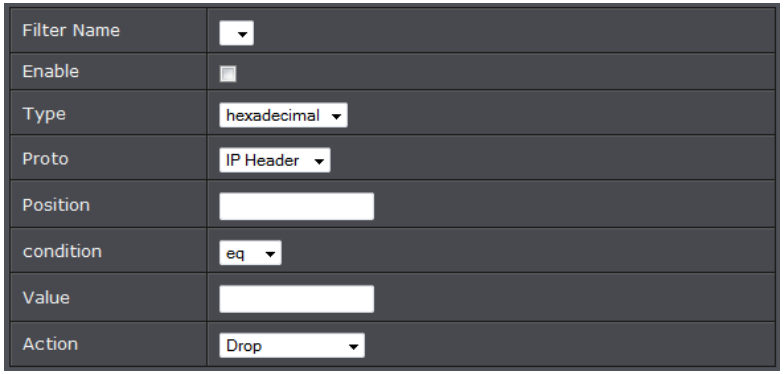
- **DSCP**: Select the DSCP value to apply
- **Source/Destination MAC Address:** Enter the source and destination MAC address of the rule.

Generic Rules

1. To create a new rule. Click Add in the Rules section.



2. Review the settings and click Apply to save.



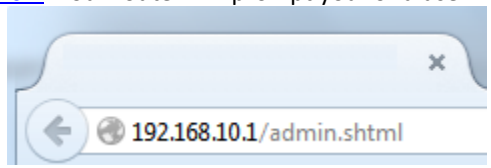
- **Filter Name:** Select the filter name to apply the rule. Enter the name of the filter.
- **Enable:** Check to enable rule
- **Type:** Select the value type to apply on the rule.
- **Proto:** Select the IP Protocol data type
- **Position:** Specify the location of the packet location
- **Condition:** Select the condition type of the rule
- **Value:** Enter the IP checksum value of the packet
- **Action:** Select the action to take of the rule.

Advanced Router Setup

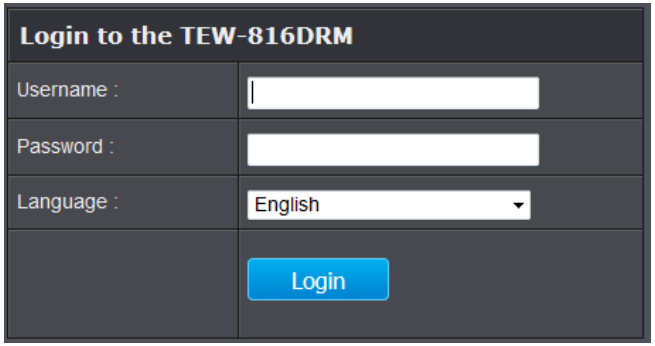
Access your router management page

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

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



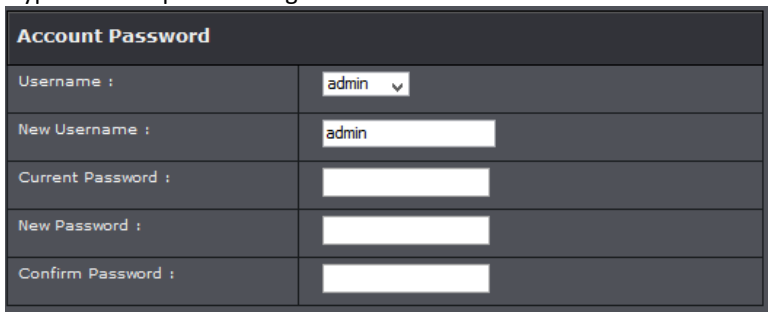
2. Enter the default user name and password and then click Login.
Default User Name: **admin**
Default Password: **xxxxxxx**



Change your router login password

Maintenance > Password

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management** and **Access Controls** and click on **Account Password**.
3. Select the user name to apply changes to. In the **Current Password** field, enter the current password. **New Password** field, enter the new password and in the **Confirm** field, retype the new password again to confirm.



4. Click **Apply** at the bottom of the page to save the changes.

Note: *If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the default password..*

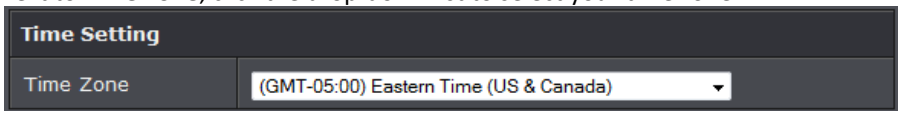
Set your router date and time

Setup > Time and Date

There are two ways to set the router's date and time. NTP (Network Time Protocol) is based on time servers. You can also manually set the router's date and time.

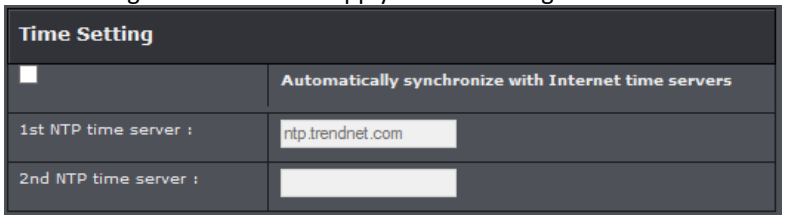
Note: *It is important that the time is configured correctly before setting any schedules. Oour router management page http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.*

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Time and Date**.
3. Next to **Time Zone**, click the drop-down list to select your time zone.



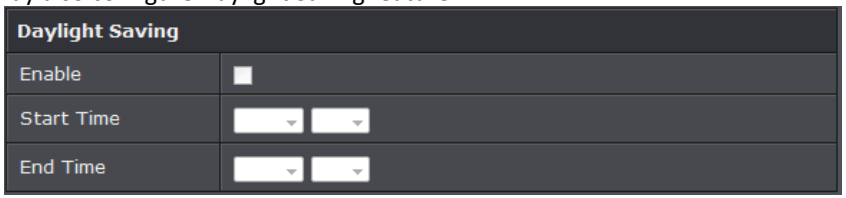
NTP

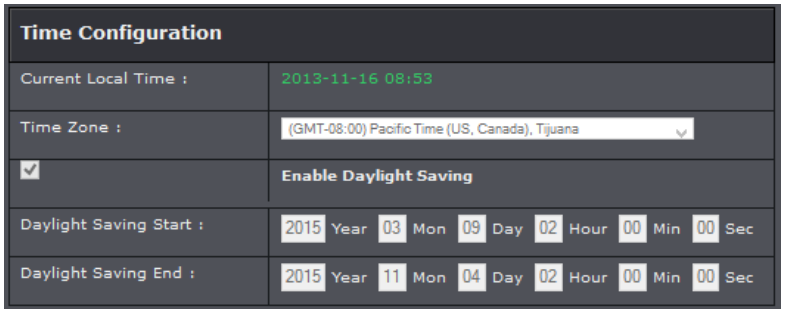
1. Review the settings below and click Apply to save settings.



- **Automatically synchronize with Internet time server:** Check option to enable NTP feature
- **Server IP:** Enter the NTP server IP address or domain to use.

You may also configure Daylight Saving feature.





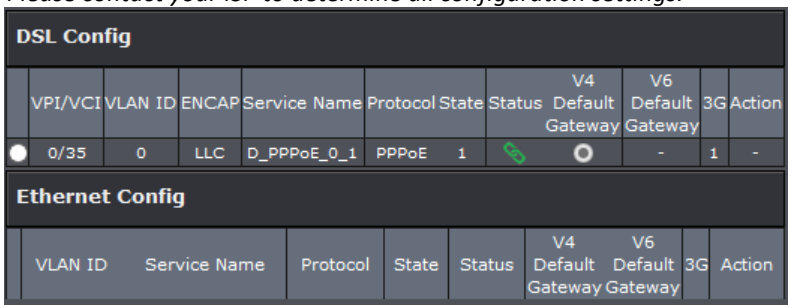
- **Time Zone:** Select your country time zone from the pull down menu.
- **Enable:** Check option to enable daylight savings
- **Start/End Time:** Configure the start and end time of daylight savings.

Manually configure your Internet connection

Setup > Internet Setup

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Internet Setup**.
3. The device supports multiple WAN types, select the WAN type you would like to configure and click **Add** to continue.

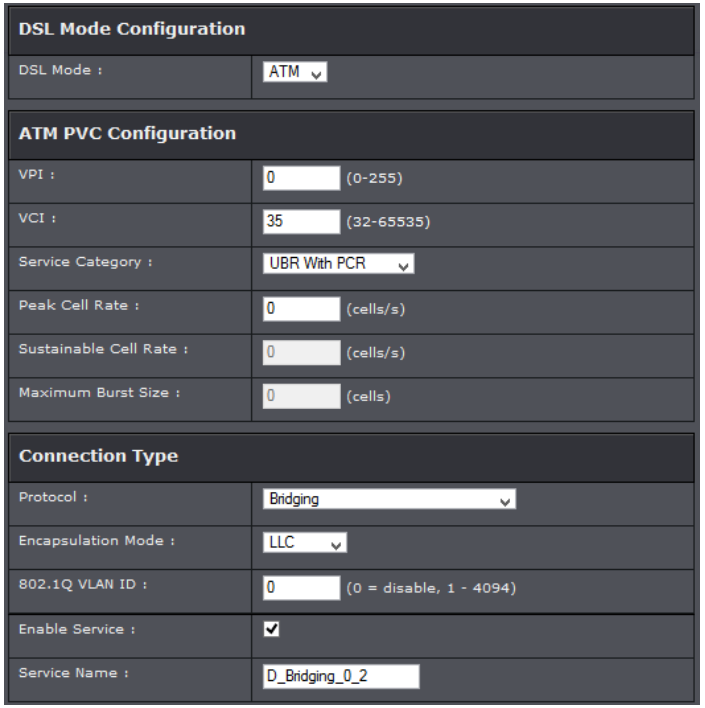
Note: *Please contact your ISP to determine all configuration settings.*



- **DSL Config:** Select this option when configuring an ADSL or VDSL connection
- **Ethernet Config:** Select this option when configuring WAN connections that will use the router's Ethernet WAN port.

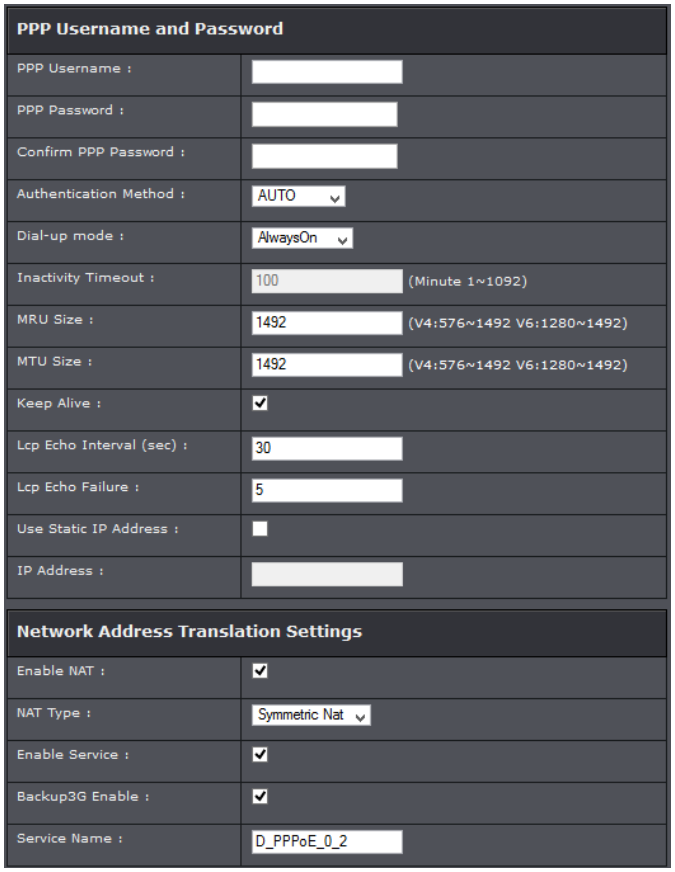
DSL Mode Configuration

Review the settings below and click Apply to save settings. Please contact your ISP to determine all configuration settings.



PPPoE / PPPoA

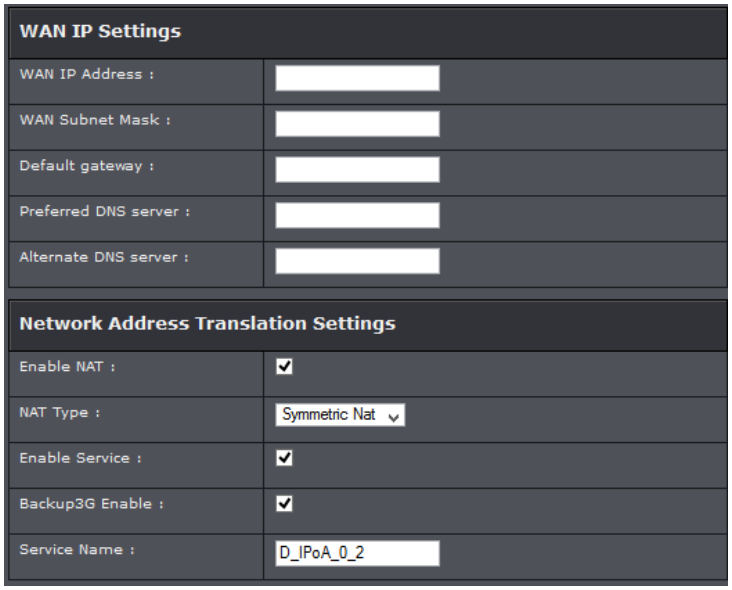
If you select PPPoE (RFC-2516 PPP over Ethernet) on the Protocol section, the screen below is displayed.



- **User Name:** Enter the user name provided by your ISP.
- **User Password:** Enter the password provided by your ISP.
- **Confirm Password:** Re-enter the password.
- Authentication Method: Select the type of authentication method to apply.
- **Dial-up Mode:** Configure how you want your modem router to connect and terminate the Internet connection. Options are:
  - **OnDemand:** Enables the modem router to cut off the Internet connection after being idle for a specified period of time. The device automatically re-establishes the connection when you try to access the Internet again. In the Idle Disconnect Time field, enter the number of seconds that you want to elapse before your modem router terminates the Internet connection.
  - **AlwaysOn:** Enables the modem router to be connected to the Internet at all times. If you are disconnected, the device will automatically re-establish the connection.
  - **Manual:** Manually configure this setting. Enter the user name and password to establish the Internet connection.
- **Inactivity Time:** View the preset idle time before the session is disconnected.
- **MRU Size:** Set the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.
- **MTU Size**: Set the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.
- **Keep Alive:** Select this option to maintain connection
- **LCP Interval:** Enter the number of seconds that you want to be the interval in sending LCP (Link Control Protocol) packets.
- **Use Static IP Address:** Select this option if you have an assigned static IP Address
- IP Address: Enter your assigned static IP Address.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **Enable Service:** Select this option to enable
- **Backup 3G Enable:** Select this option to enable 3G WAN backup connection.
- **Name:** Enter your desired connection name.

IPoA

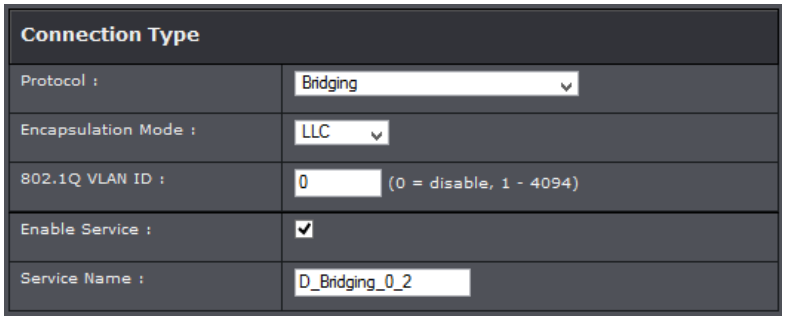
If you select IPoA, the screen below is displayed.



- **WAN IP Address:** Enter the IP address provided by your ISP.
- **Subnet Mask:** Enter the subnet mask provided by your ISP.
- **Default Gateway:** Enter the default gateway provided by your ISP.
- **Preferred/Alternate DNS** If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **Enable Service:** Select this option to enable
- **Backup 3G Enable:** Select this option to enable 3G WAN backup connection.
- **Name:** Enter your desired connection name.

Bridge Mode

If you select Bridge mode, the screen below is displayed.



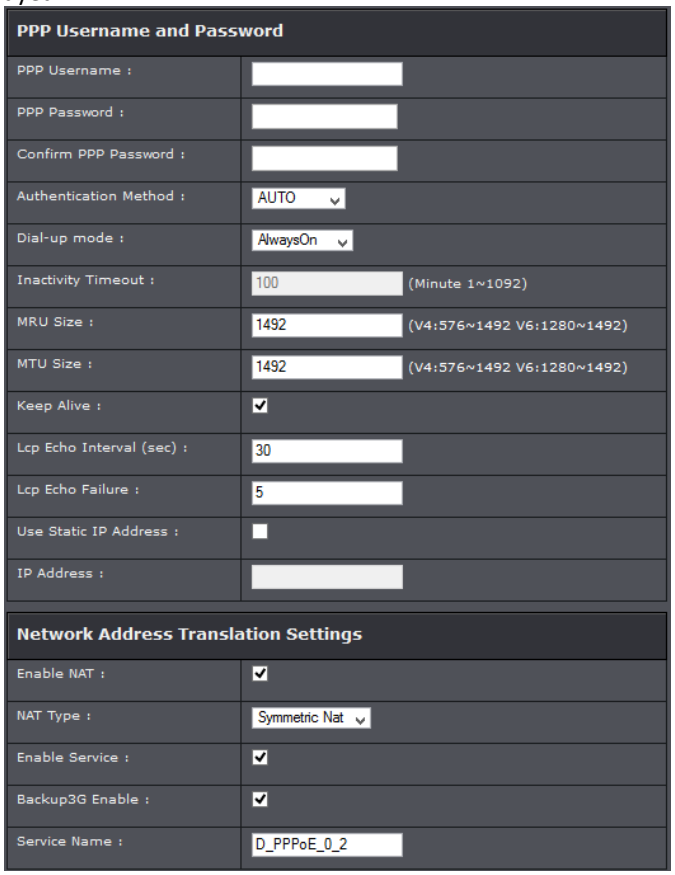
- **Enable** Service: Select to enable feature
- **Name:** Enter your desired connection name.

Ethernet Mode Configuration

Review the settings below and click Apply to save settings. Please contact your ISP to determine all configuration settings.

PPPoE

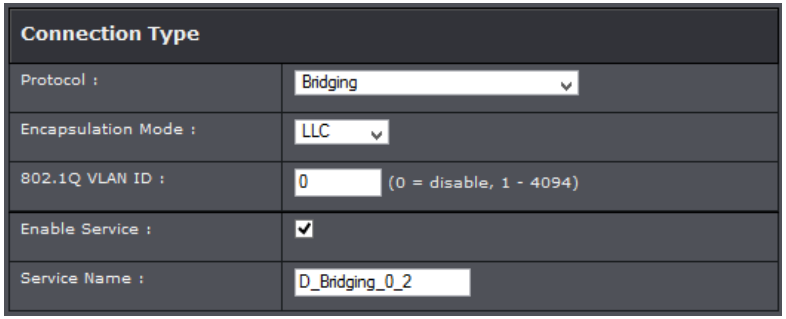
If you select PPPoE (RFC-2516 PPP over Ethernet) on the Protocol section, the screen below is displayed.



- **User Name:** Enter the user name provided by your ISP.
- **User Password:** Enter the password provided by your ISP.
- **Confirm Password:** Re-enter the password.
- Authentication Method: Select the type of authentication method to apply.
- **Dial-up Mode:** Configure how you want your modem router to connect and terminate the Internet connection. Options are:
  - **OnDemand:** Enables the modem router to cut off the Internet connection after being idle for a specified period of time. The device automatically re-establishes the connection when you try to access the Internet again. In the Idle Disconnect Time field, enter the number of seconds that you want to elapse before your modem router terminates the Internet connection.
  - **AlwaysOn:** Enables the modem router to be connected to the Internet at all times. If you are disconnected, the device will automatically re-establish the connection.
  - **Manual:** Manually configure this setting. Enter the user name and password to establish the Internet connection.
- **Inactivity Time:** View the preset idle time before the session is disconnected.
- **MRU Size:** Set the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.
- **MTU Size**: Set the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.
- **Keep Alive:** Select this option to maintain connection
- **LCP Interval:** Enter the number of seconds that you want to be the interval in sending LCP (Link Control Protocol) packets.
- **Use Static IP Address:** Select this option if you have an assigned static IP Address
- IP Address: Enter your assigned static IP Address.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **Enable Service:** Select this option to enable
- **Backup 3G Enable:** Select this option to enable 3G WAN backup connection.
- **Name:** Enter your desired connection name.

Bridge Mode

If you select Bridge mode, the screen below is displayed.



- **Enable** Service: Select to enable feature
- **Name:** Enter your desired connection name.

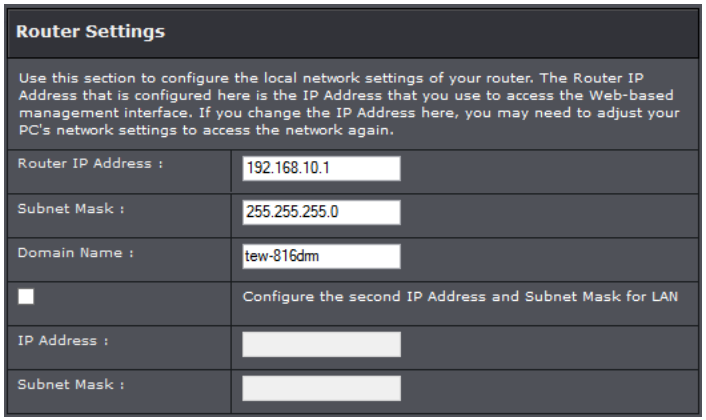
Change your router IP address

Setup > Local Network

In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.
Note: *If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.*

Default Router IP Address: 192.168.10.1
Default Router Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Local Network**.
3. Review the settings and click **Apply** to save changes.



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

  Note: *You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default http://192.168.10.1 using your new router IP address will use the following format using your new router IP address http://(new.router.ipaddress.here) to access your router management page.*
- **Subnet Mask:** Enter the subnet mask of the router (e.g. *255.255.255.0*)
- **Domain Name:** Enter the domain name to assign your router.
- **Configure second IP address and Subnet:** Click to enable option
- **IP Address:** Enter the second IP address
- **Subnet Mask:** Enter the subnet mask to assign. (e.g. *255.255.255.0*)

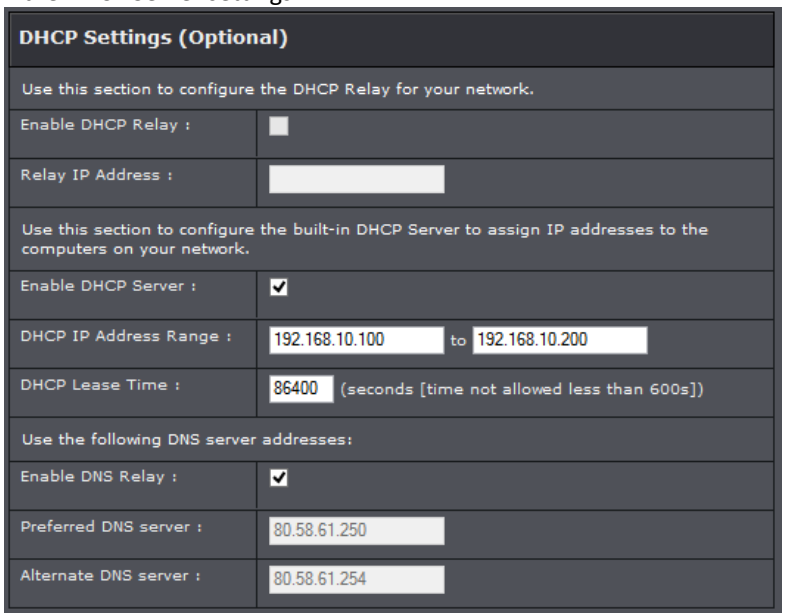
  Note: *The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.*

Set up the DHCP server on your router

Setup > Local Network

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Local Network**.
3. Review the DHCP Server settings.



- **Enable DHCP Relay:** Check option to enable
- **Relay IP Address:** Enter the your assigned DHCP relay IP address
- **DHCP Option:** Select the DHCP mode of your modem router. If you set the DHCP Option to DHCP Server, configure the following settings:
  Note: *If you set your modem router as the DHCP server, your modem router will automatically assign an IP address to each computer on your network. By default, the fields for DHCP settings have predefined values. It is recommended to retain these values unless specified by your ISP.*
- **DHCP IP Address Range:** Enter the range of IP address to assign. The default value is 192.168.10.100 to 192.168.10.200.
- **Lease Time:** Enter the lease time in seconds. The lease time is the amount of time a device is allowed connection to your modem router using its current dynamic IP address. At the end of the lease time, the lease is either renewed or a new IP address is assigned. The default value is 86400 seconds (1 day).
- DNS Relay: Check to enable option
- Preferred/Alternate DNS Server: Enter the preferred and alternate DNS IP addresses.

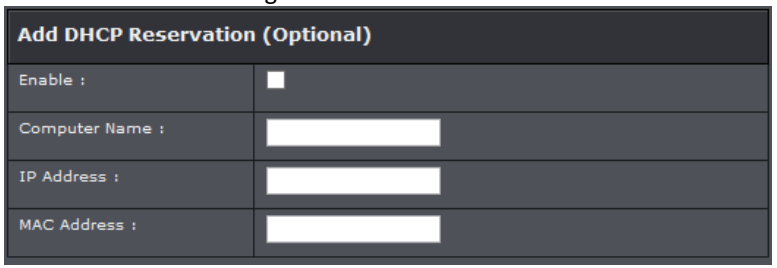
Assign specific IP address to clients

Setup > Local Network

Clients connect to your router can be assigned specific IP addresses instead of pulling DHCP from the router.

DHCP Reservation

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Local Network**.
3. Review the DHCP Server settings.



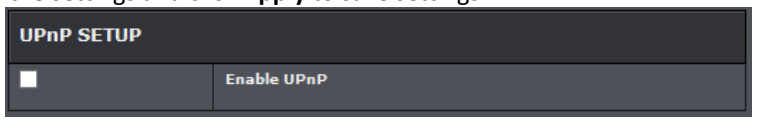
- **Enable:** Check option to enable
- **Computer Name:** Enter the name of the computer
- **IP Address:** Enter the IP assigned IP address
- **MAC Address:** Enter the MAC address of the computer of client.

Enable/disable UPnP on your router

Advanced > UPnP

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **UPnP.**
3. Review the settings and click **Apply** to save settings.



- **UPnP:** Select this option to enable UPnP

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

Configure ALG settings

Advanced > NAT > ALG

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling. If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **ALG**.
3. Review the settings and click **Apply** to save settings.

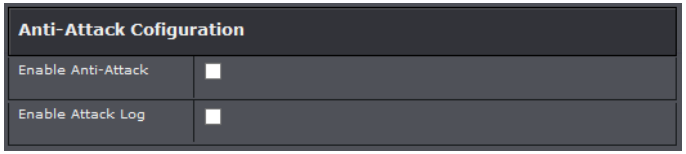
- **FTP:** File Transfer Protocol (FTP) is used to transfer files between computers on a TCP/IP based network, such as the Internet. Check this box to enable this function to work through your modem router.
- **PPTP Passthrough:** Point-to-Point Tunneling Protocol (PPTP) allows Point-to-Point protocol (PPP) to be tunneled through a network. Check this box to enable this function to work through your modem router.
- **RTSP:** Real Time Streaming Protocol (RTSP) is a network protocol used for entertainment and communication systems to control streaming media sessions. Check this box to enable this function to work through your modem router.
- **L2TP Passthrough:** Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate VPNs.
- **H323:** H.323 is a standard that provides audio-visual communication sessions on a network. It is widely implemented in voice and video conferencing equipments and is used within various Internet real-time applications such as NetMeeting. Check this box to enable this function to work
- **SIP:** Session Initiation Protocol (SIP) is a signaling protocol used to control multimedia communication sessions such as voice and video calls over Internet Protocol (IP). Check this box to enable this function to work through your modem router.
- **IPSEC Passthrough:** Internet Protocol Security (IPSec) is a protocol suite used to secure IP communications by authenticating and encrypting IP packets. Check this box to enable this function to work through your modem router.

Additional Security Settings

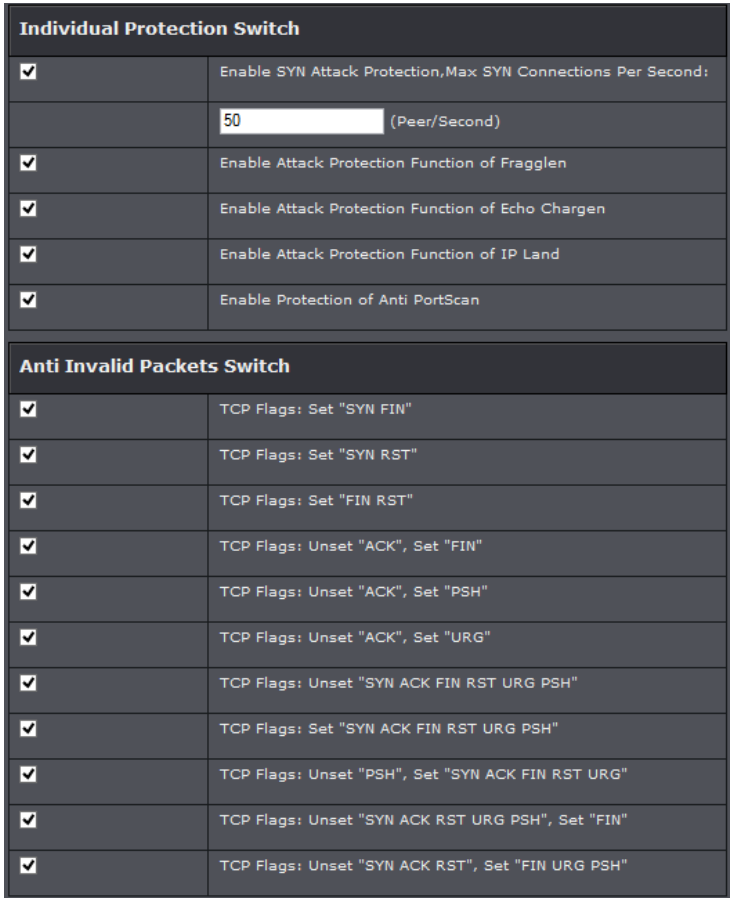
Advanced > Firewall

To provide additional security, your router offers Anti-Attack feature. You may want to enable these features for additional network security.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **Anti-Attack**.
3. Select **Enable Anti-Attack** to activate mode.



4. A complete list of added protection will appear. Select items to enable proection and click Submit to save settings.



Allow/deny multicast streaming

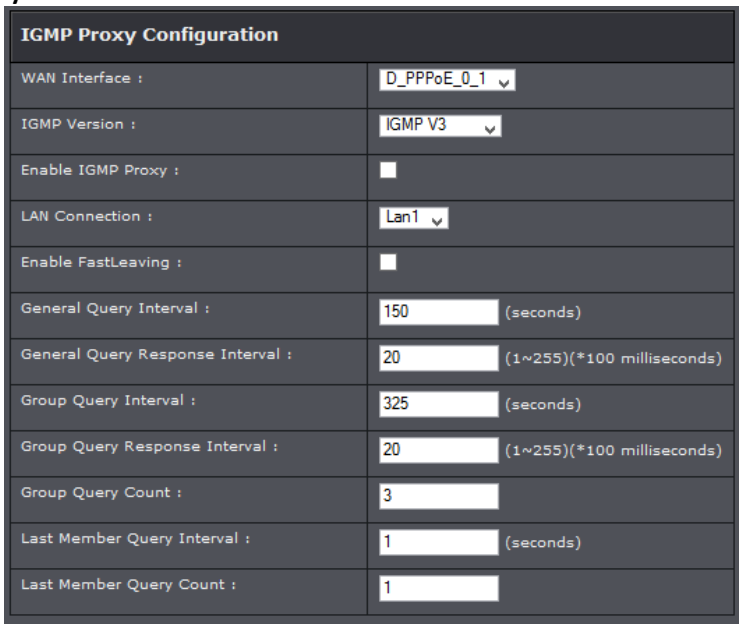
Setup > Internet Setup

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications. Multicast streaming is disabled by default on your router to deny applications that require multicast communication through your router.

IGMP

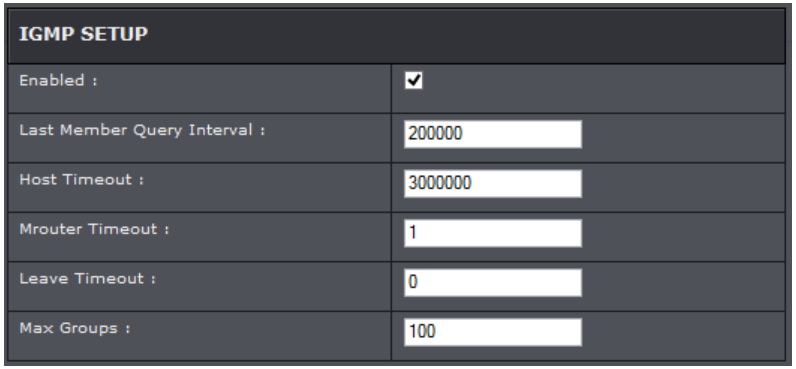
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Multicast** and select **IGMP.**
3. Under IGMP option select which IGMP to activate.

IGMP Proxy



- **WAN Interface:** Select the interface to set
- **IGMP Version:** Select the IGMP version
- **Enable IGMP Proxy:** Select to enable
- **LAN Connection:** Select the LAN interface
- **Enable Fast Leave:** Select option to enable fast leave feature
- **Query Interval:** Enter IGMP query interval
- **Query Response Interval:** Enter response interval
- **Group Query Interval:** Enter last member query interval
- **Group Query Response Interval:** Enter response query interval
- **Group Query Count:** Enter the query count
- **Last Member Query Interval:** Enter last member query interval
- **Last Member Query Count:** Enter last member query count

IGMP Snooping

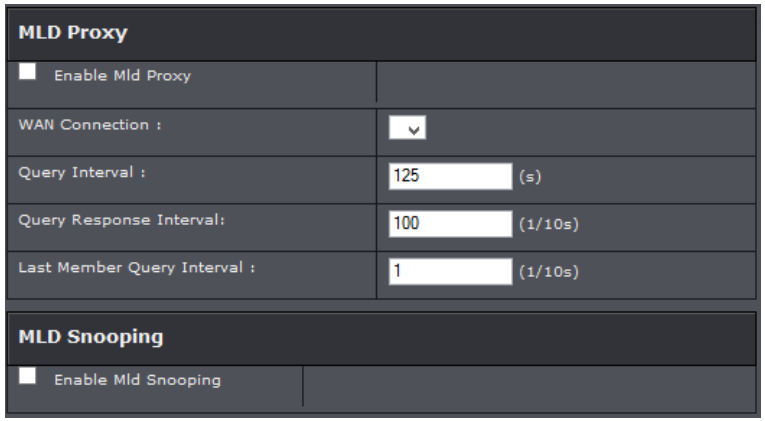


- **Enabled:** Select to enable
- **Last Member Query Interval:** Enter last member query interval
- **Host Timeout:** Enter the host timeout period
- **Mrouter Timeout:** Enter the timeout period
- **Leave Timeout:** Enter the leave timeout period
- **Max Groups:** Enter the maximum group

MLD

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Multicast** and select **IGMP.**
3. Review the settings below and click Apply to save changes.

MLD Proxy /Snooping



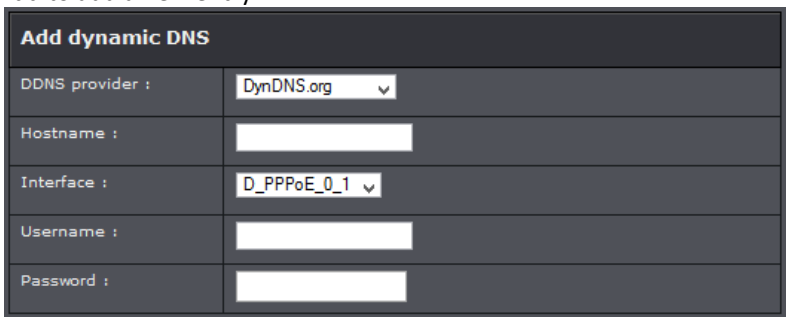
- **Enable Mild Proxy:** Select to enable
- **WAN Connection:** Select the interface to set
- **Query Interval:** Enter IGMP query interval
- **Query Response Interval:** Enter response interval
- **Last Member Query Interval:** Enter last member query interval
- **Enable Mild Snooping:** Select to enable

Identify your network on the Internet

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

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

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *dyndns.com, no-ip.com*, etc.)
2. Log into your router management page (see "Access your router management page" on page 23).
3. Click on **Advanced** and click on **Dynamic DNS**.
4. Click **Add** to add a new entry.



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

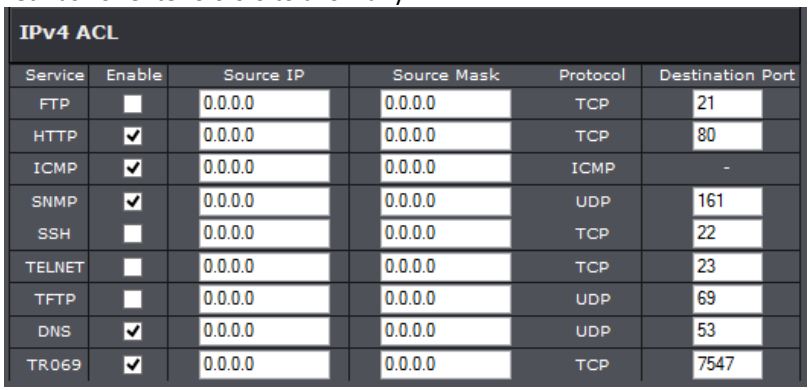
Allow remote access to your router management page

Maintenance > Remote Management

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

1. Log into your router management page (see "Access your router management page" on page 22).
2. Click on **Management**, and click on **Remote Access Control**.
3. Under the **Remote Access Control** section select the WAN connection type that will be used.

4. Select the service you would like to enable remote access. Enter a specific IP address and Netmask or enter 0.0.0.0 to allow any.



Open a device on your network to the Internet

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

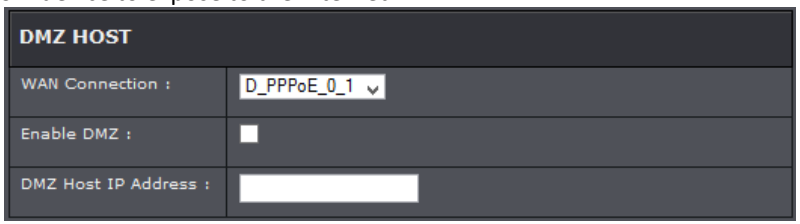
DMZ

Advanced > Firewall > DMZ

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

It is strongly recommended to use Port Forwarding to allow access to your computers or network devices from the Internet.

1. Make sure to configure your computer or network device to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 53).
2. Log into your router management page (see "Access your router management page" on page 23).
3. Click on **Advanced**, click on **DMZ**.
4. Select Enable next to DMZ.
5. In **DMZ Host IP Address** enter the IP address you assigned to the computer or network device to expose to the Internet.



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

Note: *If using ADSL WAN with multiple PVCs, click the DMZ Mode drop-down list to select Multi Mode which will allow you which PVC to assign the DMZ Host.*

Port Forwarding

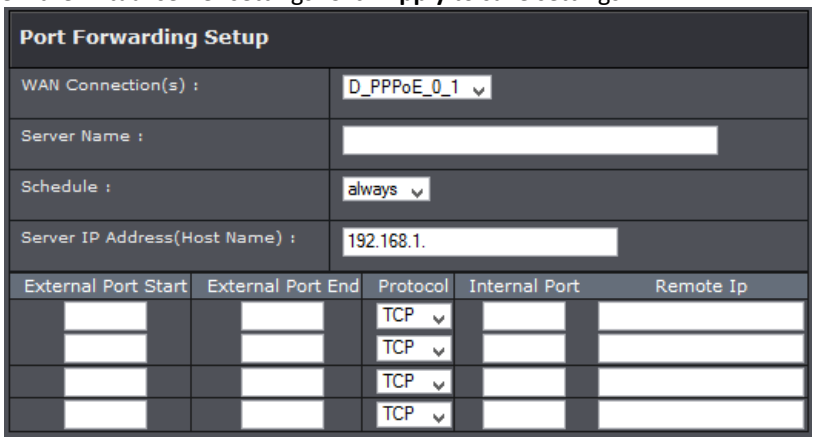
Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "DMZ" on page 35) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an network/IP camera (typically on TRENDnet IP cameras use HTTP TCP port 80 for remote access web requests) on your network for to allow remote access to it.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (See DynDNS section).

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on Port Forwarding and click **Add.**

To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify by clicking the drop down menu under rule name, otherwise, you can choose to manually add a new virtual server.

3. Review the virtual server settings. Click **Apply** to save settings.



- **WAN Connection:** Select the WAN connection you are using.
- **Server Name:** Enter the name of the rule or select from the predefine pull down menu list.
- **Schedule:** Click the drop-down list assign a pre-defined schedule when the virtual server is activated or inactive.
- **Server IP:** Enter the IP address of the device to forward the port. (e.g. *192.168.10.101)*.
- **External Port Start/End:** Enter the port number required by your device from the internet. This will be the same port number used to access the device from the Internet and will include both TCP and UDP protocols.
- **Internal Port:** Enter the port number required by your device. This will be the same port number used to access the device from your network and will include both TCP and UDP protocols.

  Note: *Please refer to the device documentation to determine which ports and protocols are required.*
- **Protocol Type:** Select the protocol to assign the rule.
- **Remote IP:** Enter the public IP that will have access to your device (you can enter 0.0.0.0 or * for all IP)

Note: *You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.*

Example: To forward TCP port 80 to your IP camera

1. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 53).
   Note: *You may need to reference your camera documentation on configuring a static IP address.*
1. Log into your router management page (see "Access your router management page" on page 23).
3. Click on **Advanced**, click on **Port Forwarding**.
4. In the **Server Name** enter Camera and select **Always** under schedule.
5. For **Server IP**, enter the IP address assigned to the camera.
6. Enter port **80** for both **External Start** and **End ports**, select **TCP** for **Protocol type**.
7. **Internal port** enter **80** and for Remote IP type 0.0.0.0 to allow any remote IP address.
8. Click **Apply** to save changes.

Port Trigger

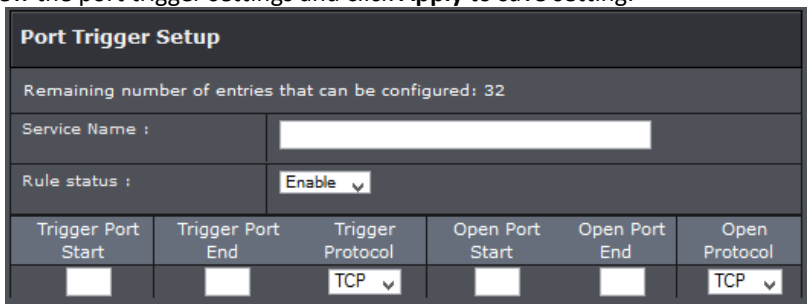
Advanced > NAT > Port Trigger

Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on page 30.

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, click on **Port Trigger.**
3. Select Enable Port trigger option and click **Apply** to save settings. Click **Add** to create a rule.

4. Review the port trigger settings and click **Apply** to save setting.



- **Service Name:** Enter the name to assign rule.
- **Rule Status:** Select enable to activate rule.
- **Trigger Port Start/End:** Port or port range requested by the device.(e.g. *2000-2001 or 2000)*

  Note: *Please refer to the device documentation to determine which ports are required.*
- **Trigger Protocol:** Select protocol to apply on rule
- **Open Port Start/End:** Enter the public port to assign on the rule
- **Open Protocol:** Select the public protocol to apply on rule.

Note: *Please refer to the device documentation to determine which ports are required.*

Prioritize traffic using QoS (Quality of Service)

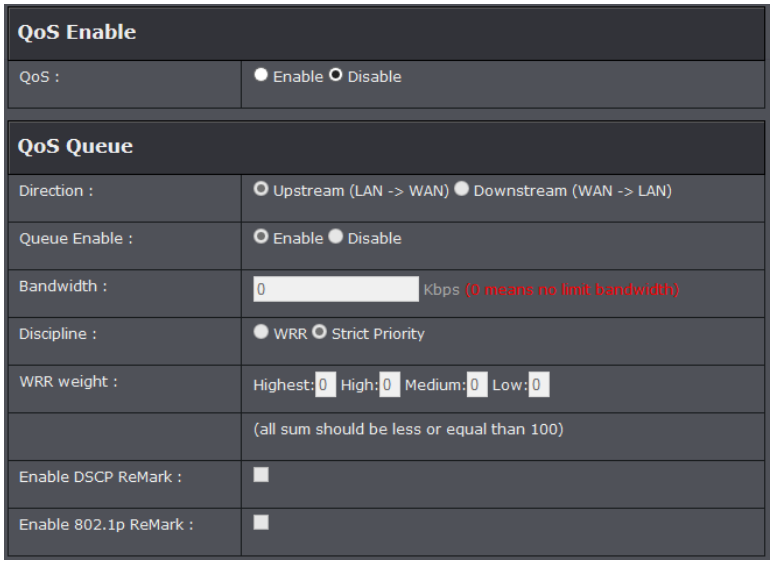
Configuration > Advanced Setting > Quality of Service

You may want to prioritize outbound traffic for specific computers or devices on your network to have higher priority.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **Quality of Service.**
3. Review the settings and click on **Apply** to save settings.

Queue Management

This page allows you to enable QoS and choose Differentiated Services Code Point (DSCP) markings to automatically mark incoming traffic without reference to a particular classifier.

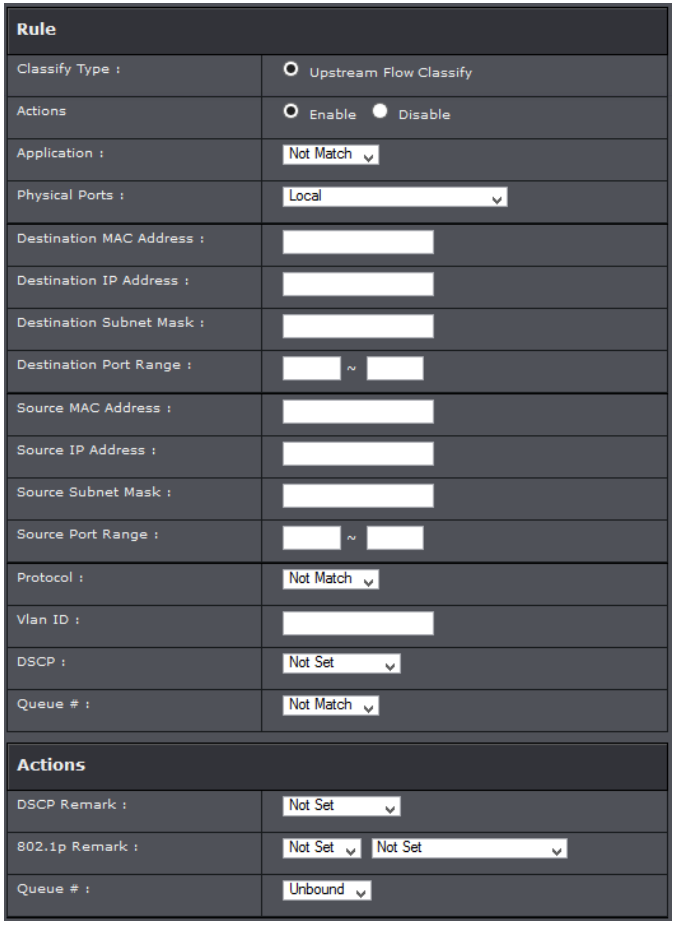


- **Enable QoS:** Check this box to enable the QoS feature.
- **Direction:** Select the direction of the traffic to configure.
- **Queue Enable:** Select to enable the queue.
- **Bandwidth:** Enter your internet Bandwidth.

- **Discipline:** Select the queue discipline.
  - **SP:** In Strict Priority (SP), packets with a high priority are processed first. Not until the first queue is empty will another queue be processed.
  - **WRR:** In Weighted Round Robin, each queue can be given a different priority level. Each traffic is assigned to a class and each class is given its own queue.
- **WRR weight:** Enter the your classified weights
- **DSCP Mark:** Select a DSCP mark. The DSCP mark is used to classify and prioritize types of packets.

Queue Rule

This page allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue configuration will be used in Queue Classification to place ingress packets appropriately.



- **Action:** Check this box to enable this queue.
- **Application:** Select in the pull down menu the application of the rule, values are preconfigured.
- **Physical Ports:** Select the interface on the pull down menu to implement this QoS queue.
- **Destination/Source MAC Address:** Enter the destination and source MAC Address to apply on the queue.
- **Destination/Source IP Address:** Enter the destination and source IP address to apply on the queue.

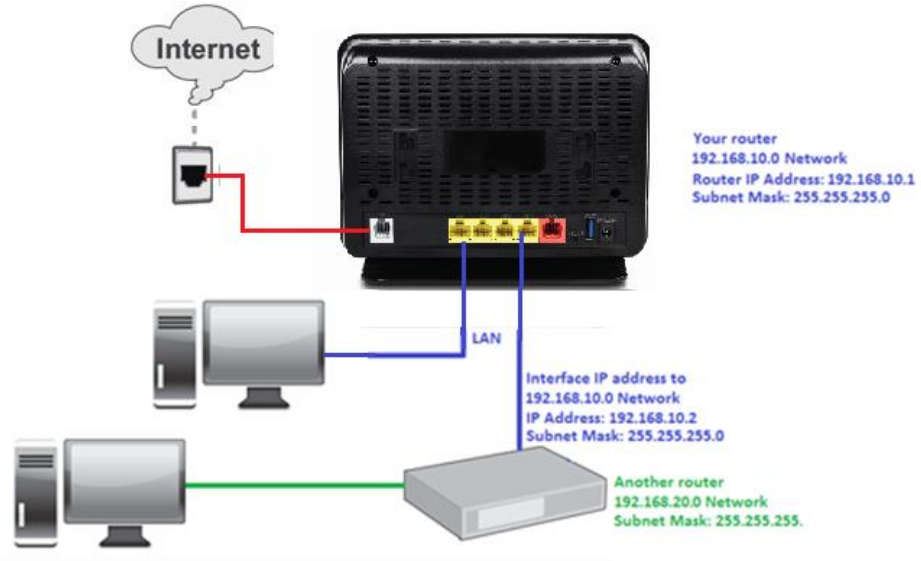
- **Destination/Source Netmask:** Enter the destination and source network mask address to apply on the queue.
- **Destination/Source Port Range:** Enter the destination and source port to apply on the queue.
- **Protocol:** Select the protocol of the queue
- **VLAN ID:** Enter the VLAN ID of the queue.
- **VLAN ID:** If Default VLAN ID is not checked, enter the preferred VLAN ID.
- **DSCP:** Select the DSCP mark.
- **Queue #:** Select the queue to apply
- **DSCP Remark:** Select the DSCP to apply
- **802.1p Remark:** Select the queue remark to apply
- **Queue #:** Select the queue to apply

Add static routes to your router

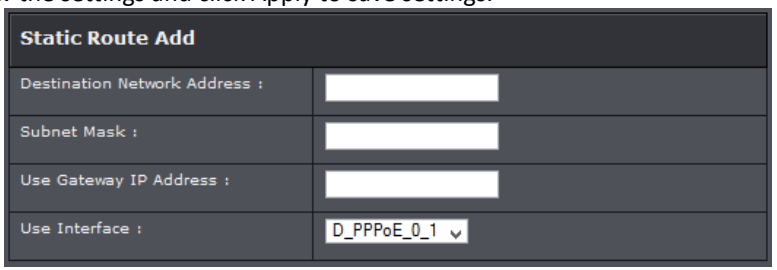
Advanced > Static Route

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

Note: *Configuring this feature assumes that you have some general networking knowledge. Similar steps can be followed when applying IPv6 static routing rule.*



1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **Static Route** or **IPv6 Static Route**.
3. Review the settings and click Apply to save settings.

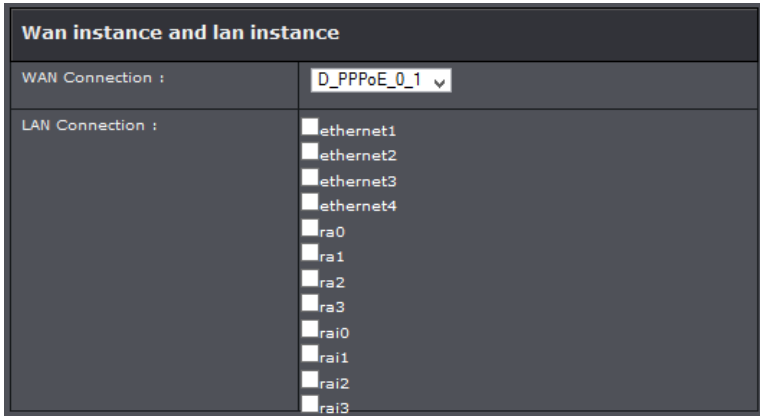


- **Destination IP:** Enter the destination IP address.
- **Subnet Mask:** Enter the subnet mask
- **Use Gateway IP Address:** Enter the gateway IP address.
- **User Interface:** Select the interface for the rule.

Policy Route

This page allows you to bind your WAN connection to one LAN interface.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **Route Policy**.
3. Click **Add** to configure settings and click **Apply** to save settings.



- **WAN Connection:** Select in the pull down menu your WAN interface.
- **LAN Connection:** Select the interfaces you would like to bind.

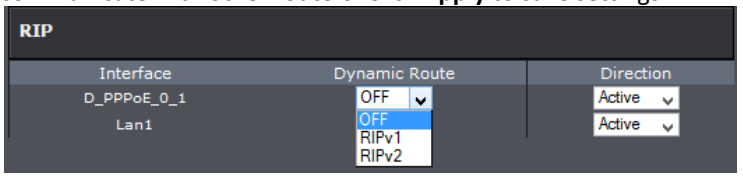
Enable dynamic routing on your router

Advanced > RIP Settings

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

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** at the top of the page, click on **Routing**, and click on **RIP.**
3. Select the Inteface to configure then select appropriate dynamic routing protocol and version communicate with other routers. Click **Apply** to save settings.



- **RIPv1:** Enables sending and receiving or exchange of routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 1 protocol.
- **RIPv2:** Enables sending and receiving routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 2 protocol

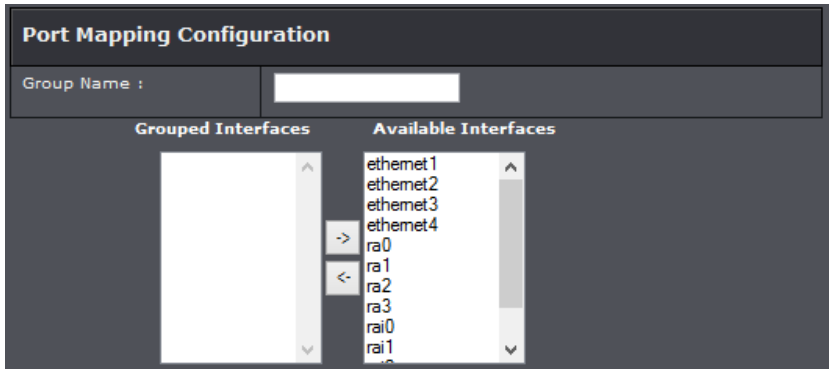
Setup Port Mapping

Advanced > Port Mapping

Port mapping allows you to group interfaces for traffic control. Traffic is isolated from group to group. Therefore, traffic coming from an interface of a group can only be flowed to the interfaces in the same group.

By default, all interfaces belong to the Default group. You can create new groups and move interfaces to other groups. However, an interface can only be a member of one group.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **Network Tools** and **Port Mapping.**
3. Under **Port Mapping** section select **Add**.
4. Click **New** to add a new group and select the interface from the Available Interfaces section.
5. Click the **<-** button to add the selected interface into the group. Or click the **->** button to remove selected interface from the group.
6. Click **Apply** to save settings.



Setup IPv6 on your router

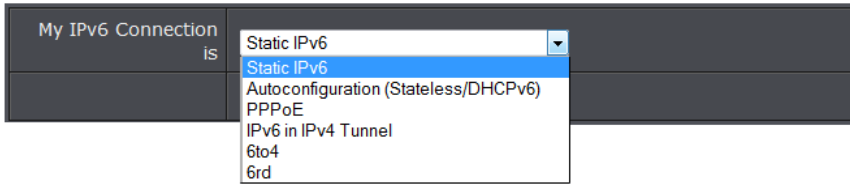
Advanced > IPv6

IPv6 (Internet Protocol Version 6) was developed to be the successor protocol to well known and widely used protocol IPv4 (Internet Protocol Version 4) for network addressing. The new addressing protocol is designed to minimize processing overhead by routers, significantly increase the available IP address space, provide integrated security, and open the possibility of more extensions and options. ISP have already transition their networks to accommodate IPv6 and are starting to offer IPv6 services.

Note: *The router offers native IPv6 as well as IPv4 to IPv6 transitional connection types.*

IPv6 WAN

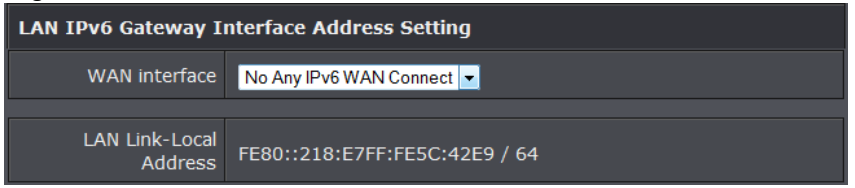
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **IPv6 WAN**.
4. Select your IPv6 WAN type and complete the fields required by your ISP. Click Apply to save settings.



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

IPv6 LAN

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **IPv6 LAN**.
4. Select your **IPv6 WAN Interface** on the pull down menu and click **Apply** to save settings.

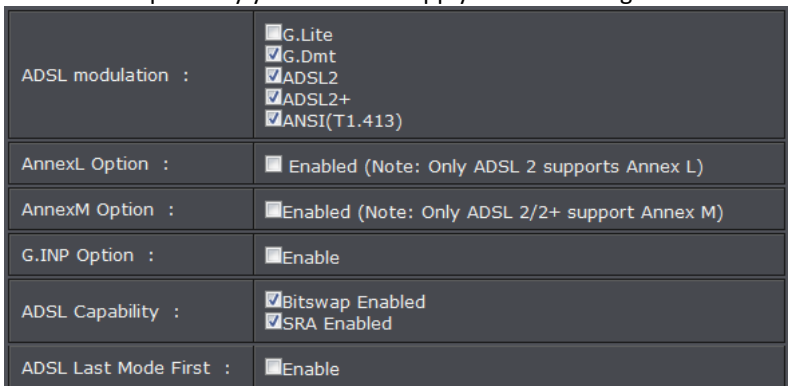


Configure ADSL settings

Advanced > ADSL

This page allows you to select ADSL modulations, capabilities, and other options. Consult your ISP to determine the appropriate settings.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **ADSL**.
4. Select the fields required by your ISP. Click Apply to save settings.



Using External USB Storage

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

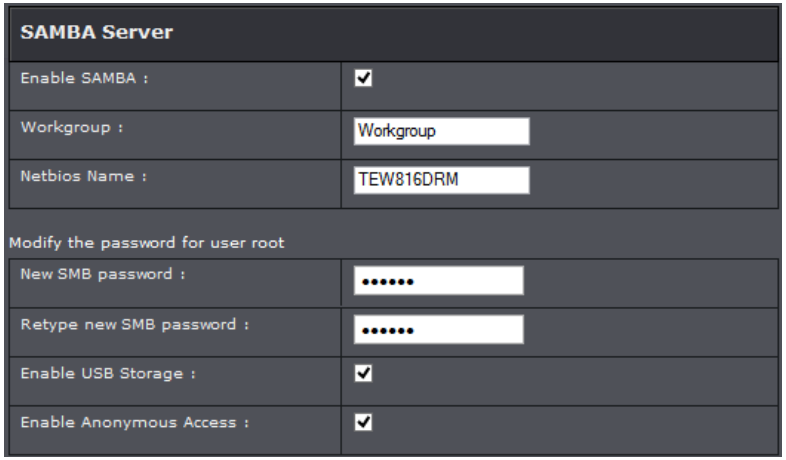
Note: *For security purposes, the USB SMB and FTP settings on your router are disabled by default. You will need to enable these settings in orders to allow access to your USB storage devices.*

File Sharing Server

Advanced > USB > File Sharing Server

SMB (Samba) is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **SAMBA**.
3. Review the setting on **SAMBA Server Information** section. Click **Apply** to save settings.



- **Enable Samba:** Select enable or disable for the feature.
- **Workgroup:** Enter the workgroup name. It is recommended to keep the standard default "WORKGROUP". If you change this setting, you will need to change the workgroup name on all computers in your network that are allowed access to the USB storage.
- **Netbios Name:** You can change the name of your server which will be the name you will when accessing your USB storage device. (***Note:*** *You can also access the USB storage using the router IP address)*
- **Password:** Enter the password for the user name. Re-type Password to confirm.
- **Enable USB Storage:** Select to enable storage
- **Enable Anonymous Access:** Select to enable anonymous access to your files

Under Windows®, you can access the USB storage device on your computer under **Computer > Network > USBSHARE > usb_A1**.

Note: *Your computer will only be able to automatically discover the USB storage if you are set to a workgroup under the default name "WORKGROUP". Your computer will not be able to automatically discover the USB storage device if under a domain or different a workgroup name.*

Under Windows®, if your computer cannot discover the USB storage automatically, you can access these files under your network map or by typing \\<routerIPaddress>\usb_A1 (ex. \\192.168.10.1\usb_A1) on your browser's or file explorer address bar. Please follow the below steps to configure the router's SMB settings

FTP (File Transfer Protocol) Server

FTP (File Transfer Protocol) is used to access shared files through the Internet. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router.

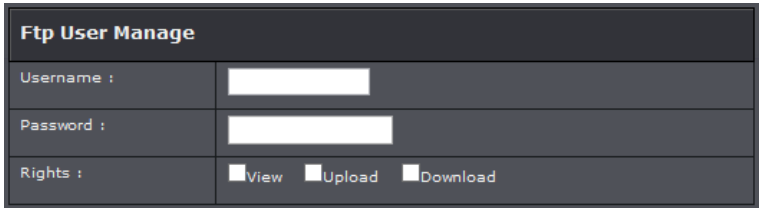
FTP Setting

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **FTP Setting**.
3. Review the administrator settings required for your **FTP server**. Click **Apply** to save settings

- **FTP Server:** Select on or off for the feature.
- **Enable FTP Server:** Select to activate FTP server
- **FTP Server Port:** Enter the port to assign FTP server.

FTP User Management

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **FTP Setting**.
3. Review the administrator settings required for your **FTP server**. Click **Apply** to save settings



- **User Name:** Enter the user name to be used to access your files.
- **Password:** Enter the password for the user name.
- **Rights:** Select the permission you will grant to the user. You can allow the user **View** (Read), **Upload** (Write) and **Download** files access.

Signing up for a Dynamic DNS service (outlined in Identify Your Network section pg.39) will provide identification of the router's network from the Internet. You can access your shared files over the Internet by typing ex.ftp://<router'sWANIPaddress> or ftp://myDDNSservice in your web browser or file explorer address bar. You can access your share files locally by typing ftp://<router'sLANIPaddress> in your web browser or file explorer address bar.

You can find your router's WAN IP address settings under *Advanced > Administrator > Status.*

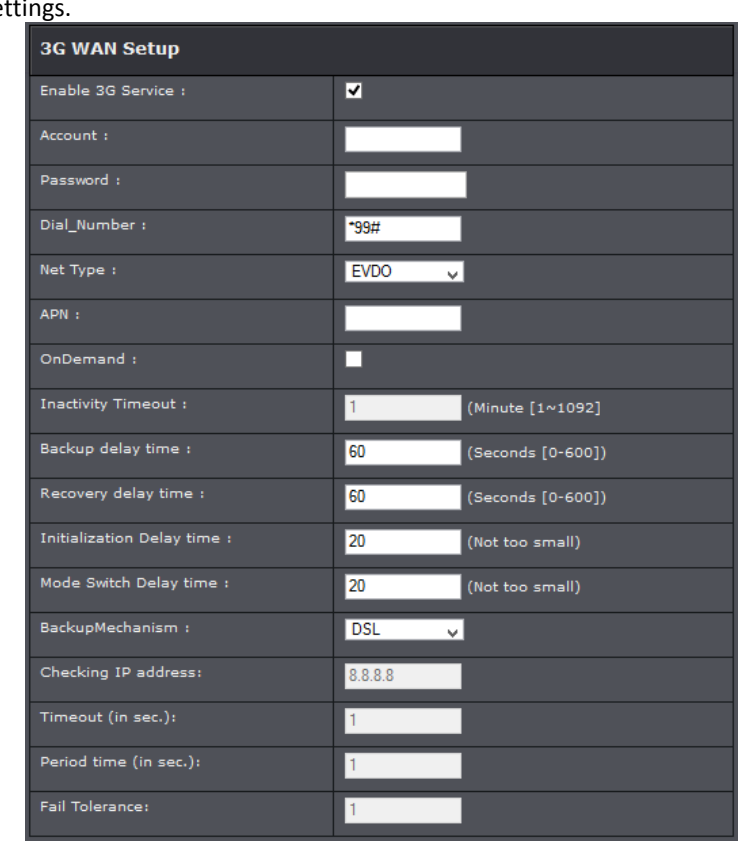
Using 3G WAN Connection

Your router's USB port can be used to connect a 3G USB dongle for 3G WAN connection. This can be beneficial when you have access to only a 3G WAN internet. For an update to date list of supported 3G WAN dongles please visit the TEW-816DRM's product page at http://trendnet.com.

Configure 3G WAN

In most cases once the 3G USB dongle is plugged into one of the USB ports the required 3G WAN settings would automatically generate. However if your are still have issues, you can manually enter required settings. Please contact your 3G ISP (Internet Service Provider) for more information. Please note it may take up to 2 minutes for the device to establish connection with your 3G network.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, and click on **3G WAN Configuration.**
3. Click **AutoSet** to have the device automatically input required settings. Click **Apply** to save settings.



Router Maintenance & Monitoring

Reset your router to factory defaults

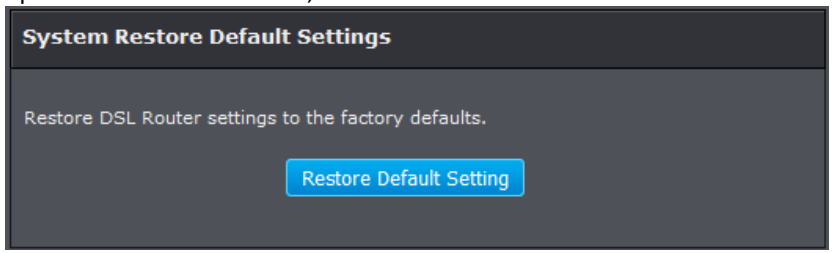
Maintenance > Configuration Backup/Restore

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on page 45.

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

- **Reset Button:** Located on the front panel of your router, see "Product Hardware Features" on page 2 . Use this method if you are encountering difficulties with accessing your router management page.
  OR
- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management,** and click on **System.**
3. Under **System Restore Default Settings**, click **Restore Default Setting**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	admin
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless	Enabled
SSID (wireless network name)	Please refer sticker or device label
Wireless Security	Please refer sticker or device label
802.11 Mode	2.4GHz 802.11b/g/n mixed mode
Channel	Auto Channel

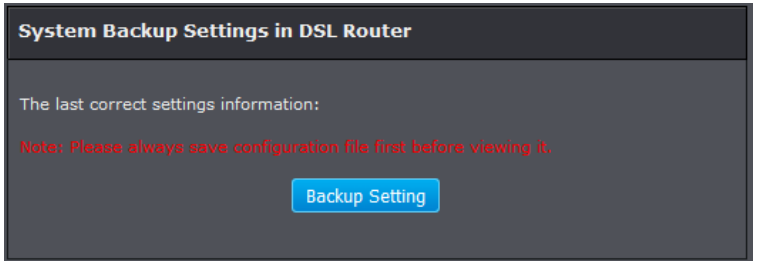
Backup and restore your router configuration settings

Maintenance > Configuration Backup/Restore

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

To backup your router configuration:

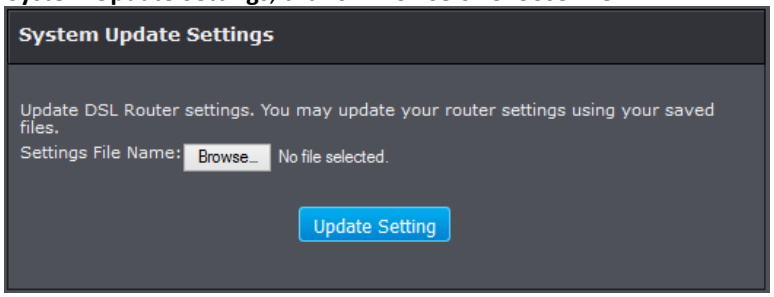
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management,** and click **System**.
3. Click **Backup Settings**.



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

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management,** and click **System**.
3. Under **System Update Settings**, click on **Browse** or **Choose File**.



A separate file navigation window should open.

4. Navigate to the location of the router configuration file to restore. (Default Filename: *config.bin*).
5. Select the router configuration file to restore and click **Update Settings**. (Default Filename: *config.bin*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Upgrade your router firmware

Maintenance > FW Upgrade

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

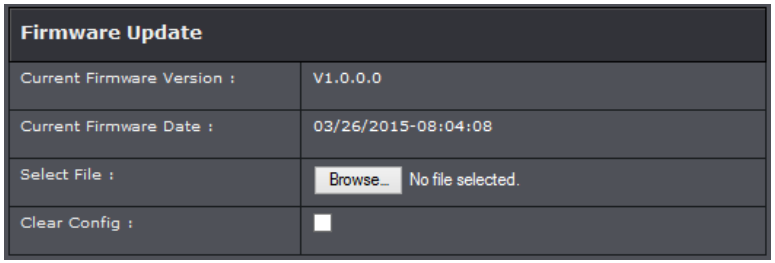
In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, and check the version located at the top right of the router management page. If there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

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

Please note the following:

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

1. Log into your router management page (see "Access your router management page" on page 23).
   Note: *You can check your router's current firmware version at the top right of the page.*
2. Click on **Management**, and click on **Firmware Update.**
   Note: *This page also displays the current firmware version of your router.*
3. Depending on your web browser, next to **Upgrade Firmware**, click **Browse** or **Choose File**.



4. Navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.
5. Select **Clear Config** to reset the unit after firmware has been updated. Click **Update Firmware** to start the firmware upgrade process. If prompted, click **yes** or **OK**.

Restart your router

Maintenance > Reboot Device

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

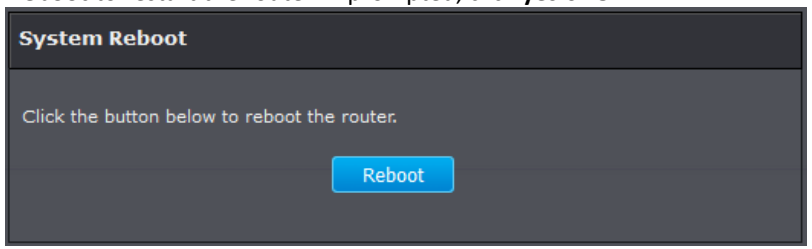
There are two methods that can be used to restart your router.

- **Turn the router off** disconnect the power adapter from the rear panel of your router for 10 seconds and reconnect the power adapter, see "Product Hardware Features" on page 2 .

  Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.

  OR
- **Router Management Page:** This is also known as a soft reboot or restart.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management,** and click on System.
3. Click **Reboot** to restart the router. If prompted, click **yes** or **OK**.

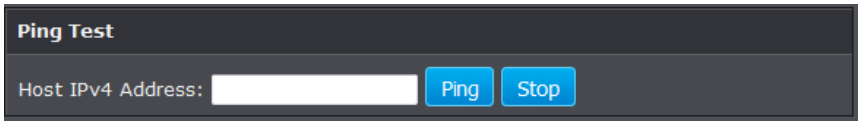


Check connectivity using the router management page

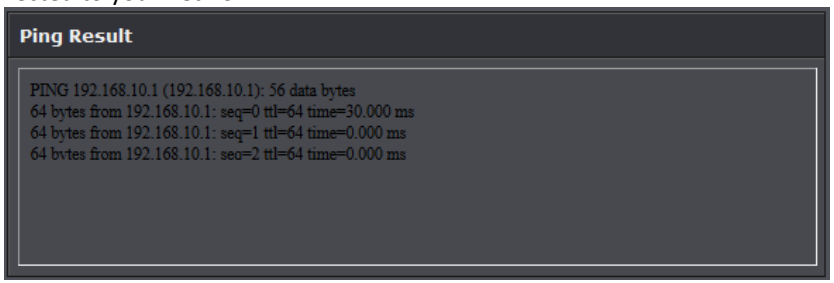
Maintenance > Ping

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) test tool on your router management page.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** and click on **Ping**.
3. Next to **Host IPv4 Address**, enter in the IP address (e.g. *192.168.10.101*) or host name (e.g. www.*trendnet.com*) to test and click **Ping**.



4. You will receive a *success* or *fail* result message of the address you entered providing a basic indicating of the router's connectivity to the Internet or devices that are connected to your network.



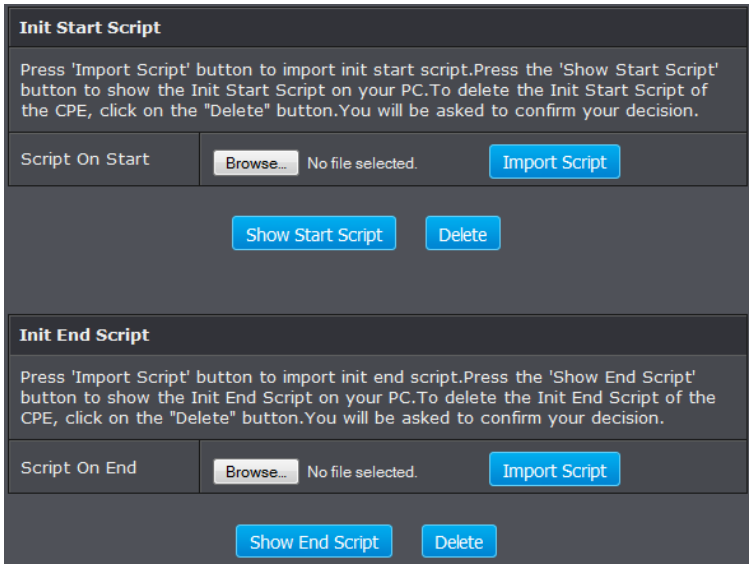
Manage Initialization Scripts

Maintenance > Init Script

This page allows you to show, delete, and import initialization scripts running on customer-premises equipment (CPE), such as telephones, routers, or set-top boxes, during system startup or shutdown.

Init start scripts are scripts that run before the system starts up. Init end scripts are scripts that run before the system shuts down.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** and click on **Init script**.
3. Click Browse and select your script.
4. Click **Import Script** to import script to router.



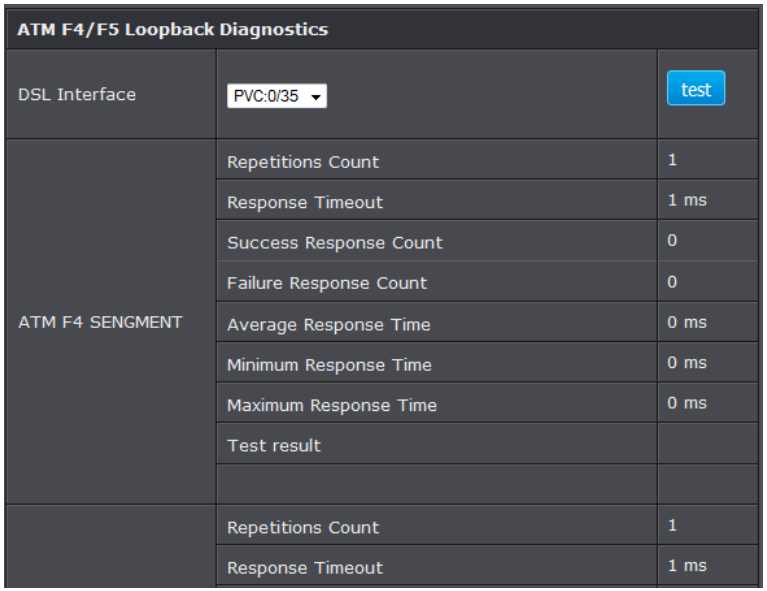
5. To show scripts on your computer click **Show script**. Press **Delete** to remove script.

Check Internet connectivity using the router management page

Maintenance > Diagnostic

This page allows you to test the connectivity of the physical and protocol layers on the WAN side.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** and click on **Diagnostic**.
3. Select your DSL interface and click **test**.



Check the router system information

Status > Summary

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status**.
3. Review the device information.

System

System	
New FirmWare	Without new firmware now
Firmware Version	V1.00.B12
Modem Type	ADSL2+ Router
Modem Vendor	TRENDNET
Modem OUI	0018E7
Modem Serial Number	0018E75C42E9
Uptime	21 hour 37 min 59 sec
Current Time	2014/09/13 13:47:53

- **Firmware Version:** Displays the firmware version currently loaded on the router
- **Modem Type:** Displays the modem type
- **Modem Vendor:** Displays modem vendor
- **Modem OUI:** Displays modem OUI
- **Modem Serial Number:** Serial number of modem
- **Uptime:** Time duration of modem up time
- **Current Time:** Time of router

DSL Link Status

DSL Link Status		
Modulation Type		
	Downstream	Upstream
Current Rate(Kbps)	0	0

- **Modulation Type:** Display the modulation applied on the router
- **Current Rate:** Downstream and upstream data rate

ATM PVC Status

ATM PVC Status	
VPI	0
VCI	35
Link Type	EoA
Encapsulation	LLC

- **VPI:** Current VPI settings applied on the router
- **VCI:** Current VCI settings applied on the router
- **Link Type:** Link type applied on the router
- **Encapsulation:** Current encapsulation applied on the router.

ATM PVC Status

Internet Connection Status	
Interface	PVC:0/35
Connection Status	Not Connected

- **Interface:** Current router PVC interface
- **Connection Status:** Current internet connection status

LAN Status

LAN Status	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
MAC Address	00:18:E7:5C:42:E9
DHCP Server	Enabled

- **IP Address:** Router's IP address
- **Subnet Mask:** Router's subnet mask
- **MAC Address:** MAC address of router
- **DHCP Server:** Current status of router's DHCP

Wireless Interface

Wireless Port			
Mode	802.11n + 802.11g + 802.11b		
Channel	6		
SSID	Enable	MAC Address	Security Mode
media722	Yes	00:18:E7:5C:42:E9	WPA2-AES-PSK
TRENDnet722_2.4GHz_Guest	Yes	00:18:E7:5C:42:EA	None

- **Mode:** Current wireless mode
- **Channel:** Wireless channel
- **SSID:** Wireless network name
- **MAC Address:** Wireless MAC address
- **Security Mode:** Wireless encryption of security

Check the router IPv6 status

Status > IPv6 Info

You may want to check the system IPv6 information of your router.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **IPv6 Info**.
3. Review the device information.

LAN Status	
LAN Link-Local Address:	fe80::218:e7ff:fe5c:42e9

Check the router IPv6 status

Status > ADSL Info

You may want to check the system ADSL information of your router.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **ADSL Info**.
3. Review the device information.

Rules	
Status	EstablishingLink
Total Time	22 hour 2 min 29 sec
Modulation Type	
Standard Used	
Standards Supported	
Link Encapsulation Used	G.992.3_Annex_K_ATM,
Link Encapsulation Supported	
Link Encapsulation Requested	
Line Encoding	DMT
Data Path	L2
Interleave Depth	
ATUR Vendor	5245544b
ATUR Country	181
ATUC Vendor	ffffffff
ATUC Country	255

	Downstream	Upstream
Current Rate(Kbps)	0	0
Noise Margin(dB)	0	0
Attenuation(dB)	0	0
Output Power(dBm)	0	0

Check the router Wireless clients

Status > Wireless Clients

This page displays all connected wireless clients.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **Wireless Clients**.
3. Review the device information.

SSID	IP Address	MAC Address	RSSI

Check the router LAN clients

Status > LAN Clients

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **LAN Clients**.
3. Review the device information.

Host Name	IP Address	MAC Address	Address Source	Lease Time
TV-IP343PI	192.168.10.107	00:0F:0D:26:40:6E	DHCP	66777
TRENDnetACER-PC	192.168.10.101	00:26:2D:5B:46:53	DHCP	86400
TV-IP302PI	192.168.10.101	00:14:D1:95:00:2D	DHCP	0
tew-820ap	192.168.10.103	D8:FE:E3:3E:B0:4D	DHCP	0
TV-IP342PI	192.168.10.105	00:0F:0D:26:9A:3E	DHCP	0
unknow	192.168.10.118	1C:75:08:A4:E0:4A	Static	0
Apple-TV	192.168.10.104	B8:17:C2:B3:B8:91	DHCP	64432
unknow	192.168.10.109	D8:EB:97:CD:4A:E8	DHCP	81439

Check the router Routing Table

Status > Routing Table

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **Routing Table**.
3. Review the device information.

Destination	Gateway	GenMask	Flags	Interface
192.168.10.0	0.0.0.0	255.255.255.0	U	br0

Check the router Basic Statistics

Status > Statistics > Basic Statistics

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **Basic Statistics**.
3. Review the device information.

Internet Connections

LAN Device	
Tx OK	110828 Packets
Rx OK	88531 Packets
Tx Error	0 Packets
Rx Error	0 Packets

Wireless Port	
Tx OK	13608 Packets
Rx OK	1477315 Packets
Tx Error	36 Packets
Rx Error	0 Packets

LAN Ports

	LAN1	LAN2	LAN3	LAN4
Link Status	up	up	up	Auto
Tx OK(Packets)	0	110441	0	0
Rx OK(Packets)	0	88379	0	0
Rx Drop (Packets)	0	0	0	0
Rx Error(Packets)	0	0	0	0

Check the router DSL Statistics

Status > Statistics > DSL Statistics

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status** and **DSL Statistics**.
3. Review the device information.

- **IP Address:** Router's IP address
- **Subnet Mask:** Router's subnet mask
- **MAC Address:** MAC address of router

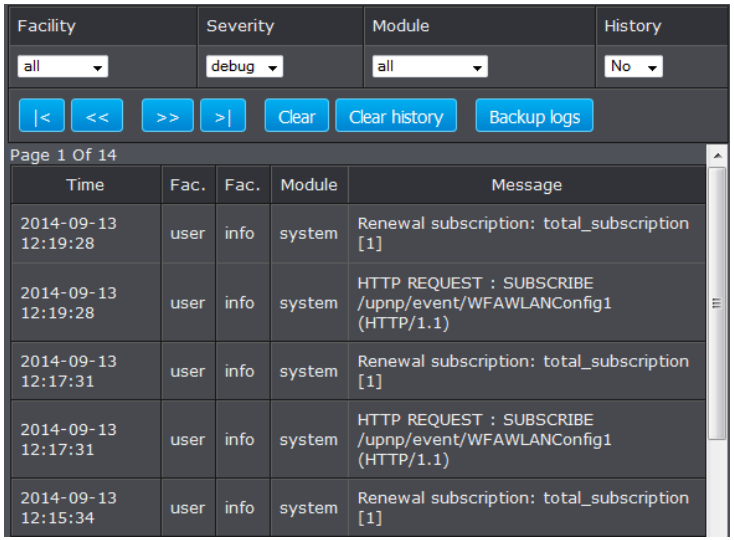
	DownstreamDownstream	Downstream
Trellis		
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power(dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
G.INP		
Rate (Kbps)	0	0
K (number of bytes in DMT frame)	0	0
R (number of check bytes in RS code word)	0	0
N (RS codeword size)		
L (number of bits in DMT frame)		
S (RS code word size in DMT frame)		

View your router log

Status > Logs

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance**, and click on **Syslog**.
3. Review the device log information. You can filter the log view by selecting a particular **Facility**, **Severity**, **Module**, or **History** option.



- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous Page:** Display the log page previous to the current. The **Page: 1/1** will display the current page.
- **Next Page:** Displays the log page next to the current.
- **Clear Log:**- Clears log entries
- **Clear History:** Clear all log entries
- **Refresh:** The **Page: 1/1** will display the current page.
- **Backup Logs:** Click to save logs to a local text file on your local hard drive.

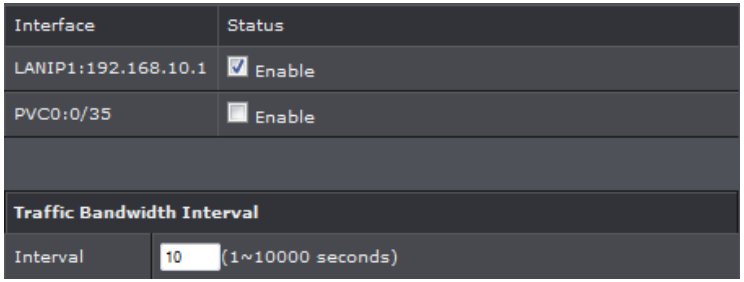
View your router traffic

Status > Traffic Meter

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Status**, and click on **Traffic Meter**.
3. On the ***Traffic Data Interface*** section, check the **Status** box of the interface to view its traffic. You may check more than one interface.

4. On the ***Traffic Bandwidth Interval*** section, enter the interval of refreshing the traffic bandwidth.



Configure your router log

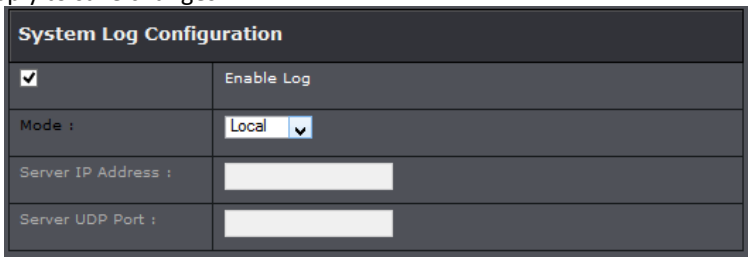
Maintenance > Syslog

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

Send router logs to an external log server

Maintenance > Syslog

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Management**, click on **System Logs**.
3. Click Apply to save changes.



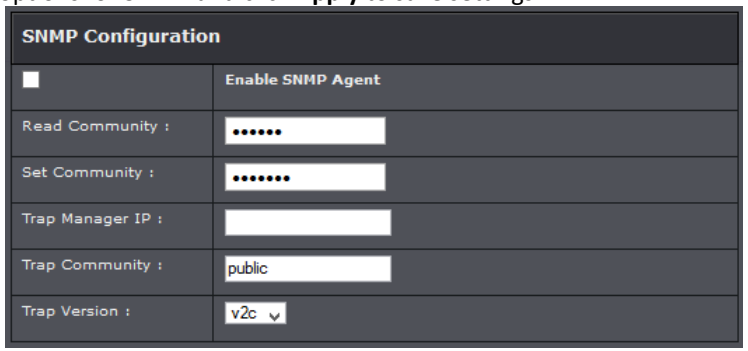
- **Enable Log:** Select to enable
- **Mode:** Select the mode you would like to have the logs go to
- **Server IP Address:** Enter the IP address to where to send the logs to
- **Sever UDP Port:** Enter the UDP port when using Remote logs.

Enable SNMP on your router

Advanced > SNMP

SNMP (Simple Network Management Protocol) is a network management protocol used to monitor (read) and/or manage (write) multiple network devices on a network. This preconfigured external SNMP server.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click **Network Tools** and then on **SNMP**.
3. Review the options for SNMP and click **Apply** to save settings..



- **Enable SNMP Agent:** Select to enable feature
- **Read/Set Community:** Enter a Read and set community name.
- **Trap manager IP:** Enter the destination IP address of the SNMP trap.
- **Trap Community:** Enter the trap community name
- **Trap Version:** Select an SNMP trap version.

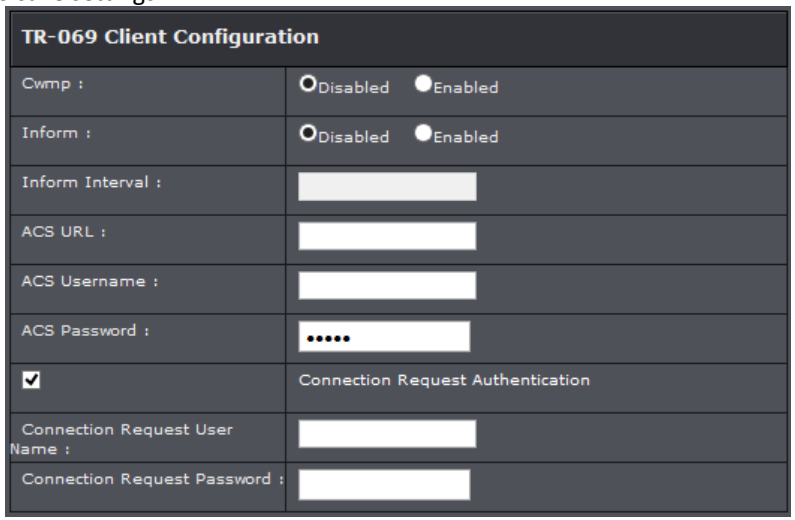
Enable TR-069 on your router

Maintenance > TR069 Setting

TR-069 is a network management protocol used to remote manage multiple network devices on a network typically by ISPs (Internet Service Providers). TR069 usually used in conjunction with ACS (Auto Configuration Servers) server managed by your ISP.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Advanced** and click on **Network Tools** and then **TR069**.
3. Please consult your ISP for the required TR069 settings for remote management. Click **Apply** to save settings.



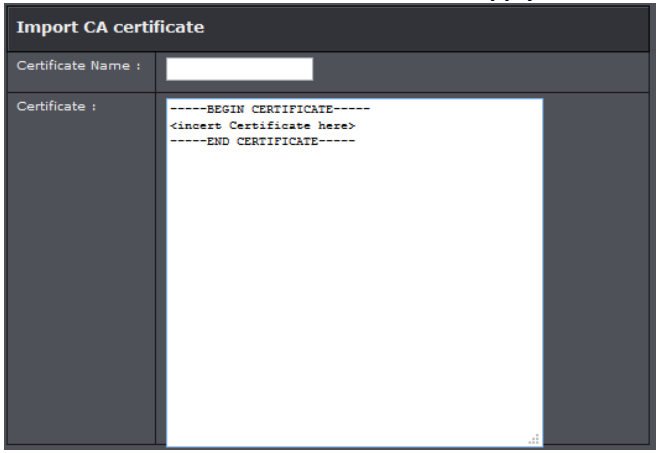
- **Cwmp:** Check this box to enable.
- **Inform:** Check this box to enable
- **Inform Interval:** Enter the interval time of sending RPCs.
- **ACS URL:** Enter the URL of the Auto-Configuration Server (ACS).
- **ACS User Name:** Enter the user name of your modem router when connecting to the ACS.
- **ACS Password:** Enter the password that your modem router should use when connecting to the ACS. Re-enter the password on the Confirm
- **Connection Request Authentication:** Check the box to enable the connection request.
- **Connection Request User Name:** Enter the connection request user name.
- **Connection Request Password:** Enter the connection request password. Re-enter the password on the Confirm Password field.

Trusted Certificates

Maintenance > TR069 Setting

CA Certificates (CA) can be sued to verify peers certificates. A single certificate can be stored on the device.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **Network Tools** and then **Certificates**.
3. Click on Input Certificate to add a new certificate. Click **Apply** to save changes.



Troubleshooting

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

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.
b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

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

Windows XP/2000

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

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

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

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

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

Q: I cannot connect wirelessly to the router. What should I do?
Answer:
1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(*model_number)*.
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see "Steps to improve wireless connectivity" on page 16 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ipconfig /alt***o display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ipconfiggetifaddr<en0 or en1>***to display the wired or wireless IP address settings.

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

Graphical Method

MAC OS 10.6/10.5

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

MAC OS 10.4

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

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

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

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

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.
b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

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

Windows XP/2000

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

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.
b. Click the **Network** icon.
c. From the **Location** drop-down list, select **Automatic**.
d. Select and view your Network connection.
   In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Network** and select the **TCP/IP** tab.
   In MAC OS 10.5/10.6, in the left column, select **Network**.
e. Configure TCP/IP to use DHCP.
   In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
   In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

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

How to find your MAC address?

In Windows 2000/XP/Vista/7,

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

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Network**.
3. On the **Network** tab, the **Network ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Network** from the list on the left.
3. Click the **Advanced** button.
3. On the **Network** tab, the **Network ID** is your MAC Address.

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

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

Windows 7

1. Open Connect to a Network by clicking the network icon ( or ) in the notification area.
2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**.  and then click **Connect To.**
2. In the **Show** list, click **Wireless**.
3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.
2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.
3. You may be prompted to enter a security key in order to connect to the network.
4. Enter in the security key corresponding to the wireless network, and click **Connect**.

Federal Communication Commission Interference Statement

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

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

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.

Operation of this device is restricted to indoor use only

IMPORTANT NOTE:

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.

Country Code selection feature to be disabled for products marketed to the US/CANADA

US/CANADA.

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

TRENDnet hereby declare that the product is in compliance with the essential requirements and other relevant provisions under our sole responsibility.

Safety

EN60950-1 : 2006 + A11 : 2009 + A1: 2010 + A12: 2011

EMC

EN 301 489-1 V1.9.2: 09-2011

EN 301 489-17 V2.2.1: 09-2012

Radio Spectrum & Health

EN 300 328 V1.8.1 : (2012-06)

EN 301 893 V1.7.1 : (2012-06)

EN 62311 : 2008

Energy Efficiency

Regulation (EC) No. 1275/2008, Regulation, No. 801/2013

This product is herewith confirmed to comply with the Directives.

Directives

Low Voltage Directive 2006/95/EC

EMC Directive 2004/108/EC

R&TTE Directive 1999/5/EC

Ecodesign Directive 2009/125/EC

RoHS Directive 2011/65/EU

REACH Regulation (EC) No. 1907/2006

Operations in the 5.15-5.25GHz / 5.470 ~ 5.725GHz band are restricted to indoor usage only.

The band from 5600-5650MHz will be disabled by the software during the manufacturing and cannot be changed by the end user. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Part 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:TI1DL01BTEW816DRM. If requested, this number must be provided to the telephone company.
This equipment uses the following USOC jacks: RJ-11/RJ45/USB/Power Jacks ！

REN (RINGER EQUIVALENT NUMBERS) STATEMENT
Notice: The Ringer Equivalence Number (0.11B) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

ATTACHMENT LIMITATIONS STATEMENT
Notice: This equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment with the Industry Canada certification number. The Department does not guarantee the equipment will operate to the user's satisfaction.
Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.
Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.
Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together.
This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

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-816DRM – 3 Years Warranty

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

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

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

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

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

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

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

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

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

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

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

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

PWP05202009v2 2015/07/23

TRENDnet®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA