User's Guide

TRENDnet®

N300 WiFi ADSL 2+ Router

TEW-723BRM

Contents

Product Overview 1

Package Contents 1

Features 1

Product Hardware Features 2

Basic Router Setup 4

Creating a Home Network 4

Modem Router Installation 5

Modem Router Installation 6

Connect additional wired devices to your network 9

Wireless Networking and Security 10

How to choose the type of security for your wireless network 10

Secure your wireless network 11

Connect wireless devices to your modem router 12

Connect wireless devices using WPS 12

Basic wireless settings 14

Steps to improve wireless connectivity 15

Advanced wireless settings 15

Multiple SSID 15

Securing Multiple SSIDs 16

Additional Wireless Settings 17

Access Control Filters 18

Access control basics 18

Wireless MAC address filters 18

Removing MAC Address 18

MAC address filters 19

Advanced MAC address filters 19

URL/Keyword Blocking 19

MAC Blocking 20

Creating a Schedule 20

IP Filtering 21

MAC Filtering 21

Advanced Router Setup 22

Access your router management page 22

Change your router login password 22

Set your router date and time 23

Manually configure your Internet connection 23

ATM Settings 24

PVC Auto Search 25

Change your router IP address 25

Set up the DHCP server on your router 26

Assign specific IP address to clients 26

Enable/disable UPnP on your router 27

Enable/disable DLNA 27

Enable SNMP on your router 27

Enable TR-069 on your router 28

Trusted Certificates 28

Blocking Applications 29

ARP Binding 29

Setting a Client Limit 29

Enable/disable Telnet 29

Configure ALG settings 30

Configure NAT Forwarding settings 30

Configure FTP ALG Config 31
Configure NAT IP Mapping 31
Additional Security Settings 31
DNS 32
Allow/deny multicast streaming 32
Identify your network on the Internet 33
Allow remote access to your router management page 33
Open a device on your network to the Internet 34
DMZ 34
Port Forwarding 34
Port Trigger 35
Prioritize traffic using QoS (Quality of Service) 36
Add static routes to your router 37
Enable dynamic routing on your router 38
Setup Port Mapping 38
Setup IPv6 on your router 39
Configure ADSL settings 39

Using 3G WAN Connection 40

Configure 3G WAN 40

Router Maintenance & Monitoring 40

Reset your router to factory defaults 40
Router Default Settings 41
Backup and restore your router configuration settings 41
Upgrade your modem router firmware 42
Restart your router 43
Check connectivity using the router management page 43
Traceroute Diagnostic 44
Check ADSL Connection using the router management page 44
Check Internet connectivity using the router management page 44
Check the router system information 44
Check the modem router ADSL status 45
Check the router Wireless clients 46
Check the router Routing Table 46
Check the router Routing Table 46
Check the router Basic Statistics 46
View your router log 47

Router Management Page Structure 48

Technical Specifications 49

Troubleshooting 51

Appendix 53

Product Overview

TEW-723BRM

Package Contents

In addition to your modem router, the package includes:

- TEW-723BRM
- Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1 m/3.28 ft.)
- RJ11 telephone cable (1 m/3.28 ft.)
- Power adapter (12 V DC, 1 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 N300 WiFi ADSL 2+ Modem Router, model TEW-723BRM, is a combination ADSL 2+ modem and wireless N300 router, which offers 300 Mbps WiFi N networking to share files, play games, and surf the internet. For your convenience, the wireless network is setup and pre-encrypted out of the box.

Features

Easy Setup

Get up and running in minutes with an intuitive guided setup

ADSL 2/2+

Compatible with most ADSL 2/2+ internet service providers

N300 Wireless

Powerful 300 Mbps Wireless N

Pre-Encrypted Wireless

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

Wireless On/Off Button

Enable or disable the wireless network with the convenient on/off wireless button

Parental Controls

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

Ethernet Ports

Ethernet ports to hardwire up to four devices

Wireless Coverage

Extended wireless coverage with 5dBi antennas, suitable for medium to large size homes

Remote Management

Remote management and troubleshooting support with TR-069

IPv6

IPv6 network support

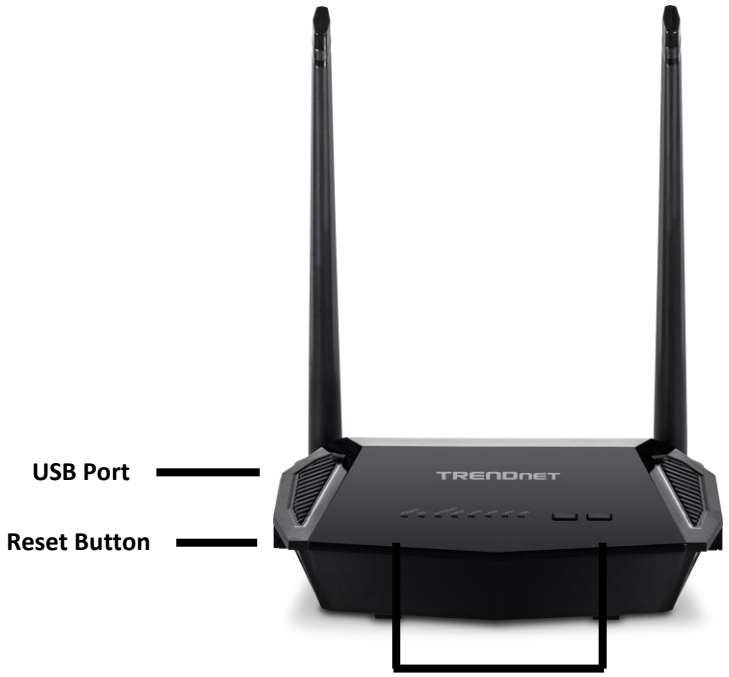
*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Product Hardware Features

Rear View

- **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.
- **Power Port:** Connect the included power adapter from your modem router power port and to an available power outlet.
- **On/Off Button:** Push the button to turn the device on and off.

Front View



- **Power LED:** This LED indicator blinks green when properly connected to a power supply. When the device is malfunctioned LED indicator will be red.
- **Internet & DSL LED:** This LED indicator is solid green when the ADSL status of the modem router has established connection to your ISP and when the modem router has been properly configured with the settings provided by 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. If only the DSL LED is blinking, then a connection has not been established with your ISP or RJ-11 cable has been unplugged.
- **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.
- **USB:** This LED indicator blinks green when a the 3G USB adapter is plugged in.
- **WLAN Button**: Push this button for 5 seconds to enable and disable your wireless network. The button will light up green if Wireless is enabled.
- **WPS Button:** Push this button for 5 seconds to setup WPS between the device and to your other clients
- **USB Port:** Connect a 3G USB Modem as a backup
- **Reset Button**: Push and hold this button for **10** seconds and release to reset your modem router to its factory defaults.

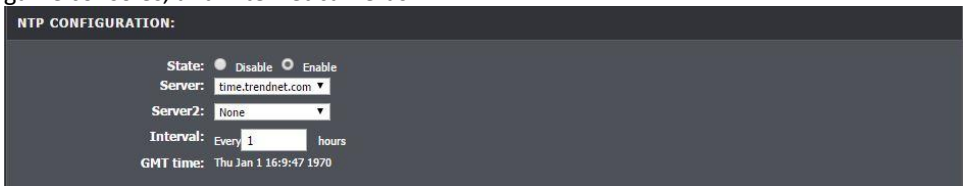
Basic Router Setup

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-723BRM 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 modem router
Refer to the Quick Installation Guide or continue to the next section "Modem 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)

Modem Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your modem router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your modem 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)

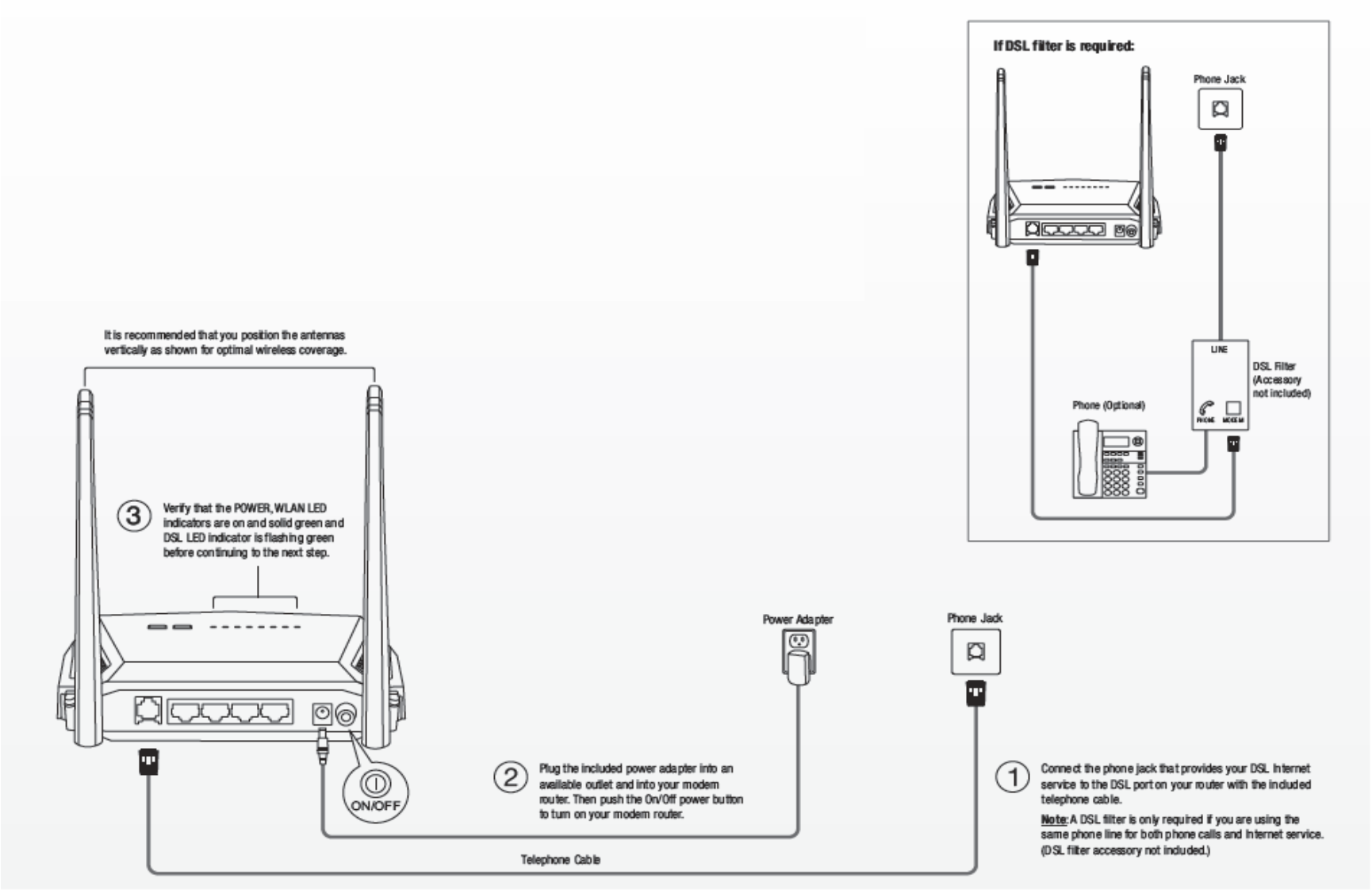
- **4a. PPPoA to obtain IP automatically**

Account/User Name: _____
Password: _____

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

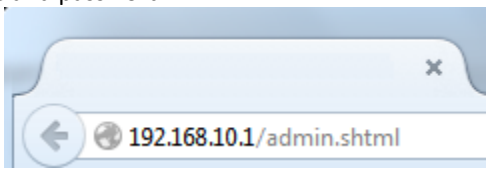
User Name: _____
Password: _____
Verify Password: _____
IP Address: ____. _____._____._____ (e.g. 215.24.24.129)
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Server Address: _____. _____._____._____

Modem Router Installation

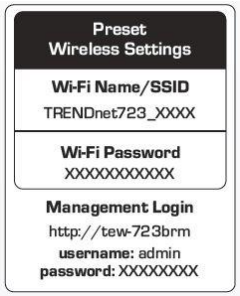


Setup Wizard

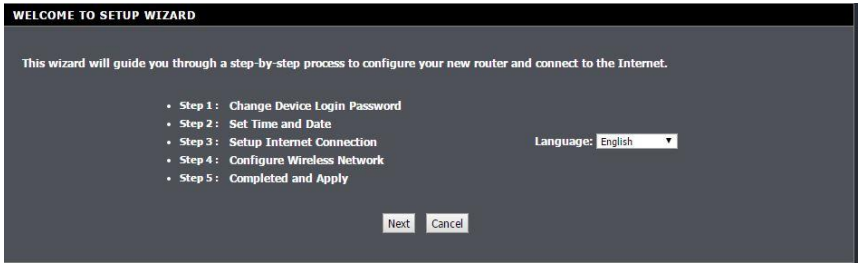
1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://tew-723brm or http://192.168.10.1. Your modem router will prompt you for a user name and password.



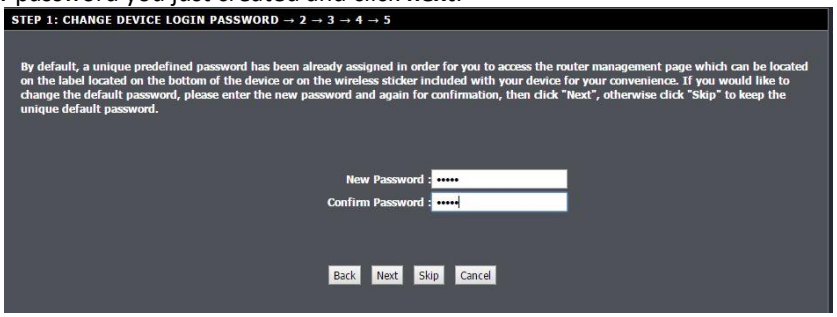
2. Your modem router will prompt you for a user name and password. For added security, the modem router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the modem router and on the label on the bottom of the modem router.



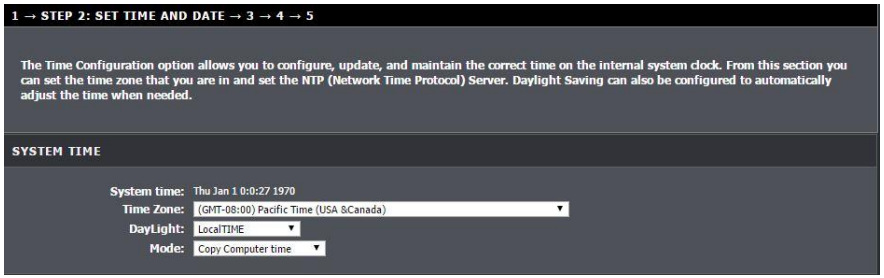
3. The first time you boot up the router, it will automatically take you through the setup process. Select your **preferred language** and click **next**.



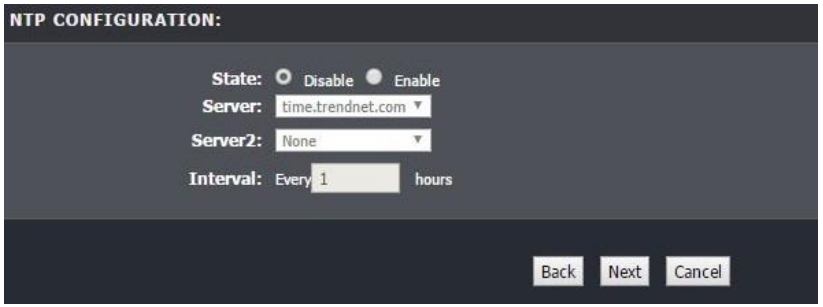
4. Create a new login **password** to login to the web management interface. Confirm the new password you just created and click **next**.



4. Setup the date and time for your unit and click **next**.

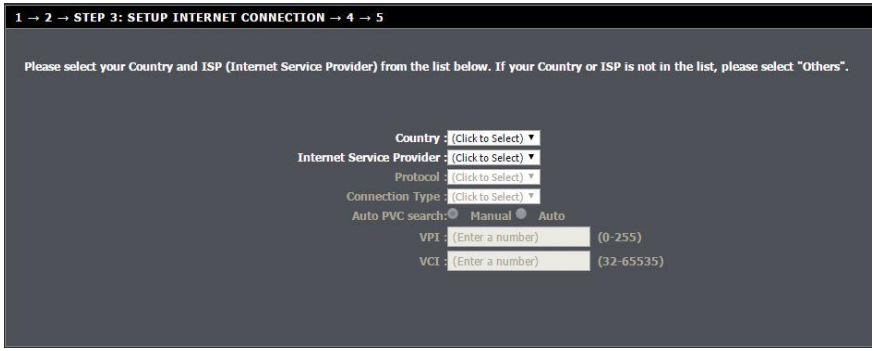


- **Time Zone:** Select the time zone you are in from the drop-down menu.
- **Daylight:** Select the Daylight Savings time from the drop-down menu.
- **Mode:** Select if you want the device to automatically pull the time from your computer or if you want it to sync with a NTP server.

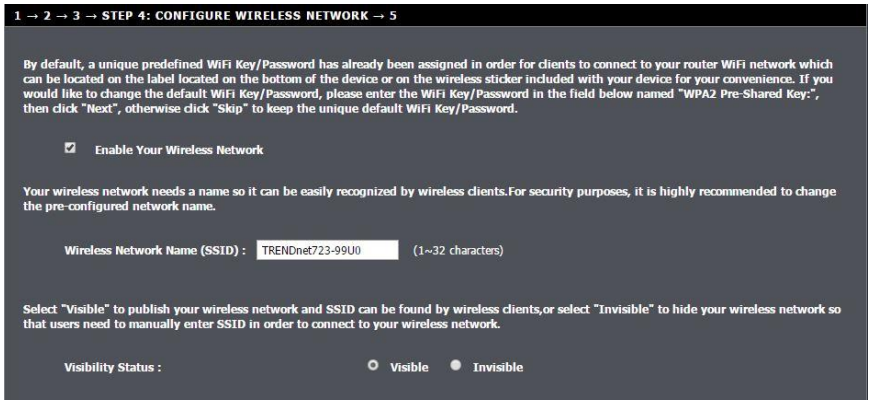


- **State:** Enable or Disable the NTP server
- **Server:** Select from the drop-down menu what server to connect to
  - If **Other** is selected, input the location of the server in the field below
- **Server2:** Select from the drop-down menu what server to connect to
  - If **Other** is selected, input the location of the server in the field below
- **Interval:** Input the length of time (in hours) that the unit will sync with the server.

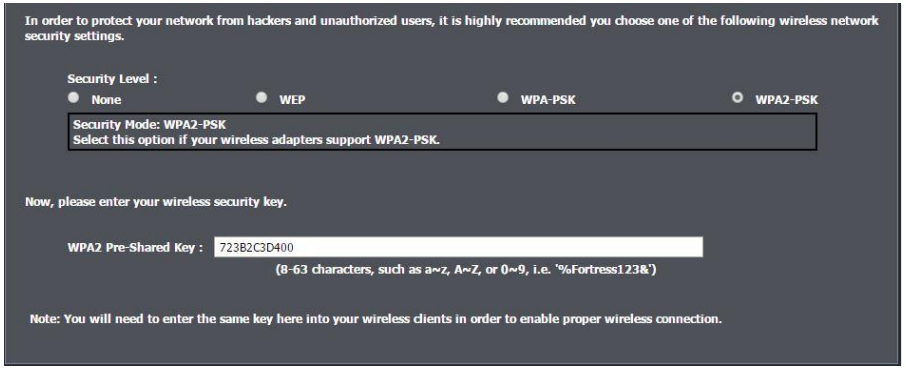
5. Configure your internet service provider settings.



6. Configure your wireless network settings and click **next**.

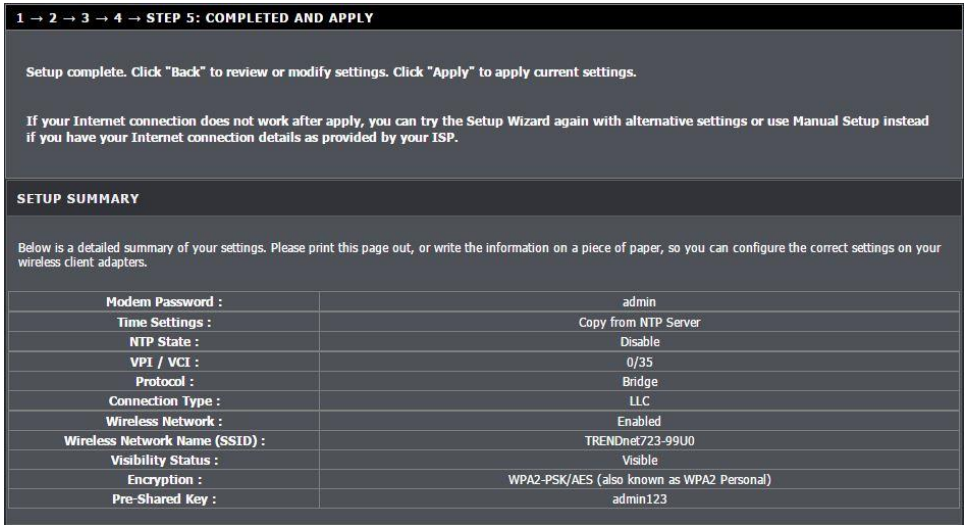


- **Enable your Wireless Network:** Check the box to turn on your wireless network.
- **Wireless Network Name (SSID):** Enter the name of your wireless network in this field
- **Visibility Status:** Enable clients connecting to the unit to search for it. If **Invisible** is selected, you would need to manually input the wireless network name (SSID)



- **Security Level:** Select the type of security for your wireless network. Please see the section on Wireless Networking and Security on page 9 for definition on the security modes.
- **Pre-Shared Key**: Input the desired password to secure your wireless network.

7. Verify the configured settings and click **Apply** when completed. Your modem router will reboot and restart.



1 → 2 → 3 → 4 → STEP 5: COMPLETED AND APPLY

Setup complete. Click "Back" to review or modify settings. Click "Apply" to apply current settings.

If your Internet connection does not work after apply, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

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.

Modem Password :	admin
Time Settings :	Copy from NTP Server
NTP State :	Disable
VPI / VCI :	0/35
Protocol :	Bridge
Connection Type :	LLC
Wireless Network :	Enabled
Wireless Network Name (SSID) :	TRENDnet723-99U0
Visibility Status :	Visible
Encryption :	WPA2-PSK/AES (also known as WPA2 Personal)
Pre-Shared Key :	admin123

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 modem 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 modem 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 modem router to WEP to allow the old adapters to connect to the modem 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 Mixed**: This setting provides the modem 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 modem router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your modem 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

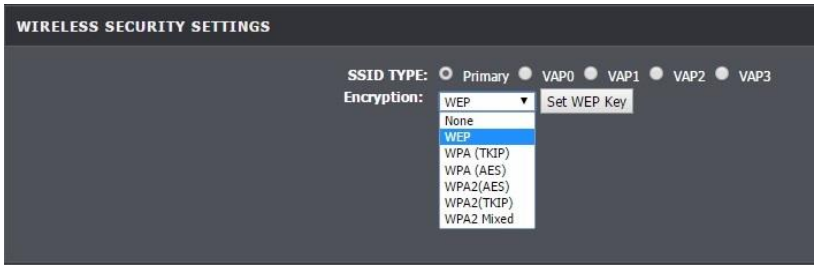
Setup > Wireless Settings

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

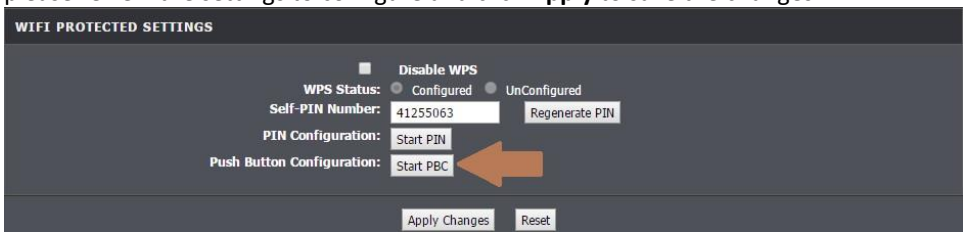
WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

Selecting 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.



- **Key Format:** 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.*
- **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**
  - This is where you enter the password or key needed for a computer to connect to the modem 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 modem router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

Selecting WPA (TKIP), WPA (AES), WPA2 (AES), WPA (TKIP) or WPA2 Mixed:
If selecting **WPA, WPA2 or WPA2 Mixed, (Wi-Fi Protected Access Pre-shared Key)** please review the settings to configure and click **Apply** to save the changes.



First, from the Security Mode drop-down list, select **WPA (TKIP), WPA (AES), WPA2 (AES), WPA (TKIP) or WPA2 Mixed.**

- 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**.

Select the type of Authentication Mode.

- **Enterprise (RADIUS):** Selecting this authentication mode allows for Enterprise level security, where a RADIUS Server will need to be set-up.

- **Personal (Pre-Shared Key):** Selecting this option allows a pre-shared key to be setup as the security feature.

Select the **Pre-Shared Key Format.**

- **Passphrase:** A password or key that is used to connect your computer to this modem router wirelessly
- **Hex:** A password or key using only HEX characters

Create your Wireless security pre-shared key (password or key):

- **Pre-share Key:** Enter the pre-shared key.
- **This is the password or key that is used to connect your computer to this modem router wirelessly**

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

If **Enterprise (RADIUS)** is selected in the above Authentication Mode, input the RADIUS Server location in the provided fields.

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

Connect wireless devices to your modem 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 modem router's wireless network.

See the "Appendix" on page 59 for general information on connecting to a wireless network.

Connect wireless devices using WPS

Advanced Wireless > WPS

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

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

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

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

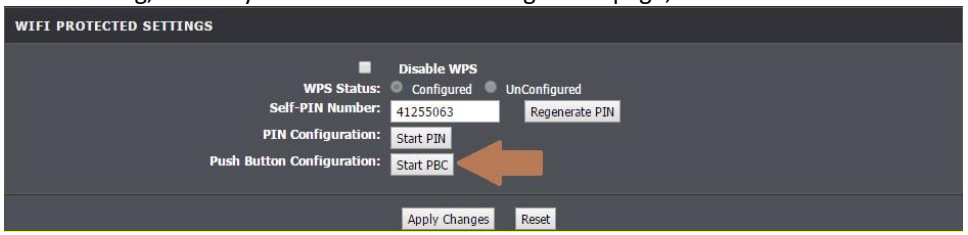
For connecting additional WPS supported devices, repeat this process for each additional device.

PBC (Software/Virtual Push Button)

Advanced Wireless > WPS

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

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced Wireless** and click **WPS**.
3. To add a wireless device to your network, simply the push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are connecting, then in your modem router management page, click the **Start PBC** button.



4. The **WPS LED Indicator** area will blink indicating WPS is activated.

Note: *You will have 2 minutes to push the WPS button on the client side.*

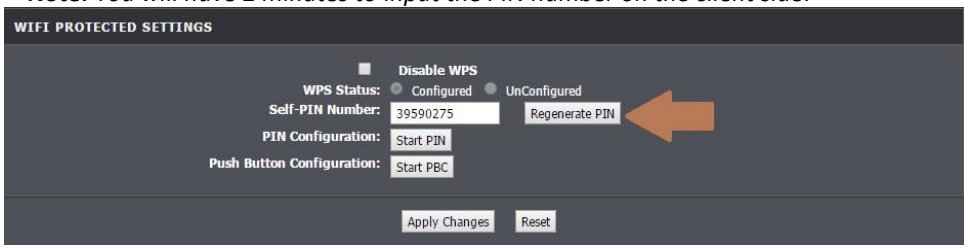
PIN (Personal Identification Number)

Advanced Wireless > WPS

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 modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced Wireless** and click **WPS**.
3. Click on **Regenerate PIN** to randomly generate a PIN.

Note: *You will have 2 minutes to input the PIN number on the client side.*

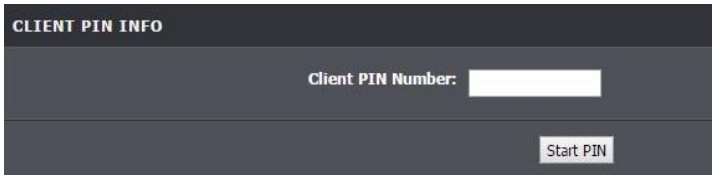


Connecting to a Client's PIN (Personal Identification Number)

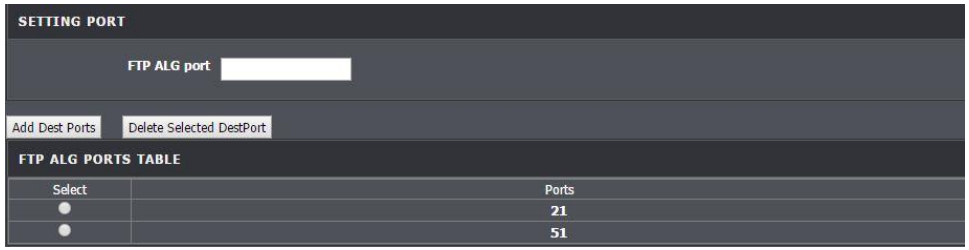
Advanced Wireless > WPS

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 modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced Wireless** and click **WPS**.
3. Input the PIN number from your device under **Client PIN Number**.



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.*

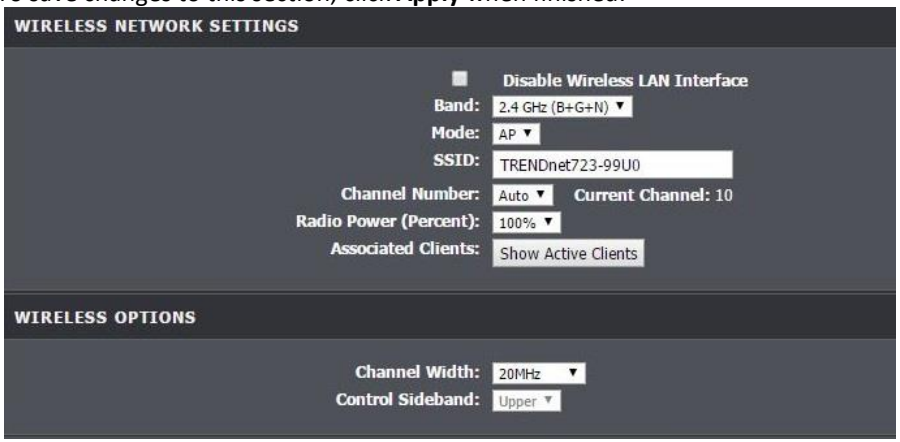


Basic wireless settings

Setup > Wireless Setup>Wireless Basic

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

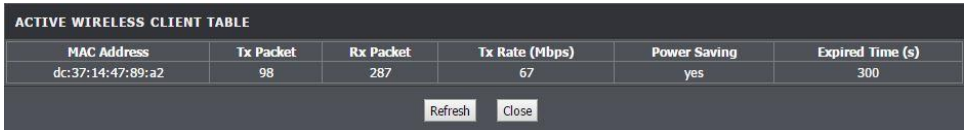
1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Setup,** click on **Wireless Setup,** and then click on **Wireless Basics**.
3. To save changes to this section, click **Apply** when finished.



- **Disable Wireless LAN Interface:** turns off wireless networking on your router
- **Band:** Select the appropriate band for your network
  - **B+G+N:** Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the modem router in addition to newer 802.11n devices.
  - **G+N:** This mode only allows devices to connect to the modem router using older and slower 802.11g or the newer 802.11n technology. Devices that are connected to the modem router on 802.11g band will reduce the modem router's maximum speed.
  - **N only:** This mode only allows newer 802.11n devices to connect to your modem 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 modem router using older and slow 802.11g technology (typically not recommended).
  - **B/G mixed:** This mode only allows devices to connect to the modem 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).
  - **G only:** This mode only allows devices to connect to the modem router using older and slower 802.11g technology. (typically, not recommended)
  - **B only:** This mode only allows devices to connect to the modem 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.*
- **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.
- **Channel Number:** 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.
- **Radio Power:** The wireless radio power can be modified to a lower setting such as 50%, 25%, and 10% if necessary. Lowering the radio power 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%)

- **Associated Clients:** Clicking on **Show Active Clients** will bring up a new window displaying the status of current devices connected to the modem router wirelessly.



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 modem 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 modem router and the wireless device, the better.
   d. Place the modem router in a location away from other electronics, motors, and fluorescent lighting.
   e. Many environmental variables can affect the modem 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.

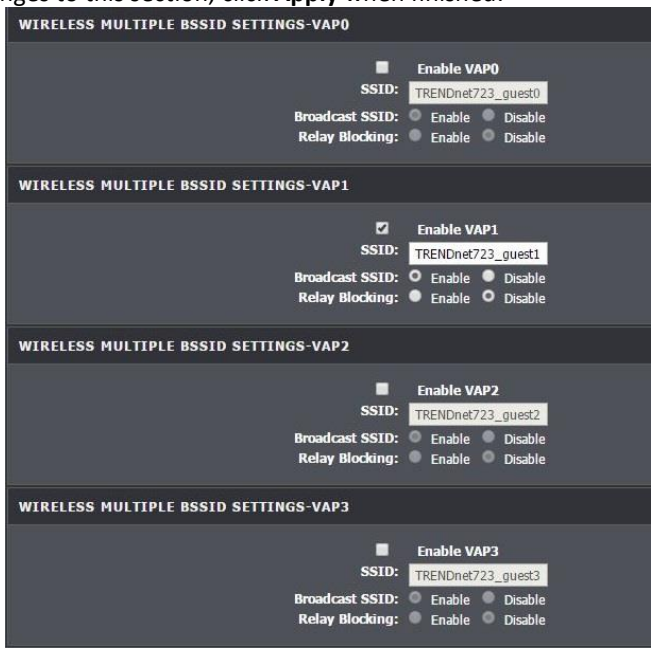
Multiple SSID

Advanced > Advanced Wireless > MBSSID

The multiple SSID feature allows you to broadcast up to four 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 **Advanced Wireless,** and then click on **MBSSID**.

3. To save changes to this section, click **Apply** when finished.



- **Enable:** Select the VAP (Virtual Access Point) you wish to enable (**VAP0**, **VAP1**, **VAP2**, or **VAP3**).
- **SSID:** Enter the wireless name or SSID of your guest network.
- **Broadcast SSID:**
  - **Enable:** turns on broadcasting or your wireless network for clients to see.
  - **Disable:** turns off broadcasting of wireless networking on your router.
- **Relay Blocking:**
  - **Enable:** Blocks all users connected to this network from each other.
  - **Disable:** Disables blocking of all users connected to this guest network from each other.

Securing Multiple SSIDs

Setup > Wireless Setup > Wireless Security

This section outlines Security for Multiple SSIDs.

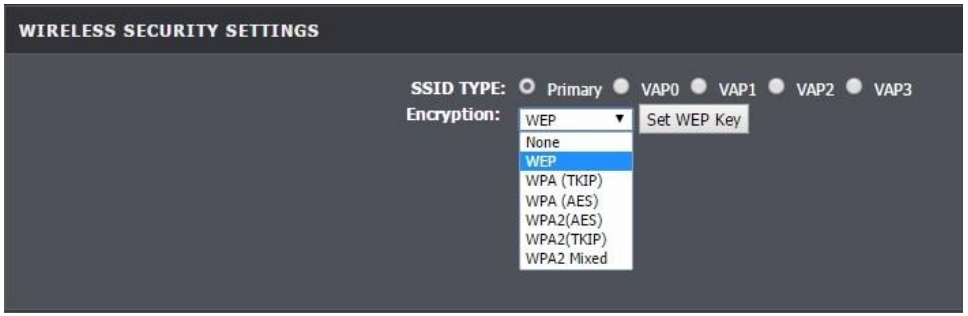
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup,** click on **Wireless Setup,** and then click on **Wireless Security**.
- 3. Select the VAP (Virtual Access Point) you wish to secure (**VAP0**, **VAP1**, **VAP2**, or **VAP3**).
3. To save changes to this section, click **Apply** when finished.

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.

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

Selecting WPA (TKIP), WPA (AES), WPA2 (AES), WPA (TKIP) or WPA2 Mixed:
If selecting **WPA, WPA2 or WPA2 Mixed, (Wi-Fi Protected Access Pre-shared Key)** please review the settings to configure and click **Apply** to save the changes.



First, from the Security Mode drop-down list, select **WPA (TKIP), WPA (AES), WPA2 (AES), WPA (TKIP) or WPA2 Mixed.**

- 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**.

Select the type of Authentication Mode.

- **Enterprise (RADIUS):** Selecting this authentication mode allows for Enterprise level security, where a RADIUS Server will need to be set-up.
- **Personal (Pre-Shared Key):** Selecting this option allows a pre-shared key to be setup as the security feature.

Select the **Pre-Shared Key Format.**

- **Passphrase:** A password or key that is used to connect your computer to this modem router wirelessly
- **Hex:** A password or key using only HEX characters

Create your Wireless security pre-shared key (password or key):

- **Pre-share Key:** Enter the pre-shared 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.)*

If **Enterprise (RADIUS)** is selected in the above Authentication Mode, input the RADIUS Server location in the provided fields.

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

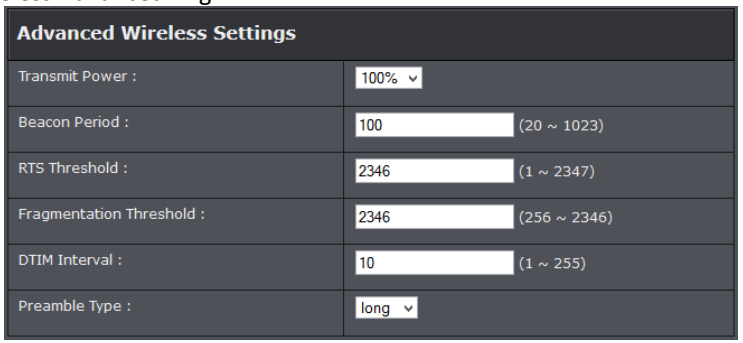
Additional Wireless Settings

Advanced > Advanced Wireless > Wireless Advanced

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

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 **Wireless Advanced**. Click **Apply** to save settings.

Insert Wireless Advanced Img.



- **Authentication Type:** Select **Open System, Shared Key,** or **Auto** type Authentication. By default, it is set to **Auto**.

  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.
Default value: 2346 (range: 256 – 2346)

- **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: 234 (range: 0-2347)
- **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: 1-1024)
- **DTIM Interval:** Is the interval of when the access point informs the clients about the presence of buffered multicast/broadcast data.
  Default Value: 1 (range: 1-255)
- **Data Rate:** The Data Rate is the rate of data that can be transferred from the modem router to devices connected on the modem router. This can be adjusted.
  Default Value: Auto
- **Preamble Type:** Select long or short preamble.
- **Broadcast SSID:** Select enable or disable to display the SSID to client devices.
- **Relay Blocking:** Select enable or disable to block all other devices connected on the wireless network from communicating with each other.
- **Ethernet to Wireless Blocking:** Select enable or disable to block the communication between wireless and wired devices connected to the modem router.
- **WiFi Multicast to Unicast:** Select enable or disable.
- **Aggregation:** Select enable or disable route aggregation.
- **Short GI:** Select enable or disable for short guard interval.

Access Control Filters

Access control basics

Wireless MAC address filters

Advanced > Advanced Wireless > Access Control

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 **Access Control**.
3. Review the settings and click **Apply** to save settings and **Add** to enter MAC addresses.

- **Wireless Access Control Mode**: Select from the drop-down menu to **Disable**, **Allow Listed** or **Deny Listed** MAC addresses.
- **MAC Address:** Enter the MAC address to apply the rule. Click Add to add MAC address to the select rule.

Removing MAC Address

Advanced > Advanced Wireless > Access Control

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 **Access Control**.

3. Review the settings and click **Apply** to save settings and **Add** to enter MAC addresses.

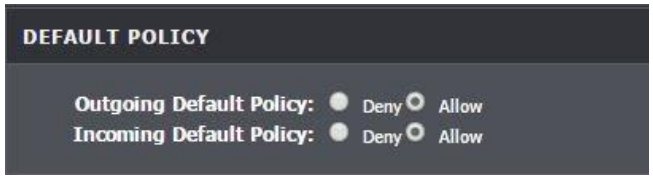
- **Current Access Control List:** In this table, you can select the MAC address you delete.
- **Delete Selected:** Remove the selected MAC address from the rule
- **Delete All:** Remove all MAC address from the rule

MAC address filters

Advanced > Filtering Options > MAC Filter

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 **Filtering Options**, and click on **MAC Filter**.
3. Select the type of default Mac filtering option to enable.
   - **Outgoing Default Policy: Allow** or **deny** clients to upload anything to the internet.
   - **Incoming Default Policy: Allow** or **deny** clients that can download anything from the internet.

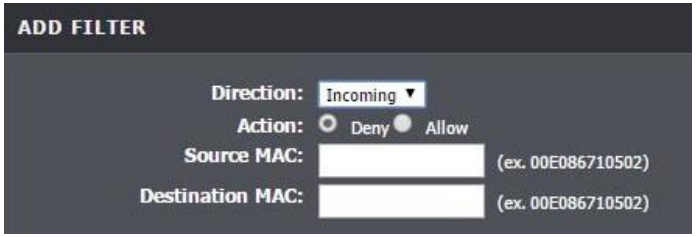


4. Click **Apply Changes** to save your settings.

Advanced MAC address filters

Advanced > Filtering Options > MAC Filter

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 **MAC Filter**.
3. Review the settings below and click **Add** to save your settings.
   - **Direction:** Select the flow of information which you wish to apply the following rule to.
   - **Action:** Select Deny or Allow
   - **Source MAC:** Enter the MAC address of the source device
   - **Destination MAC:** Enter the MAC address of the destination device



URL/Keyword Blocking

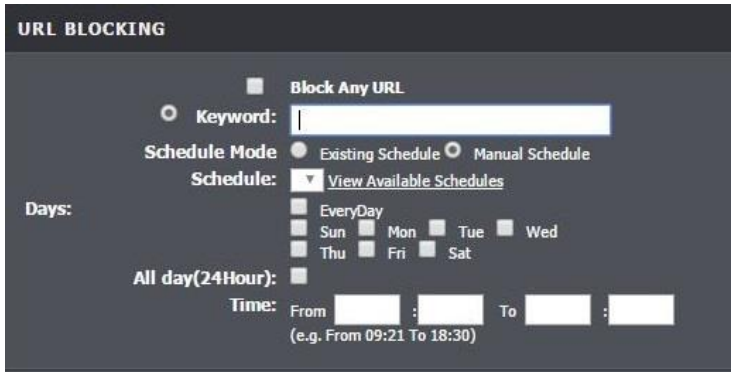
Advanced > Parental Control > URL Block

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 **URL Block**.
3. **Enable** URL or Keyword blocking.

- **Disable:** Select this option to turn off URL blocking capability
- **Enable:** Select this option to turn on URL blocking capability.

4. Review the available settings under URL Blocking and click **Add Filter** to save.



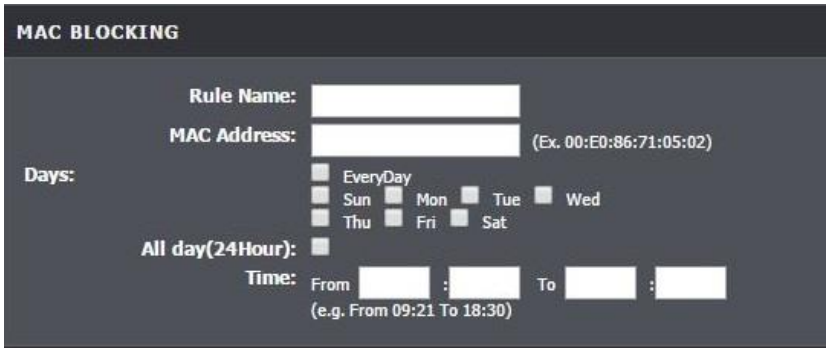
- **Block Any URL:** Select this option to block all URL addresses.
- **Keyword:** Enter the URL or keyword you are adding.
- **Schedule Mode:** Select **Existing Schedule** to select from a previously defined schedule, or **Manual Schedule** to input a new schedule.
- **Days:** Select the days you would like the rule to apply
- **All Day (24 Hour):** Select this rule if you wish to the rule to apply the whole day
- **Time:** Enter the time of when you would like the rule to apply.

MAC Blocking

Advanced > Parental Control > MAC Block

You may want to block computers or devices on your network access to websites using the devices' MAC address.

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 Block**.
3. Review the settings below and click **Add Rule** to save the settings.

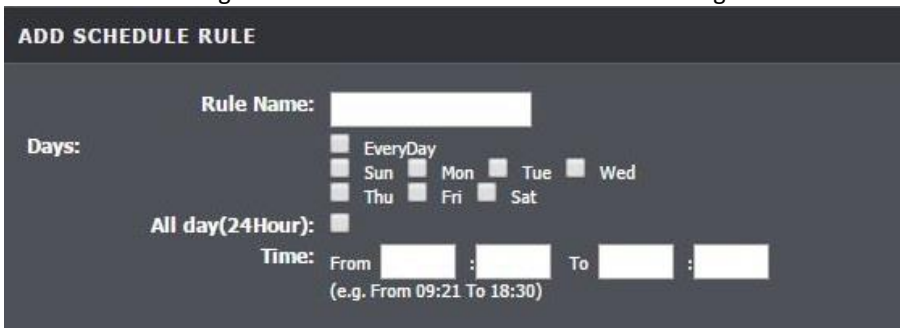


- **Rule Name:** Enter the name of the rule.
- **MAC Address:** Enter the MAC address of the computer or device you wish to add to this rule. (Only 1 computer or device can be added per rule)
- **Days:** Select the days you would like the rule to apply.
- **Time:** Select the time of the day you would like the rule to apply. (Time is in 24:00 format).

Creating a Schedule

Advanced > Parental Control > Schedules

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 **Schedules**.
3. Review the settings below and click **Add Rule** to save the settings.



- **Rule Name:** Enter the name of the rule.

- **Days:** Select the days you would like the rule to apply.
- **Time:** Select the time of the day you would like the rule to apply. (Time is in 24:00 format).

IP Filtering

Advanced > Filtering Options > IP/Port Filter

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 **IP/Port Filter** or **IPv6/Port Filter**.
3. Review the settings below and click **Apply Changes** to save the settings.

- **Rule Action:** Select **Permit** to allow access and **Deny** to deny access
- **Protocol:** Select the protocol you would like to filter
- **Direction:** The direction of the traffic you wish to apply the rule to
  - **Upstream:** Filters Local (LAN) traffic to internet (WAN) traffic.
  - **Downstream:** Filters Internet (WAN) traffic to Local (LAN) traffic.
- **Source/Dest IP:** Enter the starting and ending points of the source IP address to filer.
- **SPort/DPort:** Enter the source and destination ports of the filter IP address.
- **Mask Address:** Enter the network mask of your source
- **Start/End Destination IP Address:** Enter the starting and ending points of the source IP address to filer.

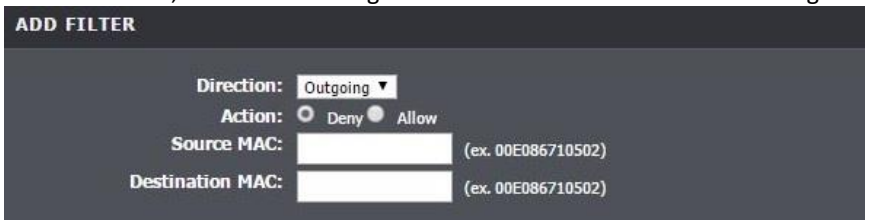
MAC Filtering

Advanced > Filtering Options > MAC Filter

You may want to block computers or devices on your network access to your network using their MAC Address.

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 **MAC Filter**
3. Click **Allow** or **Deny** to set the default incoming or outgoing traffic. Click **Apply Changes** to save the settings.

4. To add a rule, review the settings below and click **Add** to save the settings.



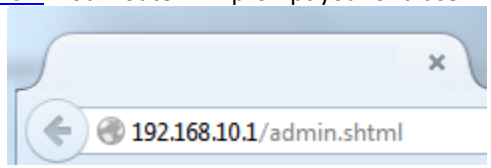
- **Direction:** The direction of the traffic you wish to apply the rule to
  - **Outgoing:** Filters Local (LAN) traffic to internet (WAN) traffic.
  - **Incoming:** Filters Internet (WAN) traffic to Local (LAN) traffic.
- **Action:** Select **Deny** to deny access or **Allow** to allow access.
- **Source MAC:** Enter the MAC address of the device at the starting point.
- **Destination MAC:** Enter the MAC address of the device at the end point.

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.

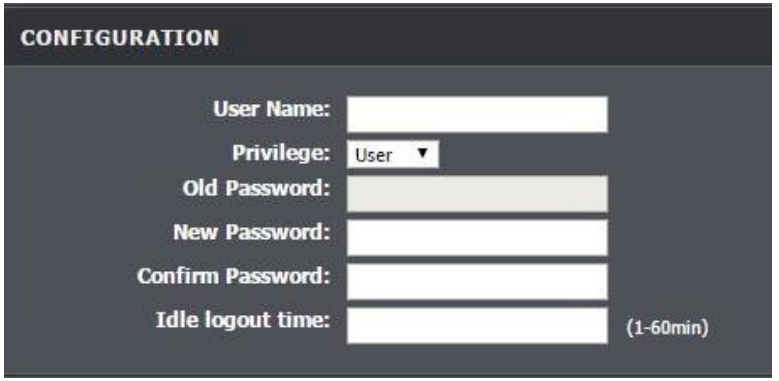


2. Enter the default user name and password and then click Login.
Default User Name: **admin**
Default Password: **xxxxxxx**

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 **Maintenance** and click on **Password**.
3. Select the user name to apply changes to in the **User Account Table**. In the **Old Password** field, enter the current password. **New Password** field, enter the new password and in the C**onfirm** 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.*

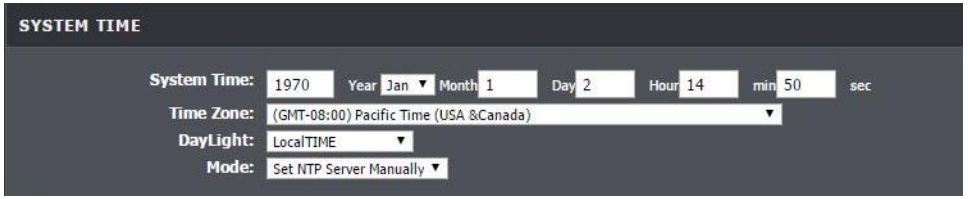
Set your router date and time

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.*

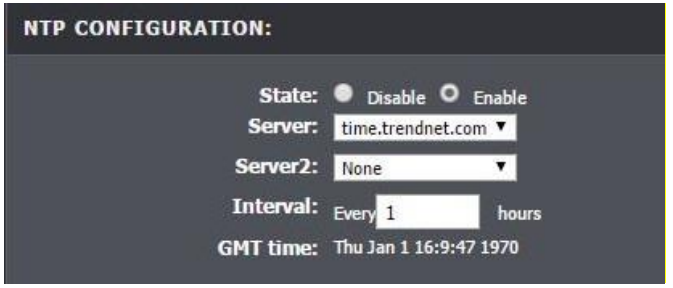
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Time and Date**.
3. Review the settings and click Apply Changes to save the settings.



- **System Time:** Displays the current time of the modem router. If the **Mode**, is set as **Set Time Manually**, then the time can be customized in this area.
- **Time Zone:** Select your country's time zone from the drop down menu.
- **DayLight:** Select day light savings time for your area.
- **Mode:**
  - **Set Time Manually:** Manually set the time of the modem router
  - **Copy Computer Time:** Automatically syncs the time that is currently on computer to the modem router.
  - **Set NTP Server Manually:** Connects your modem router to a designated server to sync the times

NTP

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



- **State:** Select **Enable** to enable the NTP feature
- **Server / Server2:** Select the server you wish to connect to. To change the default server, select **Other** from the drop down menu and click **Apply Changes**. Input the server destination in the additional field below.
- **Interval:** How often the modem router syncs with the designated server..

Manually configure your Internet connection

Setup > Internet Setup> Channel Config

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, and click on **Channel Config**.
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.*

PPPoE / PPPoA

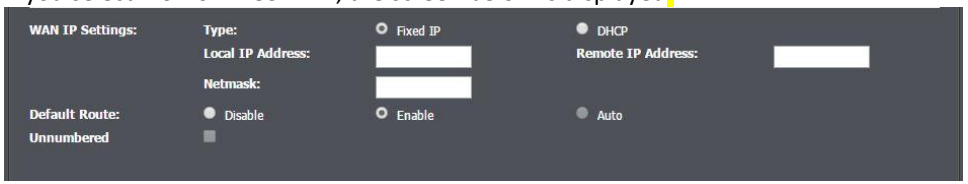
If you select PPPoE (RFC-2516 PPP over Ethernet) on the Protocol section, the screen below is displayed.

- **IP Protocol:** Select IPv4, IPv6, or IPv4/IPv6
- **User Name:** Enter the user name provided by your ISP.

- **User Password:** Enter the password provided by your ISP.
- **Type:** Configure how you want your modem router to connect and terminate the Internet connection. Options are:
  - **Connect on Demand:** 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.
  - **Continuous:** 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.

IPoA / 1483 MER

If you select IPoA or 1483 MER, the screen below is displayed.



- **Type:** Select **Fixed IP** or **DHCP**
- **Local IP Address:** Enter the IP address provided by your ISP.
- **Netmask:** Enter the subnet mask provided by your ISP.
- **Remote IP Address:** 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.

1483 Bridge Mode

If you select 1483 Bridge mode, the screen below is displayed.

- **Encapsulation:** Select **LLC** or **VC-Mux**
- **802.1q:** Select **Enable** or **Disable**.

1483 Routed

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

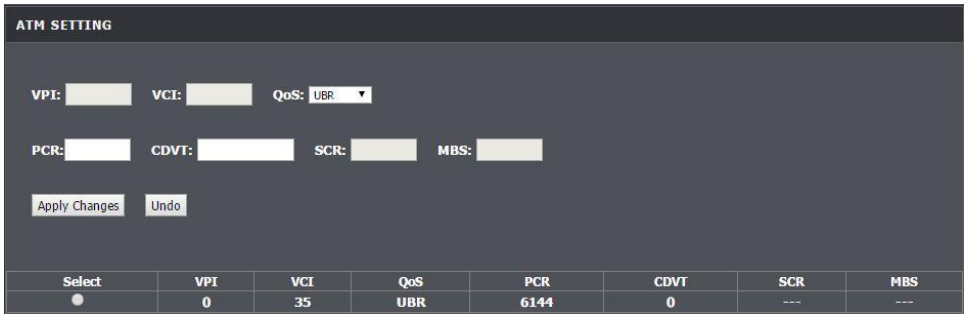
- **Local IP Address:** Enter the IP address provided by your ISP.
- **Netmask:** Enter the subnet mask provided by your ISP.
- **Remote IP Address:** Enter the default gateway provided by your ISP.

ATM Settings

Setup > Internet Setup > ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc.

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

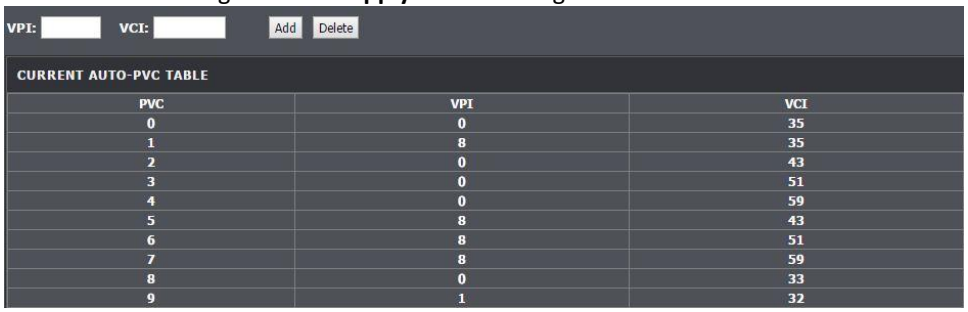


PVC Auto Search

Setup > Internet Setup > PVC Auto Search

To configure the PVC Auto Detection function, you can add or delete the auto PVC Search Table.

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



Change your router IP address

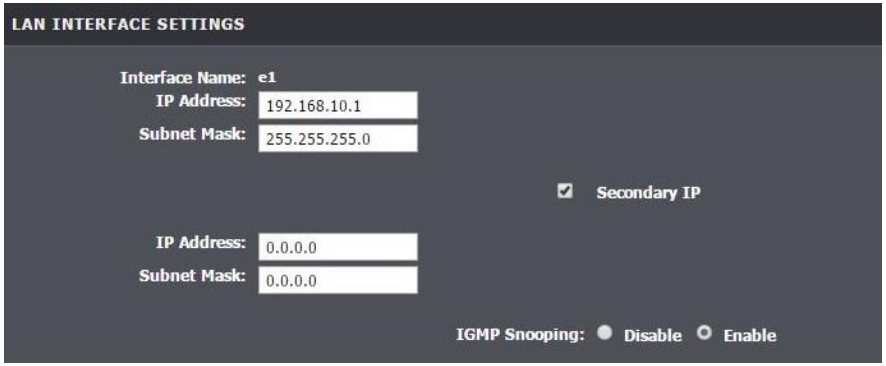
Setup > Local Network > LAN Interface

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.



- **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*)

- **Secondary IP:** Click to enable option to configure a secondary IP Address and Subnet Mask
- **IP Address:** Enter the second IP address
- **Subnet Mask:** Enter the subnet mask to assign. (e.g. *255.255.255.0*)

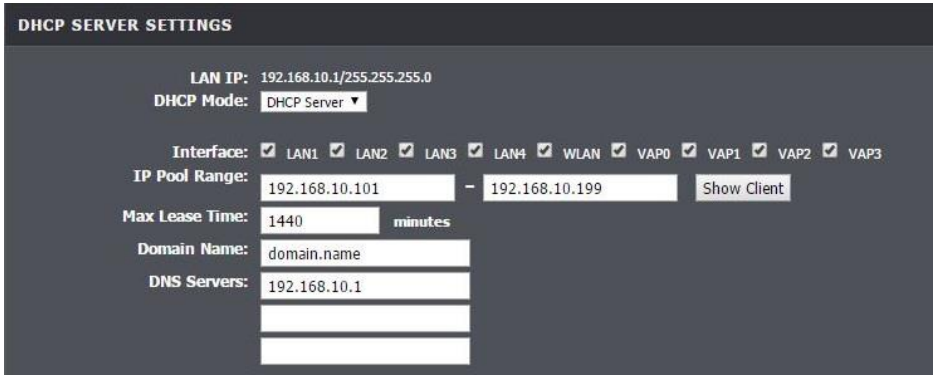
Note: *The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.*

Set up the DHCP server on your router

Setup > Local Network> DHCP Server

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

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



- **DHCP Mode:** Select the mode you wish to enable.
  - **DHCP Relay:** Select this option to enable
  - **DHCP Server:** Select this option to enable
- **Relay Server:** 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.*
- **IP Pool Range:** Enter the range of IP address to assign. The default value is 192.168.10.101 to 192.168.10.199.
- **Max 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 1440 minutes (1 day).
- **Domain Name**: Enter the domain name to connect to
- **DNS Server**: Enter the preferred and alternate DNS IP addresses.

Assign specific IP address to clients

Setup > Local Network > DHCP Reserved

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**, hover over **Local Network** and click on **DHCP Reserved**.
3. Review the DHCP Server settings.

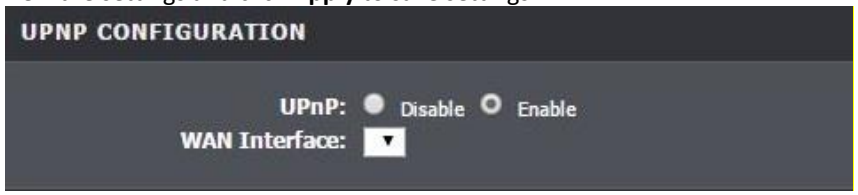
- **IP Address:** Enter the IP assigned IP address
- **MAC Address:** Enter the MAC address of the computer of client.

Enable/disable UPnP on your router

Advanced > Network Tools > 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 disabled on your router by default.

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



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

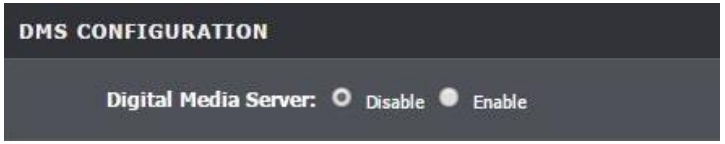
  Note: *It is recommended to leave this setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.*

Enable/disable DLNA

Advanced > Network Tools > DLNA

DLNA (Digital Living Network Alliance) allows your router to act as a bridge between various devices on your home network. With DLNA enabled, you can send various media from one device to the other (e.g. audio, videos, pictures, etc.)

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Advanced**, hover on **Network Tools** and click on **DLNA.**
3. Click **Enable** or **Disable** DLNA on your modem router.



Enable SNMP on your router

Advanced > Network Tools > 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.

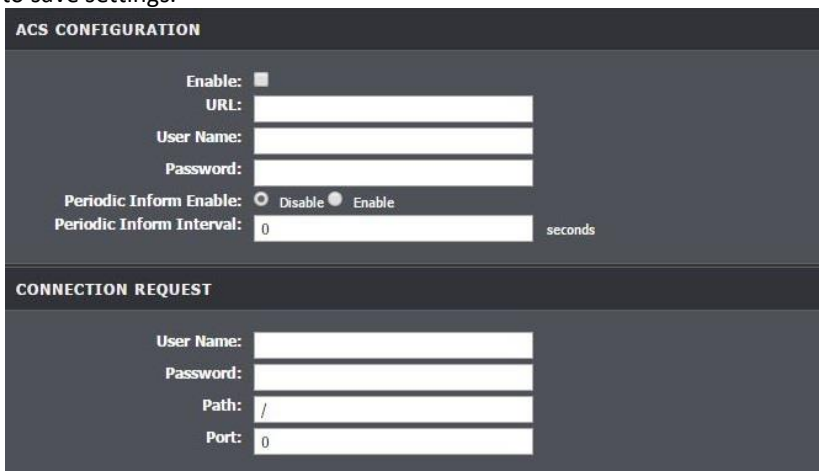
- **Enable SNMP:** Select to enable feature
- **System Contact:** Enter the contact of the system
- **System Name:** Enter the name of the system
- **System Location:** Enter the location of the system
- **Trap IP:** Enter the destination IP address of the SNMP trap.
- **Community name (read-only):** Enter the trap community name
- **Community name (read-write):** Enter the trap community name here

Enable TR-069 on your router

Advanced > Network Tools > TR-069

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 modem router management page (see "Access your router management page" on page 23).
2. Click on **Advanced** and click on **Network Tools** and then **TR-069**.
3. Please consult your ISP for the required TR069 settings for remote management. Click **Apply** to save settings.



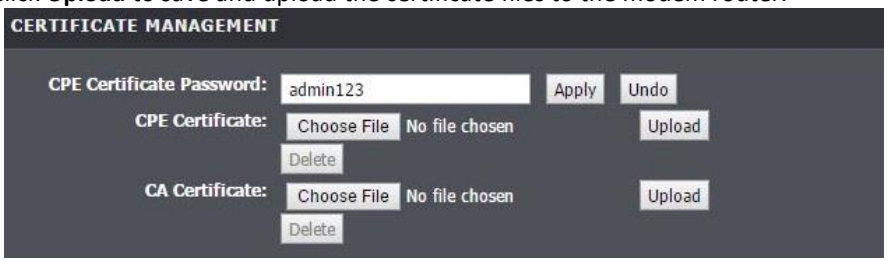
- **Enable:** Check this box to enable
- **ACS URL:** Enter the URL of the Auto-Configuration Server (ACS).
- **ACS User Name:** Enter the user name of your modem router when connecting to the ACS.
- **ACS Password:** Enter the password that your modem router should use when connecting to the ACS. Re-enter the password on the Confirm
- **Inform:** Check this box to enable
- **Periodic Inform Enable:** Select enable to enable
- **Periodic Inform Interval:** Enter the interval time of sending RPCs.
- **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.
- **Path:** Enter the path where the request will be sent to
- **Port:** Enter the port number

Trusted Certificates

Advanced > Network Tools > TR-069

CPE Certificates (CPE) and CA Certificates (CA) can be used 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 **TR-069**.
3. Click on **Browse** or **Choose File**. A separate file navigation window should open.
4. Navigate to the location of the **CPE** or **CA** Certification file.
5. Select the certification file and click **Open**. If prompted, click **Yes** or **OK**.
6. Click **Upload** to save and upload the certificate files to the modem router.



Blocking Applications

Advanced > Network Tools > Software Forbidden

This page lets you set the type of packets that can be passed through the modem router to the devices connected on the network.

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced**, hover on **Network Tools** and click on **Software Forbidden.**
3. Under **Add Forbidden Software**, select from one of the pre-defined selections.
4. Click **Add** to include the current selection into the list of restricted internet applications.

ARP Binding

Advanced > Network Tools > ARP Binding

ARP Binding is used for mapping an IP address to a device that is on the network.

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced**, hover on **Network Tools** and click on **ARP Binding.**
3. Input the **IP Address** and the **MAC address**
4. Click **Add** to save the entry.

Setting a Client Limit

Advanced > Network Tools > Client Limit

Setting a client limit can limit the number of devices that is connected to your modem router at a given time.

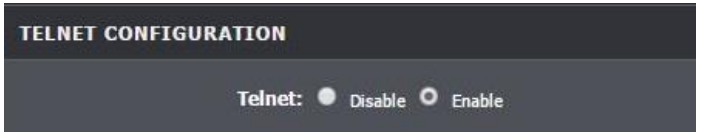
1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced**, hover on **Network Tools** and click on **Client Limit.**
3. Select **Enable** to enable a client limit.
4. Input the maximum number of devices that can be connected to the network at a given time.

Enable/disable Telnet

Advanced > Network Tools > Telnet

Telnet is a protocol that allows computers to access other computers/devices on the same network.

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced**, hover on **Network Tools** and click on **Telnet.**
3. Select **Enable** or **Disable** Telnet on your modem router.



Configure ALG settings

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

- **IPSEC Pass-through:** 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.
- **L2TP Pass-through:** Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate VPNs.
- **PPTP Pass-through:** 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.
- **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.
- **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.
- **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.

Configure NAT Forwarding settings

Advanced > NAT > NAT ALG

Setting up NAT Forwarding will allow incoming packets to be forwarded to a different IP address such as firewall or a router.

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced,** click on **NAT,** and click on **NAT Forwarding**.
3. Enter the **Remote IP Address,** and the **Local IP Address.**
4. Click **Apply Changes** to save the settings.

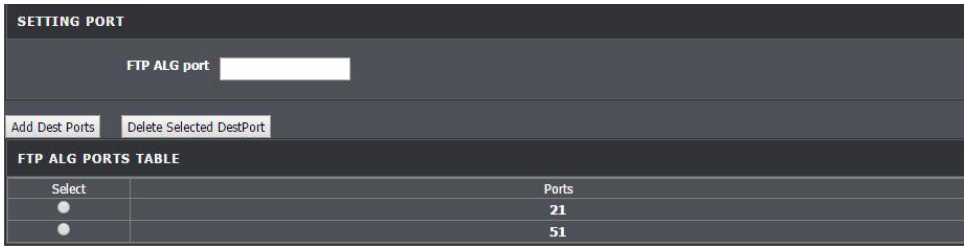
.

Configure FTP ALG Config

Advanced > NAT > FTP ALG Config

File Transfer Protocol (FTP) is a common protocol for exchanging files over IP networks.

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced,** click on **NAT,** and click on **FTP ALG Config**
3. Enter the port number in **FTP ALG port** and click on **Add Dest Ports** to save the port.
4. To remove a port from the **FTP ALG Ports Table**, select the port you wish to remove and click **Delete Selected DestPort** button.



Configure NAT IP Mapping

Advanced > NAT > NAT IP Mapping

Setting up NAT IP Mapping will allow remote access to your network with a specific IP address.

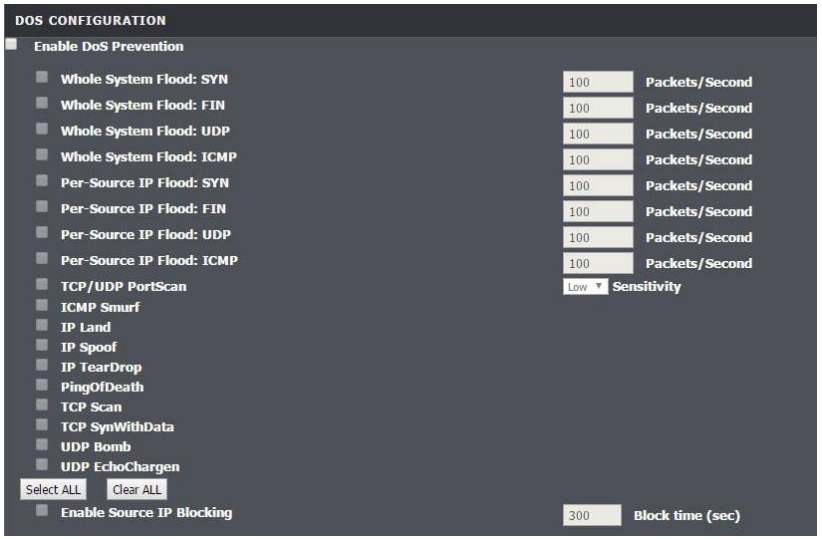
1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced,** click on **NAT,** and click on **NAT IP Mapping.**
3. Select the **Type** of NAT IP Mapping from the drop down menu.
4. Review and input the settings below and **Apply Changes** to save the settings.
   - **Local Start IP:** The start of the IP address range in your network
   - **Local End IP:** The end of the IP address range in your network
   - **Global Start IP:** The start of the public IP address that you are accessing from
   - **Global End IP:** The end of the IP address range that you are accessing from
5. To delete a setting that was setup, select the rule you wish to delete under **Action** and click **Delete Selected,** or to delete all the rules click **Delete all**.

Additional Security Settings

Advanced > DoS Settings

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

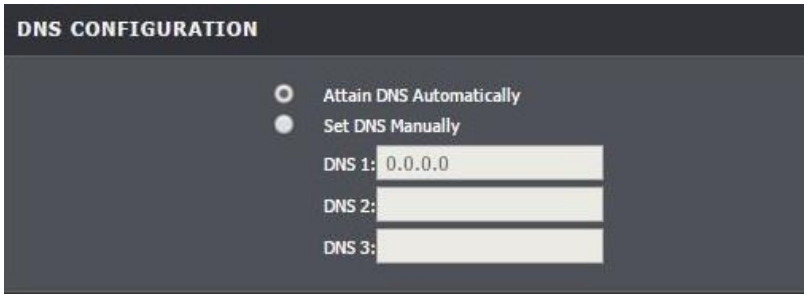
1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced** and click on **DoS Settings**.
3. Select **Enable DoS Prevention** to activate mode.
4. A complete list of added protection will appear. Select items to enable protection and click Apply Changes to save settings.



DNS

Advanced > DNS

1. Log into your modem router management page (see "Access your modem router management page" on page 23).
2. Click on **Advanced** and click on **DNS**.
3. Select **Set DNS Manually** to enable manual configuration of DNS relay.
4. Input the IP address in **DNS 1**, **DNS 2**, and **DNS 3**.
5. Click **Apply Changes** to save settings.



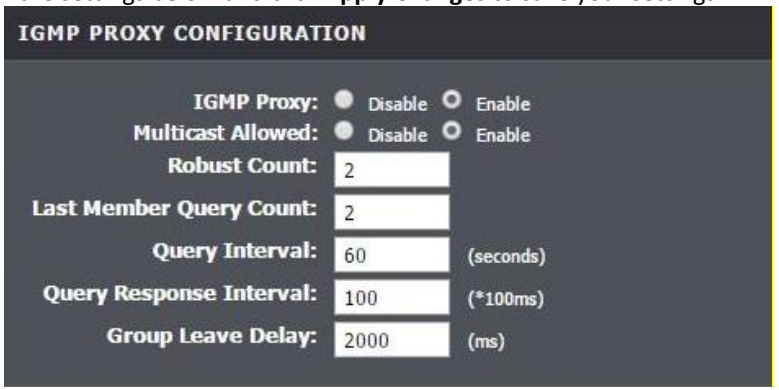
Allow/deny multicast streaming

Advanced > Network Tools > IGMP Proxy

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 Proxy

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

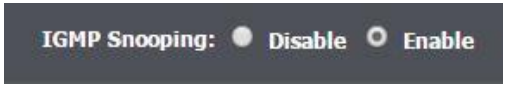


- **IGMP Proxy:** Select the Enable or Disable the IGMP Proxy
- **Multicast Allowed:** Select Enable or Disable
- **Robust Count:** Enter the query count
- **Last Member Query Count:** Enter last member query count
- **Query Interval:** Enter response query interval
- **Query Response Interval:** Enter response interval
- **Group Leave Delay:** Enter the delay interval

IGMP Snooping

Setup > Local Network > LAN Interface

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Setup**, click on **Local Network** and select **LAN Interface.**
3. Under Interface Settings, click **Enable** to enable IGMP Snooping. Click on **Apply Changes** to save your settings.

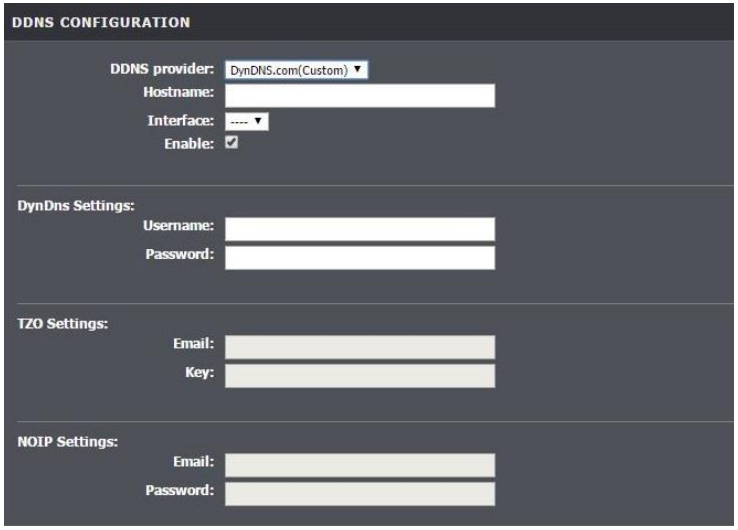


Identify your network on the Internet

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* ***DDNS provider*** *drop-down list.*

1. Sign up for one of the DDNS available service providers list under **DDNS provider**. (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 **Add**.

Allow remote access to your router management page

Advanced > Access Control List > Access Control List

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 **Advanced**, and click on **Access Control List**.

3. Under the **ACL Settings** section, enter a specific IP address and Netmask or enter 0.0.0.0 to allow any.
4. Uncheck the box **Any** to select the service from the selection.
5. Click **Add** to save your settings.

Open a device on your network to the Internet

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

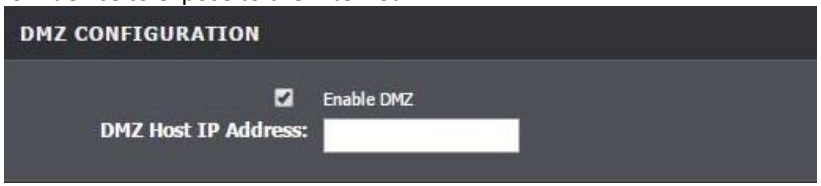
DMZ

Advanced > DMZ

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your modem 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 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.*

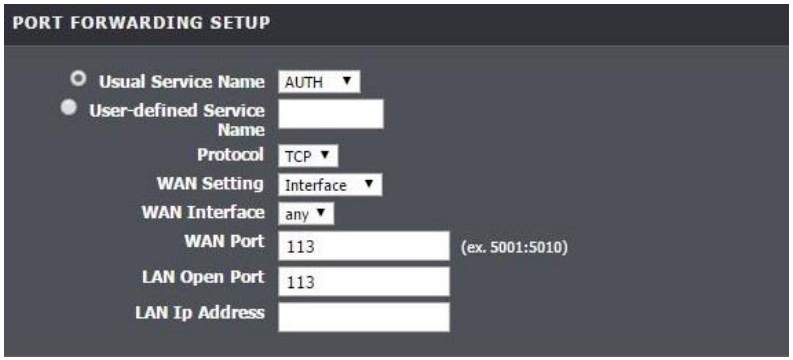
Port Forwarding

Advanced > 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**, and click on Port Forwarding**.**
   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 **Add** to save settings.



- **Usual Service Name:** Select the pre-defined WAN connection you are using from the drop down selection.
- **User=defined Service Name:** Enter the name of the rule.
- **Protocol Type:** Select the protocol to assign the rule.
- **WAN Interface:** Select the type of WAN setting
- **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)*.
- **WAN Port:** 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.
- **LAN Open 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.*

- **LAN IP Address:** 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.

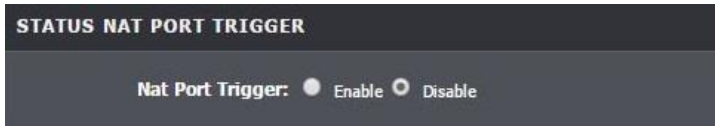
Port Trigger

Advanced > Port Triggering

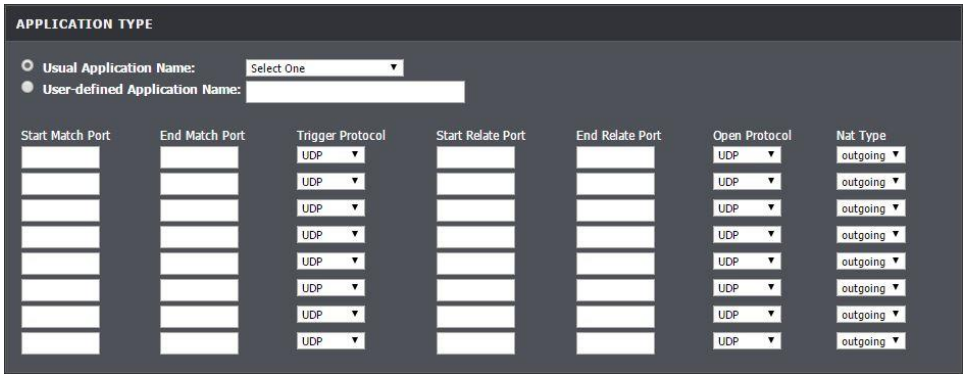
Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range 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 Changes** to save settings.



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



- **User Application Name:** Select from one of the pre-defined setups from the drop down menu.
- **User-defined Application Name:** Enter the name to assign rule.
- **Start / End Match Port:** 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
- **Start / End Relate Port:** Enter the public port to assign on the rule
- **Open Protocol:** Select the public protocol to apply on rule.
- **Nat Type:** Select whether the Nat Type is for **outgoing** or **incoming**.

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

Prioritize traffic using QoS (Quality of Service)

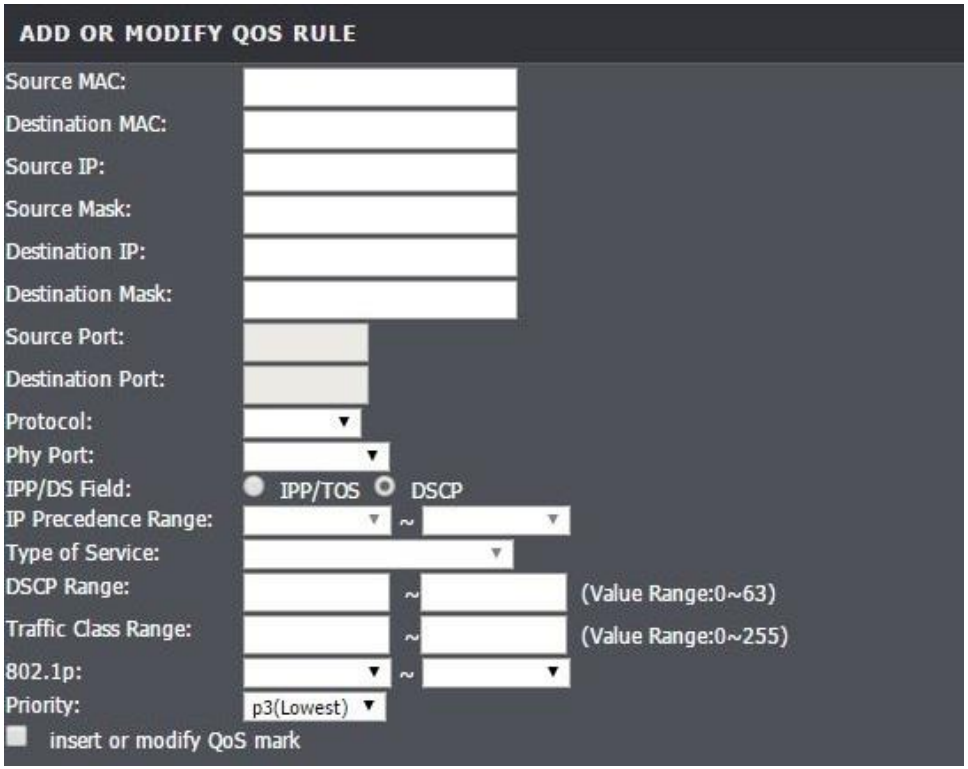
Advanced > Network Tools > IP QoS

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**, then click on **Network Tools** and click on **IP QoS.**
3. Click **enable** and click on **Apply** to turn QoS on.
4. Select the type of schedule mode for the rule.

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.

1. Click **Add Rule** to add and modify the 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 Mask:** Enter the destination and source network mask address to apply on the queue.
- **Destination/Source Port:** Enter the destination and source port to apply on the queue.
- **Protocol:** Select the protocol of the queue
- **Physical Ports:** Select the interface on the pull-down menu to implement this QoS queue.
- **IPP/DS Field:** Select either IPP/TOS or DSCP
- **IP Precedence Range**: Select in the pull-down menu the priority of the IP ranges.
- **Type of Service:** Select in the pull-down menu the application of the rule, values are preconfigured.
- **DSCP Range:** Select the DSCP range to apply
- **Traffic Class Range:** Select the Traffic Class Range to apply
- **802.1p Remark:** Select the queue range to apply
- **Priority:** Select the priority to apply for this Queue

Add static routes to your router

Advanced > Routing > 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. **Enable** static route, and review the settings.
4. Click **Add Route** or **Update** to save the settings.

- **Destination:** Enter the destination IP address.
- **Subnet Mask:** Enter the subnet mask
- **Next Hop:** Enter the gateway IP address.
- **Metric:** Enter a number to assign the route priority. The lower the number, the higher the route priority.
- **Interface:** Select the interface for the rule.

Enable dynamic routing on your router

Advanced > Routing > 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 Interface to configure then select appropriate dynamic routing protocol and version communicate with other routers. Click **Apply** to save settings.

- **RIP1:** 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.
- **RIP2:** 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

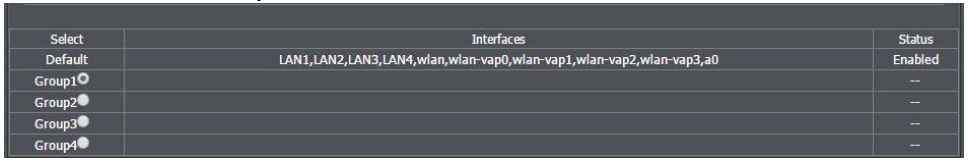
Setup Port Mapping

Advanced > Network Tools > 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.

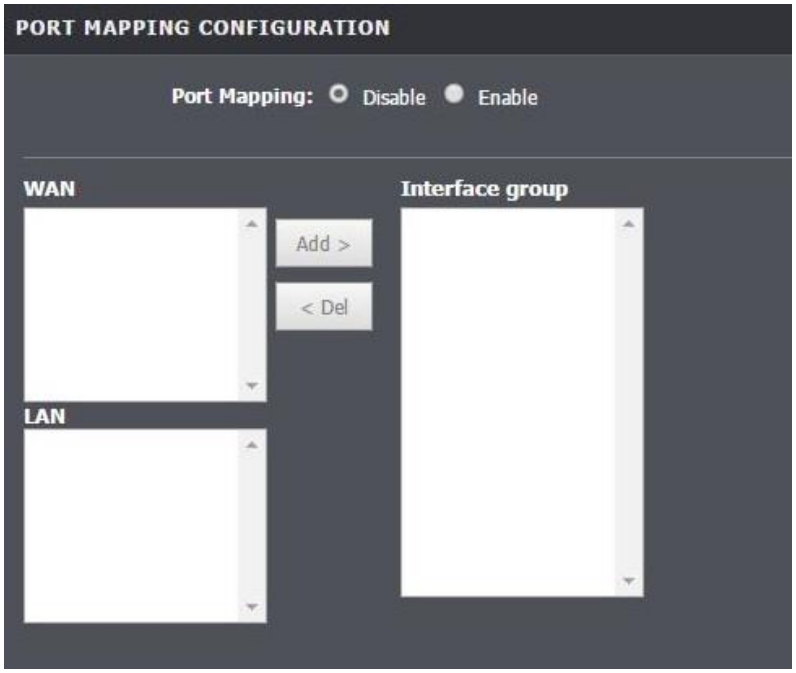
By default, all interfaces belong to the Default group. You can create new groups and move interfaces to other groups. However, an interface can only be a member of one group.

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 **Enable**.
4. Select the **New Group** to edit.

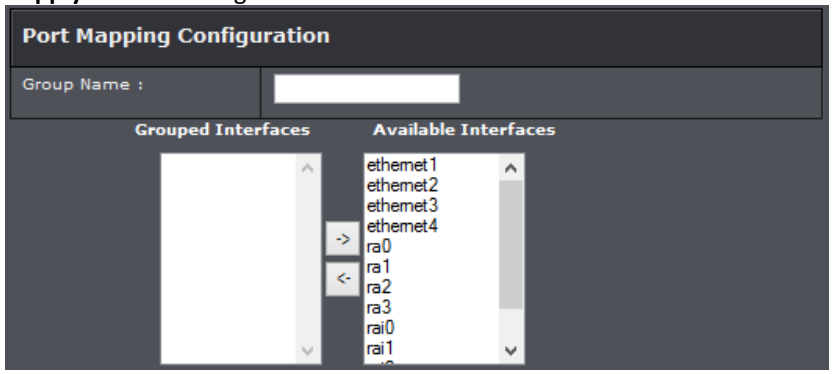


Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3,a0	Enabled
Group1		--
Group2		--
Group3		--
Group4		--

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

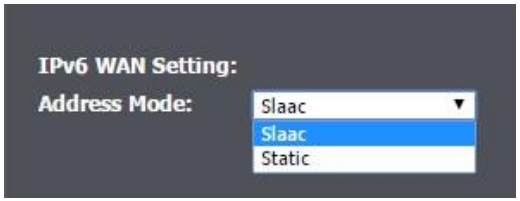
Setup > Internet Setup > Channel Config

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 **Setup**, then select **Internet Setup**, and click on **Channel Config**.
4. Select your IPv6 WAN type and complete the fields required by your ISP. Click Apply to save settings.



Configure ADSL settings

Setup > Internet Setup > ADSL Settings

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 **Setup**, click on **Internet Setup** and click on **ADSL Settings**.
4. Select the fields required by your ISP. Click Apply to save settings.

ADSL modulation :	☐G.Lite ☑G.Dmt ☑ADSL2 ☑ADSL2+ ☑ANSI(T1.413)
AnnexL Option :	☐ Enabled (Note: Only ADSL 2 supports Annex L)
AnnexM Option :	☐Enabled (Note: Only ADSL 2/2+ support Annex M)
G.INP Option :	☐Enable
ADSL Capability :	☑Bitswap Enabled ☑SRA Enabled
ADSL Last Mode First :	☐Enable

Using 3G WAN Connection

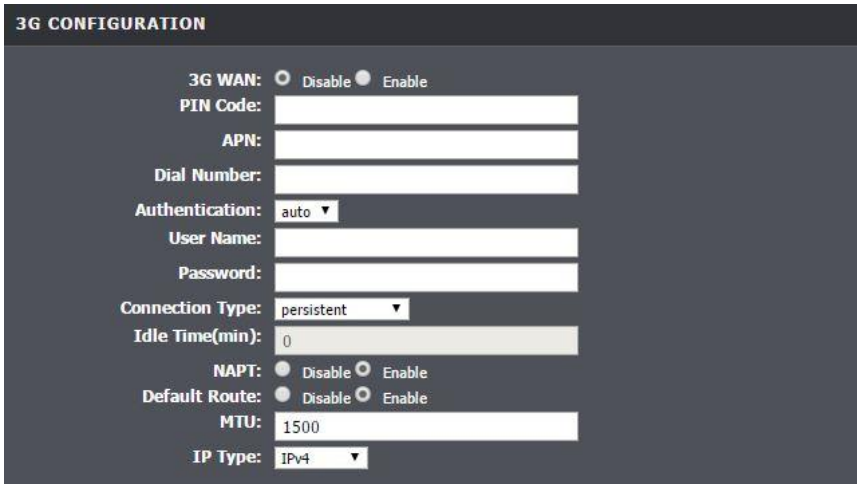
Your router's USB port can be used to connect a 3G USB dongle for 3G WAN connection. This can be beneficial when you have access to only a 3G WAN internet

Configure 3G WAN

Advanced > Network Tools > 3G Backup

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 you are still having 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 **Enable 3G WAN** to have the device automatically input required settings. Click **Apply** to save settings.



Router Maintenance & Monitoring

Reset your router to factory defaults

Maintenance > System

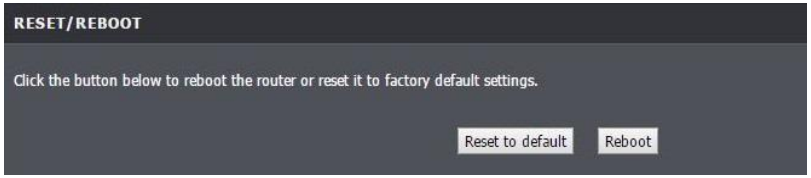
You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration 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 **Reset/Reboot**, click **Reset to default**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	admin
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless	Enabled
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

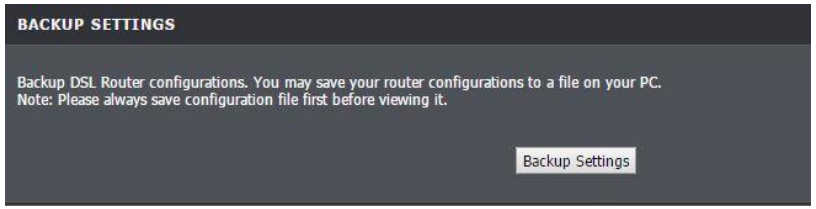
Backup and restore your router configuration settings

Maintenance > System

You may have added many customized settings to your router and in 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 modem router configuration file.

To back up your modem router configuration:

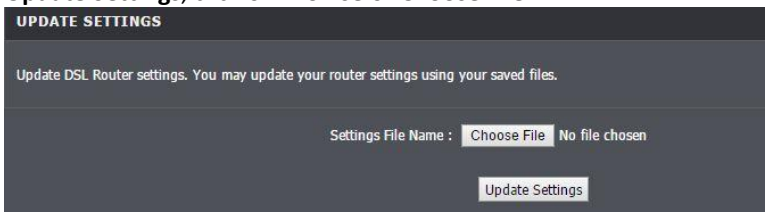
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** and click **System**.
3. Click **Backup Settings**.



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 File Type: *.cfg)*
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 **Maintenance,** and click **System**.
3. Under **Update Settings**, click on **Browse** or **Choose File**.



A separate file navigation window should open.

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

Upgrade your modem router firmware

Maintenance > Firmware Update

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet modem 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 under **Status** and **Device Info**. 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.

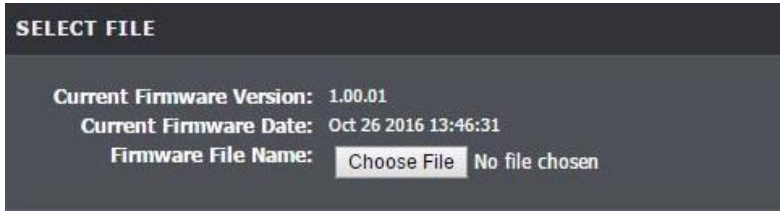
1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

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 modem 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. Click **Update Firmware** to start the firmware upgrade process. If prompted, click **yes** or **OK**.

Restart your router

Maintenance > System

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

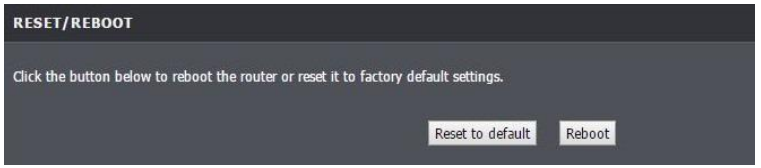
There are two methods that can be used to restart your router.

- **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 **Reset** to restart the router. If prompted, click **yes** or **OK**.



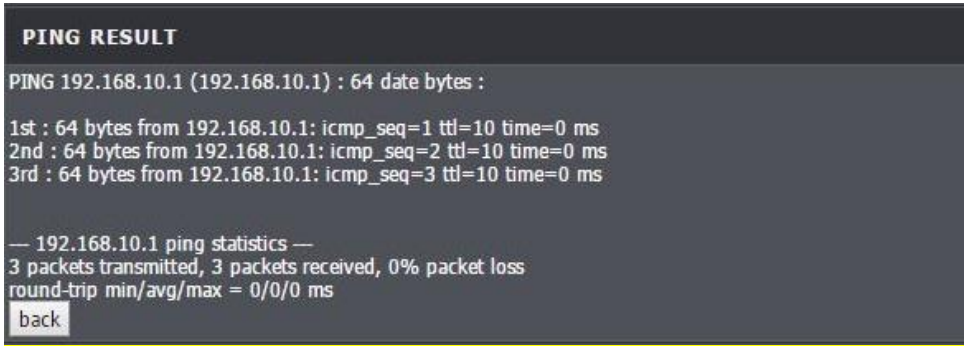
Check connectivity using the router management page

Maintenance > Diagnostic > 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**, 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.

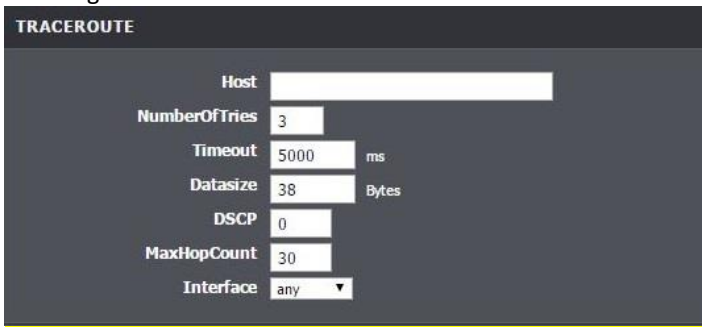


Traceroute Diagnostic

Maintenance > Diagnostics > Traceroute

Traceroute shows the pathway to a connected device on the network.

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** click on **Diagnostics,** and click on **Traceroute**
3. Review the settings and click **traceroute** to start the trace.



Check ADSL Connection using the router management page

Maintenance > Diagnostics > ADSL

Traceroute shows the pathway to a connected device on the network.

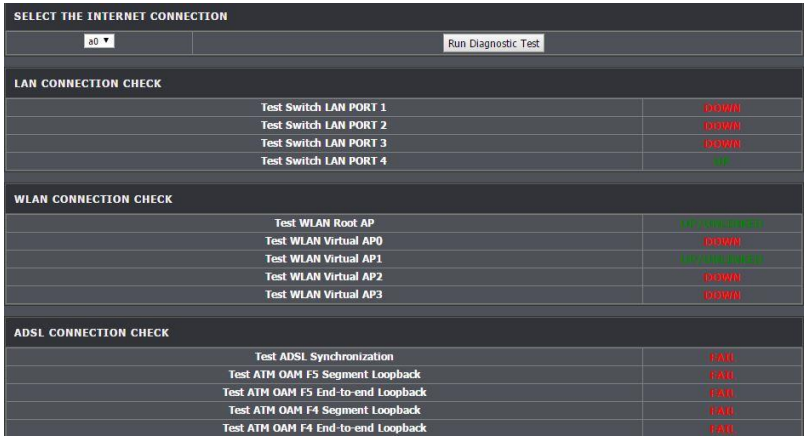
1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance,** click on **Diagnostics,** and click on **ADSL.**
3. Click the **Start** button to start running the ADSL Diagnostic Test. This test will take about 3 minutes to complete.

Check Internet connectivity using the router management page

Maintenance > Diagnostics > Diag Test

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,** click on **Diagnostics,** and click on **Diag Test**.
3. Select your DSL interface and click **Run Diagnostic Test**.



Check the router system information

Status > Device Info

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	
Alias Name	N300 WiFi ADSL 2+ Modem Router
Firmware Version	1.00.01
Uptime	0 4:46:56
Date/Time	Thu Jan 1 4:46:56 1970
Built Date	Oct 26 2016 13:46:31
Serial Number	F4A1B2C3D400

- **Alias Name:** Displays the product description
- **Firmware Version:** Displays the firmware version currently loaded on the router
- **Uptime:** Time duration of modem up time
- **Date/Time:** Time of router
- **Built Date:** Date of when the Firmware was created
- **Serial Number:** Displays the modem router's serial number

- **Modem Vendor:** Displays modem vendor
- **Modem OUI:** Displays modem OUI
- **Modem Serial Number:** Serial number of modem

DSL

DSL	
Operational Status	--
Upstream Speed	--
Downstream Speed	--

- **Operational Status:** Displays the current status of the modem
- **Upstream Speed:** Displays the upstream data rate
- **Downstream Speed:** Displays the downstream data rate

LAN Status

LAN CONFIGURATION	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	F4:A1:B2:C3:D4:00

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

Wireless Info

WIRELESS INFO	
Status:	Enabled
MAC Address:	F4:A1:B2:C3:D4:00
Network Name (SSID):	TRENDnet723-99U0
Current Channel:	2
Encryption:	WPA2/AES

- **Status:** Current wireless status
- **MAC Address:** Wireless MAC address
- **Network Name (SSID):** Wireless network name
- **Current Channel:** Wireless channel
- **Encryption:** Wireless encryption of security

DNS Status

DNS STATUS	
DNS Mode	Auto
DNS Servers	
IPv6 DNS Mode	Auto
IPv6 DNS Servers	

- **DNS Mode:** The current DNS mode
- **DNS Servers:** Current DNS server settings
- **IPv6 DNS Mode:** IPv6 DNS mode
- **IPv6 DNS Servers:** Current IPv6 DNS server settings

Check the modem router ADSL status

Status > ADSL Driver

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 Driver**.
3. Review the device information.

ADSL	
Adsl Line Status	ACTIVATING.
Adsl Mode	--
Channel Mode	--
upstream	--
downstream	--
Attenuation downstream	--
Attenuation upstream	--
SNR Margin downstream	--
SNR Margin upstream	--
Firmware Version	4926e708
CRC Errors	--
upstream BER	--
downstream BER	--
Up Output Power	--
Down Output Power	--
ES	--
SES	--
UAS	--

Check the router Wireless clients

Status > Wireless Clients

This page displays all connected wireless clients.

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

ACTIVE WIRELESS CLIENT TABLE					
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
0c:8b:fd:91:06:4f	4262	2208	71.5	no	300

Check the router Routing Table

Status > DHCP Clients

This page displays the assigned IP address, MAC address and the expiration time for each DHCP leased client.

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

Name	IP Address	MAC Address	Expiry	Type
DESKTOP-SC7AL57	192.168.10.101	0c:8b:fd:91:06:4f	In 0 days 21:50:01	Automatic
DESKTOP-SC7AL57	192.168.10.102	08:9e:01:f6:18:b3	In 0 days 23:58:47	Automatic

Check the router Routing Table

Status > Route Info

This page displays all connected clients.

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

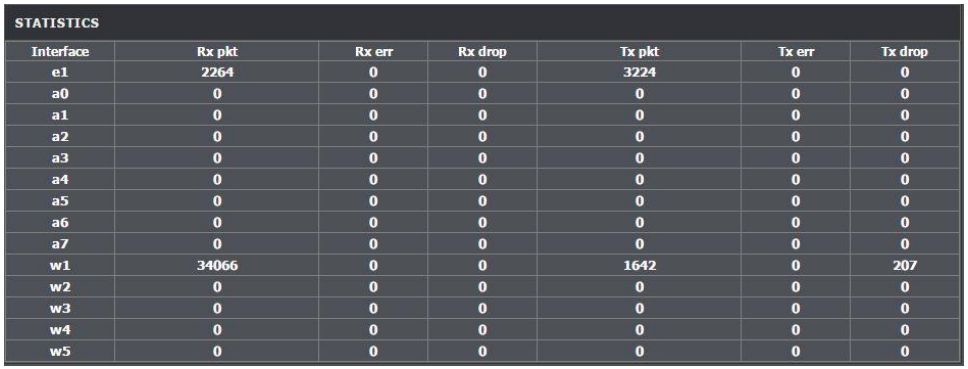
CURRENT IP ROUTING TABLE			
Destination	Subnet Mask	NextHop	Interface
192.168.10.1	255.255.255.255	*	e1

Check the router Basic Statistics

Status > Statistics

This page displays all connected clients.

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



STATISTICS

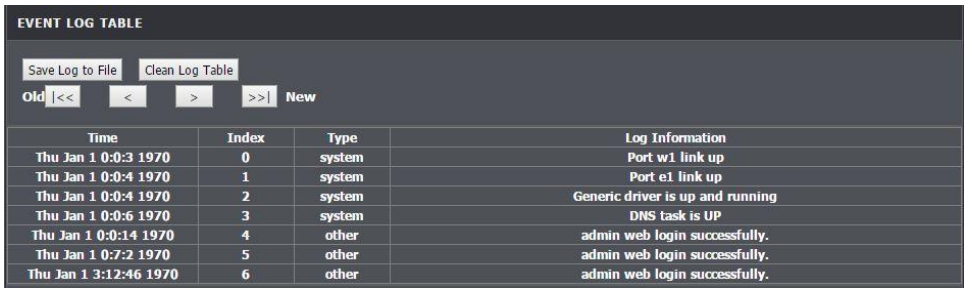
Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
e1	2264	0	0	3224	0	0
a0	0	0	0	0	0	0
a1	0	0	0	0	0	0
a2	0	0	0	0	0	0
a3	0	0	0	0	0	0
a4	0	0	0	0	0	0
a5	0	0	0	0	0	0
a6	0	0	0	0	0	0
a7	0	0	0	0	0	0
w1	34066	0	0	1642	0	207
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0

View your router log

Maintenance > System Log

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

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Maintenance**, and click on **System Log**.
3. Review the device log information. You can filter the log view by selecting **Error**, or **Notice** option.



EVENT LOG TABLE

Save Log to File | Clean Log Table

Old |<< < > >>| New

Time	Index	Type	Log Information
Thu Jan 1 0:0:3 1970	0	system	Port w1 link up
Thu Jan 1 0:0:4 1970	1	system	Port e1 link up
Thu Jan 1 0:0:4 1970	2	system	Generic driver is up and running
Thu Jan 1 0:0:6 1970	3	system	DNS task is UP
Thu Jan 1 0:0:14 1970	4	other	admin web login successfully.
Thu Jan 1 0:7:2 1970	5	other	admin web login successfully.
Thu Jan 1 3:12:46 1970	6	other	admin web login successfully.

- **Save Log to File:** Downloads and saves the log on to your computer.
- **Clean Log Table:** Clears log entries.
- **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.

Router Management Page Structure

Setup

- Wizard
- Local Network
  - LAN Interface
  - LAN IPv6 Interface
  - DHCP Server
  - DHCP Reserved
- Internet Setup
  - Channel Config
  - ATM Settings
  - ADSL Settings
  - PVC Auto Search
- Wireless Setup
  - Wireless Basics
  - Wireless Security
- Time and Date

Advanced

- Advanced Wireless
  - Wireless Advanced
  - Access Control
  - WPS
  - MBSSID
- Access Control List
  - Access Control List
  - IPv6 Access Control List
- Port Triggering
- Port Forwarding
- DMZ
- Parental Controls
  - URL Block
  - MAC Block
  - Schedules
- Filtering Options
  - IP/Port Filter
  - IPv6/Port Filter
  - MAC Filter
- DoS Settings
- DNS
  - DNS
  - IPv6 DNS
- Dynamic DNS
- Network Tools
  - Port Mapping
  - IGMP Proxy
  - IP QoS
  - UPnP
  - DLNA
  - SNMP
  - TR-069
  - Software Forbidden
  - ARP Binding
  - Client Limit
  - 3G Backup
  - Telenet
- Routing
  - Static Route
  - IPv6 Static Route
  - RIP
- NAT
  - NAT ALG
  - NAT Forwarding
  - FTP ALG Config
  - NAT IP Mapping

Maintenance

- System
- Firmware Update
- Password
- Diagnostic
  - Ping
  - Ping6
  - Traceroute
  - ADSL
  - Diag Test
- System Log

Status

- Device Info
- Wireless Clients
- DHCP Clients
- ADSL Driver
- Statistics
- Route Info

Technical Specifications

ADSL Interface Standards

- ADSL: ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt, Annex A, and Annex B), ITU G.992.2 (G.lite)
- ADSL2: ITU G.992.3 (G.dmt.bis, Annex I, Annex J, and Annex L)
- ADSL2+: ITU G.992.5 (Annex L and Annex M)

Standards

- IEEE 802.3
- IEEE 802.3x
- IEEE 802.3u
- IEEE 802.3az
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (2.4 GHz up to 300 Mbps)

Hardware Interface

- 4 x 10/100 Mbps LAN ports
- 1 x RJ-11 ADSL2/2+ port
- 1 x USB 2.0 port (3G USB Modem Backup**)
- WPS button
- WLAN on/off button
- On/Off Power button
- Reset button
- LED indicators

ATM & PPP Modes/Protocols

- VC and LLC multiplexing (Up to 8 PVCs)
- 802.1Q VLAN tagging
- 1483 Bridged
- 1483 MER (IPv4 & IPv6 Static or DHCPv4/Auto-configuration (SLAAC/DHCPv6)
- 1483 Routed (IPv4 & IPv6 Static or DHCPv4/Auto-configuration (SLAAC/DHCPv6)
- PPPoE (IPv4 & IPv6 Static or DHCPv4/Auto-configuration (SLAAC/DHCPv6)
- PPPoA (IPv4 & IPv6 Static or DHCPv4/Auto-configuration (SLAAC/DHCPv6)
- IPoA (IPv4 & IPv6 Static or DHCPv4/Auto-configuration (SLAAC/DHCPv6)

Special Features

- IPv6 Support
- 5 dBi Antennas
- Multi-Language interface: English, Spanish, Portuguese
- Pre-encrypted wireless network

Access Control

- Wireless encryption: WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise (RADIUS)
- Wireless Access Control (IPv4/IPv6) Inbound/Outbound: HTTP, FTP, SNMP, SSH, FTP, Telnet, TFTP, ping or all services
- Up to 4 additional SSIDs
- Firewall: NAT, NAPT, SPI, Port Forwarding, Port Mapping, Port Triggering, DMZ Host,
- IPv4 & IPv6 Inbound/Outbound Port filter and MAC address Inbound/Outbound filter
- ALG: FTP, H.323, SIP, RTSP, PPTP/L2TP/IPsec VPN Passthrough
- Parental Control: Schedule URL/Keyword and/or MAC Address filters
- DoS Attack Prevention
- IP to MAC Address Binding (Static ARP)
- Client limiting for devices accessing Internet
- NAT IP Mapping: One-to-One, Many-to-One, Many-to-Many, One-to-Many

Quality of Service

- WMM
- Diffserv/Differentiated Services Code Point (DSCP) – Strict Priority (SP), Weighted Fair Queuing (WFQ)
- ATM Traffic QoS Constant Bit Rate (CBR), Unspecified Bit rate (UBR), Real-Time Bit Rate (rt-VBR), Non-Real-time Variable Bit Rate (nrt-VBR)

Management & Monitoring

- Local/remote web based management
- Telnet
- TR-069
- IGMP v1/2/3 Proxy and Snooping
- SNMP v1/2c
- DHCP Server/Relay, Option 60
- IPv4/IPv6 Static Routes & Dynamic RIPv1/2
- Syslog
- UPnP
- IPv4/IPv6 ping, traceroute, ADSL & diagnostic connectivity tests
- Upgrade firmware
- Backup/restore configuration

- Reboot
- Restore to factory defaults
- Dynamic DNS support for dyn.com and no-ip.com

Frequency

- 2.412 - 2.484 GHz

Modulation

- 802.11b: CCK (11 Mbps & 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
- 802.11g: OFDM with BPSK, QPSK and 16/64-QAM
- 802.11n: BPSK, QPSK, 16-QAM, 64-QAM with OFDM

Media Access Protocol

- CSMA/CA with ACK

Antenna Gain

- 2 x 5 dBi external adjustable

Wireless Output Power

- 802.11b: FCC: 18 dBm (max.) @ 11 Mbps
- 802.11g: FCC: 15 dBm (max.) @ 54 Mbps
- 802.11n: FCC: 14 dBm (max.) @ 300 Mbps

Receiving Sensitivity

- 802.11b: -79 dBm (typical) @ 11 Mbps
- 802.11g: -65 dBm (typical) @ 54 Mbps
- 802.11n: -61 dBm (typical) @ 300 Mbps

Wireless Channels

- FCC: 1-11
- ETSI: 1-13

Power

- Input: 100 – 240 V AC, 50 - 60 Hz
- Output: 12V DC, 1A external power adapter
- Consumption: 7W max.

Operating Temperature

- 0 – 40 °C (32 – 104 °F)

Operating Humidity

- Max. 95% non-condensing

Certifications

- CE
- FCC

Dimensions

- 165 x 122 x 40 mm (6.5 x 4.8 x 1.57 in.)
- Antenna length: 195 mm (7.7 in.)

Weight

- 234 g (8.3 oz.)

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 7/8/8.1/10

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/7/8/8.1/10

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 7/8/8.1/10

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 7/8/8.1/10

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-723BRM – 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