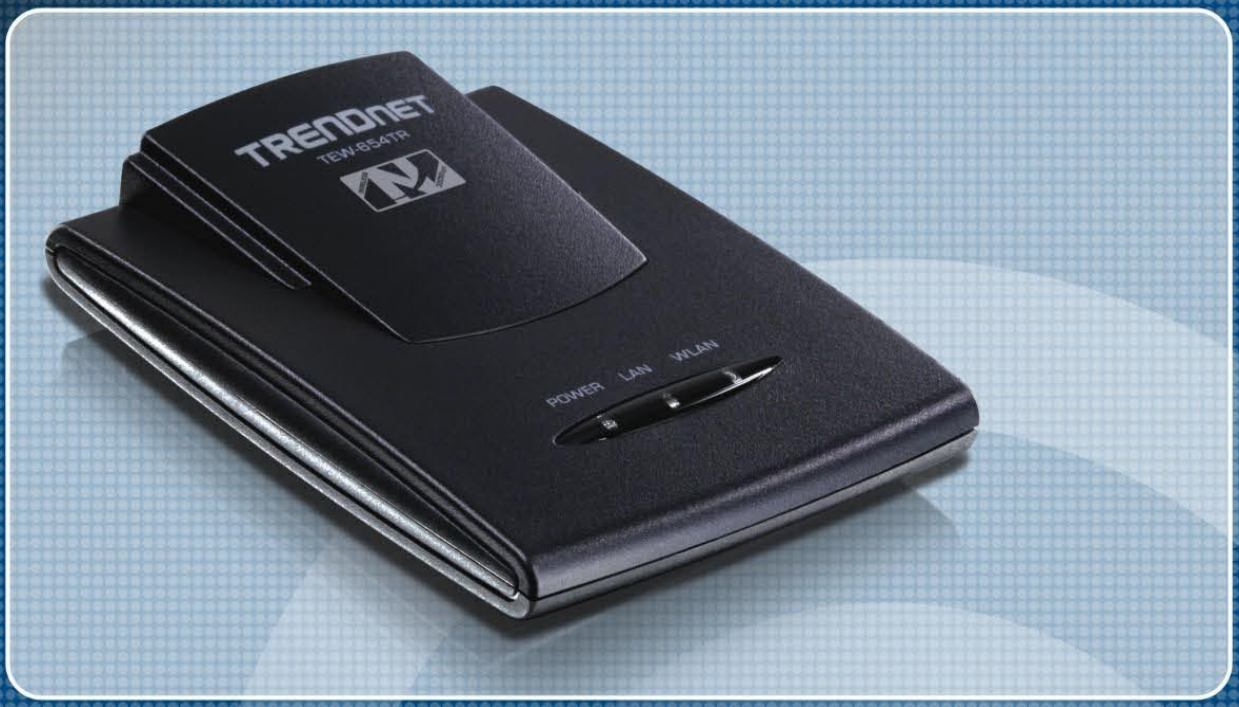
TRENDnet®



User's Guide

TEW-654TR

1.01

Contents

CHAPTER 3: CLIENT MODE

CHAPTER 4: ROUTER MODE

1 Product Overview

Congratulations on your purchase of the 3-in-1 Travel Router. The Travel Router functions as an Access Point for wireless connections, an Access Point Client for wired devices to have wireless connections, and a Router to share resources such as computers, printers, files and other devices.

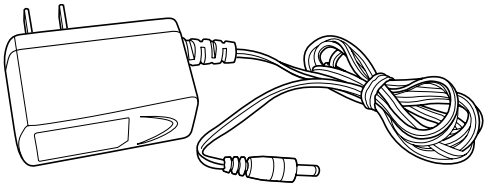
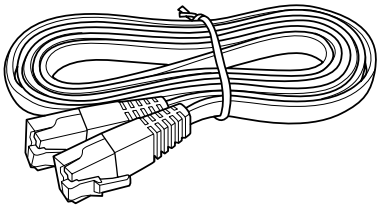
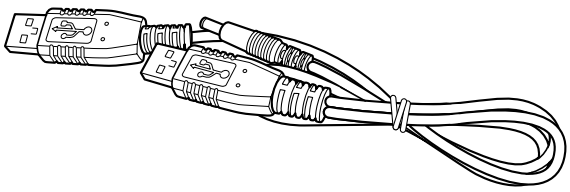
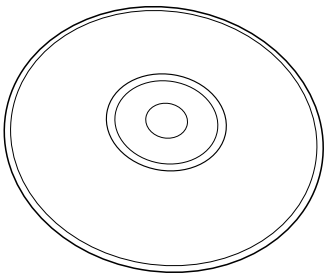
This User Manual will guide you on how to install and set up the Travel Router. Read it carefully and keep it for future reference.

1.1 Features

- 3-in-1 Operation Mode: Supports AP, Router, and AP Client modes
- Smallest Networking Device
- Fast Wireless Networking: Provides fast data rate connection up to 300Mbps for 802.11n devices
- Full range compatibility: Compatible with IEEE 802.11n, 802.11g, 802.11b and 802.3u devices
- Low Power Consumption: Consumes less than 2.5 watts
- USB Bus Powered: Provides better mobility.
- Quick and Easy Setup with Web-based Management Utility
- Strong Network Security - Supports the following features:
  - → WPA, WPA-PSK, WPA2, and WPA2-PSK security standars
  - → WPS button for Wi-Fi WPS configuration
  - → PPPoE/PPTP/L2TP protocol for DSL connections
  - → Firewall protection

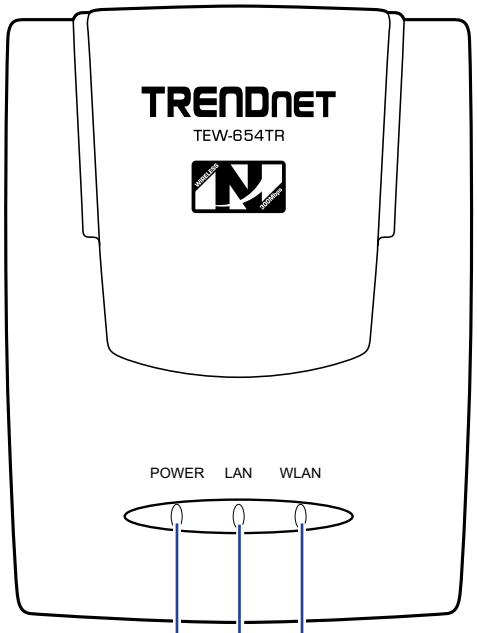
1.2 Package Contents

Check if your package comes with the following items. If any of them is missing or appears damaged, please contact your retailer.

	
Travel Router	Pouch
	
Power Adapter	Ethernet Cable
	
USB Power Cable	CD-ROM

1.3 Hardware Overview

1.3.1 LED Indicators



Power LED
Lights when the power is connected.

LAN / WAN LED

GREEN (solid)

- Lights when LAN/WAN port is connected to a DSL or cable modem successfully.

GREEN (blinks)

- Blinks when transmitting or receiving data through the LAN / WAN connection.

WLAN / WPS LED
Flashes to indicate activity.

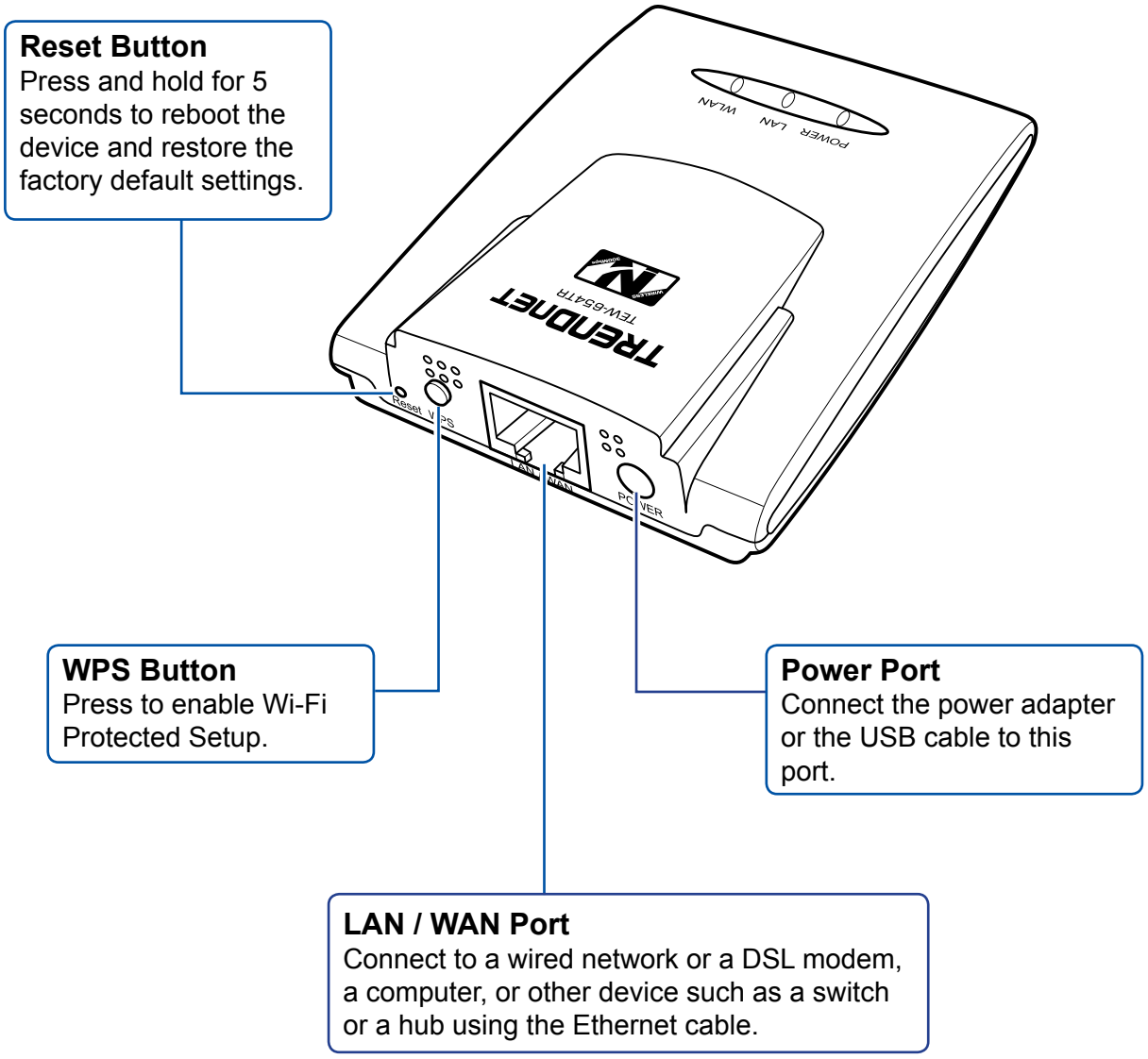
GREEN

- Blinks when a wireless device is connected.
- Blinks when data transfer is in progress.

AMBER

- Blinks when WPS is enabled.

1.3.2 Connectors



Note:

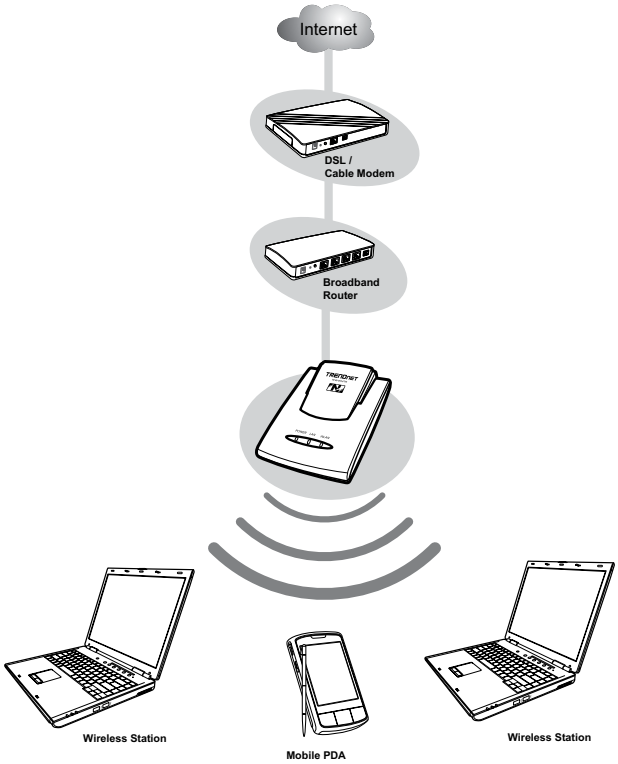
A wireless network normally requires a network name (SSID) and WPA security key to prevent unwanted access to the network. This process requires users to have knowledge of WiFi devices and their configurations. But with WPS enabled, the network name (SSID) and WPA security key of the devices are automatically configured.

1.4 Travel Router Modes

Before using the travel router, determine the type of mode you want to use:

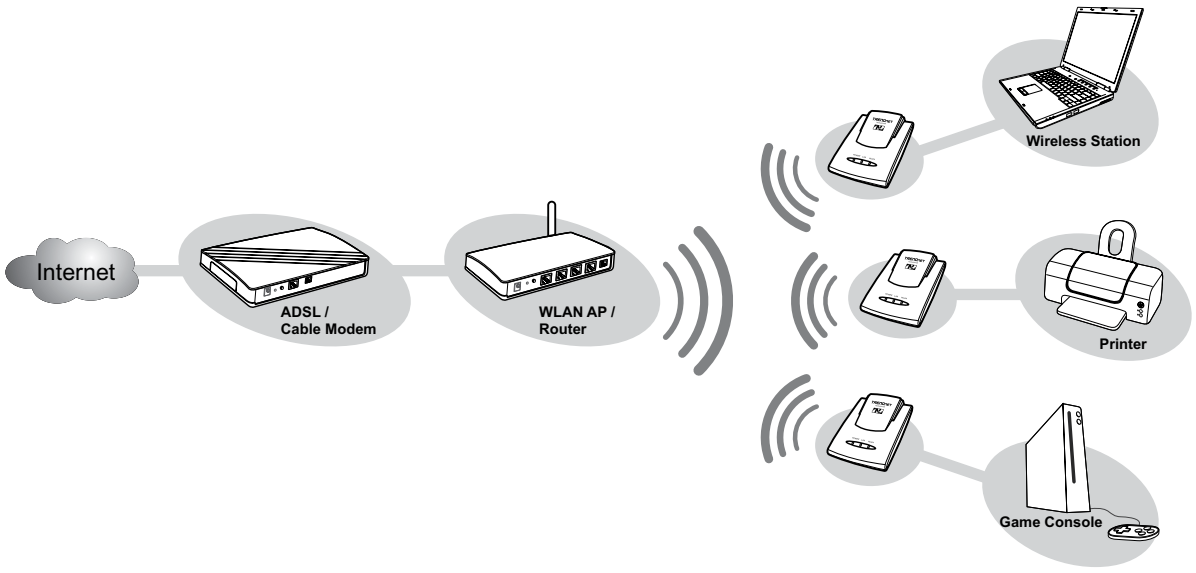
- **Access Point (AP) Mode**

  With AP mode, you can use the travel router as an access point for wireless clients to connect to the local area network (LAN) and to other wireless clients.



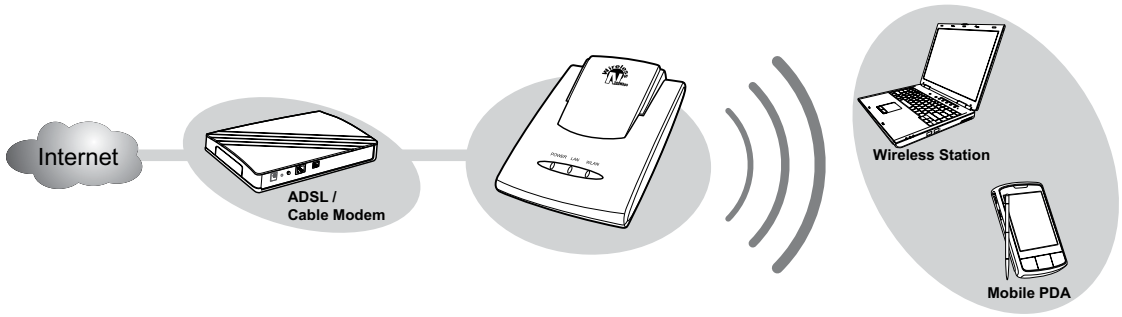
- **Client Mode**

  Switch to this AP-Client mode to connect a device to the travel router using an RJ-45 cable and use the travel router as a wireless adapter. This mode enables the Ethernet-connected device to have wireless function over a network.



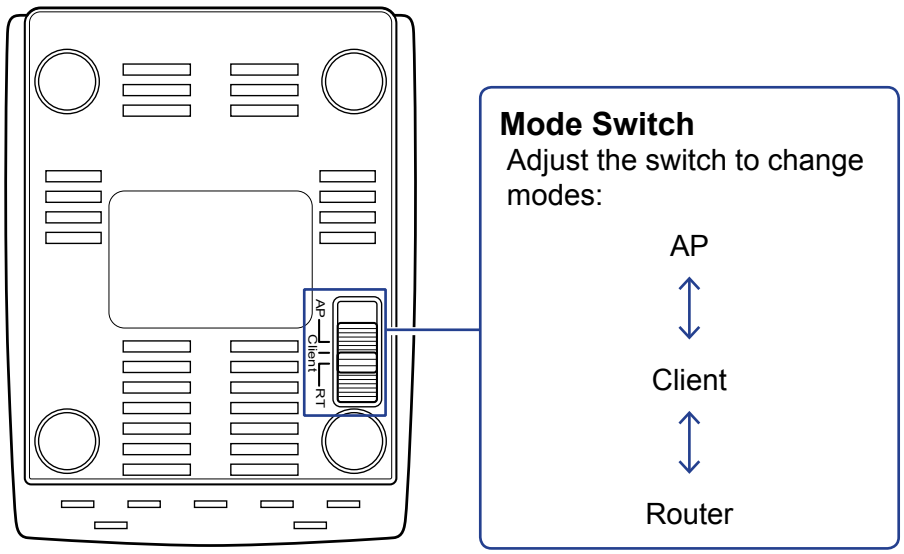
- **Router Mode**

  Use this mode to connect the travel router to a DSL or cable modem. With this mode, wireless clients connect to the Internet through the travel router using one account and one IP address.



1.4.1 Setting the Operating Mode

Use the mode switch at the bottom of the travel router to set the operating mode



1. Unplug the power source (power adapter or USB cable) if it is connected.
2. Adjust the switch to desired mode.
3. Re-connect the power source to the power port.

Note:

Make sure to unplug the power source from the power port first before switching modes.

1.5 Making Connections

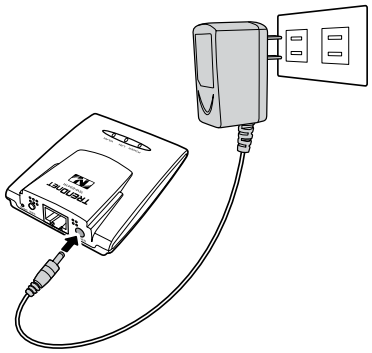
There are two ways to power up your device:

- By using the included power adapter
- By using the computer's USB ports with the included USB cable

1.5.1 Connecting the Power Adapter

Use the power adapter to directly connect to a power outlet.

1. Connect the power adapter to the power port of the travel router.
2. Plug the power adapter to an outlet or power strip.

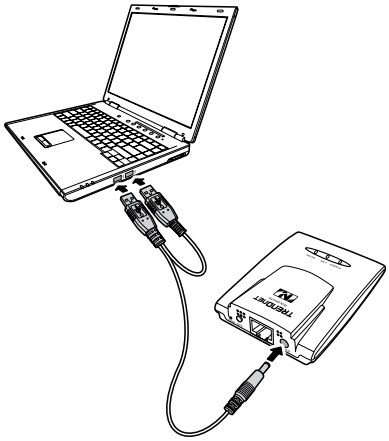


1.5.2 Connecting the USB Power Cable

Some computers have over-current protection capability. This means that when the current of a USB port goes over 500mA, the connected device will not be accessed by the computer. To avoid this risk, use the USB power cable supplied with your travel router.

To connect, follow the steps below:

1. Power up the computer.
2. Connect the two USB connectors to the computer's USB ports.
3. Connect the power jack to the travel router.



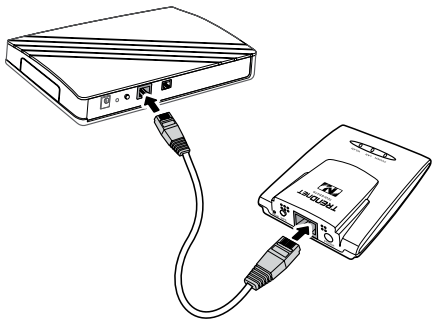
Note:

Make sure you connect the USB power cab to the computer first before connecting the travel router.

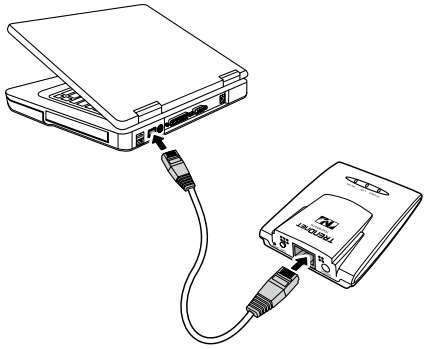
1.5.3 Connecting the Ethernet Cable

Use the Ethernet (RJ-45) cable to connect to a computer for wired connection or connect to a DSL or cable modem for internet connection.

1. Connect one end of the Ethernet cable to your computer or a DSL or cable modem.
2. Plug the other end to the LAN port of the travel router.



DSL / Cable modem connection



Wired computer connection

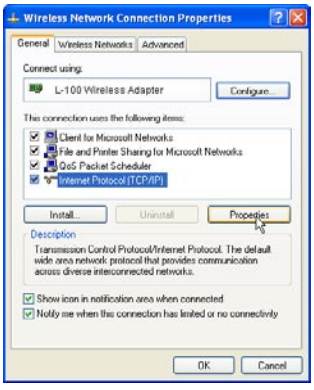
1.6 System Requirements

- Operating systems: Windows XP, Vista
- Microsoft Internet Explorer 5.5 or higher
- At least one RJ-45 Ethernet network

1.6.1 Configuring Connections

To properly detect the connections, configure your computer's network settings first. The following instructions are based on Windows XP. Non-Windows XP users will see similar screens.

1. For Windows XP, click **Start** > **Control Panel** > **Network Connections**. Right click on a connection, then select **Properties**.
2. Highlight **Internet Protocol (TCP/IP)**, then click **Properties**.
3. Click **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
4. Click **OK** and **OK** again.



2

AP Mode

With AP mode, you can use the travel router as an access point of your wireless device.

Before You Begin

Checklist

√ A valid network or Internet connection.

√ A DSL / cable modem provided by the ISP as part of the broadband connection installation.

√ A broadband router that connects to the DSL / cable modem for internet connection sharing.

You need to connect...

- Connect the travel router to your router or network that has a DHCP server. The travel router will obtain an IP address from the network automatically. Connect the LAN port of the travel router to the LAN port on your network then plug in the power adapter.
- Use wireless computers to connect to the ravel router (default SSID TRENDnet654).

2.1 Installation

Network Diagram

1 Adjust the switch to AP mode. See **1.4.1 Setting the Operating Mode** on page 10.

2 Connect one end of the RJ-45 cable to the travel router and the other end to the DSL or cable modem.

3 Turn on or plug in the DSL / cable modem and the broadband router.

4 Connect the power adapter to the travel router and plug to an outlet or power strip. Wait for the travel router to boot.

5 Check the LED indicators to verify connection.

6 Enable the wireless function of the wireless clients or devices.

The following LED indicators should be lit...

√ Power LED (solid)

√ LAN LED (solid)

Note:

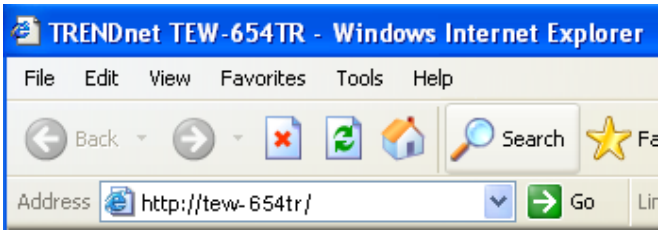
Make sure you remove the power source from the travel router first before adjusting the mode switch.

2.2 Web-Based Configuration

After making all the required connections, configure the travel router using the web-based configuration utility.

How to Access the Configuration Utility

1 Open a web-browser and enter the default address: **http://tew-654tr/**.



Notes:

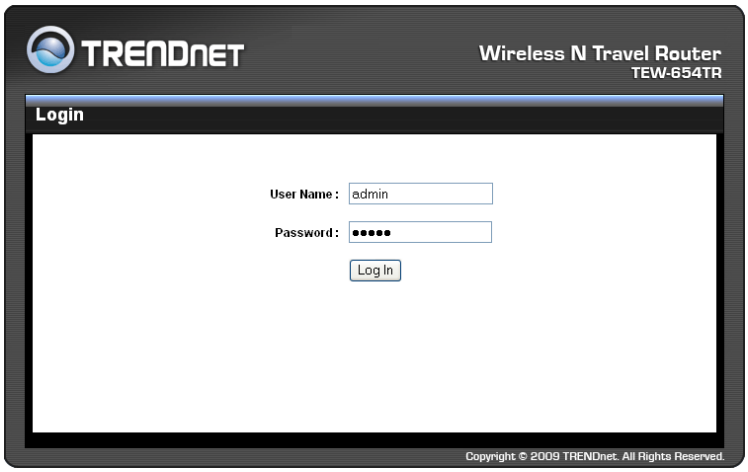
You can also access the web-based configuration by any of the following ways:

1. If your LAN connection uses DHCP, the travel router can obtain an IP address from the DHCP server. You can either enter that IP address or the default address **http://tew-654tr/** on the browser's address field to open the web-based configuration utility.
2. If your LAN connection uses Static IP, You can either enter **http://tew-654tr/** or that static IP address on the browser's address field. The default IP address is **192.168.10.1**.

If you cannot access the configuration utility:

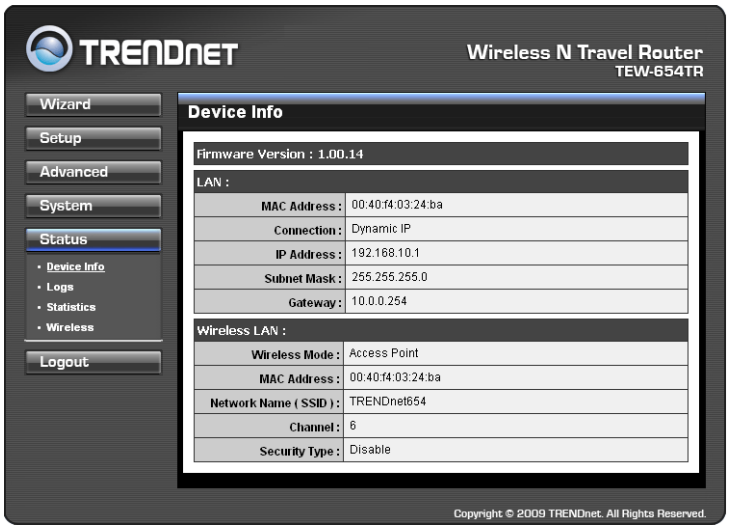
- Disable the Internet security software on the computer. The firewall may block access to the configuration page. Check the software firewall documentation for help.

2 Enter the default **User Name** and **Password**: **admin**.



2. AP MODE

After login, the **Status > Device** Info page is displayed.



To access a page, click the buttons on the right.
To logout, click **Logout**.

Note:

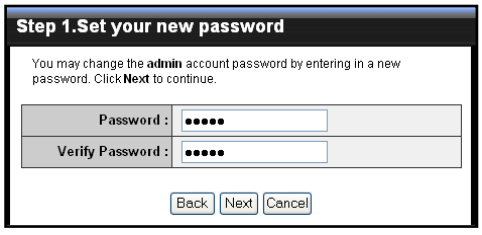
For novice users, it is recommended to use the Setup Wizard to configure the travel router.

2.2.1 Wizard

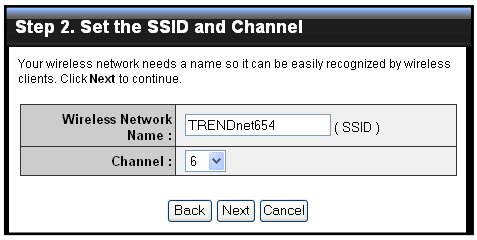
Click the **Wizard** button to configure the travel router using the setup wizard.

1 Click **Next** to continue.

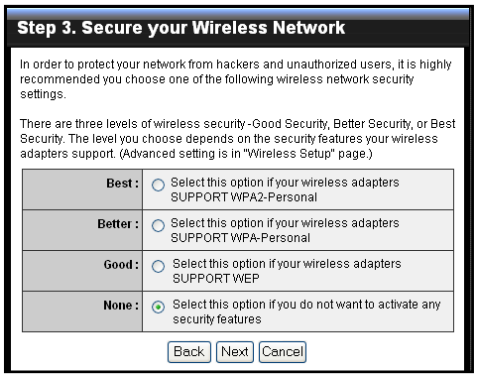
2 Create a new **Password**, then click **Next** to continue.



3 Create a new **Wireless Network Name** and select the **Channel** (6 by default). Click **Next** to continue.



4 Select the type of security, then click **Next** to continue.

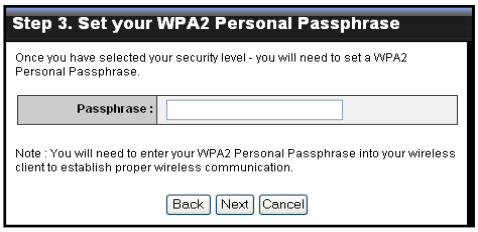


If you select **None**, skip to step 5.

If you select **Best**...

Enter the **Passphrase**, then click **Next** to continue.

Skip to step 5.



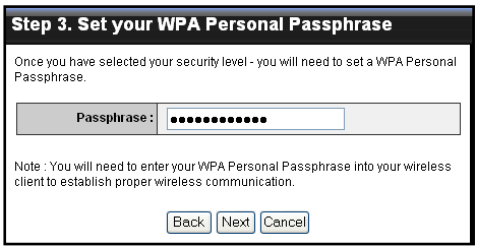
Notes:

- The Passphrase must be 8-63 ASCII characters or 64 hexadecimal characters.
- When using this mode, please make sure your wireless computer/device's wireless security also supports WPA2-Personal or WPA2-PSK.

If you select **Better**...

Enter the **Passphrase**, then click **Next** to continue.

Skip to step 5.



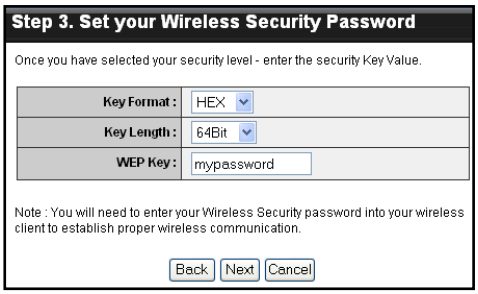
Note:

When using this mode, please make sure your wireless computer/device's wireless security also supports WPA-Personal or WPA-PSK.

If you select **Good**...

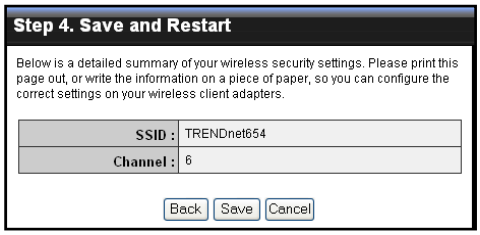
Select the **Key Format** and **Key Length**.

Enter the **WEP Key**, then click **Next** to continue.



5 The wireless security setting is displayed. Take note of the information then click **Save**.

The information shown varies depending on the selected security level.

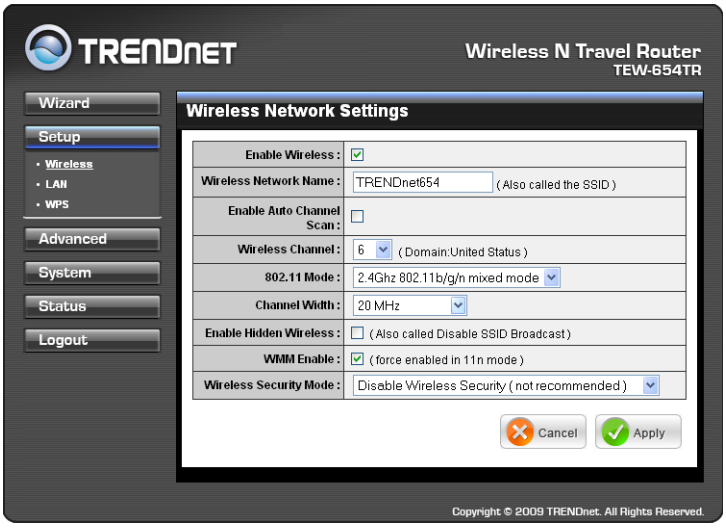


6 Click **Restart** to reboot the access point and the device.

2.2.2 Setup

The Setup menu allows you to configure basic router settings. Click the **Setup** button then the submenu to view page.

Wireless Network Settings



Enable Wireless

Check the box to enable wireless function. Uncheck to disable it.

Wireless Network Name

The name of your wireless network, also called Service Set Identifier (SSID).

Enter up to 32 characters.

Enable Auto Channel Scan

Auto channel scan selects the channel with the least amount of interference. Check to enable auto channel scan.

Wireless Channel

Manually select the channel from the list. By default, the channel is set to 6. If Enable Auto Channel Scan is checked, this box is grayed out.

802.11 Mode

Limit the type of wireless clients to allow connection with. Select any of the following modes if your clients are:

- **2.4Ghz 802.11b/g mixed mode:** a mix of 802.11b and 11g wireless devices.
- **2.4Ghz 802.11b/g/n mixed mode:** a mix of 802.11b, 11g, 11n wireless devices.
- **2.4Ghz 802.11n only mode:** all 802.11n wireless devices.

Channel Width

Select the appropriate channel width:

- **20 MHz (Default):** Select if your wireless clients are not 802.11n.
- **Auto 20/40 MHz:** Select if your wireless clients are a mix of 802.11b, 11g, 11n wireless clients. If you are not sure which wireless clients you are using, select **Auto**.

Enable Hidden Wireless

Check to hide the SSID of your wireless network to be broadcasted when wireless clients scan for wireless networks. To display the router's SSID, keep the box unchecked (default).

WMM Enable

Wi-Fi Multimedia (WMM) improves the quality of video and voice applications

transmitted over a wireless network. This function is commonly used with multimedia applications such as a game console. Check the box to enable WMM.

Wireless Security Mode

Select the security level for your wireless network. Select the wireless security mode from the list:

- **Disable Wireless Security:** (Default) Select if you do not want to use any wireless security.
- **Enable WEP Wireless Security (basic)**
- **Enable WPA Wireless Security (enhanced)**
- **Enable WPA-2 Wireless Security (enhanced)**
- **Enable WPA-Auto Wireless Security (enhanced):** Select if you are unsure which WPA wireless security to use.

The required settings vary depending on the selected mode.

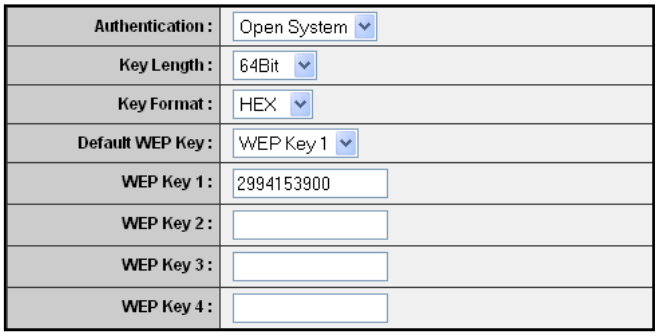
WEP

WEP (Wired Equivalent Privacy) is the basic encryption method. With WEP encryption, all wireless clients must enter the same key to connect to the access point.

Authentication

Select the type of authentication:

- **Open system:** Allows public access to the travel router via wireless communications.
- **Shared Key:** Requires users to enter the same WEP key to exchange data with other wireless devices.
- **Auto:** Select **Auto** if you are unsure which authentication suits best for your wireless clients.



Key Length

Select the key length or the level of encryption:

- **64Bit:** Select to enter 10 hexadecimal characters with any combination of 0-9 or A-F
- **128Bit:** Select to enter 26 hexadecimal characters with any combination of 0-9 or A-F

Key Format

Select the key format:

- **ASCII:** Select to enter ASCII characters.
- **HEX:** Select to enter hexadecimal characters.

Default WEP Key

The travel router supports up to 4 sets of WEP keys. Select which WEP Key is used as the default key from the list.

WEP KEY 1-4

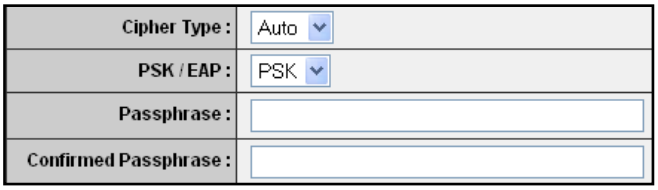
Manually enter a set of WEP key for each box. Select the default WEP key from the **Default WEP Key** list.

WPA / WPA-2 / WPA-Auto

WPA (Wi-Fi Protected Access) uses high grade encryption and authentication which is designed to improve WEP encryption. WPA / WPA-2 / WPA-Auto uses a passphrase to authenticate wireless connections.

Cipher Type

Select the encryption method:



- **TKIP:** Temporal Key Integrity Protocol.
- **AES:** Advanced Encyption Standard.
- **Auto:** Select **Auto** if you are unsure which method is suitable for your wireless clients.

PSK/EAP

Select the authentication method:

- **PSK:** Select to use a passphrase for authentication.

  Passphrase

  Create a passphrase. The passphrase must be 64 hexadecimal or 8-63 ASCII characters.

  Confirm Passphrase

  Re-enter passphrase.

- **EAP:** Select to use Extensible Authentication Protocol (EAP). This should only be used when a Radius server is connected to the travel router. You can have up to 2 Radius server settings.

  IP

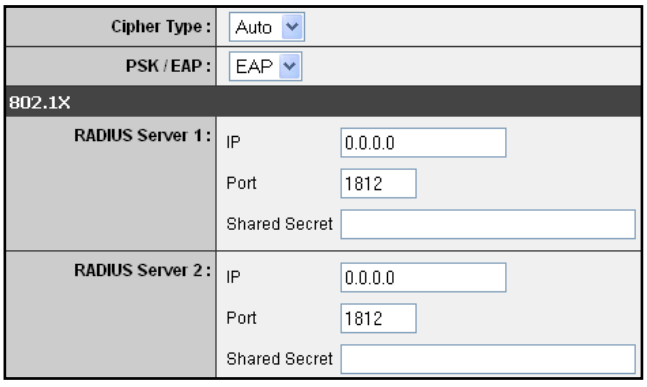
  Enter the IP address of the Radius server.

  Port

  Enter the port number of the Radius server. The default value is 1812.

  Shared Secret

  Enter the secret key shared between the travel router and the Radius server.

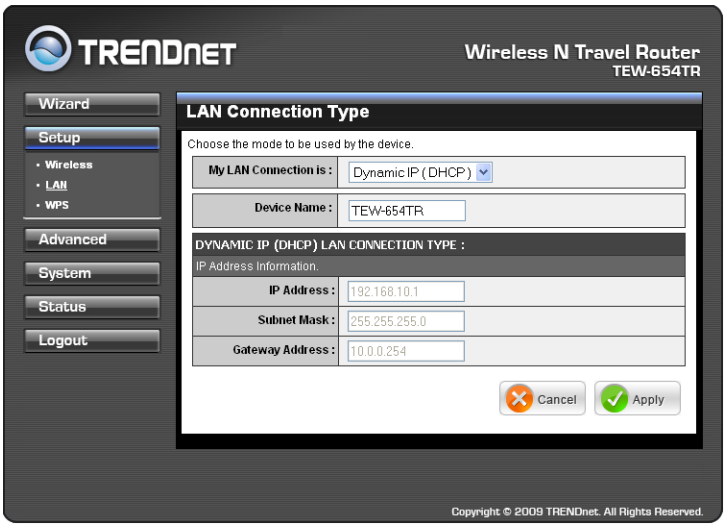


Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

2. AP MODE

Local Area Network (LAN) Settings

Dynamic IP (DHCP)



My LAN Connection is

Select **Dynamic IP (DHCP)** to obtain the IP address information automatically from your ISP. The **IP Address**, **Subnet Mask**, and **Gateway Address** are shown on the page.

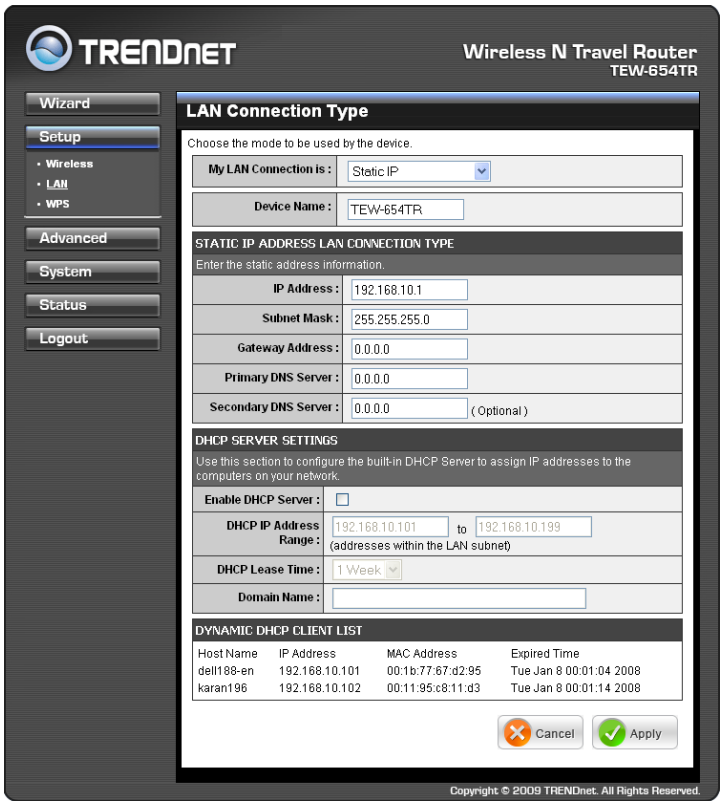
Device Name

Displays the default device name.

Static IP

My LAN Connection is

Select **Static IP** if you are required to use a permanent IP address to connect to the Internet. You need to manually enter the information provided by your ISP.



IP Address

Enter the IP address provided by your ISP.

Subnet Mask

Enter the subnet mask provided by your ISP.

Gateway Address

Enter the gateway address provided by you ISP.

Primary / Secondary DNS Server

Enter the DNS server addresses provided by your ISP.

Enable DHCP Server

Check the box to use the travel router as a DHCP server for your network. A DHCP server automatically assigns an IP address to each client on your network. This function is disabled by default.

DHCP IP Address Range

Enter the starting and ending range of IP addresses that can be assigned to clients on your network.

DHCP Lease Time

Select the length of time to “lease” the dynamic IP address from the list. The default time is **1 Week**.

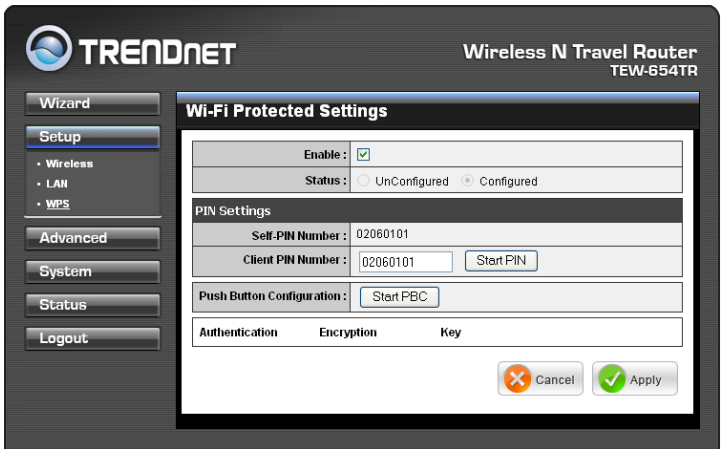
Domain Name
Enter the domain name (optional).

Dynamic DHCP Client List window
Displays the list of DHCP clients.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Wi-Fi Protected Setup (WPS) Settings

Wi-Fi Protected Setup (WPS) is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on a wireless network.



Enable
Check the box to enable WPS function.

Status
Displays WPS status: **UnConfigured** or **Configured**.

There are 2 methods used in WPS configuration:

- **Push Button:** If the client device has a WPS button.
- **PIN Number:** If the client device has a WPS PIN number.

Self-PIN Number
Displays the default PIN number of the travel router.

Client PIN Number
Enter the client's PIN number. This PIN number will be used to communicate with the travel router to connect to the network.

Start PIN
Click this button to start WPS configuration process if the client device has a WPS PIN number.

Push Button Configuration
Click the **Start PBC** button to start WPS configuration process if the client device has a WPS button.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

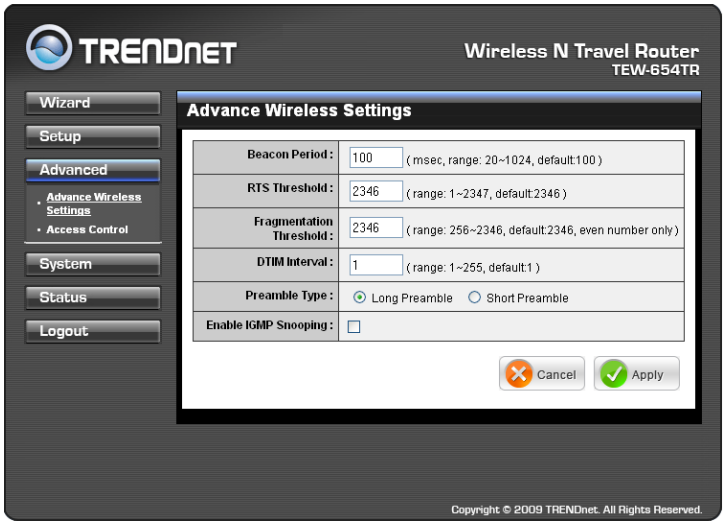
2.2.3 Advanced

The Advanced menu configurations greatly affect the operating performance of the travel router. This menu is intended for advanced users. It is recommended to retain the default settings. Do not change any of configurations if you are unsure about it.

Advanced Wireless Network Settings

Beacon Period

Enter the interval period of time for the access point to send out beacons to synchronize the wireless network. The default value is 100 milliseconds.



RTS Threshold

The default and the recommended value is 2346. Should you encounter inconsistent data flow, only minor adjustments should be made.

Fragmentation Threshold

Fragmentation threshold refers to the amount of packets that will be fragmented before transmission. The default and recommended value is 2346 bytes.

DTIM Interval

This value indicates the interval of Delivery Traffic Indication Message (DTIM). A DTIM is a countdown field informing clients of the next window for listening to broadcast and multicast messages. The default value is 1.

Preamble Type

Preamble is use to limit the packets of data for transmission. When the connection is bad, it is recommended to use the **Short Preamble**.

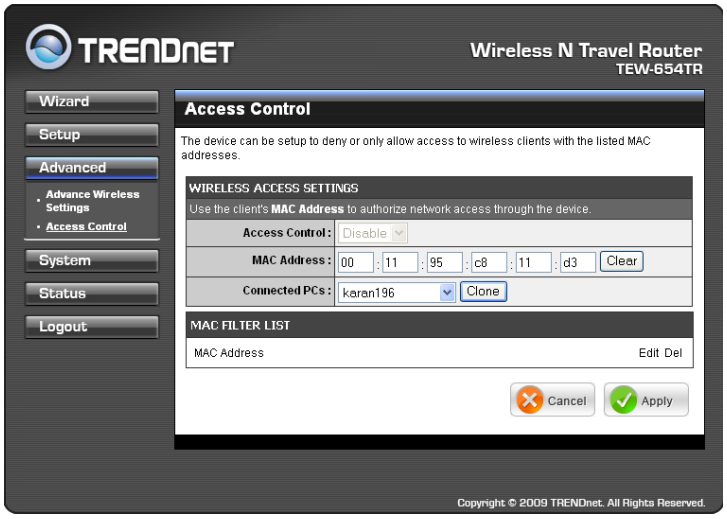
Enable IGMP Snooping

Check the box to enable Internet Group Management Protocol (IGMP) snooping. This function restrains multicast traffic in a switched network.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Access Control

The Access Control menu allows you deny or only allow access to certain wireless clients by filtering their MAC addresses.



Access Control

Select the type of access from the list:

- **Disable:** Disable access control.
- **Reject:** Deny the MAC addresses shown on the list to access the wireless network.
- **Accept:** Only allow the MAC addresses shown on the list to access to wireless network.

MAC Address

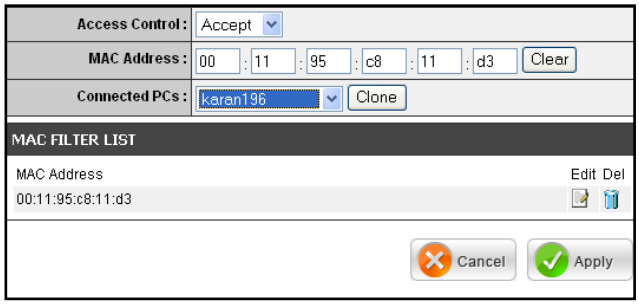
Displays the cloned MAC address. To clear the MAC address, click **Clear**.

Connected PCs

Select the name of the connected client that you want to clone. Click **Clone** to clone its MAC address.

To grant or block access:

1. Select the client from the **Connected PCs** list, then click **Clone**. The cloned MAC address is displayed in the **MAC Address** field.
2. Click **Apply** to add MAC address in the **MAC Filter List**. The system will reboot.
3. After rebooting, select the **Access Control** option: **Disable**, **Reject** or **Accept**.
4. Click **Apply** to save setting. The system will reboot for changes to take effect.
5. To add more MAC addresses, repeat steps 1-4.



To edit the access control of a MAC address, click its corresponding icon.

To delete the MAC address from the list, click its corresponding icon.

2.2.4 System

The System menu provides password configuration, backup and restore settings, firmware update and date and time settings.

Admin

The Admin submenu allows you to change the default user name and password which are use to login.

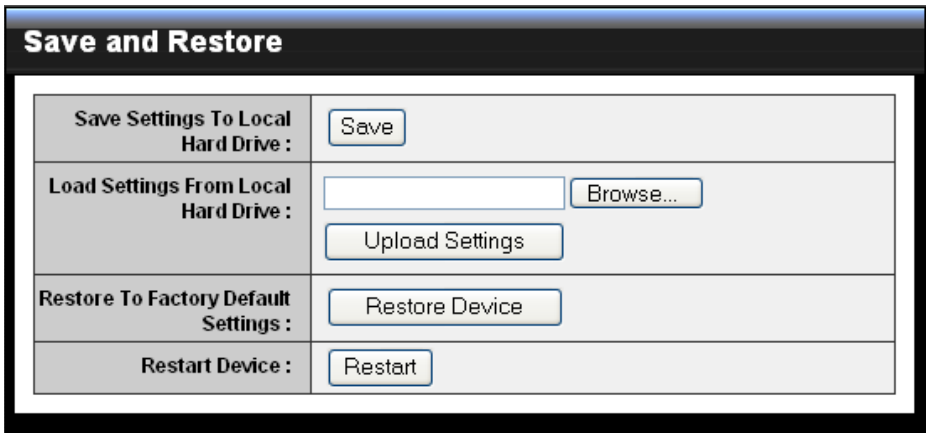
New User Name
Enter the new user name here.

New / Confirm Password
Enter the password.

Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Settings

The Settings submenu provides backup and restore setting functions.



Save Settings to Local Hard Drive
Use this function to save the current configuration settings to your local hard drive. Click **Save**, then select the folder where you want to save the file.

Load Settings From Local Hard Drive
Use this function to retrieve saved configuration settings from the local hard drive.

1. Click **Browse** to locate the file.
2. Click **Upload Settings** to transfer and apply the settings to the travel router.

Restore to Factory Default Settings
Click **Restore Device** to restore all configurations to the factory default settings. All changes in configuration will be deleted.

Restart Device
Click **Restart** to reboot the travel router.

Firmware

The Firmware submenu allows you to upgrade the firmware to the latest version.

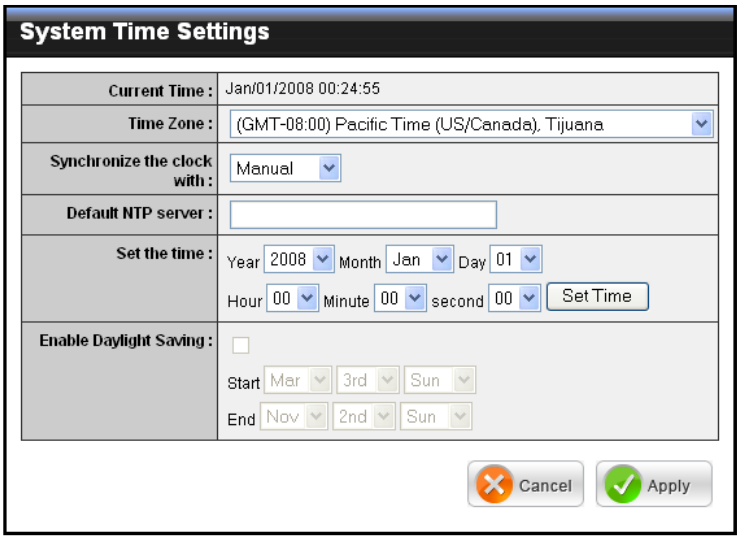
Current Firmware Version
Displays the current firmware version.

Firmware Date
Displays the date when the firmware was last updated.

1. Download the latest firmware from the manufacturer's website, and save it to a disk.
2. Click Browse to locate the file.
3. Click **Apply** to start firmware update. The system will reboot to complete update.

Time

The Time submenu allows you to manually adjust the system time settings or synchronize it with a server.



Current Time
Displays the current date and time settings.

Time Zone
Select the time zone in your area.

Synchronize the clock with
Select:

- **Manual:** To manually adjust the date and time.
- **Automatic:** To synchronize date and time with the server.

Default NTP Server
Enter the NTP server address to synchronize the date and time with.

Set the Time
Use this option to manually set the date and time. This option is only available when **Synchronize the clock with** is set to **Automatic**.

Enable Daylight Saving
Check the box to enable daylight saving time. Use the Start and End field boxes to specify the starting and ending dates.

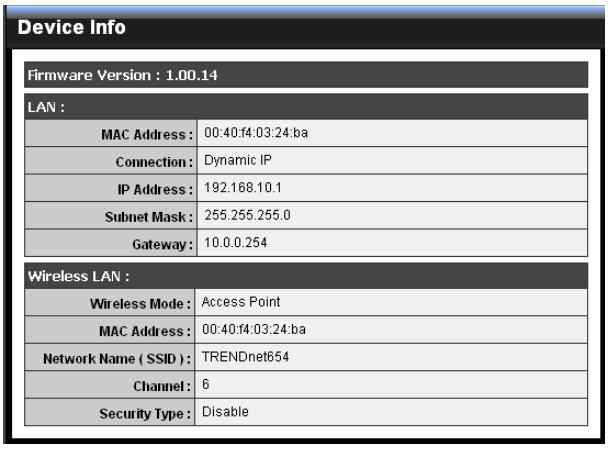
Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

2.2.5 Status

The Status menu displays device, logs, traffic, and connection information.

Device Info

This page displays the Firmware Version, LAN and Wireless LAN information.



Logs

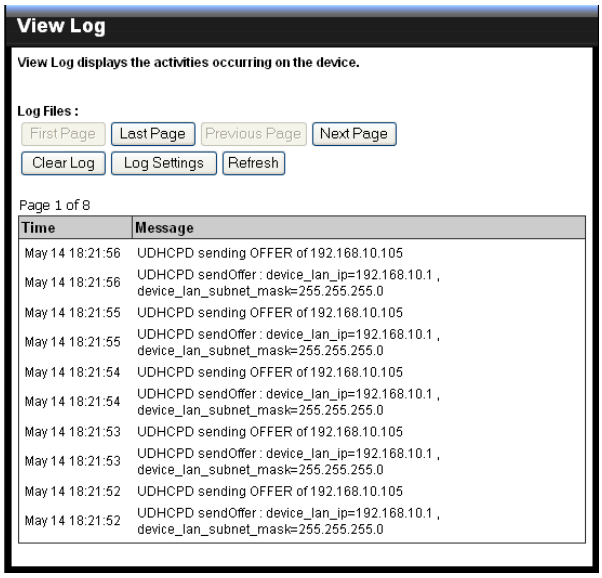
This page displays the recorded events that occur within the wireless network.

Click the following buttons to view the **First Page**, **Last Page**, **Previous Page**, and **Next Page**.

To delete log data, click **Clear Log**.

To change log settings, click **Log Settings**.

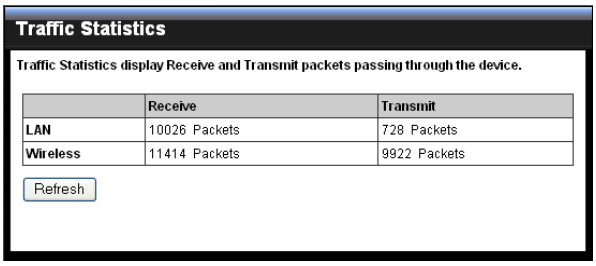
To refresh list, click **Refresh**.



Statistics

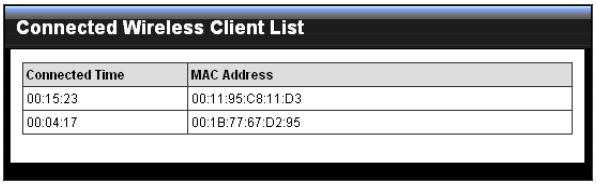
This page displays the traffic statistics of received and transmitted packets that passed through the travel router.

Click **Refresh** to refresh table.



Wireless

This page displays the information of connected wireless clients such as the time of connection and their MAC addresses.



3

Client Mode

With Client mode, you can transform Ethernet-enabled devices to have wireless function using the travel router.

Before You Begin

Checklist

√ A valid network or Internet connection.

√ A DSL / cable modem provided by the ISP as part of the broadband connection installation.

√ A broadband router that connects to the DSL / cable modem for internet connection sharing.

You need to connect...

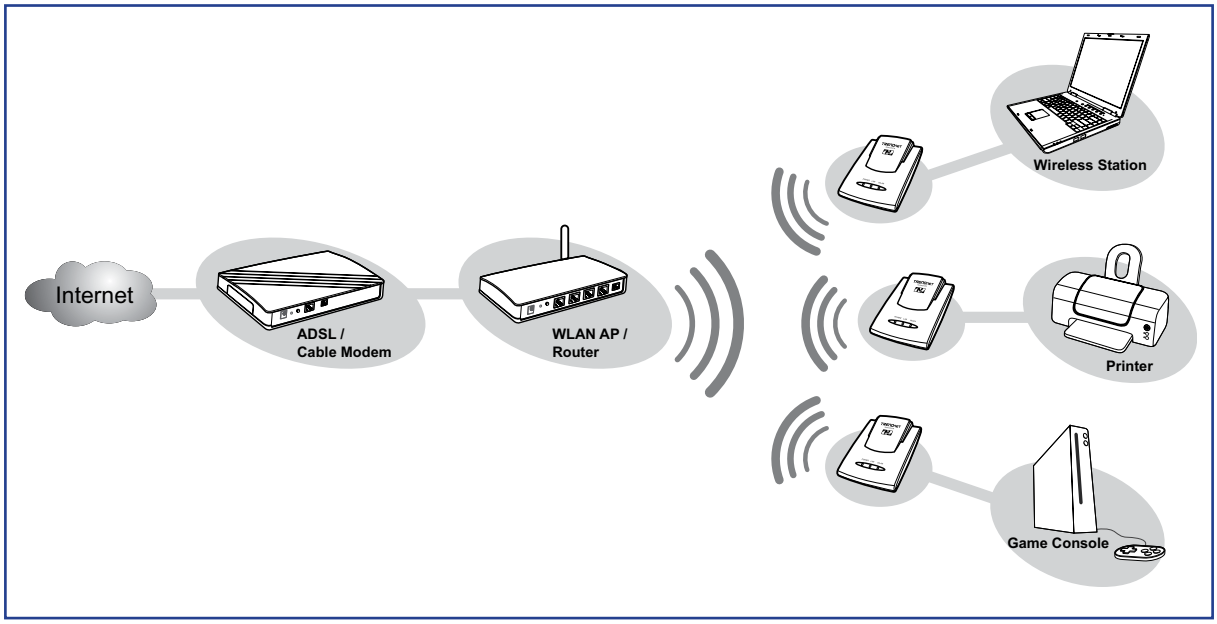
- Connect the travel router to your router or network that has a DHCP server. The travel router will obtain an IP address from the network automatically.
- Connect the LAN port of the travel router to the LAN port on your network then plug in the power adapter.
- Use wireless adapters to connect to the ravel router (default SSID TRENDnet654).

3.1 Installation

3.1.1 Infrastructure Mode

With infrastructure mode, all clients connect to a central access point (AP), all data pass through this access point.

Network Diagram



1. Adjust the switch to Client mode. See **1.4.1 Setting the Operating Mode** on page 10.
2. Connect one end of the RJ-45 cable to the travel router and the other end to the LAN port of the computer or other device.
3. Turn on or plug in the DSL / cable modem and the wireless router.
4. Connect the power adapter to the travel router and plug to an outlet or power strip. Wait for the travel router to boot.
5. Check the LED indicators to verify connection.

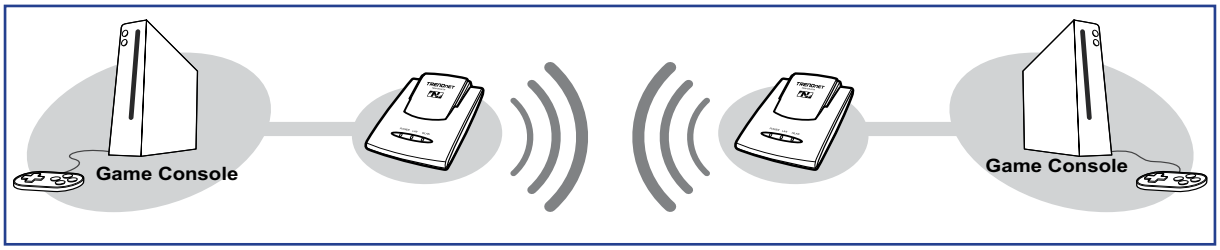
The following LED indicators should be lit...

- √ Power LED (solid)
- √ LAN LED (solid)
- √ WLAN LED (flashing green)

3.1.2 Ad-Hoc Mode

Ad-Hoc is a client setting that provides independent peer-to-peer connectivity in a wireless LAN. With this mode, devices communicate directly with each other. A good example is the communication between two game consoles. See diagram below.

Network Diagram



1. Adjust the switch to Client mode. See **1.4.1 Setting the Operating Mode** on page 10.
2. Connect one end of the RJ-45 cable to the travel router and the other end to the game console or other devices.
3. Connect the power adapter to the travel router and plug to an outlet or power strip. Wait for the travel router to boot.

The following LED indicators should be lit...

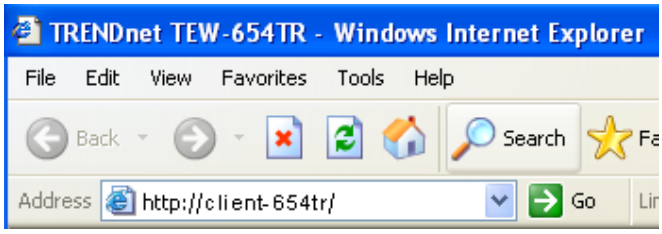
- √ Power LED (solid)
- √ LAN LED (solid)
- √ WLAN LED (flashing green)

3.2 Web-Based Configuration

After making all the required connections, configure the travel router using the web-based configuration utility.

How to Access the Configuration Utility

1 Open a web-browser and enter default address: **http://client-654tr/**.



Notes:

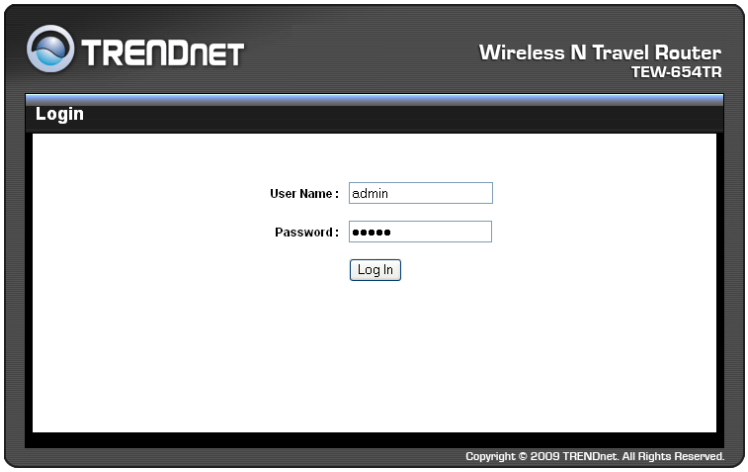
You can also access the web-based configuration by any of the following ways:

1. If your LAN connection uses DHCP, the travel router can obtain an IP address from the DHCP server. You can either enter that IP address or the default address **http://client-654tr/** on the browser's address field to open the web-based configuration utility.
2. If your LAN connection uses Static IP, You can either enter **http://client-654tr/** or that static IP address on the browser's address field. The default IP address is **192.168.10.1**.

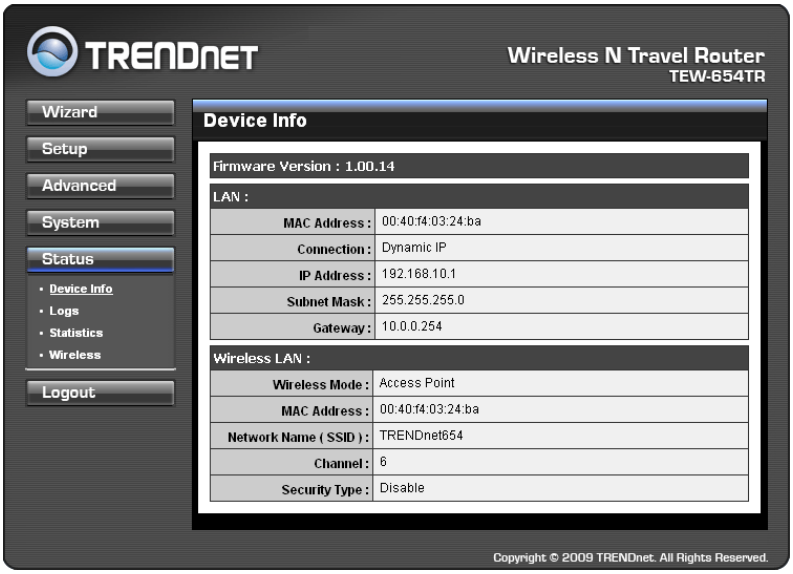
If you cannot access the configuration utility:

- Disable the Internet security software on the computer. The firewall may block access to the configuration page. Check the software firewall documentation for help.

2 Enter the default **User Name** and **Password**: **admin**.



After login, the **Status > Device** Info page is displayed.



To access a page, click the buttons on the right.
To logout, click **Logout**.

Note:

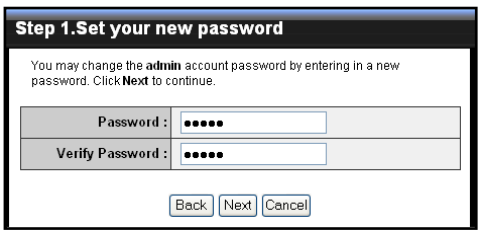
For novice users, it is recommended to use the Setup Wizard to configure the travel router.

3.2.1 Wizard

Click the **Wizard** button to configure the travel router using the setup wizard.

1 Click **Next** to continue.

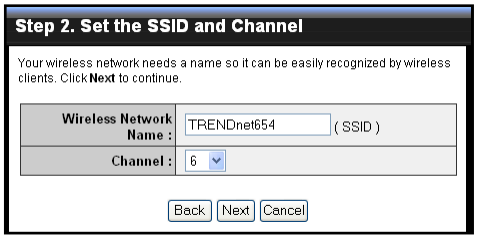
2 Create a new **Password**, then click **Next** to continue.



3. CLIENT MODE

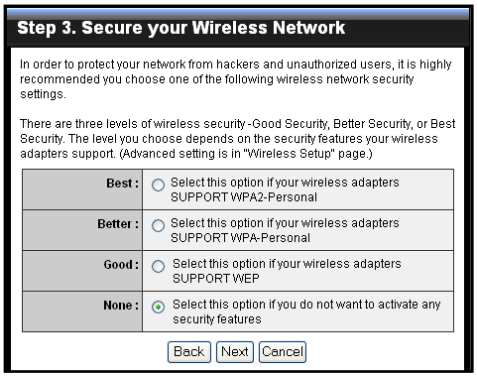
3 Create a new **Wireless Network Name** and select the **Channel** (6 by default). Click **Next** to continue.

4 Select the type of security, then click **Next** to continue.



4 Select the type of security, then click **Next** to continue.

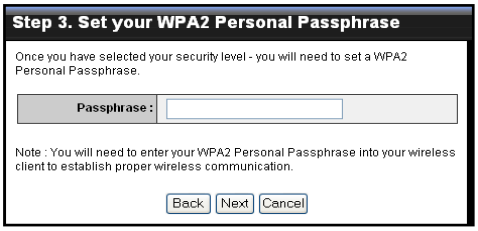
If you select **None**, skip to step 5.



If you select **Best**...

Enter the **Passphrase**, then click **Next** to continue.

Skip to step 5.



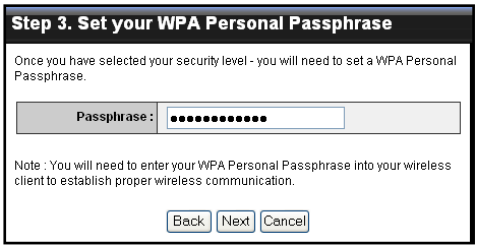
Notes:

- The Passphrase must be 8-63 ASCII characters or 64 hexadecimal characters.
- When using this mode, please make sure your wireless computer/device's wireless security also supports WPA2-Personal or WPA2-PSK.

If you select **Better**...

Enter the **Passphrase**, then click **Next** to continue.

Skip to step 5.



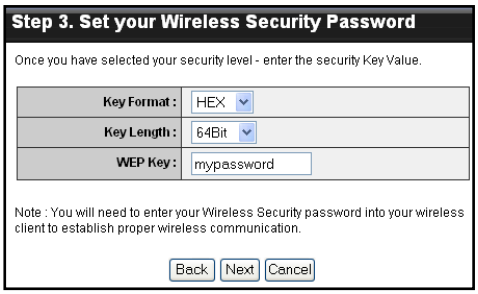
Note:

When using this mode, please make sure your wireless computer/device's wireless security also supports WPA-Personal or WPA-PSK.

If you select **Good**...

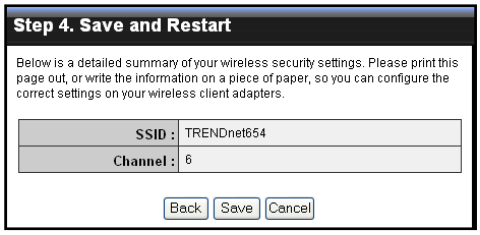
Select the **Key Format** and **Key Length**.

Enter the **WEP Key**, then click **Next** to continue.



5 The wireless security setting is displayed. Take note of the information then click **Save**.

The information shown varies depending on the selected security level.

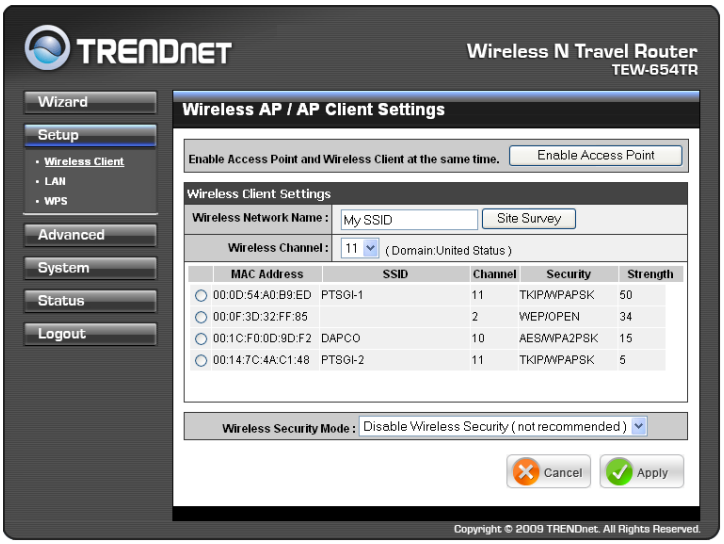


6 Click **Restart** to reboot the access point and the device.

3.2.2 Setup

The Setup menu allows you to configure basic router settings. Click the **Setup** button then the submenu to view page.

Wireless AP/ AP Client Settings



Enable Access Point

Click this button to access Wireless Network Settings page. See page 36.

Site Survey

Click this button to scan for available networks. Available networks are listed on the table. To select a network, click on the network's radio button.

Wireless Network Name

Displays the name of the selected wireless network, also called Service Set Identifier (SSID).

Wireless Channel

Displays the wireless channel of the selected network.

Wireless Security Mode

Displays the security mode of the selected network.

- **Disable Wireless Security:** No wireless security is set.
- **Enable WEP Wireless Security (basic)**
- **Enable WPA Wireless Security (enhanced)**
- **Enable WPA-2 Wireless Security (enhanced)**

The required settings vary depending on the wireless security mode.

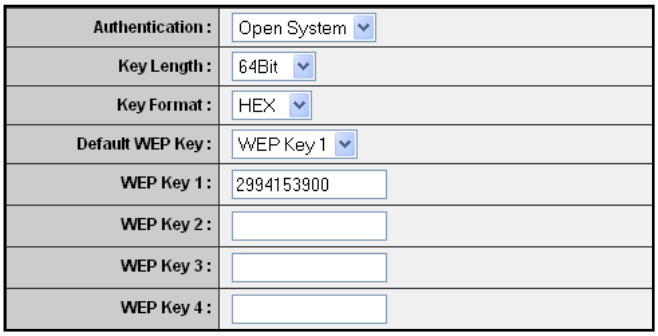
WEP

WEP (Wired Equivalent Privacy) is the basic encryption method. With WEP encryption, all wireless clients must enter the same key to connect to the access point.

Authentication

Select the type of authentication:

- **Open system:** Allows public access to the travel router via wireless communications.
- **Shared Key:** Requires users to enter the same WEP key to exchange data with other wireless devices.



- **Auto:** Select **Auto** if you are unsure.

Key Length

Select the key length or the level of encryption:

- **64Bit:** Select to enter 10 hexadecimal characters with any combination of 0-9 or A-F
- **128Bit:** Select to enter 26 hexadecimal characters with any combination of 0-9 or A-F

Key Format

Select the key format:

- **ASCII:** Select to enter ASCII characters.
- **HEX:** Select to enter hexadecimal characters.

Default WEP Key

Select which WEP Key is used as the default key from the list.

WEP KEY 1-4

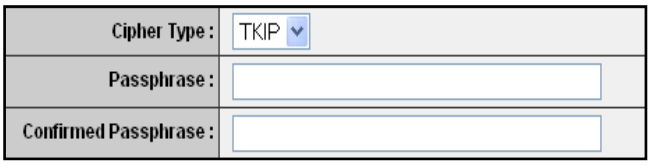
Manually enter a set of WEP key for each box. Select the default WEP key from the **Default WEP Key** list.

WPA / WPA-2

Cipher Type

Select the encryption method:

- **TKIP:** Temporal Key Integrity Protocol.
- **AES:** Advanced Encyption Standard.



Passphrase

Enter the required passphrase to connect to the selected network. The passphrase must be 64 hexadecimal or 8-63 ASCII characters.

Confirm Passphrase

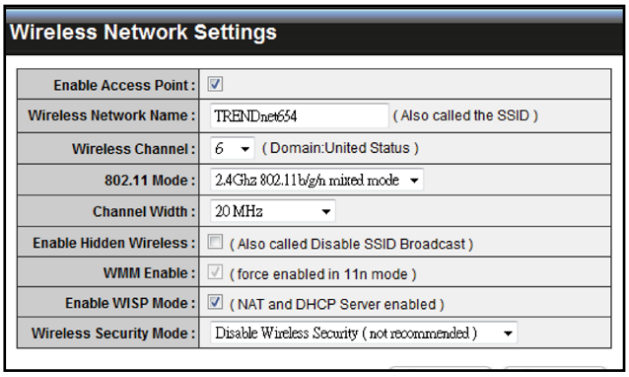
Re-enter passphrase.

Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

3. CLIENT MODE

Wireless Network Settings

Use this page to enable and setup the travel router as an access point and wireless client at the same time.



Enable Access Point

Check the box to enable access point function. Uncheck to disable it.

Wireless Network Name

The name of your wireless network, also called Service Set Identifier (SSID). Enter up to 32 characters.

Enable Auto Channel Scan

Auto channel scan selects the channel with the least amount of interference. Check to enable auto channel scan.

Wireless Channel

Manually select the channel from the list. By default, the channel is set to 6. If Enable Auto Channel Scan is checked, this box is grayed out.

802.11 Mode

Limit the type of wireless clients to allow connection with. Select any of the following modes if your clients are:

- **2.4Ghz 802.11b/g mixed mode:** a mix of 802.11b and 11g wireless devices.
- **2.4Ghz 802.11b/g/n mixed mode:** a mix of 802.11b, 11g, 11n wireless devices.
- **2.4Ghz 802.11n only mode:** all 802.11n wireless devices.

Channel Width

Select the appropriate channel width:

- **20 MHz (Default):** Select if your wireless clients are not 802.11n.
- **Auto 20/40 MHz:** Select if your wireless clients are a mix of 802.11b, 11g, 11n wireless clients. If you are not sure which wireless clients you are using, select **Auto**.

Enable Hidden Wireless

Check to hide the SSID of your wireless network to be broadcasted when wireless clients scan for wireless networks. To display the router's SSID, keep the box unchecked (default).

WMM Enable

Wi-Fi Multimedia (WMM) improves the quality of video and voice applications transmitted over a wireless network. This function is commonly used with multimedia applications such as a game console. Check the box to enable WMM.

Enable WISP Mode

Check the box to enable Wireless Internet Service Provider (WISP). WISP is commonly used in wireless hotspots, such as coffee shops, airports. etc. When the travel router is connected to a wireless hotspot, it connects with a WISP account

and is assigned a public IP address. This account and public IP address are then shared and used by all connected clients. The connected clients receive private IP addresses from the travel router. If WISP is disabled, the travel router does not share the WISP account, instead, connected clients must connect to the wireless network directly.

Wireless Security Mode

Select the security level for your wireless network. Select the wireless security mode from the list:

- **Disable Wireless Security:** (Default) Select if you do not want to use any wireless security.
- **Enable WEP Wireless Security (basic)**
- **Enable WPA Wireless Security (enhanced)**
- **Enable WPA-2 Wireless Security (enhanced)**
- **Enable WPA-Auto Wireless Security (enhanced):** Select if you are unsure which WPA wireless security to use.

The required settings vary depending on the selected mode.

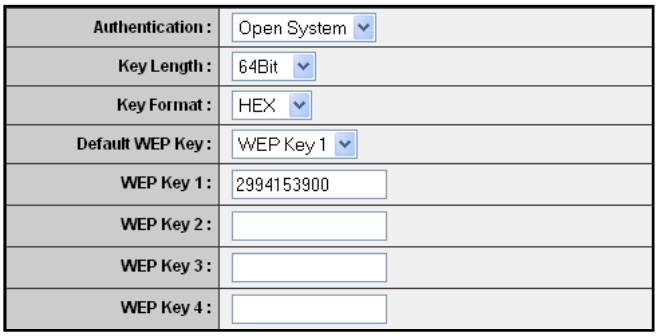
WEP

WEP (Wired Equivalent Privacy) is the basic encryption method. With WEP encryption, all wireless clients must enter the same key to connect to the access point.

Authentication

Select the type of authentication:

- **Open system:** Allows public access to the travel router via wireless communications.
- **Shared Key:** Requires users to enter the same WEP key to exchange data with other wireless devices.
- **Auto:** Select **Auto** if you are unsure which authentication suits best for your wireless clients.



Key Length

Select the key length or the level of encryption:

- **64Bit:** Select to enter 10 hexadecimal characters with any combination of 0-9 or A-F
- **128Bit:** Select to enter 26 hexadecimal characters with any combination of 0-9 or A-F

Key Format

Select the key format:

- **ASCII:** Select to enter ASCII characters.
- **HEX:** Select to enter hexadecimal characters.

Default WEP Key

The travel router supports up to 4 sets of WEP keys. Select which WEP Key is used as the default key from the list.

3. CLIENT MODE

WEP KEY 1-4

Manually enter a set of WEP key for each box. Select the default WEP key from the **Default WEP Key** list.**WPA / WPA-2 / WPA-Auto**

WPA (Wi-Fi Protected Access) uses high grade encryption and authentication which is designed to improve WEP encryption. WPA / WPA-2 / WPA-Auto uses a passphrase to authenticate wireless connections.

Cipher Type

Select the encryption method:

- **TKIP:** Temporal Key Integrity Protocol.
- **AES:** Advanced Encyption Standard.
- **Auto:** Select **Auto** if you are unsure which method is suitable for your wireless clients.

PSK/EAP

Select the authentication method:

- **PSK:** Select to use a passphrase for authentication.

  #### Passphrase

  Create a passphrase. The passphrase must be 64 hexadecimal or 8-63 ASCII characters.

  #### Confirm Passphrase

  Re-enter passphrase.

- **EAP:** Select to use Extensible Authentication Protocol (EAP). This should only be used when a Radius server is connected to the travel router. You can have up to 2 Radius server settings.

  #### IP

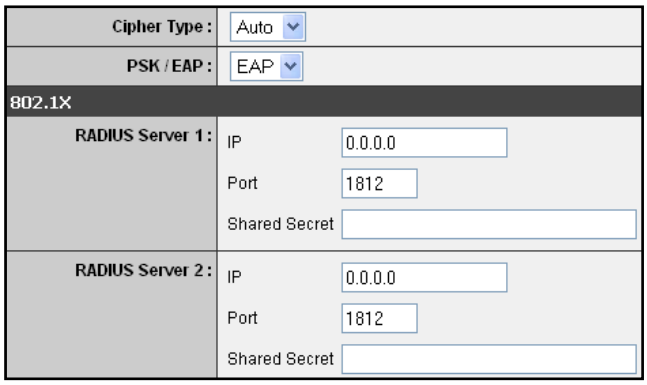
  Enter the IP address of the Radius server.

  #### Port

  Enter the port number of the Radius server. The default value is 1812.

  #### Shared Secret

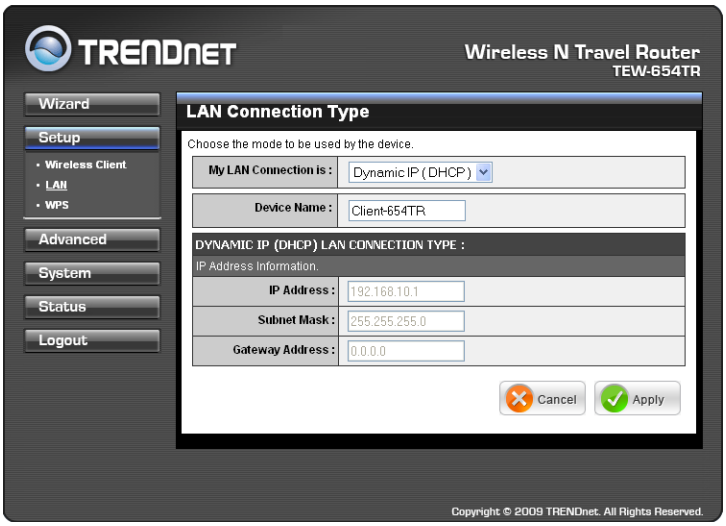
  Enter the secret key shared between the travel router and the Radius server.



Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Local Area Network (LAN) Settings

Dynamic IP (DHCP)



My LAN Connection is

Select **Dynamic IP (DHCP)** to obtain the IP Address information automatically from your ISP. The **IP Address**, **Subnet Mask**, and **Gateway Address** are shown on the page.

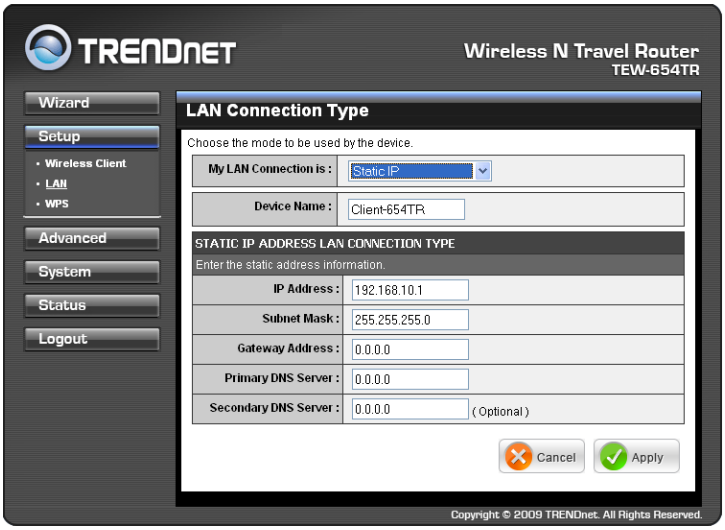
Device Name

Displays the default device name.

Static IP

My LAN Connection is

Select **Static IP** if you are required to use a permanent IP Address to connect to the Internet. You need to manually enter the information provided by your ISP.



IP Address

Enter the IP address provided by your ISP.

Subnet Mask

Enter the subnet mask provided by your ISP.

Gateway Address

Enter the gateway address provided by you ISP.

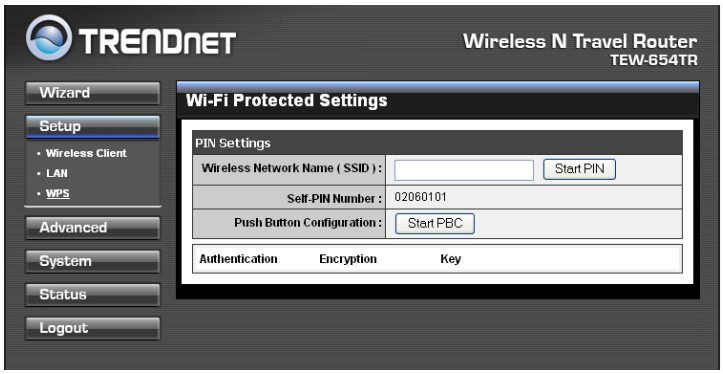
Primary / Secondary DNS Server

Enter the DNS server addresses provided by your ISP.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Wi-Fi Protected Setup (WPS) Settings

Wi-Fi Protected Setup (WPS) is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on a wireless network.



Wireless Network Name (SSID)

The name of the wireless network you want to PIN, also called Service Set Identifier (SSID).

Start PIN

Click this button to start WPS configuration process if the client device has a WPS PIN number.

Self-PIN Number

Displays the default PIN number of the travel router.

Push Button Configuration

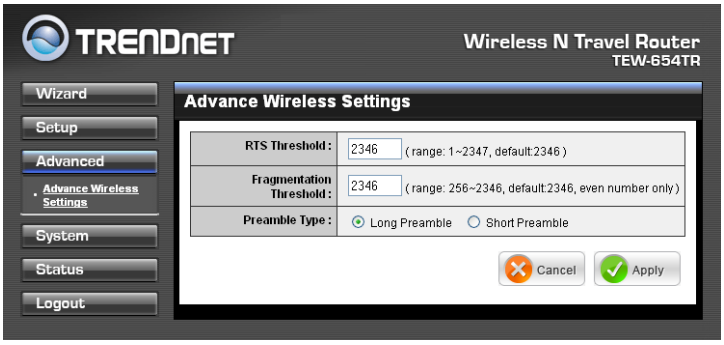
Click the **Start PBC** button to start WPS configuration process if the client device has a WPS button.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

3.2.3 Advanced

The Advanced menu configurations greatly affect the operating performance of the travel router. This menu is intended for advanced users. It is recommended to retain the default settings. Do not change any of configurations if you are unsure about it.

Advanced Wireless Network Settings



RTS Threshold

The default and the recommended value is 2346. Should you encounter inconsistent data flow, only minor adjustments should be made.

Fragmentation Threshold

Fragmentation threshold refers to the amount of packets that will be fragmented before transmission. The default and recommended value is 2346 bytes.

Preamble Type

Preamble is use to limit the packets of data for transmission. When the connection is bad, it is recommended to use the **Short Preamble**.

3.2.4 System

The System menu provides password configuration, backup and restore settings, firmware update and date and time settings.

Admin

The Admin submenu allows you to change the default user name and password which are use to login.

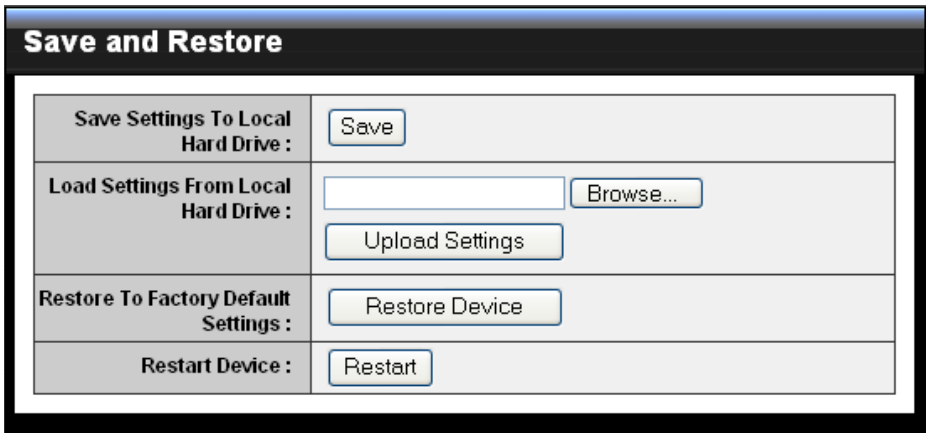
New User Name
Enter the new user name here.

New / Confirm Password
Enter the password.

Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Settings

The Settings submenu provides backup and restore setting functions.



Save Settings to Local Hard Drive
Use this function to save the current configuration settings to your local hard drive. Click **Save**, then select the folder where you want to save the file.

Load Settings From Local Hard Drive
Use this function to retrieve saved configuration settings from the local hard drive.

1. Click **Browse** to locate the file.
2. Click **Upload Settings** to transfer and apply the settings to the travel router.

Restore to Factory Default Settings
Click **Restore Device** to restore all configurations to the factory default settings. All changes in configuration will be deleted.

Restart Device
Click **Restart** to reboot the travel router.

3. CLIENT MODE

Firmware

The Firmware submenu allows you to upgrade the firmware to the latest version.

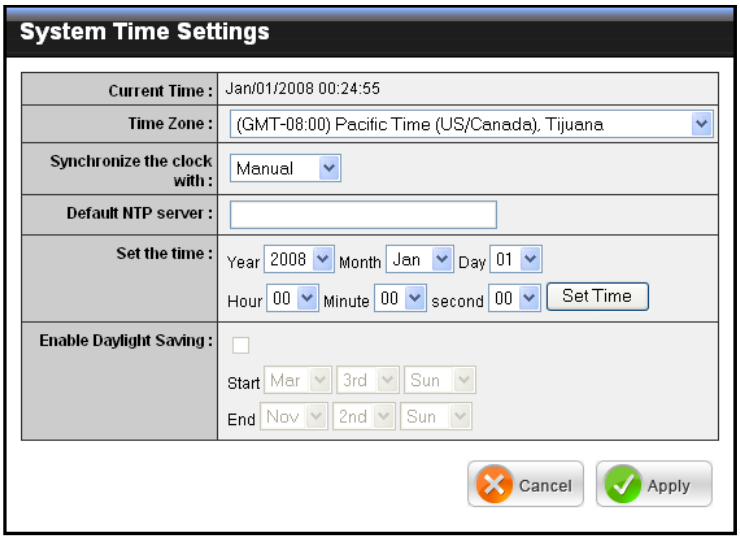
Current Firmware Version
Displays the current firmware version.

Firmware Date
Displays the date when the firmware was last updated.

1. Download the latest firmware from the manufacturer's website, and save it to a disk.
2. Click **Browse** to locate the file.
3. Click **Apply** to start firmware update. The system will reboot to complete update.

Time

The Time submenu allows you to manually adjust the system time settings or synchronize it with a server.



Current Time
Displays the current date and time settings.

Time Zone
Select the time zone in your area.

Synchronize the clock with
Select:

- **Manual:** To manually adjust the date and time.
- **Automatic:** To synchronize date and time with the server.

Default NTP Server
Enter the NTP server address to synchronize the date and time with.

Set the Time
Use this option to manually set the date and time. This option is only available when **Synchronize the clock with** is set to **Automatic**.

Enable Daylight Saving
Check the box to enable daylight saving time. Use the Start and End field boxes to specify the starting and ending dates.

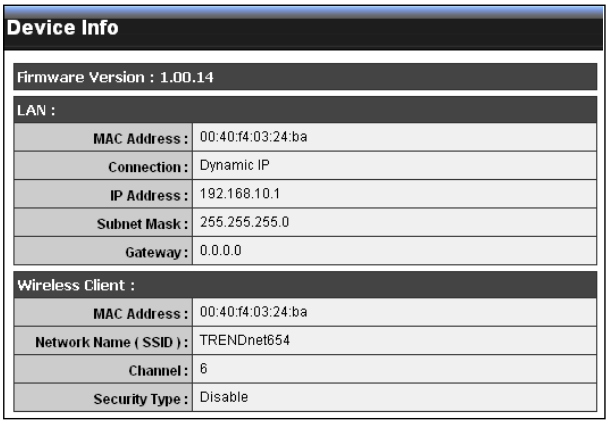
Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

3.2.5 Status

The Status menu displays device, logs, traffic, and connection information.

Device Info

This page displays the Firmware Version, LAN and Wireless Client information.



Logs

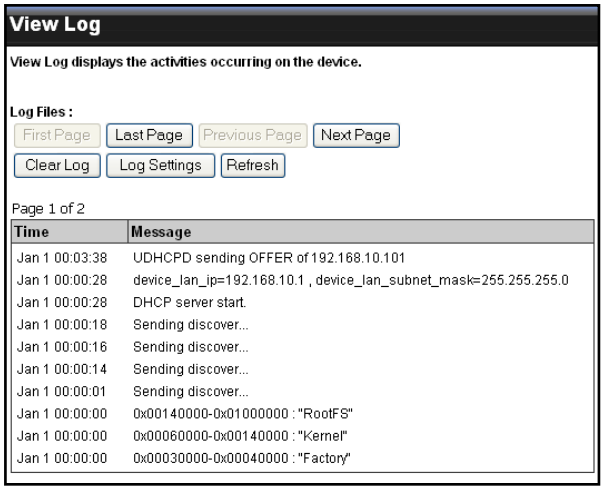
This page displays the recorded events that occur within the wireless network.

Click the following buttons to view the **First Page**, **Last Page**, **Previous Page**, and **Next Page**.

To delete log data, click **Clear Log**.

To change log settings, click **Log Settings**.

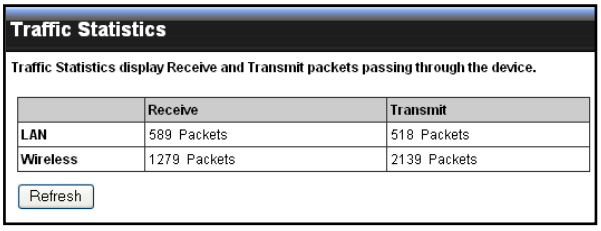
To refresh list, click **Refresh**.



Statistics

This page displays the traffic statistics of received and transmitted packets that passed through the travel router.

Click **Refresh** to refresh table.



4

Router Mode

With Router mode, you can connect and share Internet connections, files, printers, etc. between computers on the network.

Before You Begin

Checklist

√ A broadband Internet connection.

√ A DSL / cable modem provided by the ISP as part of the broadband connection installation.

√ A broadband router that connects to the DSL / cable modem for internet connection sharing.

You need to connect...

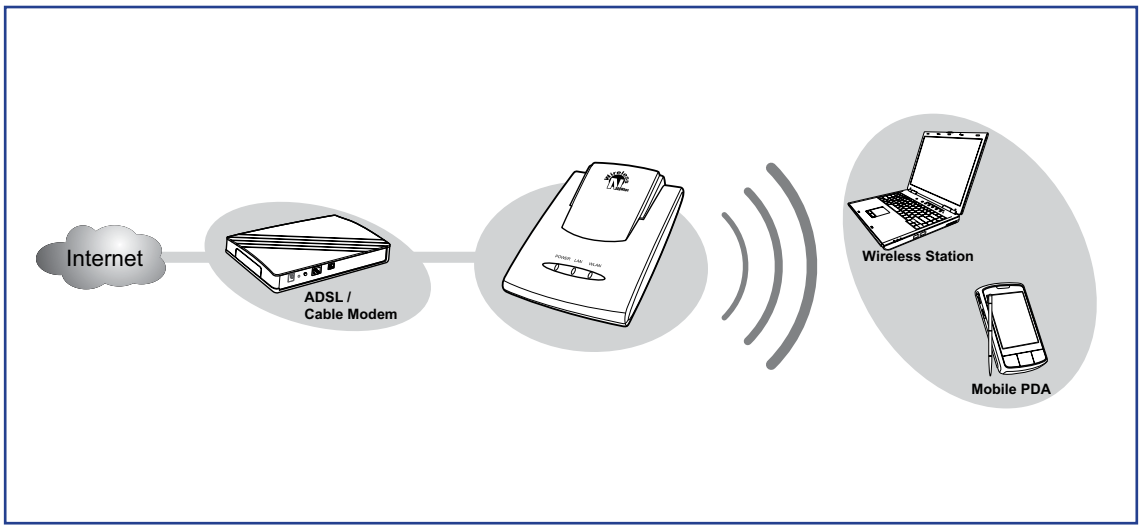
- Connect the DSL / cable modem to the WAN port or Internet port of the broadband router using an RJ-45 Ethernet cable.
- If you are currently connected to a network, disable that network connection before you connect and configure the travel router.
- Configure your computer's Internet protocol (TCP/IP) settings. See "1.6.1 Configuring Connections".

Note:

Although you can connect the DSL or cable modem directly to your computer's network card, it is recommend to use a broadband router as an intermediary device to delegate the handling of the Internet connection and to easily configure and share the Internet connection with other computers on a home network.

4.1 Installation

Network Diagram



1. Adjust the switch to Router mode. See **1.4.1 Setting the Operating Mode** on page 10.
2. Connect one end of the RJ-45 Ethernet cable to the travel router and the other end to the broadband router.
3. Turn on or plug in the DSL / cable modem and the broadband router.
4. Connect the power adapter to the travel router and plug to an outlet or power strip. Wait for the travel router to boot.
5. Check the LED indicators to verify connection.
6. Enable the wireless function of the wireless clients or devices.

The following LED indicators should be lit...

- √ Power LED (solid)
- √ LAN LED (solid)
- √ WLAN LED (flashing green)

Note:

Make sure you remove the power source from the travel router first before adjusting the mode switch.

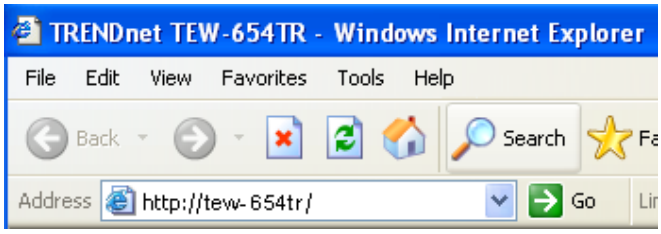
4.2 Web-Based Configuration

After making all the required connections, configure the travel router using the web-based configuration utility.

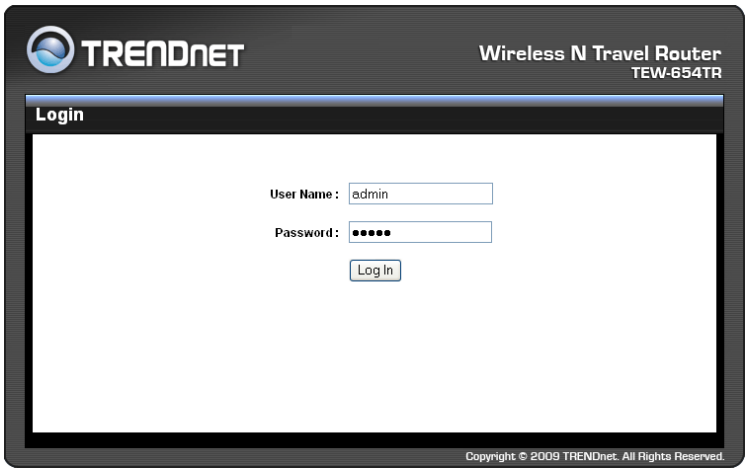
How to Access the Configuration Utility

In Router mode, the travel router's IP address is automatically set as **192.168.10.1**, and the device name is **tew-654tr**. To access the web-based configuration utility, do the following steps:

1 Open a web-browser, on the address field, enter either of the following defaults: **http://tew-654tr/** or **http://192.168.10.1/**.



2 Enter the default **User Name** and **Password**: **admin**.

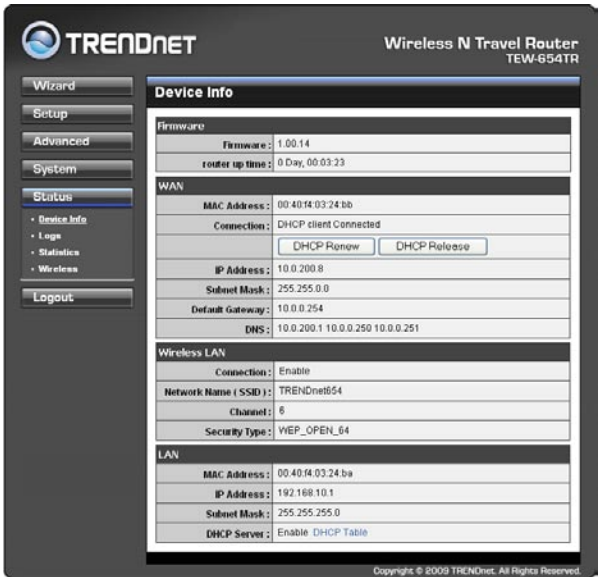


Note:

If you cannot access the configuration utility, disable the Internet security software on the computer. The firewall may block access to the configuration page. Check the software firewall documentation for help.

After login, the **Status > Device** Info page is displayed.

To access a page, click the buttons on the right.
To logout, click **Logout**.



Note:

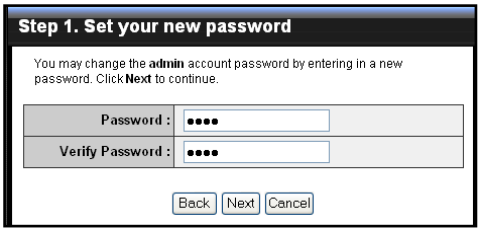
For novice users, it is recommended to use the Setup Wizard to configure the travel router.

4.2.1 Wizard

Click the **Wizard** button to configure the travel router using the setup wizard.

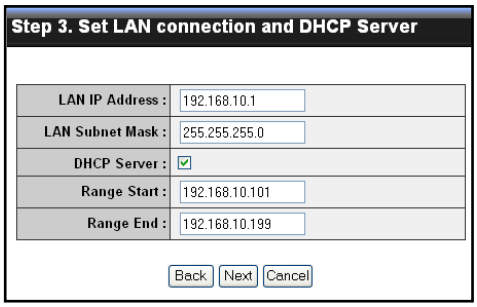
1 Click **Next** to continue.

2 Create a new **Password**, then click **Next** to continue.

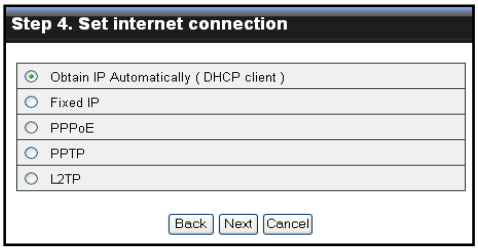


3 Choose the time zone from the list. Click **Next** to continue.

4 Set the **LAN connection** and **DHCP Server**. Click **Next** to continue.



5 Select the type of Internet connection you use, then click **Next** to continue.



Note:

The Passphrase must be 8-63 ASCII characters or 64 hexadecimal characters.

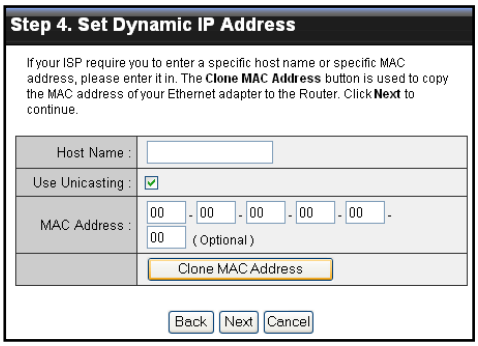
If you selected **Obtain IP Automatically (DHCP Client)**...

Enter the **Host Name** (optional).

You may need to enter the **MAC Address** of the computer that was last connected to a modem. To do this, click **Clone MAC Address**.

Click **Next** to continue.

Skip to step 6.

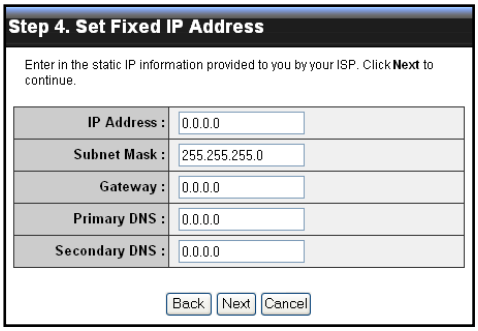


If you selected **Fixed IP**...

Enter the information provided by your ISP: **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS** (optional).

Click **Next** to continue.

Skip to step 6.



If you selected **PPPoE**...

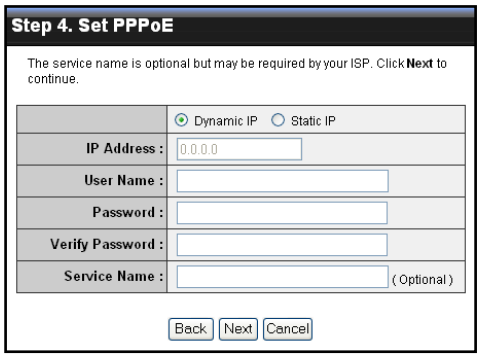
Select either **Dynamic IP** or **Static IP**.

If you selected **Dynamic IP**, enter the **User Name** and **Password**.

If you selected **Static IP**, enter the **IP Address**, **User Name**, and **Password** provided by your ISP.

Click **Next** to continue.

Skip to step 6.



If you selected **PPTP**...

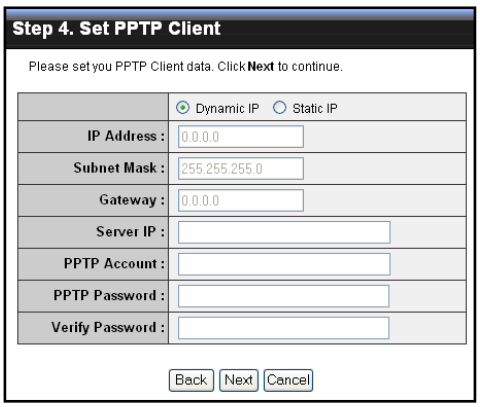
Select either **Dynamic IP** or **Static IP**.

If you selected **Dynamic IP**, enter the **Server IP**, **PPTP Account**, and **PPTP Password** (optional).

If you selected **Static IP**, enter the **IP Address**, **Subnet Mask**, **Gateway**, **Server IP**, **PPTP Account**, and **PPTP Password** (optional) provided by your ISP.

Click **Next** to continue.

Skip to step 6.



If you selected **L2TP**...

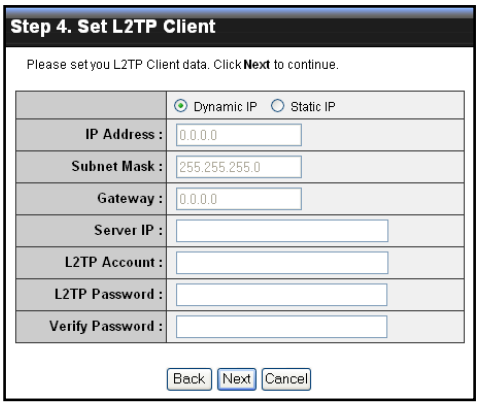
Select either **Dynamic IP** or **Static IP**.

If you selected **Dynamic IP**, enter the **Server IP**, **L2TP Account**, and **L2TP Password** (optional).

If you selected **Static IP**, enter the **IP Address**, **Subnet Mask**, **Gateway**, **Server IP**, **L2TP Account**, and **L2TP Password** (optional) provided by your ISP.

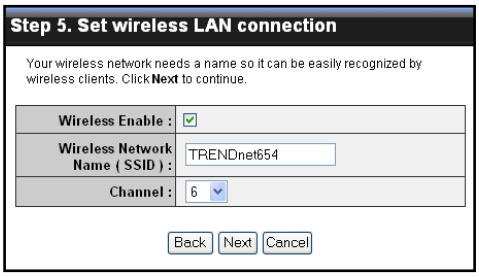
Click **Next** to continue.

Skip to step 6.



5 Check the **Wireless Enable** box to enable wireless function. Create a new Wireless Network Name and select the Channel (6 by default).

Click **Next** to continue.

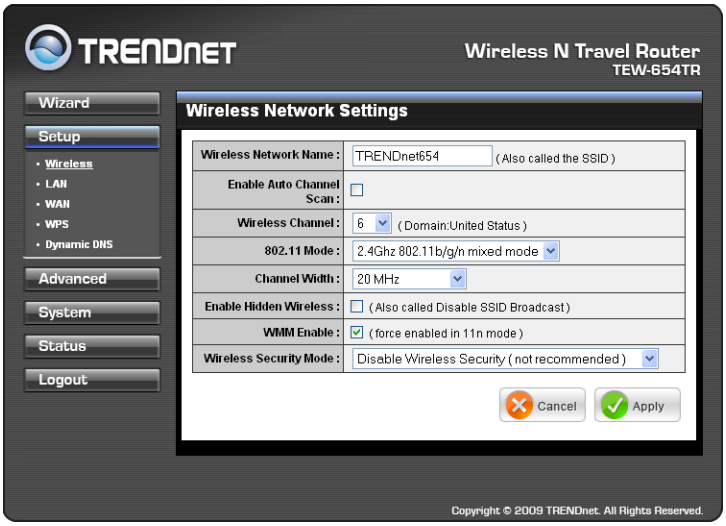


6 Click **Save** to save the settings and reboot the device.

4.2.2 Setup

The Setup menu allows you to configure basic router settings. Click the **Setup** button then the submenu to view page.

Wireless Network Settings



Wireless Network Name

The name of your wireless network, also called Service Set Identifier (SSID).

Enter up to 32 characters.

Enable Auto Channel Scan

Auto channel scan selects the channel with the least amount of interference. Check to enable auto channel scan.

Wireless Channel

Manually select the channel from the list. By default, the channel is set to 6. If **Enable Auto Channel Scan** is checked, this box is grayed out.

802.11 Mode

Limit the type of wireless clients to allow connection with. Select any of the following modes if your clients are:

- **2.4Ghz 802.11b/g mixed mode:** a mix of 802.11b and 11g wireless devices.
- **2.4Ghz 802.11b/g/n mixed mode:** a mix of 802.11b, 11g, 11n wireless devices.
- **2.4Ghz 802.11n only mode:** all 802.11n wireless devices.

Channel Width

Select the appropriate channel width:

- **20 MHz (Default):** Select if your wireless clients are not 802.11n.
- **Auto 20/40 MHz:** Select if your wireless clients are a mix of 802.11b, 11g, 11n wireless clients. If you are not sure which wireless clients you are using, select **Auto**.

Enable Hidden Wireless

Check to hide the SSID of your wireless network to be broadcasted when wireless clients scan for wireless networks. To display the router's SSID, keep the box unchecked (default).

WMM Enable

Wi-Fi Multimedia (WMM) improves the quality of video and voice applications transmitted over a wireless network. This function is commonly used with multimedia applications such as a game console. Check the box to enable WMM.

Wireless Security Mode

Select the security level for your wireless network. Select the wireless security mode from the list:

- **Disable Wireless Security:** (Default) Select if you do not want to use any wireless security.
- **Enable WEP Wireless Security (basic)**
- **Enable WPA Wireless Security (enhanced)**
- **Enable WPA-2 Wireless Security (enhanced)**
- **Enable WPA-Auto Wireless Security (enhanced):** Select if you are unsure which WPA wireless security to use.

The required settings vary depending on the selected mode.

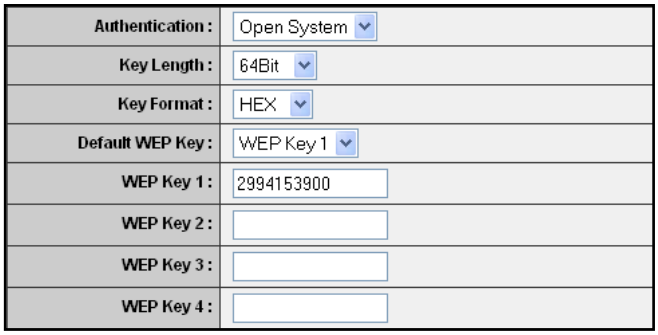
WEP

WEP (Wired Equivalent Privacy) is the basic encryption method. With WEP encryption, all wireless clients must enter the same key to connect to the access point.

Authentication

Select the type of authentication:

- **Open system:** Allows public access to the travel router via wireless communications.
- **Shared Key:** Requires users to enter the same WEP key to exchange data with other wireless devices.
- **Auto:** Select **Auto** if you are unsure which authentication suits best for your wireless clients.



Key Length

Select the key length or the level of encryption:

- **64Bit:** Select to enter 10 hexadecimal characters with any combination of 0-9 or A-F
- **128Bit:** Select to enter 26 hexadecimal characters with any combination of 0-9 or A-F

Key Format

Select the key format:

- **ASCII:** Select to enter ASCII characters.
- **HEX:** Select to enter hexadecimal characters.

Default WEP Key

The travel router supports up to 4 sets of WEP keys. Select which WEP Key is used as the default key from the list.

WEP KEY 1-4

Manually enter a set of WEP key for each box. Select the default WEP key from the **Default WEP Key** list.

4. ROUTER MODE

WPA / WPA-2 / WPA-Auto

WPA (Wi-Fi Protected Access) uses high grade encryption and authentication which is designed to improve WEP encryption. WPA / WPA-2 / WPA-Auto uses a passphrase to authenticate wireless connections.

Cipher Type

Select the encryption method:

- **TKIP:** Temporal Key Integrity Protocol.
- **AES:** Advanced Encryption Standard.
- **Auto:** Select **Auto** if you are unsure which method is suitable for your wireless clients.

PSK/EAP

Select the authentication method:

- **PSK:** Select to use a passphrase for authentication.

  Passphrase

  Create a passphrase. The passphrase must be 64 hexadecimal or 8-63 ASCII characters.

  Confirm Passphrase

  Re-enter passphrase.

- **EAP:** Select to use Extensible Authentication Protocol (EAP). This should only be used when a Radius server is connected to the travel router. You can have up to 2 Radius server settings.

  IP

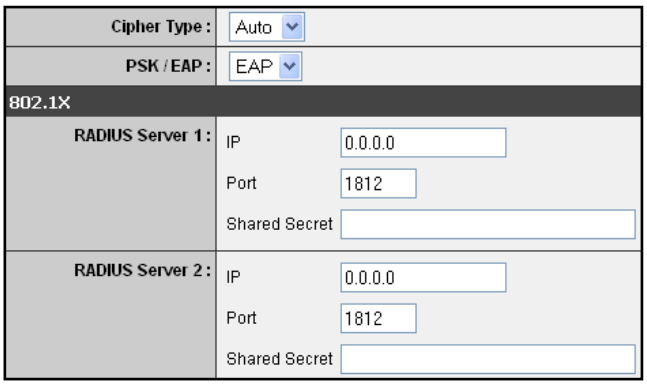
  Enter the IP address of the Radius server.

  Port

  Enter the port number of the Radius server. The default value is 1812.

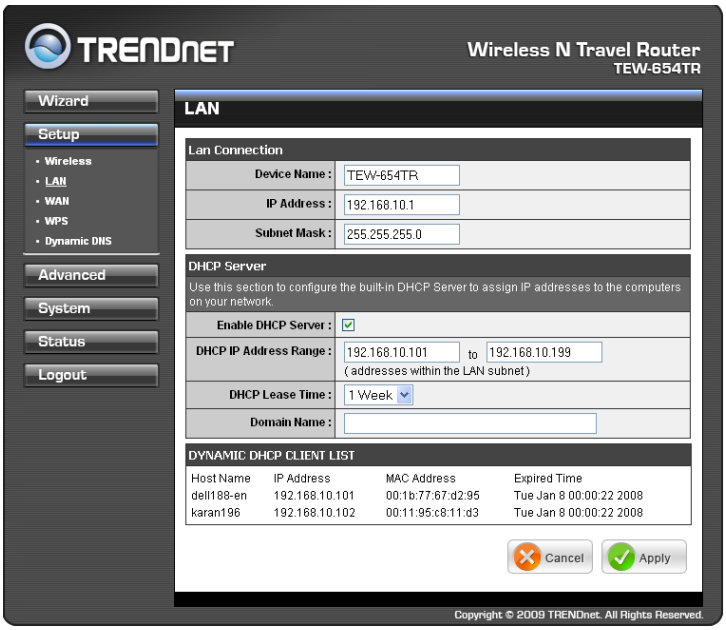
  Shared Secret

  Enter the secret key shared between the travel router and the Radius server.



Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Local Area Network (LAN) Settings



Device Name
Create the device name. The default name is TEW-654TR.

IP Address
Enter the IP address provided by your ISP.

Subnet Mask
Enter the subnet mask provided by your ISP.

Enable DHCP Server
Check the box to allow the travel router to automatically assign an IP address to each connected devices. This function is enabled by default.

DHCP IP Address Range
Enter the starting and ending range of IP addresses that can be assigned to clients on your network.

DHCP Lease Time
Select the length of time to “lease” the dynamic IP address from the list. The default time is **1 Week**.

Domain Name
Enter the domain name (optional).

Dynamic DHCP Client List window
Displays the list of DHCP clients.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

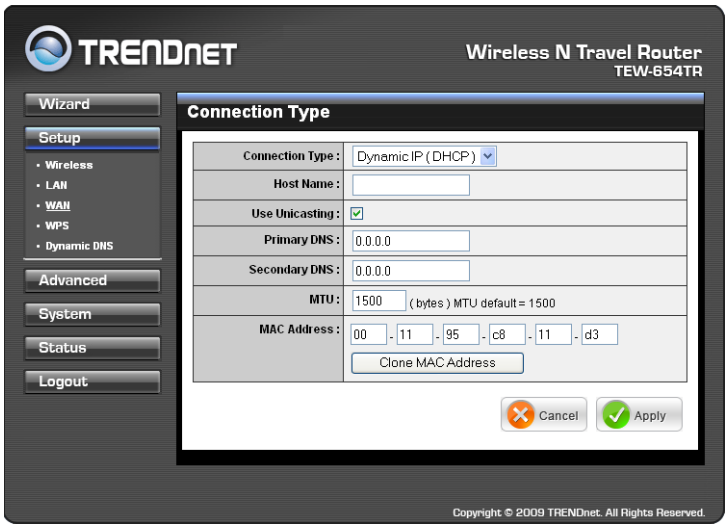
4. ROUTER MODE

Wide Area Network (WAN) Settings

Connection Type

Select the type of Internet connection that you use from the list. The required fields may vary depending on the selected connection type.

Dynamic IP (DHCP)



Host Name

Enter the host name. This field is optional but may be required by some ISPs.

Use Unicasting

If you have problems obtaining an IP address from your ISP. check this box to enable unicasting. Enabled by default.

Primary / Secondary DNS

Enter the DNS server addresses provided by your ISP.

MTU

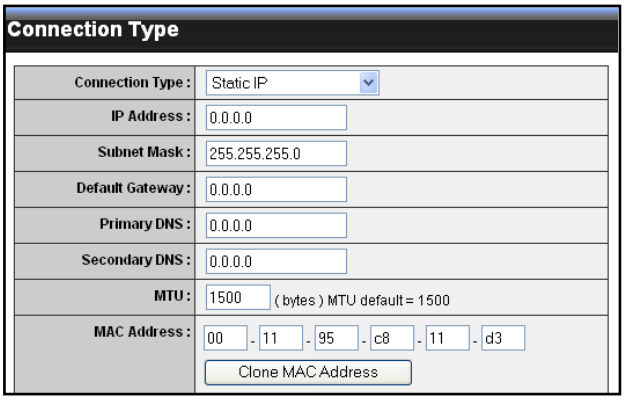
Adjust the MTU (Maximum Transmission Unit) for optimal performance with your ISP. The default value is 1500.

MAC Address

Enter the MAC address of the computer that was last connected to a modem. To enter the MAC address of your current computer, click **Clone MAC Address**.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Static IP



IP Address

Enter the IP address provided by your ISP.

Subnet Mask

Enter the subnet mask provided by your ISP.

Default Gateway

Enter the gateway provided by your ISP.

Primary / Secondary DNS

Enter the DNS server address provided by your ISP.

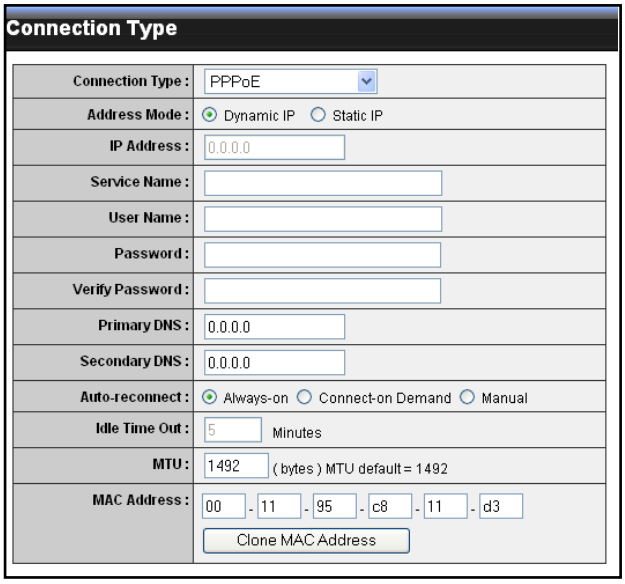
MTU
Adjust the MTU (Maximum Transmission Unit) for optimal performance with your ISP. The default value is 1400.

MAC Address
Enter the MAC address of the computer that was last connected to a modem. To enter the MAC address of your current computer, click **Clone MAC Address**.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

PPPoE
Select PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provided you with a user name and password.

Address Mode
Select **Dynamic IP** (default) or **Static IP** if your ISP provided you with the IP address, subnet mask, and DNS server addresses.



IP Address
Enter the IP address provided by your ISP. This field is only available when **Access Mode** is set to **Static IP**.

Service Name
Enter the ISP's service name (optional).

User Name
Enter the user name provided by your ISP.

Password
Enter the password.

Primary / Secondary DNS
Enter the DNS server addresses provided by your ISP.

Auto-reconnect
Select reconnect option: **Always-on**, **Connect-on Demand**, and **Manual** .

Idle Time Out
Enter the time wherein the travel router will cut off the Internet connection after the specified period of inactivity (in minutes). This field is disabled when **Auto-reconnect** is **Always-on**.

MTU
Adjust the MTU (Maximum Transmission Unit) for optimal performance with your ISP. The default value is 1492.

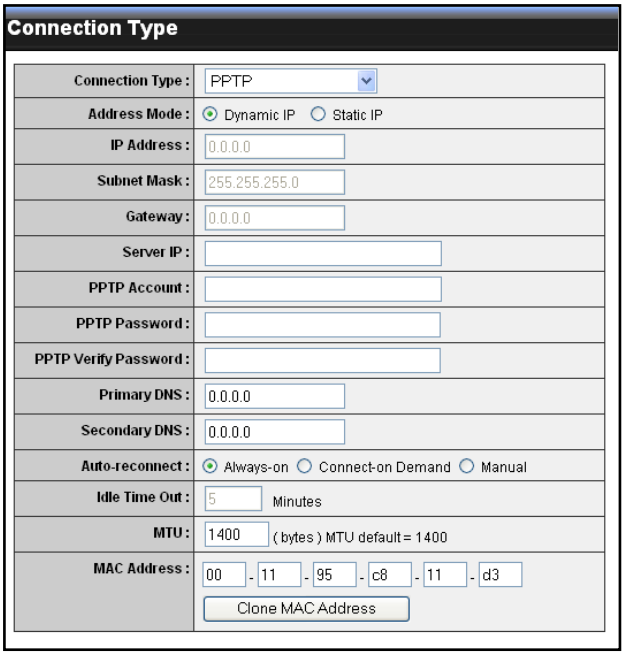
4. ROUTER MODE

MAC Address
Enter the MAC address of the computer that was last connected to a modem. To enter the MAC address of your current computer, click **Clone MAC Address**.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

PPTP
Select PPTP (Point to Point Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provided you with a user name and password.

Address Mode
Select **Dynamic IP** (default) or **Static IP** if your ISP provided you with the IP address, subnet mask, and DNS server addresses.



IP Address
Enter the IP address provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Subnet Mask
Enter the subnet mask provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Gateway
Enter the gateway provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Server IP
Enter the server IP address provided by your ISP.

PPTP Account
Enter the PPTP account name provided by your ISP.

PPTP Password
Enter the PPTP password provided by your ISP.

Primary / Secondary DNS
Enter the DNS server addresses provided by your ISP.

Auto-reconnect
Select reconnect option: **Always-on**, **Connect-on Demand**, and **Manual** .

Idle Time Out
Enter the time wherein the travel router will cut off the Internet connection after the specified period of inactivity (in minutes). This field is disabled when **Auto-reconnect**

is **Always-on**.

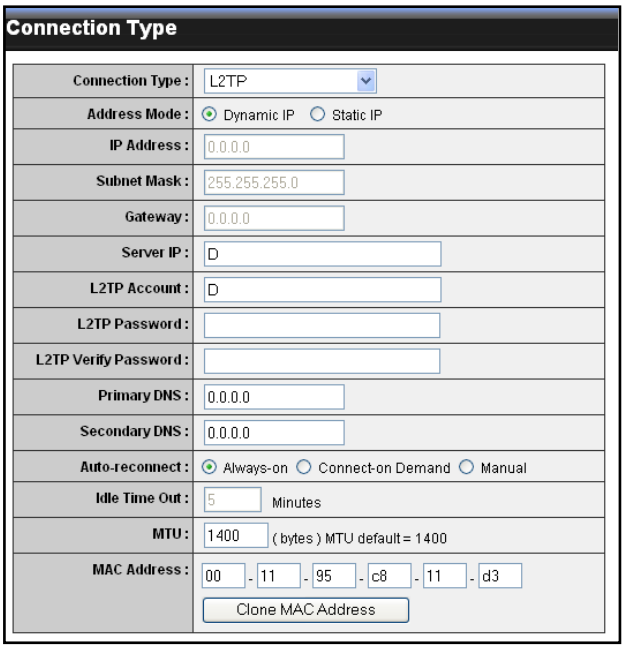
MTU
Adjust the MTU (Maximum Transmission Unit) for optimal performance with your ISP. The default value is 1500.

MAC Address
Enter the MAC address of the computer that was last connected to a modem. To enter the MAC address of your current computer, click **Clone MAC Address**.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

L2TP
Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. Your ISP will provided you with a user name and password.

Address Mode
Select **Dynamic IP** (default) or **Static IP** if your ISP provided you with the IP address, subnet mask, and DNS server addresses.



IP Address
Enter the IP address provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Subnet Mask
Enter the subnet mask provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Gateway
Enter the gateway provided by your ISP. This field is available only when **Access Mode** is set to **Static IP**.

Server IP
Enter the server IP address provided by your ISP.

L2TP Account
Enter the L2TP account name provided by your ISP.

L2TP Password
Enter the L2TP password provided by your ISP. Then re-enter it into the next field.

Primary / Secondary DNS
Enter the DNS server addresses provided by your ISP.

Auto-reconnect
Select reconnect option: **Always-on**, **Connect-on Demand**, and **Manual** .

Idle Time Out
Enter the time wherein the travel router will cut off the Internet connection after the specified period of inactivity (in minutes). This field is disabled when **Auto-reconnect** is **Always-on**.

MTU
Adjust the MTU (Maximum Transmission Unit) for optimal performance with your ISP. The default value is 1400.

MAC Address
Enter the MAC address of the computer that was last connected to a modem. To enter the MAC address of your current computer, click **Clone MAC Address**.

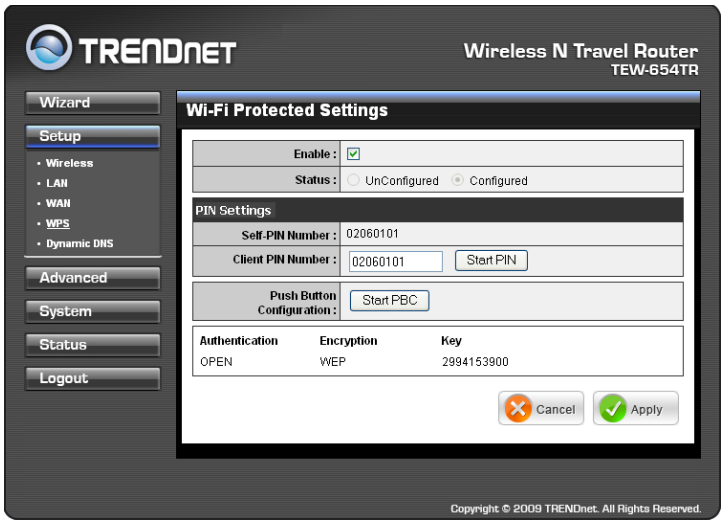
Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Wi-Fi Protected Setup (WPS) Settings

Wi-Fi Protected Setup (WPS) is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on a wireless network.

Enable
Check the box to enable WPS function.

Status
Displays WPS status: **UnConfigured** or **Configured**.



There are 2 methods used in WPS configuration:

- **Push Button:** If the client device has a WPS button.
- **PIN Number:** If the client device has a WPS PIN number.

Self-PIN Number
Displays the default PIN number of the travel router.

Client PIN Number
Enter the client's PIN number. This PIN number will be used to communicate with the travel router to connect to the network.

Start PIN
Click this button to start WPS configuration process if the client device has a WPS

PIN number.

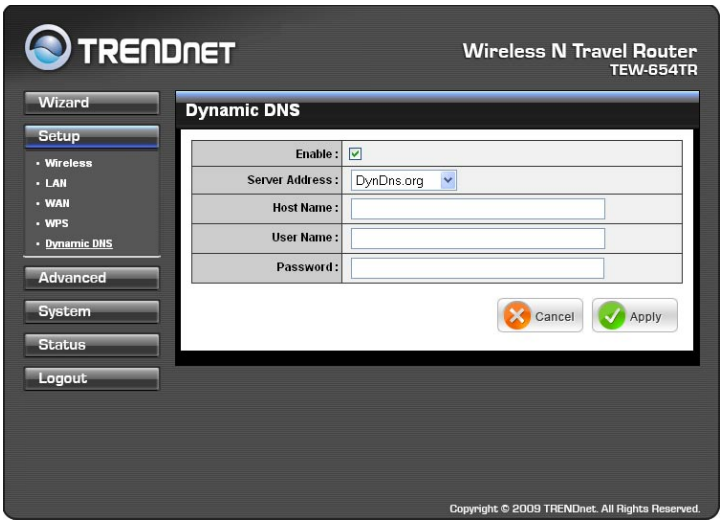
Push Button Configuration

Click the **Start PBC** button to start WPS configuration process if the client device has a WPS button.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Dynamic DNS Settings

Use the Dynamic DNS submenu to synchronize the dynamic DNS server with your current public IP address when you are online.



Enable

Check the box to enable dynamic DNS function. If this box is unchecked, the fields below are all disabled.

Server Address

Select the server address from the list of available servers.

Host Name

Enter the host name.

User Name

Enter the user name.

Password

Enter the password.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

4.2.3 Advanced

The Advanced menu configurations greatly affect the operating performance of the travel router. This menu is intended for advanced users. It is recommended to retain the default settings. Do not change any of the configurations if you are unsure about it.

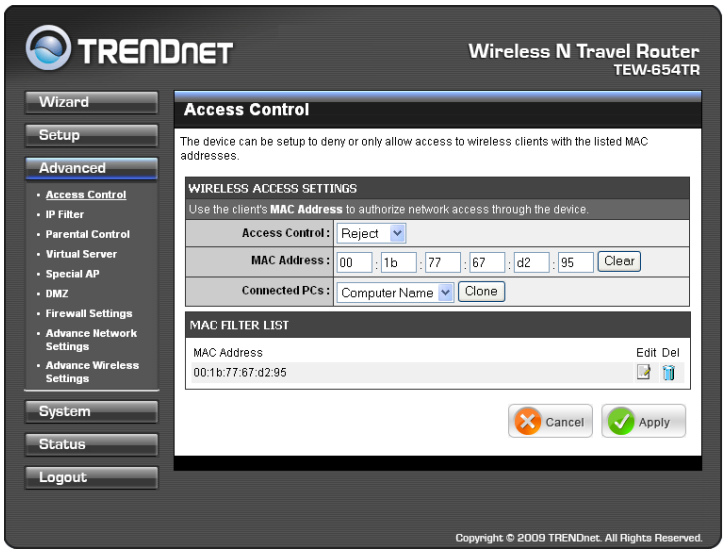
Access Control

The Access Control menu allows you deny or only allow access to certain wireless clients by filtering their MAC addresses.

Access Control

Select the type of access from the list:

- **Disable:** Disable access control.
- **Reject:** Deny the MAC addresses shown on the list to access the wireless network.
- **Accept:** Only allow the MAC addresses shown on the list to access the wireless network.



MAC Address

Displays the cloned MAC address. To clear the MAC address, click **Clear**.

Connected PCs

Select the name of the connected client that you want to clone. Click **Clone** to clone its MAC address.

To grant or block access:

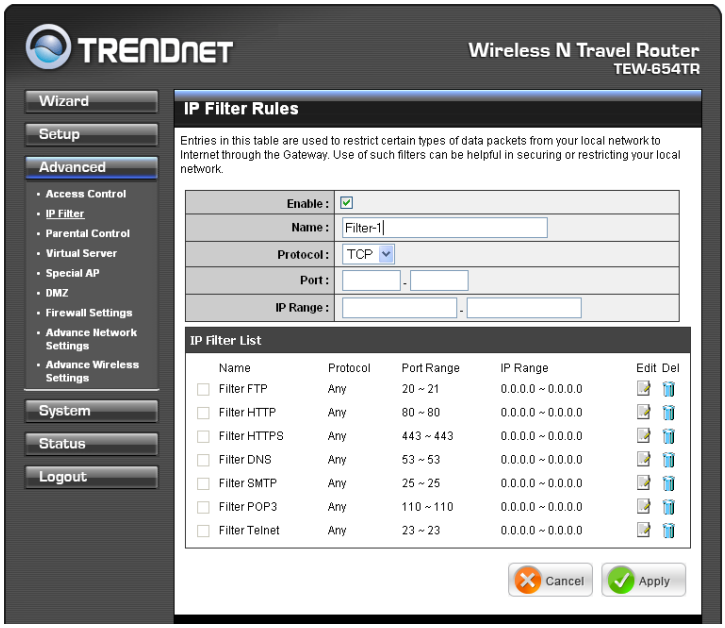
1. Select the client from the **Connected PCs** list, then click **Clone**. The cloned MAC address is displayed in the **MAC Address** field.
2. Click **Apply** to add MAC address in the **MAC Filter List**. The system will reboot.
3. After rebooting, select the **Access Control** option: **Disable**, **Reject** or **Accept**.
4. Click **Apply** to save setting. The system will reboot for changes to take effect.
5. To add more MAC addresses, repeat steps 1-4.

To edit the access control of a MAC address, click its corresponding icon.

To delete the MAC address from the list, click its corresponding icon.

IP Filter

The IP Filter menu allows you to restrict a range of IP adresses to access the Internet.



Enable
Check the box to enable filter. Uncheck to disable filter.

Name
Create a filter name.

Protocol
Select the type of protocol to use: **TCP**, **UDP**, or ***** (any).

Port
Enter the port range of the protocol.

IP Range
Enter the starting and ending IP addresses which are not allowed to access the Internet.

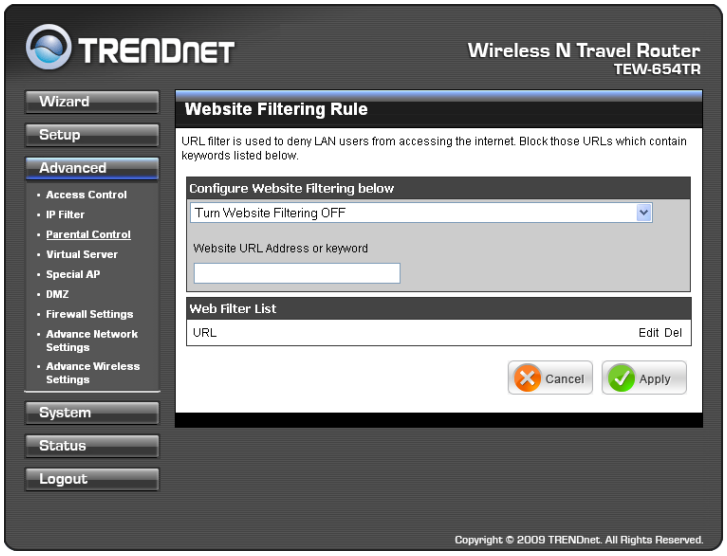
IP Filter List
Displays the list of filter profiles. By default, a number of profiles have been created and are all disabled. A checkmark before the filter name indicates that the profile is enabled.

To edit a profile, click the corresponding icon.
To delete a profile, click the correspond icon.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Parental Control

The Parental Control menu allows you to restrict or only allow computers from accessing specific websites.



To configure website filtering, do the following:

1. Select the type of filter from the list:
   - **Turn Website Filtering OFF**: All website can be accessed by the computers on the network.
   - **Turn Website Filtering ON and ALLOW computers access to ONLY these sites**: Computers can only access the website or website with the keywords specified on the **Website URL Address or keyword** box.
   - **Turn Website Filtering ON and DENY computers access to ONLY these sites**: Computer cannot access the website or website with the keywords specified on the **Website URL Address or keyword** box.
2. Enter the URL Address or keywords to set filter on the **Website URL Address or keyword** box.

Website Filter List

Displays the list of filter profiles.

To edit a filter profile, click the corresponding icon.

To delete a filter profile, click the correspond icon.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Virtual Server

The Virtual Server menu allows you to configure the travel router as a virtual server. Remote users accessing the Web or FTP services through the WAN can be automatically redirected to local servers in the LAN.

Enable
Check the box to enable virtual server. Uncheck to disable.

Name
Create a virtual server name.

Protocol
Select the type of protocol to use: **TCP**, **UDP**, or **Both**.

Private Port
Enter the port number of the being used as a virtual server.

Public Port
Enter the port number of the of the WAN that will be used to provide access to the virtual server.

LAN Server
Enter the LAN IP address that will be assigned to the virtual server.

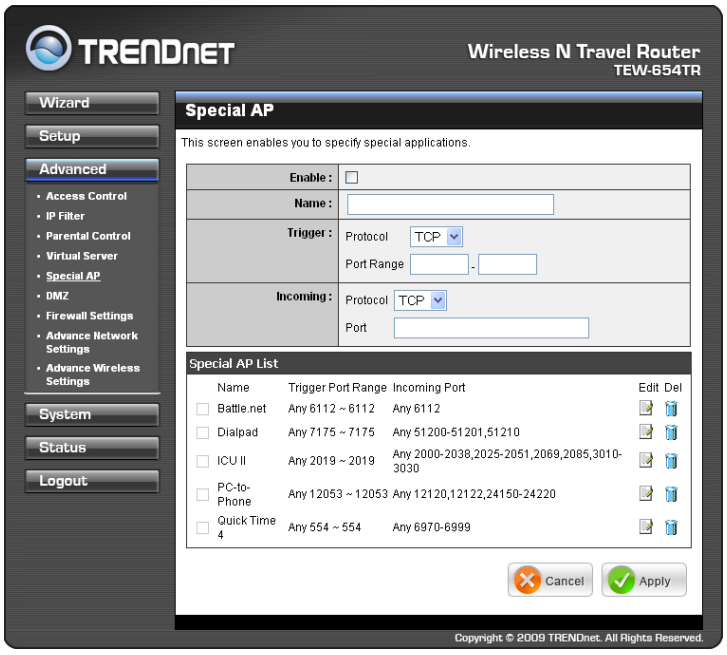
Virtual Server List
Displays the list of virtual server profiles. By default, a number of profiles have been created and are all disabled. A checkmark before the virtual server name indicates that the profile is enabled.

To edit a profile, click the corresponding icon.
To delete a profile, click the correspond icon.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Special AP

Some applications such as Internet games, video conferences, and others, require multiple connections that are usually blocked by NAT (Network Address Translation). The Special AP menu allows you to configure special applications that will connect via the travel router's WAN connection.



Enable
Check the box to enable special AP function. Uncheck to disable.

Name
Create a special AP name.

Trigger
Defines whether the user has access to the application.

- **Protocol:** Select the protocol to access the application: **TCP**, **UDP**, or ***** (any).
- **Port Range:** Enter the port range that can access the application.

Incoming
Defines the incoming communication that users are permitted to connect with.

- **Protocol:** Select the protocol for incoming communication: **TCP**, **UDP**, or ***** (any).
- **Port Range:** Enter the port range for incoming communication.

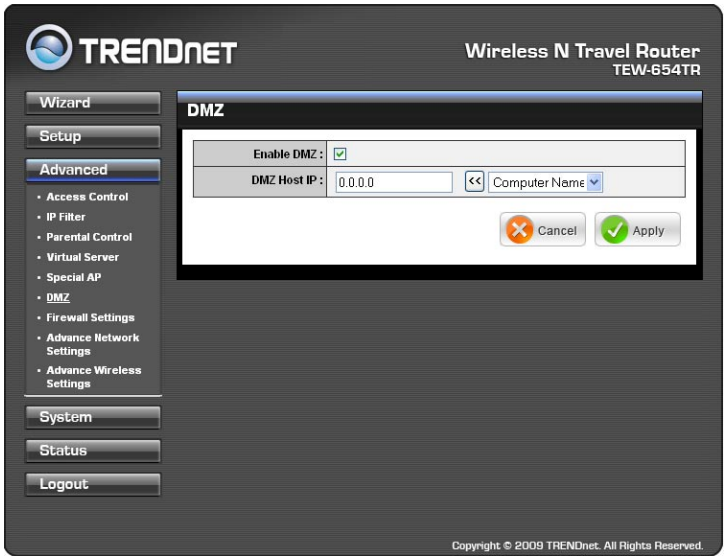
Special AP List
Displays the list of special AP profiles. By default, a number of profiles have been created and are all disabled. A checkmark before the special AP name indicates that the profile is enabled.

To edit a profile, click the corresponding icon.
To delete a profile, click the correspond icon.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

DMZ

The DMZ (Demilitarized Zone) menu allows you to create a DMZ for computers that cannot access Internet applications properly and have security settings. All access will be redirected to the DMZ host.



Enable

Check the box to enable DMZ function. Uncheck to disable.

DMZ Host IP

The host IP address to act as a DMZ host with unlimited Internet access. You can either type an IP address or generate it from a list of computers.

To generate the IP address:

1. Select the computer name from the list.
2. Click the **<<** button. The computer's IP address is shown on the **DMZ Host IP** box.

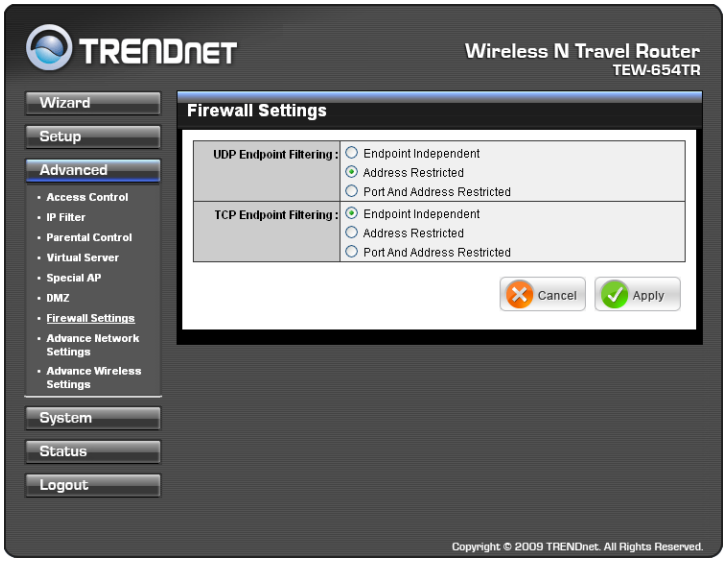
Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Note:

Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.

Firewall Settings

A firewall protects your network from outsiders or unauthorized users or other networks.



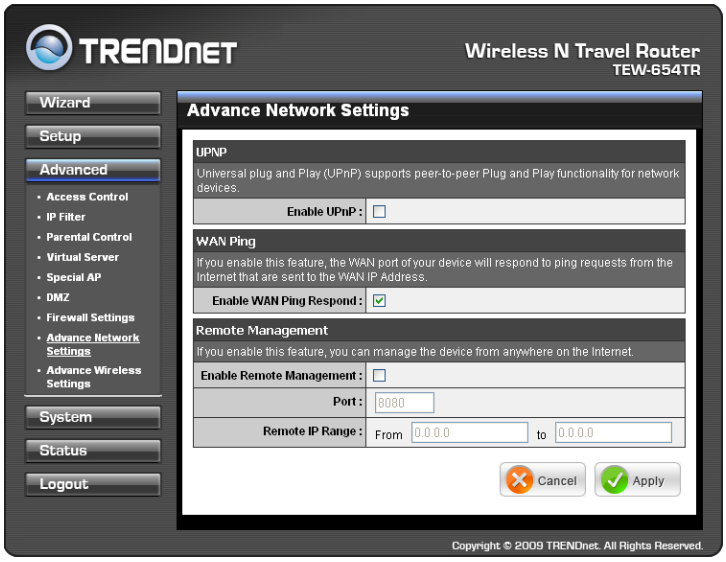
UDP / TCP Endpoint Filtering

Select any of the following options:

- **Endpoint Independent:** Once a LAN application has created a connection through a specific port, all incoming traffic will be forwarded to the same port. There is a risk in security.
- **Address Restricted:** Incoming traffic will be forwarded to the same IP address of the outgoing connection. This provides better security than endpoint independent.
- **Port and Address Restricted:** Incoming traffic is sourced from the IP address you originally connected to, and that it is replying from the same port that you connected to. This provides the best security.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Advanced Network Settings



UPNP

Check the **Enable UPnP** box to use UPnP (Universal Plug and Play) feature. UPnP supports peer-to-peer functionality for network devices.

WAN Ping

Check the **Enable WAN Ping Respond** box to allow the travel router to respond to ping requests from the Internet.

Remote Management

This feature allows you to configure the travel router from the Internet by a web browser.

Enable Remote Management

Check the box to enable remote management. Uncheck to disable.

Port

The port number used for web configuration.

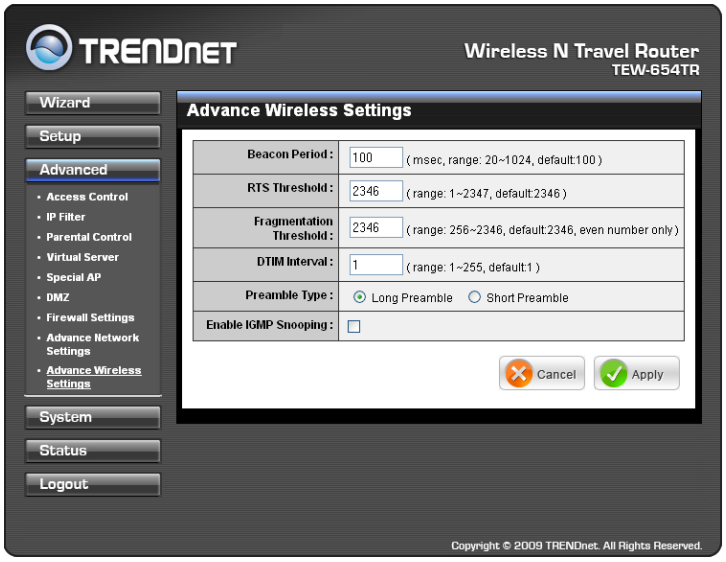
Remote IP Range

Enter the starting and ending IP addresses to allow remote management.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

4. ROUTER MODE

Advanced Wireless Network Settings



Beacon Period

Enter the interval period of time for the access point to send out beacons to synchronize the wireless network. The default value is 100 milliseconds.

RTS Threshold

The default and the recommended value is 2346. Should you encounter inconsistent data flow, only minor adjustments should be made.

Fragmentation Threshold

Fragmentation threshold refers to the amount of packets that will be fragmented before transmission. The default and recommended value is 2346 bytes.

DTIM Interval

This value indicates the interval of Delivery Traffic Indication Message (DTIM). A DTIM is a countdown field informing clients of the next window for listening to broadcast and multicast messages. The default value is 1.

Preamble Type

Preamble is use to limit the packets of data for transmission. When the connection is bad, it is recommended to use the **Short Preamble**.

Enable IGMP Snooping

Check the box to enable Internet Group Management Protocol (IGMP) snooping. This function restrains multicast traffic in a switched network.

Once configuration is complete, click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

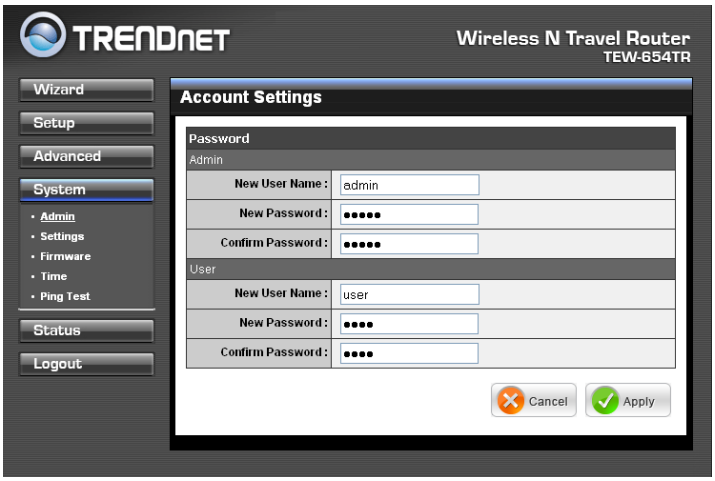
4.2.4 System

Admin

The Admin submenu allows you to change the administrator (Admin) user name and password, as well as setup another User account.

Administrator
The administrator has overall rights to view and edit the web configurations. The default user name and password are “admin”.

User
The user can only view the web configurations but cannot edit them.



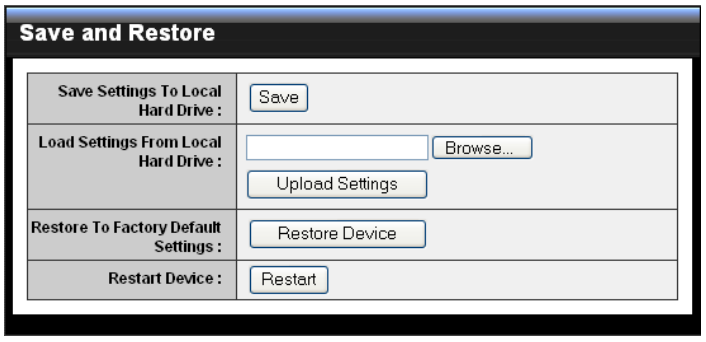
New User Name
Enter the new user name.

New / Confirm Password
Enter the password.

Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Settings

The Settings submenu provides backup and restore setting functions.



Save Settings to Local Hard Drive
Use this function to save the current configuration settings to your local hard drive. Click **Save**, then select the folder where you want to save the file.

Load Settings From Local Hard Drive
Use this function to retrieve saved configuration settings from the local hard drive.

1. Click **Browse** to locate the file.
2. Click **Upload Settings** to transfer and apply the settings to the travel router.

Restore to Factory Default Settings
Click **Restore Device** to restore all configurations to the factory default settings. All changes in configuration will be deleted.

Restart Device
Click **Restart** to reboot the travel router.

4. ROUTER MODE

Firmware

The Firmware submenu allows you to upgrade the firmware to the latest version.

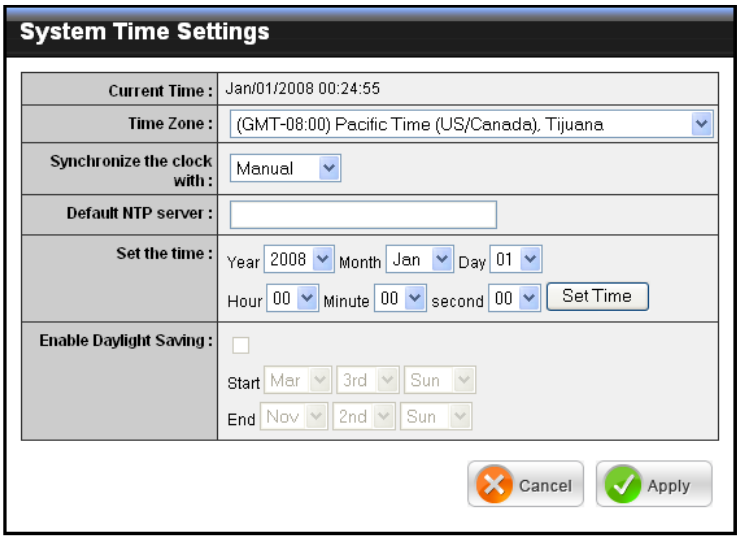
Current Firmware Version
Displays the current firmware version.

Firmware Date
Displays the date when the firmware was last updated.

1. Download the latest firmware from the manufacturer's website, and save it to a disk.
2. Click Browse to locate the file.
3. Click **Apply** to start firmware update. The system will reboot to complete update.

Time

The Time submenu allows you to manually adjust the system time settings or synchronize it with a server.



Current Time
Displays the current date and time settings.

Time Zone
Select the time zone in your area.

Synchronize the clock with
Select:

- **Manual:** To manually adjust the date and time.
- **Automatic:** To synchronize date and time with the server.

Default NTP Server
Enter the NTP server address to synchronize the date and time with.

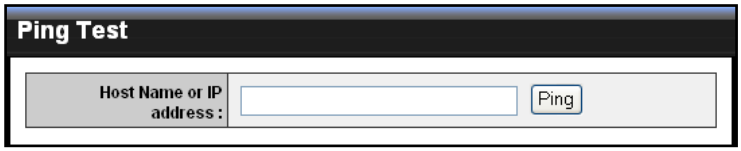
Set the Time
Use this option to manually set the date and time. This option is only available when **Synchronize the clock with** is set to **Automatic**.

Enable Daylight Saving
Check the box to enable daylight saving time. Use the Start and End field boxes to specify the starting and ending dates.

Click **Apply** to save and apply settings, or click **Cancel** to cancel changes. The travel router will restart for new settings to take effect.

Ping Test

Enter the host name or the IP address on the box, then click **Ping** to check the status of the connection and determine whether the specified host name or IP address is present on the Internet.

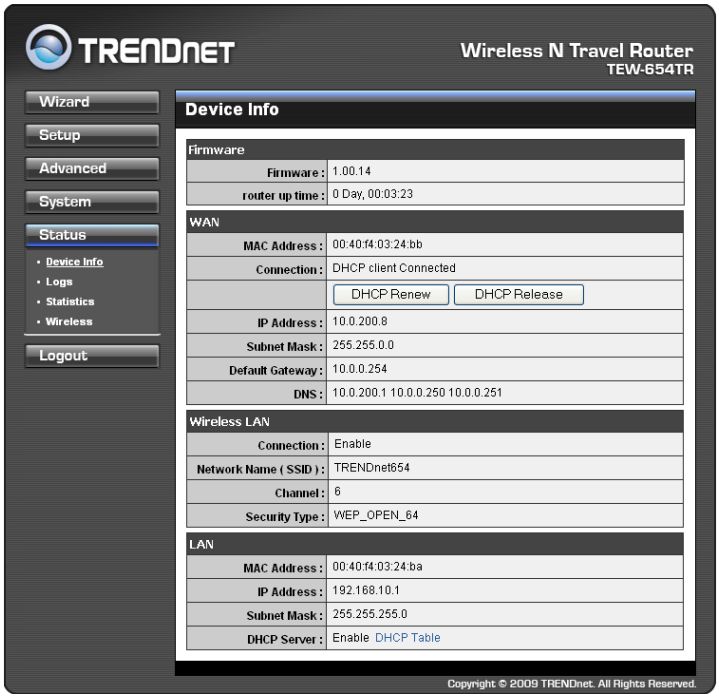


4.2.5 Status

The Status menu displays device, logs, traffic, and connection information.

Device Info

This page displays the Firmware Version, WAN, Wireless LAN and LAN information.



DHCP Renew

Click to reassign IP addresses to client stations connected to the WAN via the travel router.

DHCP Release

Click to release all IP addresses assigned to client stations connected to the WAN via the travel router.

DHCP Table

Click to view DHCP list.****

4. ROUTER MODE

Logs

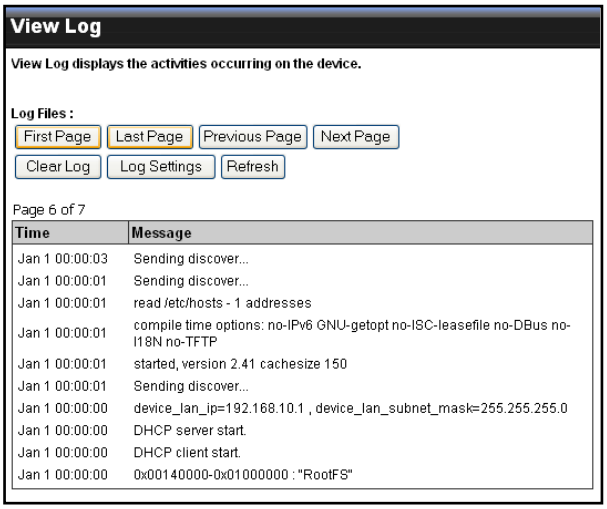
This page displays the recorded events that occur within the wireless network.

Click the following buttons to view the **First Page**, **Last Page**, **Previous Page**, and **Next Page**.

To delete log data, click **Clear Log**.

To change log settings, click **Log Settings**.

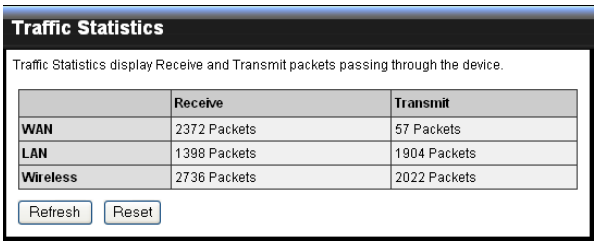
To refresh list, click **Refresh**.



Statistics

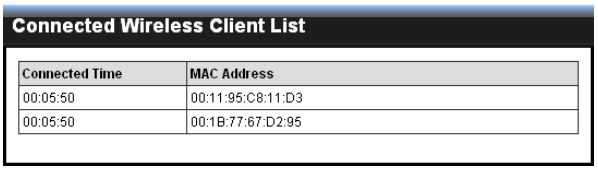
This page displays the traffic statistics of received and transmitted packets that passed through the travel router.

Click **Refresh** to refresh table.



Wireless

This page displays the information of connected wireless clients such as the time of connection and their MAC addresses.



Appendix A: Regulatory & Safety Information

Wireless LAN, Health and Authorization

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- Onboard airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

FCC (Federal Communications Commission) 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 interference, and
2. This device must accept any interference, including interference that may cause undesired operation of this device.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

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

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

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

Europe - EU Declaration of Conformity

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

EN60950-1: 2006

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.3.2 (2008-04)

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

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

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

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

CE 0560 !

APPENDIX

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-654TR je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-654TR overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-654TR in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-654TR vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, TRENDnet, declares that this TEW-654TR is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-654TR cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΩΝΕΙ ΟΤΙ TEW-654TR ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-654TR est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-654TR è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TEW-654TR atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-654TR atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-654TR in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-654TR jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-654TR megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-654TR jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	TRENDnet declara que este TEW-654TR está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-654TR v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TEW-654TR spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-654TR tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-654TR står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

NCC 警語：

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Appendix B: Specifications

Hardware	
Interface	1x 10/100Mbps Auto-MDIX port
Standards	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0) IEEE 802.3/IEEE 802.3u Fast Ethernet IEEE 802.3x Flow Control
Supported Protocol	TCP/IP, NAT, PPPoE/PPTP/L2TP, HTTP, DHCP Server/Client
LED Indicator	Power LAN: Link, ACT WLAN: ACT
Power Consumption	2.5 watts (max)
Power Adapter	5V, 1.2A or power via the included USB cable from PC
Dimensions (LxWxH)	60 x 80 x 18.5mm (2.4 x 3.2 x 0.7in)
Weight	50g (1.6oz)
Temperature	Operating: 0° ~ 40° C (32° ~ 104° F) Storage: -10° ~ 70° C (14° ~ 158° F)
Humidity	10% ~ 90% max (non-condensing)
Certification	FCC, CE
Wireless	
Module Technique	DBPSK/DQPSK/CCK/OFDM (BPSK/QPSK/16-QAM/64-QAM)
Antenna	2 on-board antennas
Frequency	2.412 ~ 2.484 GHz
Data Rate (auto fallback)	802.11b: 11Mbps, 5.5Mbps, 2Mbps, and 1Mbps 802.11g: 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps,12Mbps, 9Mbps, and 6Mbps 802.11n: up to 300Mbps
Output Power	802.11b: 14dBm (typical) 802.11g: 14dBm (typical) 802.11n: 12dBm (typical)
Receiving Sensitivity	802.11b: -85dBm (typical) at 11Mbps 802.11g: -68dBm (typical) at 54Mbps 802.11n: -59dBm at 135Mbps
Security	64/128-bit WEP (Hex & ASCII), WPA/WPA2-Radius (802.1x), WPA-PSK/WPA2-PSK MAC address, IP and URL filtering
Channels	1 ~ 11 (FCC), 1~13 (ETSI)

Appendix C:
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-654TR – 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

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