

User's Guide

TRENDnet[®]



AC 1750 Dual Band Wireless Router

TEW-823DRU

Table of Contents

Product Overview.....	4
Features.....	4
Package Contents	4
Hardware Overview.....	5
<i>Front View</i>	5
<i>Rear View</i>	5
Wireless Considerations	6
<i>Connection Performance</i>	6
<i>Security Checklist</i>	6
Installation	6
Connect the Power.....	6
Connect the Computer.....	6
Check the Installation.....	7
Initial Setup.....	7
Configure the Computer.....	7
<i>Windows 7/8/8.1</i>	7
<i>Windows XP/2000</i>	7
<i>Windows Vista</i>	7
<i>MAC OS 10.4/10.5/10.6</i>	7
Setup Wizard	8
Basic Router Settings	8
Log in to Management Page.....	8
Management Page Structure.....	9
Wireless Settings	10
Guest Network	12

Parental Control	12
Wireless Networking and Security	14
Tips to Improve Wireless Reception.....	14
<i>Device Orientation</i>	15
Choose the Security Type for Wireless Network	15
<i>Wireless Encryption Types</i>	15
Connect Wireless Devices using WPS.....	18
<i>Hardware Push Button (PBC) Method (recommended)</i>	18
<i>PBC (Software/Virtual Push Button)</i>	18
<i>PIN (Personal Identification Number)</i>	19
Connect Wireless Devices Using MAC Filter.....	19
Advanced Wireless Settings.....	20
<i>Multiple SSID Connections</i>	20
<i>Wireless Bridging Using WDS</i>	21
<i>Advanced Settings</i>	23
Advanced Router Settings.....	24
Configure Manually the Internet Connection.....	24
Clone a MAC address.....	25
Change the IP Address.....	25
Configure the DHCP Server	26
Configure DHCP Reservation	26
Add Static Routes	27
Enable Dynamic Routing.....	28
Enable/Disable UPnP	29
Identify Your Network on the Internet	29
Configure IPv6 Settings.....	30

Create Schedules	30
Configure Access Control Rules	31
<i>Block a specific service or multiple services</i>	31
<i>Block All Services</i>	32
Configure Inbound Filter Rules	32
Configure Firewall Settings	33
DMZ	33
Virtual Server	33
Special Applications	34
Gaming	35
ALG	36
Enable Remote Access	37
Allow/Deny Ping Requests from the Internet	37
Configure Quality of Service Settings	38
Using External USB Storage	40
Configure File Sharing Server	40
Configure FTP Server	41
Maintenance	42
Change Login Password	42
Set the Date and Time	42
Backup System Settings	43
Load System Settings	43
Reset to Factory Defaults	44
Reboot the System	44
Update System Firmware	44
View Wireless Client List	45

View System Information	45
IPv6 Status	47
View Events Log	47
Appendix	48
Regulatory and Safety Information	48
Federal Communication Commission Interference Statement	48
Europe – EU Declaration of Conformity	48
Specifications	50

Product Overview

TRENDnet's AC1750 Dual Band Wireless Router, model TEW-823DRU, produces the ultimate wireless experience with gigabit wireless speeds. Manage two wireless networks—the 1300 Mbps Wireless AC band for the fastest wireless available and the 450 Mbps Wireless N band to connect common wireless devices. The TEW-823DRU can easily handle the demands of multiple HD streams in a busy connected home.

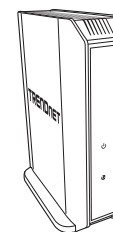
Features

- ✓ Compatible with IEEE 802.11ac technology provides 3TX/3RX wireless speed up to 1300Mbps data rate.
- ✓ Compatible with IEEE 802.11n high rate standard to provide wireless speed of 450Mbps data rate.
- ✓ Compatible with IEEE 802.11g high rate standard to provide wireless speed of 54Mbps data rate.
- ✓ Simultaneously transmit both 2.4 GHz and 5 GHz wireless networks.
- ✓ IEEE 802.11b/g/n/ac Infrastructure operating modes.
- ✓ 4 x 10/100/1000Mbps Gigabit Ethernet port for LAN with Auto MDI-X function.
- ✓ 1 x 10/100/1000Mbps Gigabit Ethernet WAN port for ADSL / Cable Modem with Auto MDI-X function.
- ✓ Supports Multiple Input Multiple Output(MIMO) technology with 3TX/3RX(11a/b/g/n/ac).
- ✓ Allow auto fallback data rate for optimized reliability, throughput and transmission range.
- ✓ Supports enhance security for WPA-PSK, WPA2-PSK, WPA and WPA2.
- ✓ Advance wireless security of up to WPA2-RADIUS.
- ✓ Web-based configuration tools and management via WEB Browser.
- ✓ Supports Wi-Fi Multimedia(WMM).
- ✓ Supports WPS (Wi-Fi Protected Setup Specification Windows).
- ✓ Supports PPPoE / PPTP / L2TP protocol for ADSL.
- ✓ Supports NAT for share 1 IP address to all LAN user.
- ✓ Supports DHCP Server / Client.
- ✓ Supports Firewall protection, Virtual server mapping, Special application setting.

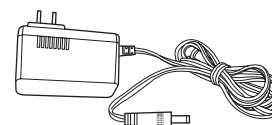
- ✓ Supports UPnP.
- ✓ Supports statistics information.
- ✓ Supports IPv6 (Internet Protocol v6).
- ✓ Supports Wireless Distribution System (WDS) for wireless network bridging.
- ✓ Plug in a USB flash or storage drive to share content across the network.

Package Contents

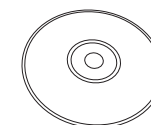
Check if your package contains the following items. If any item is missing or appears damaged, contact your dealer.



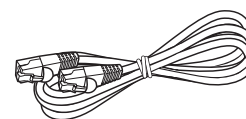
TEW-823DRU Router



Power adapter (12V, 2A)



CD-ROM with User's Guide



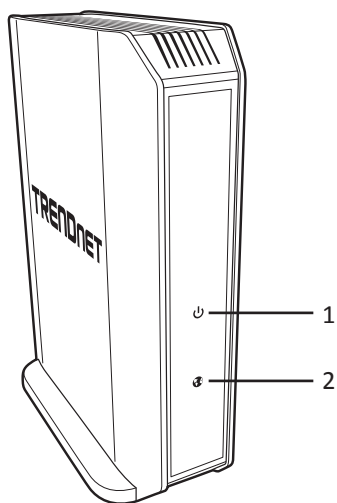
RJ-45 Ethernet cable (1.5m / 5ft.)



Multi- Language Quick Installation Guide

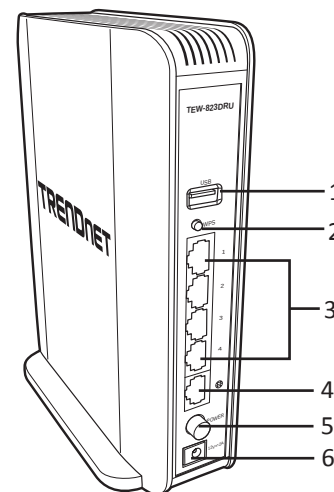
Hardware Overview

Front View



No.:	Item	Description
1	Power LED	Lights up when the router is powered on. • Solid GREEN: Normal operation. • Blinking GREEN: WPS is activated. • Off: No power. <i>Note: The LED will stop blinking and remains solid GREEN automatically after the WPS process is completed.</i>
2	Internet port (Link/Activity) LED	Lights up to indicate Internet connection status. • Solid GREEN: Router is physically connected to the modem network or Ethernet port with a network or Ethernet cable. • Blinking GREEN: Data is transmitted or received through the Internet port of the router. • Off: No active Internet connection.

Rear View



No.:	Item	Description
1	USB 2.0 port	Connect USB storage devices to share over the network via FTP or Windows® SMB/CIFS, Samba.
2	WPS (Wi-Fi Protected Setup) button	Press to activate WPS. <i>Note: The Power LED will blink when WPS is activated.</i>
3	LAN ports 1~4	Connect the Ethernet cables from the router LAN ports to your wired network devices.
4	Internet port	Connect an Ethernet cable from the router Internet port to your modem.
5	Power switch	Push to switch the router on or off.
6	DC-in port	Connect the supplied DC power input connector here.

Wireless Considerations

Connection Performance

A number of factors affect the performance of wireless connection. Consider the following guidelines to ensure high-range and stable connectivity.

- ✓ Keep the router and other wireless devices away from obstructions, such as walls or buildings. Each obstruction can reduce the range of a wireless device.
- ✓ Keep the router and other wireless devices away from devices that produce radio frequency (RF) noise, such as microwave ovens or radios.
- ✓ Keep the router and other wireless devices away from any device operating on the 2.4GHz frequency, such as cordless phones or remote controls.
- ✓ Antenna orientation affects the wireless signal. Determine the best orientation and adjust the antenna position of your device.

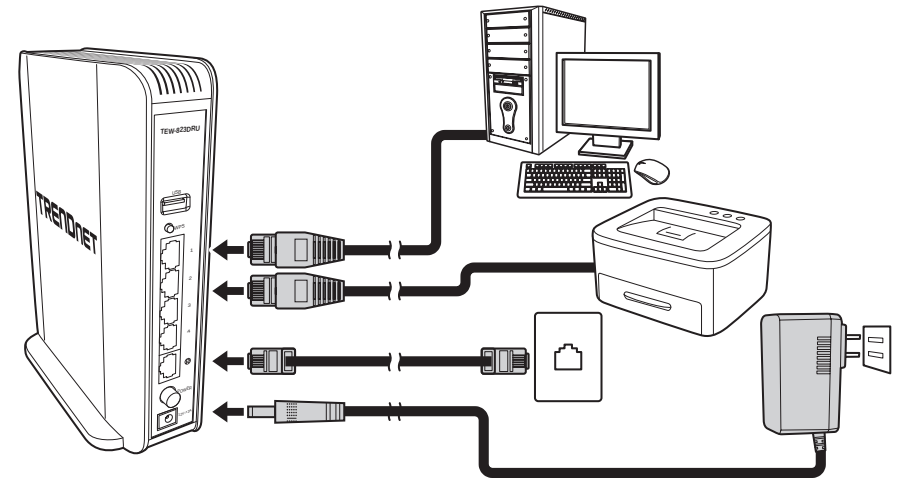
Security Checklist

Wireless networks are easy to install and convenient to use. However, wireless network signals can also be intercepted easily. To prevent unauthorized users from connecting to your wireless network, follow the guidelines below.

- ✓ Change the default wireless network name.
Your device has a default Service Set Identifier (SSID) which is the wireless network name. Change the SSID with a unique name to identify your network. The SSID can be up to 32 characters in length.
- ✓ Change the default password.
Your device has a default password. You have to enter this password to change your network settings. Change the password to prevent unauthorized user from intruding into your network and changing the settings.
- ✓ Enable MAC address filtering.
Your device supports Media Access Control (MAC) address filtering. You can assign a MAC address on each computer that you want to connect to your wireless network. When MAC address filtering is enabled, only the computers with the specified MAC addresses are allowed access.
- ✓ Enable encryption
Your device supports Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WAP/WPA2) encryption. To ensure a high level of security, enable the highest security encryption and use strong passphrases, avoid using words that can be found in the dictionary.

Installation

Make sure that all devices are powered off before starting installation.



Connect the Power

- 1 Connect the power adapter to the power port of your router.
- 2 Plug the power adapter to a power outlet.
- 3 Push the **Power** button to turn your router on.

⚠ *Note: Use only the supplied power adapter. Using other power adapters may cause damage to the device.*

Connect the Computer

- 1 Connect one end of the RJ-45 cable to the LAN port of your router.
- 2 Connect the other end of the RJ-45 cable to the LAN port of the computer.

Check the Installation

To ensure that all devices are properly connected, check the LED indicators on the front of your router. For basic installation, the following LED must be lit:

- ✓ Power LED
- ✓ Internet port LED

The lighted LED indicators vary depending on the type of connection that you make. Refer to *"Front View"* on page 5 for more information about the LED indicators.

Initial Setup

Configure the Computer

Note: The following procedures on configuring the network settings can be used as general guidelines. It is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring the network settings.

Windows 7/8/8.1

- 1 Open **Control Panel** and click **Network and Sharing Center**.
- 2 Click **Change Adapter Settings** and right-click the **Local Area Connection** icon.
- 3 Click **Properties > Internet Protocol Version 4 (TCP/IPv4)**.
- 4 Click **Obtain an IP address automatically** and click **OK**.

Windows XP/2000

- 1 Open **Control Panel** and double-click the **Network Connection** icon.
- 2 Right-click the **Local Area Connection** icon and then click **Properties**.
- 3 Click **Internet Protocol (TCP/IP) > Properties**.
- 4 Click **Obtain an IP address automatically** and click **OK**.

Windows Vista

- 1 Open **Control Panel** and click **Network and Internet**.
- 2 Click **Manage Network Connections** and right-click the **Local Area Connection** icon > **Properties**.
- 3 Click **Internet Protocol Version (TCP/IPv4) > Properties**.
- 4 Click **Obtain an IP address automatically** and click **OK**.

MAC OS 10.4/10.5/10.6

- 1 From the **Apple**, drop-down list, select **System Preferences**.
- 2 Click the **Network** icon.
- 3 From the **Location** drop-down list, select **Automatic**.
- 4 Select and view your Ethernet connection. Do one of the following:
 - » In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
 - » In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

5 Configure TCP/IP to use DHCP. Do one of the following:

- » In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
- » In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

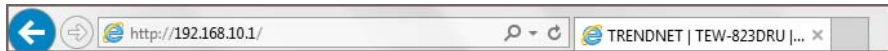
6 Restart your computer.

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

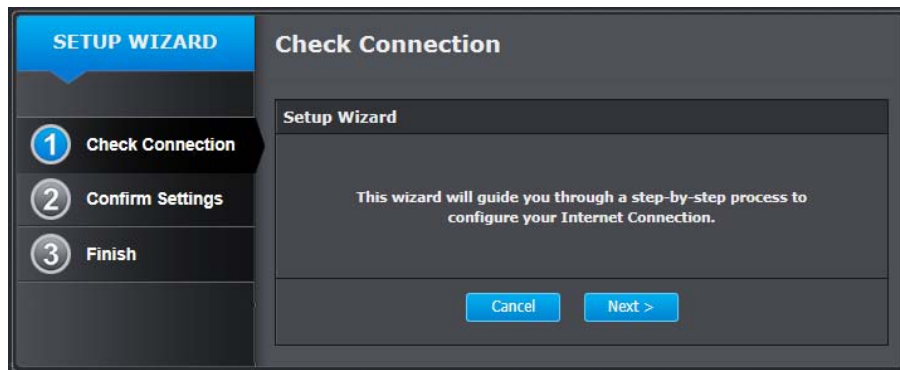
Setup Wizard

1 Open your web browser and enter the URL/domain name <http://tew-823dru> or IP address <http://192.168.10.1>. The wizard will automatically appear.

- ⓘ *Note: If you have already configured your router before, the wizard will no longer appear automatically. In your web browser, enter <http://tew-823dru> or you can access the router management using the default IP address <http://192.168.10.1>. Your router will prompt you for a user name and password. Enter your user name and password and click **Advanced** > **Setup** > **Wizard**.*



2 Follow the on-screen instructions to configure your Internet Connection.

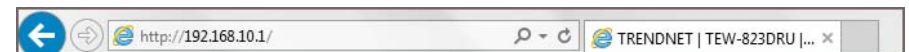


Basic Router Settings

Log in to Management Page

- ⓘ *Note: You can access your through the use of your Internet web browser, such as Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™.*

1 Open your web browser and enter the URL/domain name <http://tew-823dru> or IP address <http://192.168.10.1>.



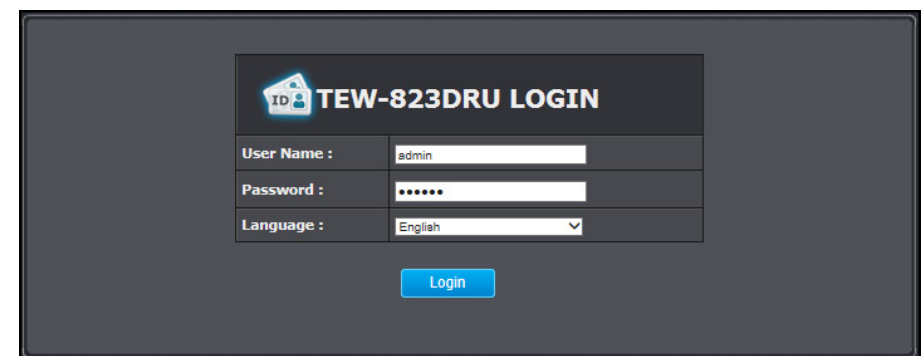
2 Enter the user name, password, and select your preferred language.

- ⓘ *Note:*

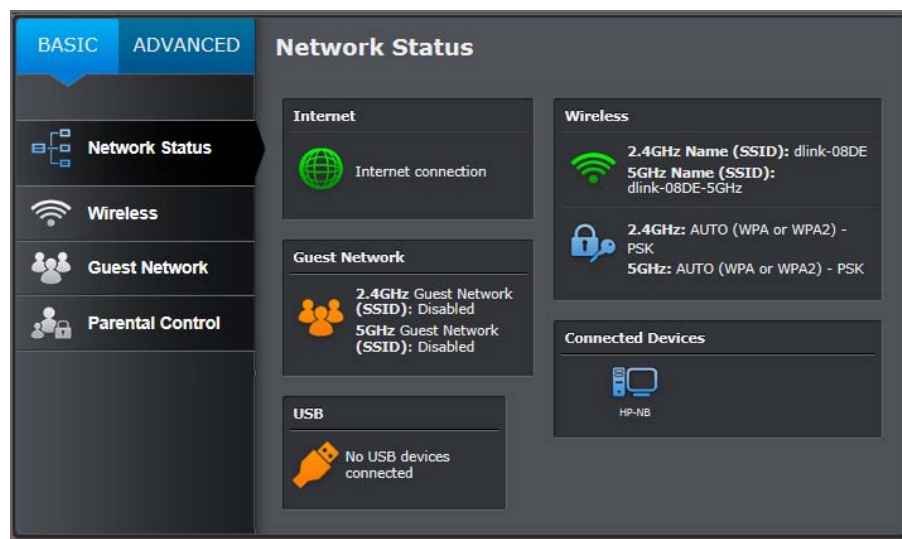
- The default user name is "admin".
- For security purposes, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router.
- User name and password are case sensitive.



3 Click Login.



The management page opens.



Management Page Structure

Basic

- Network Status
- Wireless
 - ◆ 2.4GHz Settings & Security
 - ◆ 5GHz Settings & Security
- Guest Network
- Parental Control
 - ◆ MAC/IP Address Filter
 - ◆ Website Filter

Advanced

- Administrator
 - ◆ Status Information
 - ◆ IPv6 Status Information
 - ◆ System Log
 - ◆ Advanced Network (UPnP)
 - ◆ Settings Management (Export/Import configuration / Reset to factory default / Reboot)
 - ◆ Time and Date Settings
- Setup
 - ◆ LAN Settings (IP Address Settings / DHCP Server Setting / DHCP Reservation)
 - ◆ WAN Settings
 - ◆ Routing
 - ◆ IPv6 Settings
 - ◆ Schedule
 - ◆ Firmware
 - ◆ Management (Administrator Password / Dynamic DNS / Remote Management)

Advanced (continued)

- ◆ QoS
- ◆ Wizard
- Wireless 2.4GHz
 - ◆ WDS
 - ◆ Advanced
 - ◆ Multiple SSID
 - ◆ MAC Filter (Wireless)
 - ◆ WPS
 - ◆ Station List
- Wireless 5GHz
 - ◆ WDS
 - ◆ Advanced
 - ◆ Multiple SSID
 - ◆ MAC Filter (Wireless)
 - ◆ WPS
 - ◆ Station List
- Security
 - ◆ Access Control (IP Protocol Filter)
 - ◆ Inbound Filter
- Firewall
 - ◆ DMZ
 - ◆ Virtual Server
 - ◆ Special Applications
 - ◆ Gaming
 - ◆ ALG
- USB
 - ◆ File Sharing Server
 - ◆ FTP Server

Wireless Settings

Basic > Wireless (2.4GHz or 5GHz)

Note: Refer to "Choose the Security Type for Wireless Network" on page 15 for information on choosing the security type for wireless network.

This section allows you to configure the basic settings required for your wireless network such as your wireless network name (SSID) and Wi-Fi key.

1 Log into your router management page (refer to "Log in to Management Page" on page 8).

2 Click on **Basic > Wireless** tab.

3 Modify any of the settings in **Wireless 2.4GHz** or **Wireless 5GHz** section and click **Apply** to save the changes.

» **Radio On/Off:** Click the radio on/off button to enable/disable the wireless radio.

Note: It is recommended to keep wireless radios enabled.

New Schedule: Click **New Schedule** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Please refer to "Set the Date and Time" on page 42 and "Create Schedules" on page 30 to create a schedule.

Radio On/Off	RADIO OFF	Always ▼	New Schedule
--------------	-----------	----------	--------------

» **Wireless Mode:** Select the appropriate transmission mode. When applying the Wireless Mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Wireless devices that support 802.11ac are backwards compatible and can connect wirelessly at 802.11n or 802.11a.
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Connecting at 802.11a or 802.11n will limit the capability of your 802.11ac supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Allowing 802.11a or 802.11n devices to connect to an 802.11ac capable wireless

network may degrade the wireless network performance below the higher performance and data rates of 802.11ac.

- Wireless devices that only support 802.11n or 802.11a will not be able to connect to a wireless network that is set to 802.11ac only mode.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.
- Wireless devices that only support 802.11a will not be able to connect to a wireless network that is set to 802.11n only mode.

Wireless 2.4GHz

Wireless Mode	2.4GHz 802.11 b/g mixed mode 2.4GHz 802.11 n only 2.4GHz 802.11 b/g/n mixed mode
---------------	--

Wireless 5GHz

Wireless Mode	5GHz 802.11 a only 5GHz 802.11 n only 5GHz 802.11 a/n mixed mode 5GHz 802.11 a/n/ac mixed mode
---------------	---

» **Wireless Network Name (SSID):** Enter the wireless name (SSID) for your wireless network.

Note: This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you.

By default, the router's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.

Wireless Network Name (SSID)	dlink-08DE-5GHz
------------------------------	-----------------

» **Broadcast Network Name (SSID)**

- **Enable:** Allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
- **Disable:** Turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network. Disabling this setting will disable WPS functionality.

Broadcast Network Name (SSID)	☐ Enable ☒ Disable
-------------------------------	---

- » **Enable Auto Channel Scan:** Check this option to set your router to scan for which wireless channels to use automatically.
- » **Frequency (Channel):** Selecting the Auto option will set your router to scan for the appropriate wireless channel to use automatically. Click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighbouring wireless networks.

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

- » **Channel Width:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n and 802.11ac.

- For greater 802.11n performance, select Auto 20/40MHz.
- For greater 802.11ac performance, select Auto 20/40/80MHz.

It is recommended to use the default channel width settings.

- ⓘ *Note: Please note that the default settings may provide more stability than the higher channel bandwidth settings such as Auto 20/40/80MHz for connectivity in busy wireless environments where there are several wireless networks in the area.*

- **20MHz:** This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than 20/40MHz (Auto) for connectivity in busy wireless environments where there are several neighbouring wireless networks in the area.
- **Auto 20/40MHz (11n) or Auto 20/40/80MHz (11ac):** When this setting is active, this mode is capable of providing higher performance only if the wireless devices support the channel width settings. Enabling Auto 20/40MHz or Auto 20/40/80MHz typically results in substantial performance increases when connecting an 802.11ac/n wireless client.

Channel Width	☒ 20 MHz ☐ Auto 20/40 MHz
---------------	--

Channel Width	☐ 20 MHz ☒ Auto 20/40 MHz ☐ Auto 20/40/80 MHz
---------------	--

- 4 In **Security** section, click **Security Mode** drop-down list to select your wireless security type.

Security Mode	Disable WEP-OPEN WEP-SHARED WEP-AUTO WPA WPA-PSK WPA2-PSK WPA2-Personal Mixed WPA2 WPA2-Enterprise Mixed
---------------	--

For more information on security, refer to [“Choose the Security Type for Wireless Network” on page 15.](#)

Guest Network

Basic > Guest Network (2.4GHz or 5GHz)

Creating an isolated and separate wireless guest network (2.4GHz or 5GHz) allows wireless clients to connect to your network for Internet access only and keep your local LAN network safe by restricting guest access to your LAN network resources such as shared documents and media files on your computers, network storage, and printers.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Basic > Guest Network** tab.
- 3 Modify any of the settings in **Guest Network - 2.4GHz** or **Guest Network - 5GHz** section and click **Apply** to save the changes.
 - » **Radio On/Off:** Check this option to enable the wireless guest network.
New Schedule: Click **New Schedule** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.
 - ⚠ *Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Please refer to [“Set the Date and Time” on page 42](#) and [“Create Schedules” on page 30](#) to create a schedule.*

Radio On/Off	☐	Always ▼	New Schedule
--------------	--------------------------	----------	--------------

- » **Wireless Network Name (SSID):** Enter the wireless name (SSID) for your wireless network.

Wireless 2.4GHz

Wireless Network Name (SSID)	TRENDnet823_2.4GHz
------------------------------	--------------------

Wireless 5GHz

Wireless Network Name (SSID)	TRENDnet823_5GHz_gu
------------------------------	---------------------

- » **WLAN Partition:** When this options is enabled, wireless client devices connected to your guest network(s) will be restricted from accessing other guests.

WLAN Partition	☐ Disable ☒ Enable
----------------	---

- » **Internet Access Only:** When this option is checked, wireless client devices connected to your guest network(s) will be restricted from accessing your private LAN and wireless clients connected to your primary wireless network, Internet access only. If unchecked, allows wireless client devices connected your guest network(s) complete access to your private LAN, primary wireless network, and Internet.

- 4 In **Security** section, click **Security Mode** drop-down list to apply a different wireless security type and key to the guest network.

Security Mode	Disable WEP-OPEN WEP-SHARED WEP-AUTO WPA WPA-PSK WPA2-PSK WPA2-Personal Mixed WPA2 WPA2-Enterprise Mixed
---------------	--

For more information on security, refer to [“Choose the Security Type for Wireless Network” on page 15](#).

Parental Control

Basic > Parental Control

Parental control settings allow you to set up restrictions/filters specifically who is allowed or denied access to your network for a specified period of time and restricted access to web content.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Basic > Parental Control** tab.
- 3 Add an access rule.

Access Rule (MAC/IP Filter)

Every network device has a unique, 12-digit MAC (Media Access Control) address. Every network device must be assigned or configured with a specific IP address in order to communicate with your network which is typically assigned by your router DHCP server automatically. Using access rules, you can deny specific computers and other devices from using this router's wired or wireless network by specifying the MAC address or IP address.

- » **Rule Enable:** Check the checkbox to enable the access rule.

Rule Enable	☐
-------------	--------------------------

» **Rule Name:** Enter the rule name.

Rule Name	
-----------	----------------------

» **Address Type:** Select which **Address Type** to apply the filter. (MAC Address or IP Address).

Address Type	☐ IP ☒ MAC
--------------	---

Note: If your device is not listed, please refer to your computer or device documentation to find the MAC address.

» **IP Address/MAC Address:** Manually enter the **MAC Address** or **IP Address** in the field.

ⓘ *Note: If the network device is connected to your router, you can also click the drop-down list to choose one of the network devices (MAC Address/IP Address) detected by your router.*

IP Address		<<	Host Name	▼
------------	----------------------	----	-----------	---

» **Schedule (Optional):** Click to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

ⓘ *Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Please refer to "Set the Date and Time" on page 42 and "Create Schedules" on page 30 to create a schedule.*

Schedule	Always ▼
----------	----------

4 Click **Add** to add the access rule to the **Access Rule List**. Wait of the rule to be added.

Note:

- Clicking **Reset** will discard your settings and clear all fields.
- In the Access Rule List, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the Delete column next to the rule you would like to delete.

5 In Website Filter section, configure the website filter.

Website Filter

You may want to block computers or devices on your network access to specific websites (e.g. www.xxxxxxxx.com, etc.), also called domains or URLs (Uniform Resource Locators). You may also apply a schedule when these websites are allowed or denied.

Website Filter	
Configure Website Filter below	Disable DENY computers access to ONLY these sites ALLOW computers access to ONLY these sites

» **Disable:** Disables website filtering.

» **DENY computers access to ONLY these sites:** Only **Deny** computers/devices access to the listed websites and allow access to others.

» **ALLOW computers access to ONLY these sites:** Only **Allow** computers/devices access to the listed websites and deny access to others.

6 Do the following to add a web pages URL filter rule.

» **Rule Enable:** Check the checkbox to enable the access rule.

Rule Enable	☐
-------------	--------------------------

» **Rule Name:** Enter the rule name.

Rule Name	
-----------	----------------------

» **URL:** Enter a URL (ex. www.xxxxxxxx.com) to apply for the filter or block.

URL	
-----	----------------------

» **Schedule (Optional):** Select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

ⓘ *Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Please refer to "Set the Date and Time" on page 42 and "Create Schedules" on page 30 to create a schedule.*

Schedule	Always ▼
----------	----------

7 Click **Add** to add the access rule to the **Access Rule List**. Wait of the rule to be added.

Note:

- Clicking **Reset** will discard your settings and clear all fields.
- In the URL Filter Rule List, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Wireless Networking and Security

Tips to Improve Wireless Reception

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

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

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

Device Orientation

The antenna configuration has been optimized for performance and connectivity when wireless client devices are located on either side of the router compare to the front (LED panel) or back (Ports).



Choose the Security Type for Wireless Network

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

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

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

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

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router.

Note: This encryption standard will limit connection speeds to 54Mbps.

- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
- **WPA-Auto:** This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption.

Note: WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps.

- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.

Note: Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.

The following table is a brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n/ac
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 300Mbps (11n) or 867Mbps (11ac)
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

⚠ *Note: The compatible wireless standard depends on the data rate supported by the device:*

- **802.11n:** 150Mbps.
- **802.11ac:** 433Mbps, 867Mbps.

Selecting WEP

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

Security	
Security Mode	WEP-OPEN ▼
WEP	
Default Key	Key 1 ▼
WEP Key 1 :	0000000000 Hex ▼
WEP Key 2 :	0000000000 Hex ▼
WEP Key 3 :	0000000000 Hex ▼
WEP Key 4 :	0000000000 Hex ▼

» **Security Mode:** Choose **WEP-OPEN**, **WEP-SHARED**, or **WEP-AUTO**.

⚠ *Note: It is recommended to use Open because it is known to be more secure than Shared Key.*

» **Default Key:** Enter the WEP key. This is the password or key that is used to connect your computer to this router wirelessly. You can enter 64-bit or 128-bit key. You can enter up to four keys but only the one chosen as the Default Key will be used.

⚠ *Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.*

» **Hex/ASCII:** Enter the WEP key format. Refer to the table below for the acceptable characters and lengths for each format.

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

Selecting WPA-PSK / WPA2-PSK / WPA2-Personal Mixed

In the **Security Mode** drop-down list, select **WPA-PSK**, **WPA2-PSK**, or **WPA2-Personal Mixed**. Please configure the settings and click **Apply** to save the changes.

Note: If selecting WPA or WPA2 security along with the TKIP cipher, the device will be limited to operate in 802.11a/g modes with data rates up to 54Mbps.

Security	
Security Mode	WPA2-Personal Mixed ▼
If selecting WPA or WPA2 security along with the TKIP cipher, please note that the device will be limited to operate in 802.11a/g modes with data rates of only up to 54Mbps.	
WPA	
WPA Cipher	☐ TKIP/AES
Pre-Shared Key	yjgle89078
Key Update Interval	3600 seconds

The following section outlines options when selecting **WPA-PSK**, **WPA2-PSK**, or **WPA2-Personal Mixed**,

- » **WPA Cipher:** The available Cipher Type for WPA-PSK is **TKIP** and for WPA2-Personal Mixed is **TKIP/AES**. For WPA2-PSK the default Cipher Type is **AES** but if you need the backward-compatibility (so it would accept WPA connections), choose **TKIP/AES**
 - » **WPA Pre-Shared Key:** Enter the passphrase.
 - This is the password or key that is used to connect your computer to this router wirelessly.
 - » **Key Update Interval:** Enter the time interval (seconds) of when the network passphrase will rotate.
- Note:** It is recommended to use the default interval time. Your passphrase will not change, rotation of the key is part of the WPA protocol and designed to increase security.

Selecting WPA / WPA2 / WPA2-Enterprise Mixed

In the **Security Mode** drop-down list, select **WPA**, **WPA2**, or **WPA2-Enterprise Mixed**. Please configure the settings and click **Apply** to save the changes.

Note:

- If selecting WPA or WPA2 security along with the TKIP cipher, the device will be limited to operate in 802.11a/g modes with data rates up to 54Mbps.
- This security type requires an external RADIUS server.

Security	
Security Mode	WPA2-Enterprise Mixed ▼
If selecting WPA or WPA2 security along with the TKIP cipher, please note that the device will be limited to operate in 802.11a/g modes with data rates of only up to 54Mbps.	
WPA	
WPA Cipher	☐ TKIP/AES
Key Update Interval	3600 seconds
Radius Server	
IP Address	0.0.0.0
Port	1812
Shared Secret	

The following section outlines options when selecting **WPA**, **WPA2**, or **WPA2-Enterprise Mixed**,

- » **WPA Cipher:** The available Cipher Type for WPA is **TKIP** and for WPA2-Enterprise Mixed is **TKIP/AES**. For WPA2 the default Cipher Type is **AES** but if you need the backward-compatibility (so it would accept WPA connections), choose **TKIP/AES**.
 - » **Key Update Interval:** Enter the time interval (seconds) of when the network passphrase will rotate.
- Note:** It is recommended to use the default interval time. Your passphrase will not change, rotation of the key is part of the WPA protocol and designed to increase security.
- » **IP Address:** Enter the IP address of the RADIUS server. For example, 192.168.10.250.

- » **Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
 ⓘ *Note: It is recommended to use port 1812 which is the default RADIUS port.*
- » **Shared Secret:** Enter the shared secret used to authorize your router with your RADIUS server.

Connect Wireless Devices using WPS

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

- ⓘ *Note: You will not be able to use WPS if you set the SSID Broadcast setting to Disabled or if you are using WEP security.*

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

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

- ⓘ *Note: Please refer to your wireless device documentation for details on the operation of WPS.*

Hardware Push Button (PBC) Method (recommended)

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

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. The WPS LED will blink to indicate WPS has been activated on your router. Please refer to ["Product Overview" on page 4](#).

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

PBC (Software/Virtual Push Button)

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

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

- 1 Log into your router management page (refer to ["Log in to Management Page" on page 8](#)).
- 2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > WPS > WPS Action**.
- 3 To add a wireless device to your network, next to **PBC**, click the **Start Push Button** button. Then push the WPS button on the wireless device (consult wireless device's User's Guide for length of time) you are connecting.

WPS Action	
If you are using the Virtual Push Button method, click Start Push Button, then push and activate WPS on your wireless client device. If you are using the PIN method, enter the wireless client device PIN in the field and click Start PIN, then activate the WPS PIN method on your wireless client device.	
PIN	Start PIN
PBC	Start Push Button

- 4 Wait for your router to finish the WPS process.

- ⓘ *Note: You should see a message on your WPS client device indicating the WPS was successful.*

WPS Summary	
WPS Current Status	Processing...63
WPS Configured	Yes
WPS SSID	dlink-08DE
WPS Security Mode	WPA2 Only - PSK
WPS Encrypt Type	AES
WPS Key	yjgle89078
AP PIN	95048109

PIN (Personal Identification Number)

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

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

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > WPS > WPS Action**.
- 3 To add a wireless device to your network, next to **PIN**, enter the 8-digit numeric PIN number of the wireless client device and click **Start PIN**.

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

WPS Action	
If you are using the Virtual Push Button method, click Start Push Button, then push and activate WPS on your wireless client device. If you are using the PIN method, enter the wireless client device PIN in the field and click Start PIN, then activate the WPS PIN method on your wireless client device.	
PIN	XXXXXXXX Start PIN
PBC	Start Push Button

- 4 Wait for your router to finish the WPS process.

ⓘ *Note: You should see a message on your WPS client device indicating the WPS was successful.*

WPS Summary	
WPS Current Status	Processing...63
WPS Configured	Yes
WPS SSID	dlink-08DE
WPS Security Mode	WPA2 Only - PSK
WPS Encrypt Type	AES
WPS Key	yjgle89078
AP PIN	95048109

Connect Wireless Devices Using MAC Filter

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

This MAC filter is dedicated to filter on each band and each SSID. Every network device has a unique, 12-digit MAC (Media Access Control) address. Every network device must be assigned or configured with a specific IP address in order to communicate with your network which is typically assigned by your router DHCP server automatically. Using access rules, you can deny specific computers and other devices from using this router's wired or wireless network by specifying the MAC address or IP address.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > Security > Wireless MAC Filter**.
- 3 Review the MAC Filter options. Click **Apply** to save changes.

Select SSID

- » **Select SSID:** If you have multiple SSIDs configured, click the drop-down list to select which SSID to apply the MAC filter.

Wireless MAC Filter

» Filter Mode:

- **Disabled:** Disables MAC address filter.
- **Allow** (listed computes access and deny all others): Selecting this function allows computers/devices with MAC addresses listed to access the local network (LAN/WLAN), web management, and the Internet.
- **DENY listed computes access and deny all others:** Selecting this function denies computers/devices with MAC addresses listed from access to the local network (LAN/WLAN), web management, and the Internet.

- » **MAC Address:** Enter the MAC address of the wireless device to apply to this filter.

Select SSID	
Select SSID	TRENDnet823_2.4GHz_guest ▼

Wireless MAC Filter	
Filter Mode	Disable ▼
MAC Address	(Ex: 00:11:22:33:44:55)

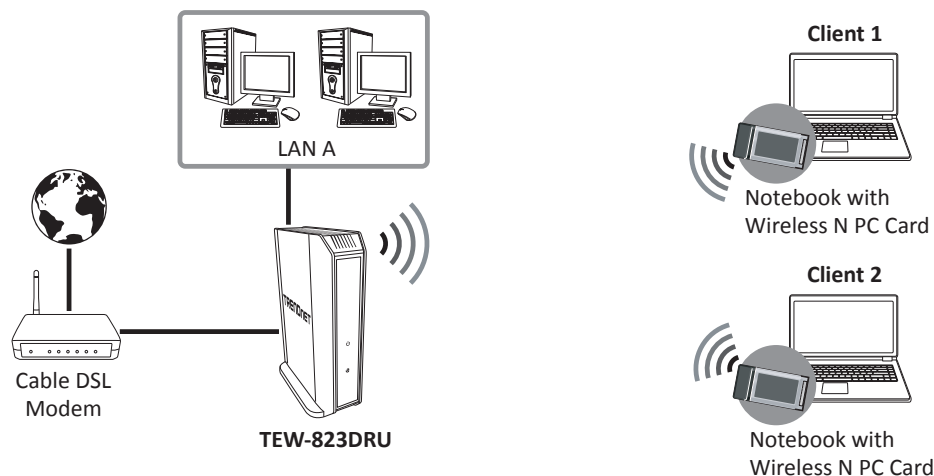
Advanced Wireless Settings

The advanced wireless features provide can provide you with additional options for setting up your wireless network such as multiple SSID and WDS (Wireless Distribution System) or wireless bridging.

Multiple SSID Connections

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

The multiple SSID feature allows you to broadcast up to 2 SSIDs (or wireless network names). When wireless devices are searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Since they appear as separate wireless networks, they are also referred to as virtual APs (Access Points) since they appear as separate wireless access points but are actually all being broadcasting and managed by a single wireless access point. Each virtual AP can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private. The diagram shows an example of a client connecting to SSID 1 and another client connecting to SSID 2.



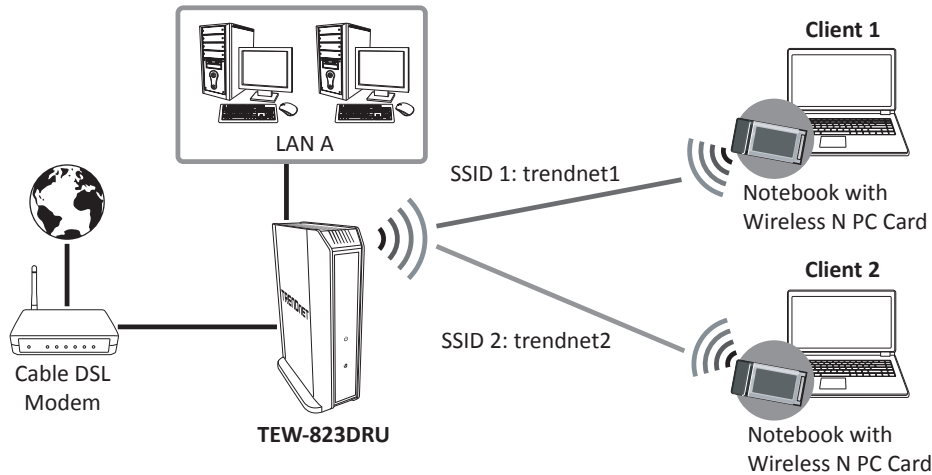
To configure multiple SSID on your router, do the following:

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > Multiple SSID**.
- 3 In Multiple SSID1 or SSID2, configure the following parameters:
 - » **Radio On/Off:** Check the checkbox to enable the additional SSID.
 - **New Schedule:** The schedule function allows you to define a schedule when the additional SSID should be turned on. To define a new schedule, click **New Schedule** and refer to [“Create Schedules” on page 30](#). After you have created a new schedule, click the drop-down list and the new schedule will be available for selection.
 - » *Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Please refer to [“Set the Date and Time” on page 42](#) and [“Create Schedules” on page 30](#) to create a schedule.*
 - » **Wireless Network Name (SSID):** Enter the wireless name (SSID) for additional SSID.
- 4 In **Security** section, click **Security Mode** drop-down list to apply a different wireless security type and key to the guest network.

Wireless Network Name (SSID)	trendnet2
------------------------------	-----------

Security Mode	Disable WEP-OPEN WEP-SHARED WEP-AUTO WPA WPA-PSK WPA2-PSK WPA2-Personal Mixed WPA2 WPA2-Enterprise Mixed
---------------	--

The following diagram shows an example of a client connecting to SSID 1 and another client connecting to SSID 2.



5 Click **Apply** to save the changes.

Note: To discard the changes, click **Cancel**.

Wireless Bridging Using WDS

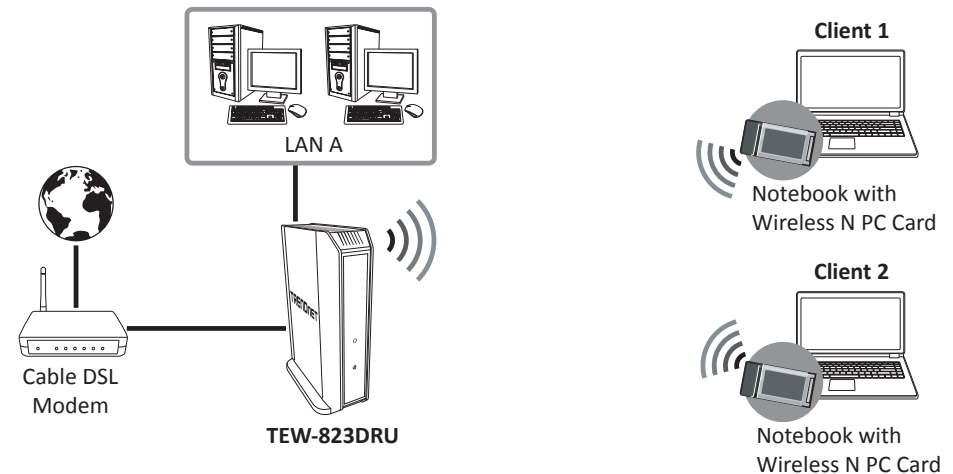
Advanced > Wireless (2.4GHz or 5GHz) > WDS

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

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

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

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



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

- Make sure different IP addresses are assigned to each WDS supported device used for bridging to avoid IP address conflict. For example, 192.168.10.1; 192.168.10.2; 192.168.10.3. Refer to ["Change the IP Address" on page 25](#) for changing the LAN IP address.
- If you are using more than one WDS supported router, ensure the LAN DHCP server is enabled on only one router and disabled on all the others to avoid IP address conflict. Refer to ["Configure the DHCP Server" on page 26](#) for DHCP server options.
- Configure the same wireless channel and use the same on all WDS supported wireless devices. Refer to ["Wireless Settings" on page 10](#) for configuring basic wireless settings.
- Configure the same wireless security and key on all WDS supported devices. Refer to ["Wireless Settings" on page 11](#) for configuring wireless security settings.

To configure WDS bridging between TEW-823DRU routers, do the following:

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > WDS**.
- 3 Click on the **WDS** drop-down list and select **Enable**.

IMPORTANT: Ensure the basic wireless security (Basic > Wireless > Security) on router is set to **WEP** or **Disabled** mode. WDS cannot function in **WPA** or **WPA2** mode.

WDS	Enable	Site survey
-----	--------	-------------

Note: Click Site survey to search for Access Point's MAC address to connect.

- 4 Enter the MAC address of the other WDS supported wireless device you are bridging. For example, 00:11:22:AA:BB:CC.

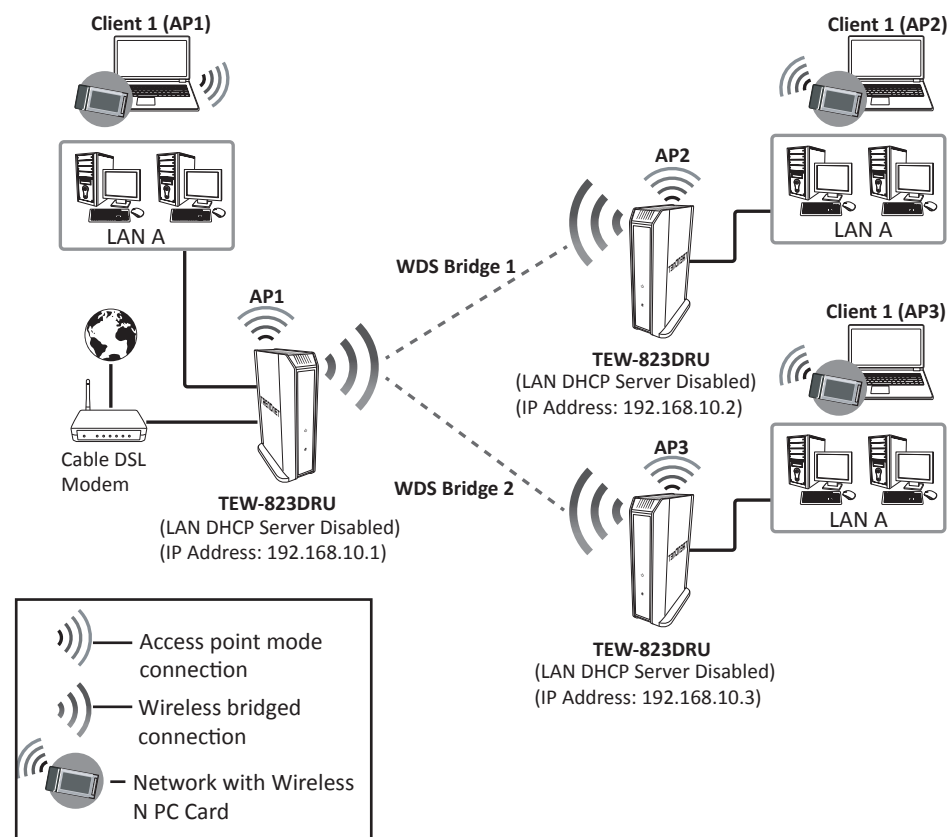
Remote AP MAC Address	
Remote AP MAC Address	
Remote AP MAC Address	
Remote AP MAC Address	

- 5 Click **Apply** to save the changes.

Note: To discard the changes, click **Cancel**.

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

The following illustration shows the access point with WDS enabled connection diagram.



Advanced Settings

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

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

1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).

2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > Advanced**.

3 In Advanced Wireless section, configure the following parameters:

- » **Beacon Period:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information on the router's wireless network. The interval is the amount time between each beacon transmission.
Default Value: 100 milliseconds (range: 100-1000)
- » **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- » **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- » **RTS Threshold:** The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2347 (range: 1-2347).
- » **TX Power:** This setting allows you to adjust the wireless transmit power to a lower setting. In busy wireless environments, lowering the transmit power may improve better performance and connectivity and decrease interference with neighbouring

wireless networks.

- » **Short Preamble:** Using a short preamble can potentially increase throughput as the transfer time is 96 microseconds versus the more commonly used long preamble 192 microseconds. However, using a short preamble is not supported using 802.11b legacy devices, in some cases cause wireless interoperability issues, and increase the error rate in some installations. The preamble is the information sent from the wireless transmitter to the receiver indicating when data is incoming.

Advanced Wireless		
Beacon Period	100	ms (range 100 - 1000, default 100)
DTIM	1	(range 1 - 255, default 1)
Fragment Threshold	2346	(range 256 - 2346, default 2346)
RTS Threshold	2347	(range 1 - 2347, default 2347)
TX Power	Full	▼
Short Preamble	☐ Enable ☒ Disable	

4 In HT Physical Mode section, configure the following parameters:

- » **20/40 Coexistence (2.4GHz only):** 20/40MHz Coexistence allows for the auto-fallback from 40MHz to 20MHz channel width operation when neighbouring 802.11 wireless networks are detected.
- » **Guard Interval:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections.
- » **MCS:** Allows you to lock down the wireless transmission rate.
- » **Extension channel:** Allows you to assign either the upper or lower extension channels to use for channel bonding when establishing connectivity at the higher channel widths 40MHz and 80MHz.
- » **A-MPDU:** Using Aggregate Multiple Protocol Data Unit will allow the all frames transmitted to be aggregated into larger size A-MPDU formatted frames before sending and receiving potentially increasing the overall throughput.

HT Physical Mode	
20/40 Coexistence	☐ Disable ☐ Enable
Guard Interval	☐ long ☐ Auto
MCS	Auto
Extension Channel	2417MHz (Channel 2)
A-MPDU	☐ Enable ☒ Disable

5 Next to **Multicast-to-Unicast Converter**, select the option to enable or disable.

Multicast-to-Unicast Converter	
Multicast-to-Unicast	☐ Enable ☒ Disable

6 Click **Apply** to save the changes.

*Note: To discard the changes, click **Cancel**.*

Advanced Router Settings

Configure Manually the Internet Connection

Advanced > Setup > WAN Settings

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Setup > WAN Settings**.
- 3 In WAN Connection Type section, click the drop-down list and select the type of Internet connection.

WAN Connection Type	
Connection Type	STATIC DHCP PPPoE L2TP PPTP Russia PPPoE Russia L2TP Russia PPTP

4 Enter the necessary network parameters.

5 Click **Apply** to save the changes.

Note: If you are not sure which Internet connection type you are using, please contact your local Internet Service Provider (ISP).

Clone a MAC address

Advanced > Setup > WAN Settings

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and to prevent the re-provisioning and registration process of a new MAC address with your ISP, then you can clone the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from the previous device (computer or old router that directly connected to the modem, you should first determine the MAC address of the device or computer and manually enter it into your router using the clone MAC address feature.

Note: For many ISPs that provide dynamic IP address automatically, typically, the stored MAC address in the modem is reset each time you restart the modem. To clear your modem stored MAC address, typically the procedure is to disconnect power from the modem for approximately for one minute, then reconnect the power. For more details on this procedure, refer to your modem's User Guide/Manual or contact your ISP.

- 1 Log into your router management page (refer to "[Log in to Management Page](#)" on page 8).
- 2 Click on **Advanced > Setup > WAN Settings**.
- 3 In MAX Address Clone section, click **Copy Your PC's MAC Address** to copy your computer's MAC address in the **MAC Address** field.

MAC Address Clone	
MAC Address	(Ex: 00:11:22:33:44:55) Copy Your PC's MAC Address

- 4 Click **Apply** to save the changes.

Note: To discard the changes, click **Cancel**.

Change the IP Address

Advanced > Setup > LAN Settings

Usually, you do not need to change your router IP address settings. Typically, the router IP address settings only need to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

Note: It is recommended to keep your router IP address settings as default.

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

- 1 Log into your router management page (refer to "[Log in to Management Page](#)" on page 8).
- 2 Click on **Advanced > Setup > LAN Settings**.
- 3 In LAN Interface Settings section, modify the following settings:
 - » **IP Address:** Enter the new router IP address. For example, 192.168.200.1.
 - » **Subnet Mask:** Enter the new router subnet mask. For example, 255.255.255.0.

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

LAN Interface Setting	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
MAC Address	C0:A0:BB:6E:08:DE

- 4 Click **Apply** to save the changes.

Note:

- To discard the changes, click **Cancel**.
- You will need to access your router management page using your new router IP address. For example, instead of using the default <http://192.168.10.0> your new router IP address will use the format [http://\(new.ipaddress.here\)](http://(new.ipaddress.here)) to access the router management page. You can also continue using the default login URL <http://tew-823DRU>.

Configure the DHCP Server

Advanced > Setup > LAN Settings

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

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Setup > LAN Settings**.
- 3 In DHCP Server Settings section, review and modify the following settings:
 - » **DHCP Server:** Enable or disable the DHCP server.
 - » **DHCP Start IP:** Change the starting address for the DHCP server range. For example, 192.168.10.20.
 - » **DHCP End IP:** Change the ending address for the DHCP server range. For example, 192.168.10.30.
 - » **DHCP Lease Time:** Enter the DHCP lease time in minutes.

🔗 *Note: The DHCP lease time is the amount of time a computer or device can keep an IP address or assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.*

DHCP Server Setting	
DHCP Server	Enable ▼
DHCP Start IP	192.168.10.100
DHCP End IP	192.168.10.199
DHCP Lease Time	1440 (minutes)

- 4 Click **Apply** to save the changes.

🔗 *Note: To discard the changes, click **Cancel**.*

Configure DHCP Reservation

Advanced > Setup > LAN Settings

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, refer to [“Virtual Server” on page 33](#)) or special applications (also called port triggering, refer to [“Special Applications” on page 34](#)).

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Setup > LAN Settings**.
- 3 In Add DHCP Reservation section, do the following:
 - » **Enable:** Enable or Disable the DHCP reservation.
 - » **Computer Name:** Enter a name of the device you will assign the DHCP reservation.
 - 🔗 *Note: Next to the **Computer Name** field, you can click the **Host Name** drop-down list to select an available computer from the DHCP server listing. Click on the available computer to copy the computer's name/IP address, and MAC address information into the respective fields.*
 - » **IP Address:** Enter the IP address to assign to the reservation. For example, 192.168.10.101.
 - » **MAC Address:** Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. For example, 00:11:22:AA:BB:CC.
 - » **Copy your PC's MAC:** To copy your current computer's MAC address to the field, click **Copy**.

Add DHCP Reservation	
Enable	☐
Computer Name	<< Host Name ▼
IP Address	
MAC Address	(Ex: 00:11:22:33:44:55)
Copy your PC's MAC	Copy

- 4 Click **Add** to save the reservation.

🔗 *Note: To discard the changes, click **Clear**.*

You will see the new reservation added to the DHCP Reservations Ready Group section. This is a temporary list until you save changes by clicking **Apply**. You can continue to add more DHCP reservation entries which will appear in this list. Once you have saved the settings, the entries will appear under the DHCP Reservations list. You can click **Reset** to clear the entries in the list or check the Delete option, next to the entry to remove and click **Delete**.

DHCP Reservations Ready Group					
No.	Enable	Computer Name	IP Address	MAC Address	Delete
1	☒	Default	192.168.10.101	B4:99:BA:F5:E9:F9	☐

5 In DHCP Reservation List section, do any of the following:

- » To edit the reservation, click .
- » To delete the single reservation, check the **Delete** checkbox.
- » To delete all the reservations, click **Delete All**.

*Note: To discard the changes, click **Clear**.*

DHCP Reservations List					
Enable	Computer Name	IP Address	MAC Address	Edit	Delete
1 ☒	Default	192.168.10.101	B4:99:BA:F5:E9:F9		☐

Add Static Routes

Advanced > Setup > Routing

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

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

1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).

2 Click on **Advanced > Setup > Routing**.

3 In Add Static Route section, modify the following settings:

- » **Destination IP Address:** Enter the IP network address of the destination network for the route. For example, 192.168.20.0.
- » **Destination IP Netmask:** Enter the subnet mask of the destination network for the route. For example, 255.255.255.0.
- » **Gateway:** Enter the gateway to the destination network for the route. For example, 192.168.10.2.
- » **Metric:** Enter the metric or priority of the route. The metric range is 1-15, the lowest number 1 being the highest priority. For example, 1.
- » **Interface:** Select the interface to assign the route.

Add Static Route	
Destination IP Address :	0.0.0.0
Destination IP Netmask :	0.0.0.0
Gateway :	0.0.0.0
Metric :	1
Interface :	WAN

- 4 Click **Add** to add the static route. The static route information appears on the Static Route List section.

🔗 *Note: To discard the changes, click **Cancel**.*

Delete a Route

To delete a route, check the box in the **No.** column to select which routes to delete, then click **Delete**.

Static Route List					
No.	IP	Netmask	Gateway	Metric	Interface
1 ☐	192.168.20.0	255.255.255.0	10.10.10.2	1	WAN

Enable Dynamic Routing

Advanced > Setup > Routing

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate between the two separate networks, static routing needs to be configured. If you have other routing devices that support dynamic routing protocol, you can enable these routing protocols on your router to learn and automatically generate the routes needed between these networks.

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

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).

- 2 Click on **Advanced > Setup > Routing**.

- 3 In RIP section, do the following:

- » **Enable RIP:** Click the drop-down list to enable or disable RIP dynamic routing protocol.
- » **RIP mode:** Depending on which RIP version dynamic routing protocols your other routing devices support, click the appropriate version v1 or v2.

🔗 *Note: If selecting RIP v2, this requires basic password authentication between routing devices using this protocol. The password must match on all routing devices connected in order successfully exchange routing information.*

RIP	
Enable RIP	Enable ▼
RIP mode	☐ v1 ☒ v2

- 4 Click **Apply** to save the changes.

🔗 *Note: To discard the changes, click **Cancel**.*

The current routing table is visible in Routing Table section.

Routing Table				
IP	Netmask	Gateway	Metric	Interface
10.0.0.0	255.255.0.0	0.0.0.0	0	WAN
0.0.0.0	0.0.0.0	10.0.0.254	0	WAN
127.0.0.0	255.0.0.0	0.0.0.0	0	undefined
192.168.10.0	255.255.255.0	0.0.0.0	0	LAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	undefined
192.168.20.0	255.255.255.0	10.10.10.2	1	WAN

Enable/Disable UPnP

Advanced > Administrator > Advanced Network

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

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Administrator > Advanced Network**.
- 3 In UPnP section, enable or disable UPnP.

UPnP	
UPnP	Enable ▼

- 4 Click **Apply** to save the changes.

🔗 *Note:* To discard the changes, click **Reset**.

Identify Your Network on the Internet

Advanced > Setup > Management

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

🔗 *Note:* First, you need to sign up for one of the DDNS service providers listed in the **Dynamic DNS Provider** drop-down list.

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Setup > Management**.
- 3 In DDNS Settings section, modify the following settings:
 - » **Dynamic DNS Provider:** Click the drop-down list to select your DDNS service.
 - » **Host Name:** Enter the personal URL provided to you by your Dynamic DNS service provider. For example, www.trendnet.dyndns.biz.
 - » **Account:** Enter the user name needed to log in to your Dynamic DNS service account.
 - » **Password:** Enter the password to gain access to Dynamic DNS service for which you have signed up to. (NOT your router or wireless network password).

DDNS Settings	
Dynamic DNS Provider	None ▼
Host Name	
Account	
Password	••••••••

- 4 Click **Apply** to save the changes.

🔗 *Note:* To discard the changes, click **Cancel**.

Configure IPv6 Settings

Advanced > Setup > IPv6 Settings

IPv6 (Internet Protocol Version 6) is a new protocol that significantly increases the number of available Internet public IP addresses due to the 128-bit IP address structure versus IPv4 32-bit address structure. In addition, there are several integrated enhancements compared to the most commonly used and well known IPv4 (Internet Protocol Version 4) such as:

- Integrated IPsec: Better Security.
- Integrated Quality of Service (QoS): Lower latency for real-time applications.
- Higher Efficiency of Routing: Less transmission overhead and smaller routing tables.
- Easier configuration of addressing.

Note: In order to use IPv6 Internet connection settings, it is required that your ISP provide you with the IPv6 service. Please contact your ISP for available and more information on the IPv6 service.

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Setup > IPv6 Settings**.
- 3 Review the IPv6 Internet Connection settings and enter information settings specified by your ISP.

Note: Please contact your ISP for IPv6 service availability.

IPv6 Connection Type	
IPv6 Connection Type	Static Autoconfiguration (SLAAC/DHCPv6) Link-local Only PPPoE 6to4

Select the IPv6 connection type provided by your ISP.

- 4 Click **Apply** to save the changes.

Note: To discard the changes, click **Cancel**.

Create Schedules

Advanced > Setup > Schedule

For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly.

Note: You can apply a predefined schedule to the following features:

- Wireless (2.4GHz and 5GHz)
- Guest Network
- Parental Control (MAC/IP Filters)
- Access Control (IP Protocol Filters)
- Virtual Server
- Special Applications
- Gaming

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Setup > Schedule**.
- 3 In Add Schedule Rule section, modify the following values:

- » **Rule Name:** Enter a name for the schedule you would like to apply.
- » **Day(s):** Check **Select Day(s)** to select the specific days or select **All Week** to set the schedule for all days.

Note: Check the checkbox next to the day(s) when you want to run the schedule.

- » **All Day – 24 Hours:** Check the option to set the schedule to 24 hours.
- » **Start/End Time:** Select the start and end time you would like the schedule to follow.

Add Schedule Rule	
Rule Name	
Day(s)	☒ Select Day(s) ☐ All Week
	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
All Day - 24hrs	☐
Start Time	:
End Time	:

- 4 Click **Apply** to save the changes.

Note: To discard the changes, click **Clear**.

Configure Access Control Rules

Advanced > Security > Access Control

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

Block a specific service or multiple services

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Security > Access Control**.
- 3 In Access Control section, click the **Enable** option.

Access Control	
Enable Access Control	☐ Enable ☒ Disable

- 4 In Add Services Block Rule section, modify the following values:

- » **Policy Enable:** Checking this option turns on the Protocol/IP Filter and unchecking turns it off.
- » **Policy Name:** Enter a name for the Protocol/IP Filter.
- » **Schedule (Optional):** Select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

⚠ *Note: Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Refer to "Set the Date and Time" on page 42 and "Create Schedules" on page 30 to create a schedule.*

- » **Client IP Address Range:** Enter the IP address or IP address range to apply the protocol/IP filter. For example, 192.168.10.20-192.168.10.20 or 192.168.10.20-192.168.10.30.

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

Add Services Block Rule	
Policy Enable	☐
Policy Name	
Schedule	Always ▼
Client IP Address Range	~

To simplify configuration, there is a list of commonly used pre-defined Protocol/IP Filters to modify otherwise, you can choose to manually add a new Protocol/IP Filter.

- » **Rule Define:** Select **Special Service** to select from the predefined services listed or select **User Define** to specifically enter the TCP or UDP port number or port range numbers to block. For example, 80-80 or 20-21.

Rule Define	☐ Special Service ☒ User Define	
Service	Description	Enabled
WWW	HTTP, TCP Port 80	☐
Email Sending	SMTP, TCP Port 25	☐
Email Receiving	POP3, TCP Port 110	☐
File Transfer	FTP, TCP Port 21	☐
Telnet Service	TCP Port 23	☐
DNS Query	UDP Port 53	☐
TCP Protocol	All TCP Port	☐
UDP Protocol	All UDP Port	☐

TCP Ports		Ex: 21 or 300-500
UDP Ports		Ex: 21 or 300-500

- 5 Click **Add** to save the rule.

⚠ *Note: To discard the changes, click **Cancel**.*

 *Note:* In the Services Block Rule List section, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Block All Services

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Security > Access Control**.
- 3 In Access Control section, click the **Enable** option.

Access Control	
Enable Access Control	☐ Enable ☒ Disable

- 4 In Add Services Block Rule section, modify the following values:
 - » **Rule Enable:** Checking this option turns on the Protocol/IP Filter and unchecking turns it off.
 - » **Rule Name:** Enter a name for the Protocol/IP Filter.
 - » **IP Address:** Enter the IP address or IP address range to apply the protocol/IP filter. For example, 192.168.10.1, 192.168.10.0/24 or 192.168.10.1-192.168.10.30.

 *Note:* The filter will not be applied to IP addresses outside of the range specified.
 - » **Schedule (Optional):** Select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

 *Note:* Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Refer to “[Set the Date and Time](#)” on page 42 and “[Create Schedules](#)” on page 30 to create a schedule.

Add All Services Block Rule	
Rule Enable	☐
Rule Name	
IP Address	 (ex: 192.168.10.1, 192.168.10.0/24, 192.168.10.1-192.168.10.20)
Schedule	Always 

- 5 Click **Add** to save the rule.

 *Note:* To discard the changes, click **Reset**.

 *Note:* In the All Services Block Rule List section, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Configure Inbound Filter Rules

Advanced > Security > Inbound Filter

Inbound Filters allows you to allow or deny a specific range of IP addresses. You can create a predefined range of IP addresses to apply to a specific feature.

 *Note:* You can apply a predefined inbound filter to the following features:

- Virtual Server
- Gaming
- Remote Management

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Security > Inbound Filter**.
- 3 In Add Inbound Filter Rule, modify the following values:
 - » **Filter Name:** Enter a name for the IP address range.
 - » **Rule Action:** Select **Allow** to allow the specified IP address range or **Deny** to deny the specified IP address range.
 - » **IP Address:** Enter the IP address. For example, 192.168.1.20-192.168.1.30.

Add Inbound Filter Rule	
Rule Name	
Rule Action	☐ Allow ☒ Deny
IP Address	

- 4 Click **Add** to save the Inbound Filter.

 *Note:* To discard the changes, click **Clear**.

 *Note:* In the Inbound Filter List, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Configure Firewall Settings

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

DMZ

Advanced > Firewall > DMZ

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

It is strongly recommended to use **Virtual Server** (also called port forwarding, refer to ["Virtual Server" on page 33](#)) to allow access to your computers or network devices from the Internet.

- 1 Log into your router management page (refer to ["Log in to Management Page" on page 8](#)).
- 2 Click on **Advanced > Firewall > DMZ**.
- 3 In DMZ Settings section, select **Enable** from the **DMZ Settings** drop-down list.

DMZ Settings	
DMZ Settings	Enable ▼

- 4 Enter the IP address you assigned to the computer or network device to expose to the Internet.

DMZ IP Address	192. 168. 10. 1
----------------	-----------------

- 5 Click **Apply** to save the changes.

⚠ *Note:* To discard the changes, click **Reset**.

Virtual Server

Advanced > Firewall > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (refer to ["DMZ" on page 33](#)) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet. To open several ports please refer to ["Gaming" on page 35](#).

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (outlined in ["Identify Your Network on the Internet" on page 29](#)).

- 1 Log into your router management page (refer to ["Log in to Management Page" on page 8](#)).
- 2 Click on **Advanced > Firewall > Virtual Server**.
- 3 In Add Virtual Server section, modify the following settings:
 - » **Rule Enable:** Check the option to enable the virtual server.
 - » **Rule Name:** Enter a name for the virtual server.
 - » **IP Address:** Enter the IP address of the device to forward the port. For example, 192.168.10.101.
 - » **Protocol:** Select the protocol required for your device. TCP, UDP, or Both (TCP and UDP).
 - » **Public Port:** Enter the port number used to access the device from the Internet.
 - » **Private Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
 - ⚠ *Note:* The Public Port can be assigned a different port number than the Private Port (also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required. It is recommended to assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.
 - » **Inbound Filter:** Select the defined IP address range to allow access.
 - » **Schedule:** Click **New Schedule** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

 *Note:* Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Refer to [“Set the Date and Time” on page 42](#) and [“Create Schedules” on page 30](#) to create a schedule.

Add Virtual Server	
Rule Enable	☐
Rule Name	
IP Address	
Protocol	TCP ▼
Public Port	
Private Port	
Inbound Filter	Allow All ▼ New Inbound Filter
Schedule	Always ▼ New Schedule

 *Note:* In the Virtual Server List section, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Example: To forward the TCP port 80 to your IP camera, you need to do the following:

- 1 Setup DynDNS service. Refer to [“Identify Your Network on the Internet” on page 29](#).
- 2 Access TRENDnet IP Camera management page and forward Port 80 (refer to the product documentation).
- 3 Make sure to configure your network/IP camera to use a static IP address.

 *Note:* You may need to reference your camera documentation on configuring a static IP address.

- 4 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 5 Click on **Advanced > Firewall > Virtual Server**.
- 6 Check the **Rule Enable** option to enable the Virtual Server.
- 7 Enter the IP address of the camera. For example, 192.168.10.101.
- 8 Next to **Protocol**, make sure **TCP** is selected from the drop-down list.
- 9 The **Private Port** and **Public Port**, enter the port number 80 for both.
- 10 Click **Add** to save the settings.

Special Applications

Advanced > Firewall > Special Applications

Application rules (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. Refer to [“Enable/Disable UPnP” on page 29](#).

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

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Firewall > Special Applications**.
- 3 In Port Trigger Function section, click the **Port Triggering** drop-down menu and choose **Enable**.

Port Trigger Function	
Port Triggering	Enable ▼

- 4 Click **Apply** to save the changes.
- 5 In Add Port Trigger Rule section, review and modify the following settings:
 - » **Rule Enable:** Check the option to enable the port trigger rule.
 - » **Rule Name:** Enter a name for the port trigger rule.
 - » **Match Protocol:** Select the protocol for the firewall ports required for your device. The available options are **TCP**, **UDP**, or **Any** (TCP and UDP).
 - » **Match Port:** Enter the ports or port range to be forwarded to the device. For example, 2000-2038,2200-2210.
 - » **Trigger Protocol** (Trigger): Select the trigger port protocol requested by the device. The available options are **TCP**, **UDP**, or **Any**.
 - » **Trigger Port:** Enter the port requested by the device. For example, 554-554 or 6112-6112).

» **Schedule:** Click **New Schedule** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

⚠ *Note:* Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Refer to [“Set the Date and Time” on page 42](#) and [“Create Schedules” on page 30](#) to create a schedule.

Add Port Trigger Rule	
Rule Enable	☐
Rule Name	
Match Protocol	TCP ▼
Match Port	
Trigger Protocol	TCP ▼
Trigger Port	
Schedule	Always ▼ New Schedule

6 Click **Add** to save the settings.

⚠ *Note:* In the Rule List section, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

Gaming

Advanced > Firewall > Gaming

Gaming allows you to define multiple ports (used or required by a specific application or game) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (refer to [“DMZ” on page 33](#)) in which DMZ forwards all ports instead of only specific ports used by an application. Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (refer to [“Identify Your Network on the Internet” on page 29](#)).

1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).

2 Click on **Advanced > Firewall > Gaming**.

3 In Add Gaming Rule section, modify the following values:

» **Rule Enable:** Check the option to enable the gaming rule.

» **Rule Name:** Enter a name for the gaming rule.

» **IP Address:** Enter the IP address of the device to forward the ports. For example, 192.168.10.101.

» **TCP Ports to Open:** Enter the TCP port you would like to set.

» **UDP Ports to Open:** Enter the UDP port you would like to set.

⚠ *Note:* Please refer to the device documentation to determine which ports and protocols are required. You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

» **Inbound Filter:** Select the defined IP address range to allow access.

» **Schedule:** Click **New Schedule** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule.

⚠ *Note:* Before applying scheduling, please ensure your Time settings are configured correctly and you have defined a schedule. Refer to [“Set the Date and Time” on page 42](#) and [“Create Schedules” on page 30](#) to create a schedule.

Add Gaming Rule	
Rule Enable	☐
Rule Name	<< Application Name ▾
IP Address	
TCP Ports To Open	(ex. 80, 689, 50-60, 1020-5000)
UDP Ports To Open	(ex. 80, 689, 50-60, 1020-5000)
Inbound Filter	Allow All ▾ New Inbound Filter
Schedule	Always ▾ New Schedule

4 Click **Add** to save the settings.

 *Note:* In the Gaming Rule List section, you can edit a rule by clicking  in the **Edit** column next to the rule you would like to edit. To delete the rule, click  in the **Delete** column next to the rule you would like to delete.

ALG

Advanced > Firewall > ALG

You may want to configure your router to allow computers the use of specific high layer applications or service sessions to pass through. Application Layer Gateways (ALG) allows you to easily enable or disable these applications to pass through your router.

 *Note:* It is recommended to leave these settings enabled.

- 1 Log into your router management page (refer to “[Log in to Management Page](#)” on page 8).
- 2 Click on **Advanced > Firewall > ALG**.
- 3 In Application Level Gateway (ALG) Configuration section, modify the following values:
 - » **Streaming Media:** Check this option to allow RTSP protocol through your router typically used in streaming media applications.
 - » **Streaming Media-VoIP:** Check this option to allow SIP protocol through your router typically used in VoIP applications.
 - » **Streaming Media-VoIP:** Check this option to allow H.323 protocol through your router typically used in video/audio conferencing applications.
 - » **File Transfer:** Check this option to allow FTP protocol through your router used for file transfer over a network or the Internet.
 - » **File Transfer:** Check this option to allow TFTP protocol through your router used for file transfer over a network or the Internet.
 - » **VPN Pass-Through:** Check this option to allow client connections through your router.

Application Level Gateway (ALG) Configuration

Service Name	Description	Enable
Streaming Media	Real Time Streaming Protocol (RTSP)	☒
Streaming Media-VoIP	Session Initiation Protocol(SIP)	☒
Streaming Media-VoIP	NetMeeting (H.323)	☒
File transfer	File Transfer Protocol (FTP)	☒
File transfer	Trivial File Transfer Protocol (TFTP)	☒
VPN Pass-Through		☒

4 Click **Save Status** to save the settings.

 *Note:* To discard the changes, click **Cancel**.

Enable Remote Access

Advanced > Setup > Management

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

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
 - 2 Click on **Setup > Management**.
 - 3 In Remote Management section, modify the following values:
 - » **Remote Control (via Internet)**: Click the drop-down list and select **Enable** to enable remote management or **Disable** to disable remote management.
 - » **Remote Port**: Enter the port to assign remote access to the router. It is recommended to leave this setting as 8080.
- 🔗 *Note: If you have configured port 8080 for another configuration section, such as virtual server or special application, please change the port to use. Recommended port range is 1024 to 65534.*

Remote Management	
Remote Control (via Internet)	Enable ▼
Remote Port	8080

- 4 Click **Apply** to save the changes.

🔗 *Note: To discard the changes, click **Reset**.*

Allow/Deny Ping Requests from the Internet

Advanced > Administrator > Advanced Network

To provide additional security, you may want to disable your router from responding to ping or ICMP (Internet Control Message Protocol) requests from the Internet. A ping is network communication test to check if a device with IP address is alive or exists on the network. By disabling this feature, you can conceal your router's IP address and existence on the Internet by denying responses to ping requests from the Internet. You can additionally use this feature as a tool for troubleshooting purposes.

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Administrator > Advanced Network**.
- 3 In WAN Ping section, click the **WAN Ping Respond** drop-down list and select the desired settings.
 - » **Enable** to allow your router to respond to ping requests from the Internet.
 - » **Disable** to block WAN ping requests from the Internet.

WAN Ping	
WAN Ping Respond	Disable ▼

- 4 Click **Apply** to save the changes.

🔗 *Note: To discard the changes, click **Reset**.*

Configure Quality of Service Settings

Advanced > Setup > QoS

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

1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).

2 Click on **Advanced > Setup > QoS**.

3 In QoS Setting section, modify the following settings:

- » **Enable QoS:** Click **Enabled** to allow the Quality of service through the router. You can also click **Disable** to disable the Quality of service through the router.
- » **Prioritize ACK:** Click **Enabled** to prioritize the acknowledgment packets.
- » **Prioritize ICMP:** Click **Enabled** to prioritize the ICMP requests. You can also click **Disabled** if you do not want to prioritize the ICMP requests.

⚠ *Note: The ICMP requests are basically ping requests. It is recommended to disable it unless you wish to run a game server where it is important to maintain low level of ping for players to determine the latency.*

QoS Setting	
Enable QoS	Enabled ▼
Prioritize ACK	Enabled ▼
Prioritize ICMP	Enabled ▼

4 In Traffic Class Setting section, click the **Default Traffic Class** drop-down list and select the traffic class you would like to configure for the QoS rule.

Traffic Class Setting	
Default Traffic Class	Highest High Medium Low Lowest

5 In Inbound Class Setting section, modify the following settings:

- » **BW Max Inbound:** Enter the maximum download speed of your ISP (Internet Service Provider).
- » **Highest/High/Medium/Low/Lowest:** Enter the download speeds you would like to apply on each state of download speeds. This setting is similar to setting the priority speeds of each class.

Inbound Class Setting		
Inbound Classes (% Max Input BW)		
BW Max Inbound	1500	Kbit/s
	%BW	
Highest	50	Kbit/s
High	30	Kbit/s
Medium	10	Kbit/s
Low	5	Kbit/s
Lowest	1	Kbit/s

6 In Outbound Class Setting section, modify the following settings:

⚠ *Note: The fields will automatically populate when Inbound Class is configured but you can also modify the settings manually.*

- » **BW Max Outbound:** Enter the maximum upload speed of your ISP (Internet Service Provider).
- » **Highest/High/Medium/Low/Lowest:** Enter the upload speeds you would like to apply on each state of download speeds. This setting is similar to setting the priority speeds of each class.

Outbound Class Setting				
Outbound Classes (% Max Output BW)				
BW Max Outbound	384		Kbit/s	
	%BWMin	%BWMax		
Highest	80	100	--	Kbit/s
High	10	100	--	Kbit/s
Medium	5	100	--	Kbit/s
Low	3	100	--	Kbit/s
Lowest	2	95	--	Kbit/s

7 Click **Apply** to save the changes.

⚠ *Note: To discard the changes, click **Cancel**.*

8 In QoS Rule Add section, modify the following values:

- » **Rule Enable:** Check this option to enable the QoS rule.
- » **IP/MAC Address Filter:** Click on the drop-down menu and choose the type of the IP address or MAC address. Then enter the IP address and/or MAC address to the **Address** field(s).
- » **Protocol Filter:** Select the protocol you would like to apply on the QoS rule.
- » **Port Filter:** Select the port from the drop-down menu you would like to assign on the QoS rule. Then enter the port number to the **Port List** field.
- » **Class Assigned:** Select the class that you have assigned to the QoS rule.
- » **Description:** Enter the QoS description that best describes the rule.

QoS Rule Add	
Add QoS Rule	
Rule Enable	☐
IP/MAC Address Filter	Any v Address:
Protocol Filter	Any v
Port Filter	Any v Port List:
Class Assigned	Highest v
Description	

9 Click **Add** to save the settings.

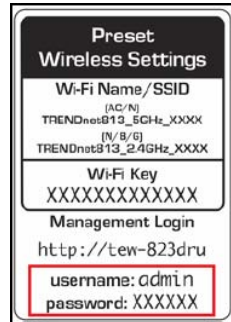
⚠ *Note: To discard the changes, click **Clear**.*

Using External USB Storage

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

Note:

- For security purposes, the USB SMB and FTP settings on your router are disabled by default. You will need to enable these settings in order to allow access to your USB storage devices.
- For security purposes, the default USB SMB and FTP admin password is configured to the same predefined password used to log into your router management page.



Configure File Sharing Server

Advanced > USB > File Sharing Server

1 Log into your router management page (refer to “Log in to Management Page” on page 8).

2 Click on **Advanced > USB > File Sharing Server**.

3 In Server Information section, modify the following values:

- » **Samba (SMB) Server:** Select enable or disable for the feature.
 - » **Server Name:** You can change the name of your server which will be the name you will when accessing your USB storage device.
- Note:** You can also access the USB storage using the router IP address.
- » **Workgroup:** Enter the workgroup name. It is recommended to keep the standard default “WORKGROUP”. If you change this setting, you will need to change the workgroup name on all computers in your network that are allowed access to the USB storage.
 - » **Description (optional):** Enter a description of the server.

Server Information	
Samba (SMB) Server	☐ Enable ☒ Disable
Server Name	USBSHARE
Workgroup	WORKGROUP
Description (optional)	SMB_Server

4 In Set Administrator section, review the administrator settings required for your **File Sharing (SMB) Server**. Administrator will have read and write access to the files. To define user accounts, continue in the respective section.

- » **Administrator:** Modify the Administrator account user name.
- » **New Password/Re-type Password:** Enter the new password for the Administrator. Re-type the password to confirm.

Set Administrator	
Administrator	admin
New Password	
Re-type Password	

5 Click **Apply** to save the changes.

Note: To discard the changes, click **Clear**.

6 In User Account List section, you can add users to your **File Sharing (SMB) Server**.

- » **User Name:** Enter the user name to be used to access your files.
- » **Password:** Enter the password for the user name.
- » **Permission:** Select the permission you will grant to the user. You can allow the user **Read Only** or **Read-Write** access to the USB storage.

User Account List	
User Name	
Password	
Permission	Read Only ▼

7 Click **Add** to add the account.

Note:

- To discard the changes, click **Clear**.
- Use **Current User Account List** to review all the user accounts. Click **Delete** to delete the selected user account.

Note:

- In Windows® operating system, you can access the USB storage device on your computer in the following path: **Computer > Network > USBSHARE > usb_A1**.
- Your computer will only be able to automatically discover the USB storage if you are set to a workgroup under the default name "WORKGROUP". Your computer will not be able to automatically discover the USB storage if it is connected to a domain or configured with a different workgroup name.



- In Windows® operating system, if your computer cannot discover the USB storage automatically, you can access the files in your server, using the network map or by typing \\<routerIPaddress>\usb_A1 on your browser's or file explorer address bar. For example, \\192.168.10.1\usb_A1.

Configure FTP Server

Advanced > USB > FTP Server

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

1 Log into your router management page (refer to "Log in to Management Page" on page 8).

2 Click on **Advanced > USB > FTP Server**.

3 In Server Information section, modify the following values:

- » **FTP Server:** Select enable or disable for the feature.
- » **Authentication:** Select **Enable** to activate user name and password authentication in order to access the USB storage using FTP. Select **Disable** to let user to anonymously access the USB storage using FTP.
- » **Access From Internet:** Select **Enable** to allow access to the USB storage using FTP over the Internet (WAN) and local (LAN) networks. Select **Disable** to disable FTP access over the Internet and allow LAN access only.

4 In File Server Codepage section, you can define which character set to use when transferring data using FTP.

Note: It is recommended to leave these settings as default "Western European".

Server Information	
FTP Server	☐ Enable ☒ Disable
Authentication	☐ Enable ☒ Disable
Access From Internet	☒ Enable ☐ Disable
File Server Codepage	
Language	Western European ▼

5 Click **Apply** to save the changes.

6 In User Account List section, you can add users to your **FTP Server**.

- » **User Name:** Enter the user name to be used to access your files.
- » **Password:** Enter the password for the user name.
- » **Permission:** Select the permission you will grant to the user. You can allow the user **Read Only** or **Read-Write** access to the USB storage.

User Account List	
User Name	
Password	
Permission	Read Only ▼

7 Click **Add** to add the account.

Note:

- To discard the changes, click **Clear**.
- Use **Current User Account List** to review all the user accounts. Click **Delete** to delete the selected user account.

Note: Signing up for a Dynamic DNS service (outlined in "Identify Your Network on the Internet" on page 29) will provide identification of the router's network from the Internet. You can access your shared files over the Internet by typing, for example <ftp://<router'sWANIPaddress>> or <ftp://myDDNSservice> in your web browser or file explorer address bar. You can access your share files locally by typing <ftp://<router'sLANIPaddress>> in your web browser or file explorer address bar.

Maintenance

Change Login Password

Advanced > Setup > Management

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Setup > Management**.
- 3 In Administrator Settings section, modify the following parameters:
 - » **Account:** Enter the new user name for the router's Administrator account.
 - » **Password:** Enter the password.
 - 🔗 *Note: The maximum password length is 16 characters.*
 - » **Idle Timeout:** The idle timeout setting is used to define the period of inactivity in the router management page before you are automatically logged out.
- 4 Click **Apply** to save the changes.
 - 🔗 *Note: To discard the changes, click **Cancel**.*

Administrator Settings	
Account	admin
Password	 (Max: 16 characters)
Idle Timeout	3600 (120-3600 seconds)

- 🔗 *Note: If you change the router login user name or password, you will need to access the router management page using the new user name and new password instead of the predefined default password. If you reset the device to defaults, you will need to access the router management page using the predefined settings on the side or bottom labels.*

Set the Date and Time

Advanced > Administrator > Time

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Administrator > Time**.
- 3 In Time Configuration section, review the system time.
 - » **System Time:** Displays the current device time and date information.

Time Configuration	
System Time	Thu May, 22, 2014 14:51:37

- 4 In Daylight Saving Time section, modify the following:
 - » **Enable Daylight Saving:** Check the option to enable daylight savings time.
 - » **Daylight Saving Offset:** Select the time zone offset in your location.
 - » **Daylight Saving Dates:** Select the daylight saving start and end dates.

Daylight Saving Time					
Enable Daylight Saving	☒				
Daylight Saving Offset	+1:00 ▼				
Daylight Saving Dates	Month	Week	Day of Week	Hour	
	DST Start	Mar ▼	3rd ▼	Sun ▼	1 ▼
	DST End	Nov ▼	2nd ▼	Sun ▼	1 ▼

5 You can choose to set the device time and date automatically synchronize with the Internet Time Server or manually set the time. Do one of the following:

- » **Enable NTP Server:** Check to enable the NTP server option. This option lets you to synchronize the time and date in router with an NTP (Network Time Protocol) server.
- » **NTP Server:** Enter the NTP server address. For example, pool.ntp.org.
- » **Time Zone:** Click to select the time zone from the drop-down list.
- » **NTP synchronization:** Change the NTP synchronization period.

NTP Settings	
Enable NTP Server	☒
NTP Server	Select NTP Server ▼
Time Zone	(GMT-08:00) Pacific Time (US/Canada), Tijuana ▼
NTP synchronization	188 (1~300) Minute

» You can set the router's time and date manually in Date and Time Settings section.

🔗 *Note: Time is specified in 24-hour format.*

Date and Time Settings	
Date And Time	Year 2014 ▼ Month Jun ▼ Day 24 ▼
	Hour 13 ▼ Minute 48 ▼ Second 39 ▼

6 Click **Apply** to save the changes.

🔗 *Note: To discard the changes, click **Cancel**.*

Backup System Settings

Advanced > Administrator > Settings Management

This option allows you to backup your access point configuration.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Administrator > Settings Management**.
- 3 In Export Settings section, click **Export**.

Export Settings	
Export	Export

🔗 *Note: Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. An example filename, **TEW-823DRU_config.bin**.*

Load System Settings

Advanced > Administrator > Settings Management

This option allows you to load the system settings after the firmware upgrade or reset to factory defaults.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Administrator > Settings Management**.
- 3 In Import Settings section, click **Browse** to load the settings file.

Import Settings	
Settings file location	Browse...

- 4 A separate file navigation window should open.
- 5 Select the router configuration file to restore and click **Import**. The default filename is **TEW-823DRU_config.bin**. If prompted, click **Yes** or **OK**.
- 6 Wait for the router to restore the settings.

Reset to Factory Defaults

Advanced > Administrator > Settings Management

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, refer to [“Backup System Settings” on page 43](#).

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Administrator > Settings Management**.
- 3 In Reset to Factory Defaults section, click **Load Default**.



- 4 You are prompted to confirm to reset to factory default settings. Click **OK**.

Reboot the System

Advanced > Administrator > Settings Management

To reload the system parameters, you may need to reboot the router.

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Administrator > Settings Management**.
- 3 In System Reboot section, click **Reboot**.



- 4 You are prompted to confirm to reboot the device. Click **OK**.

Update System Firmware

Advanced > Setup > Update Firmware

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

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

To download the firmware, do the following:

- 1 Enter the web browser URL field <http://www.trendnet.com/downloads/> and download the firmware to your computer.
- 2 Unzip the file to a folder on your computer.

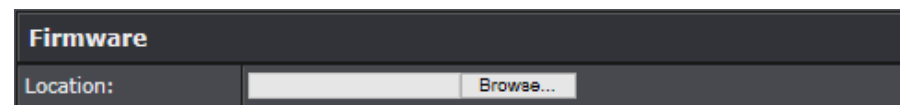
Note:

- Do not interrupt the firmware upgrade process.
- Do not turn off the device during the upgrade.
- If you are upgrading the firmware, using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.

IMPORTANT: Do not interrupt the firmware upgrade process as it may damage your device. Please wait until the firmware upload has fully completed and the device has successfully rebooted.

To start the firmware upgrade, do the following:

- 1 Log into your router management page (refer to [“Log in to Management Page” on page 8](#)).
- 2 Click on **Advanced > Setup > Update Firmware**.
- 3 In Firmware section, click **Browse** to load the upgrade file.



- 4 Navigate to the folder on your computer where the unzipped firmware file (*.bin) is located and select it.
- 5 Click **Apply**. If prompted, click **Yes** or **OK**.

Note: To discard the changes, click **Cancel**.

View Wireless Client List

Advanced > Wireless (2.4GHz or 5GHz) > Station List

You can view the list of active wireless devices currently connected to your router.

1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).

2 Click on **Advanced > Wireless (2.4GHz or 5GHz) > Station List**.

3 In Wireless Network section, review the connected devices.

- » **MAC Address:** Display the current MAC address of your 2.4GHz or 5GHz wireless client.
- » **Mode:** Display the 802.11 mode associated with the client.
- » **Rate:** Display the estimated data rate established with the client.
- » **Signal:** Display the estimated signal strength associated with the client.

Wireless Network			
MAC Address	Mode	Rate	Signal
64:80:99:3E:31:C4	802.11n	52M	92%

View System Information

Advanced > Administrator > Status

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

1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).

2 Click on **Advanced > Administrator > Status**.

3 In System Info section, view the following values:

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

System Info	
Firmware Version	1.00 , 21, May, 2014
System Time	Thu May, 22, 2014 17:19:41
System Up Time	0 Day, 0:54:20

4 In Internet Configuration section, view the following values:

- » **Connected Type:** Display the current WAN connection type applied.
- » **WAN IP Address:** Display the current IP address assigned to your router WAN port or interface configuration.
- » **Subnet Mask:** Display the current subnet mask assigned to your router WAN port or interface configuration.
- » **Default Gateway:** Display the current gateway assigned to your router WAN port or interface configuration.
- » **Primary/Secondary DNS (Domain Name System) Server:** Display the current DNS address(es) assigned to your router port or interface configuration.

Internet Configuration	
Connected Type	Dynamic IP (DHCP)
WAN IP Address	10.0.11.216
Subnet Mask	255.255.0.0
Default Gateway	10.0.0.254
Primary Domain Name Server	10.0.0.51
Secondary Domain Name Server	10.0.0.250

⚠ *Note:*

- **Renew/Release** buttons will be available only for DHCP WAN type. The **Renew** button allows to renew your WAN IP address and **Release** button allows you to release the WAN IP address of your router.
- **Connect/Disconnect** buttons will be available only for PPPoE DHCP WAN type. The **Connect** button allows the connection to your DSL ISP and **Disconnect** button allows to disconnect from your DSL ISP.

5 In LAN section, view the following values:

- » **MAC Address:** Display the current MAC address of your router's wireless or interface configuration.
- » **IP Address:** Display your router's current IP address.
- » **Subnet Mask:** Display your router's current subnet mask.

LAN	
MAC Address	C0:A0:BB:6E:08:DE
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

6 In 2.4GHz Wireless section, view the following values:

- » **MAC Address:** Display the MAC address of your router's 2.4GHz wireless LAN interface configuration.
- » **Network Name (SSID) / Security Mode:** The displays the current 2.4GHz primary wireless network name and security mode assigned to your router.
- » **Multiple SSID1 / Security Mode:** Display the current 2.4GHz wireless network name and security mode of multiple SSID1 assigned to your router.
- » **Multiple SSID2 / Security Mode:** Display the current 2.4GHz wireless network name and security mode of multiple SSID2 assigned to your router.
- » **Guest Network / Security Mode:** Display the current 2.4GHz wireless network name and security mode of the guest network assigned to your router.

2.4GHz Wireless	
MAC Address	C0:A0:BB:6E:08:DE
Channel	
Network Name (SSID) / Security Mode	dlink-08DE / WEP
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	

7 In 5GHz Wireless section, view the following values:

- » **MAC Address:** Display the MAC address of your router's 5GHz wireless LAN interface configuration.
- » **Network Name (SSID) / Security Mode:** Display the current 5GHz primary wireless network name and security mode assigned to your router.
- » **Multiple SSID1 / Security Mode:** Display the current 5GHz wireless network name and security mode of multiple SSID1 assigned to your router.
- » **Multiple SSID2 / Security Mode:** Display the current 5GHz wireless network name and security mode of multiple SSID2 assigned to your router.
- » **Guest Network / Security Mode:** Display the current 5GHz wireless network name and security mode of the guest network assigned to your router.

5GHz Wireless	
MAC Address	C0:A0:BB:6E:08:E0
Channel	
Network Name (SSID) / Security Mode	dlink-08DE-5GHz / WPA2 Only - PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	

IPv6 Status

Advanced > Administrator > IPv6 Status

You can view the current IPv6 status on your router.

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Administrator > IPv6 Status**.

IPv6 Connection Information	
IPv6 Connection Type	Auto Configuration (SLAAC/DHCPv6)
Network Status Address	Disconnected
Renew Release	
WAN IPv6 Address	
IPv6 Default Gateway	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	fe80::c2a0:bbff:fe6e:8de/64
Primary DNS Server	
Secondary DNS Server	
IPv6 Network assigned by DHCP-PD	
LAN IPv6 Computers	
IPv6 Address	Name (if any)

View Events Log

Advanced > Administrator > System Log

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

- 1 Log into your router management page (refer to *"Log in to Management Page" on page 8*).
- 2 Click on **Advanced > Administrator > System Log**.
- 3 In System Log section, check the **Enable System Log** option to enable logging. The logging will display in the log window.
- 4 Enter the system log server IP address to **Syslog Server IP Address** field.

System Log	
Enable System Log	☒
Syslog Server IP Address	192.168.10.101 << Computer Name ▾

- 5 Do any of the following:
 - » Click **Apply** button to save the changes.
 - » Click **Refresh** button to refresh the log window to ensure the most recent logging information is displayed.
 - » Click **Clear** button to clear and delete all of the current logging information.

Log Window:

```

May 22 01:50:26 info using nameserver 10.0.0.51#53
May 22 01:50:26 info using nameserver 10.0.0.250#53
May 22 01:50:26 info using nameserver 10.0.0.251#53
May 22 01:50:26 info reading /etc/resolv.conf
May 22 01:50:19 info Lease of 10.0.11.216 obtained, lease time 600
May 22 01:45:30 info using nameserver 10.0.0.51#53
May 22 01:45:30 info using nameserver 10.0.0.250#53
May 22 01:45:30 info using nameserver 10.0.0.251#53
  
```

Appendix

Regulatory and Safety Information

Federal Communication Commission Interference Statement

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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



IMPORTANT NOTE:

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

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC.

Regulation (EC) No. 1275/2008

Regulation (EC) No. 278/2009

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

Safety of Information Technology Equipment.

EN 62311: 2008

Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz-300 GHz).

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

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

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

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

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

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems.

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

Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive This device is a 2.4/5G 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.

 Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-823DRU je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-823DRU overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.
 Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-823DRU in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-823DRU vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this TEW-823DRU is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-823DRU cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, 2009/125/CE y.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙΤΕW-823DRUΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ, 2006/95/ΕΚ, 2009/125/ΕΚ και.
 Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-823DRU est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-823DRU è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
 Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-823DRU atbilstDirektīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.

 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruojama, kad šis TEW-823DRU atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-823DRU in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
 Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-823DRU jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-823DRU megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-823DRU jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
 Português [Portuguese]	TRENDnet declara que este TEW-823DRU está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
 Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-823DRU v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES in 2009/125/ES.
 Slovensky [Slovak]	TRENDnettýmto vyhlasuje, že TEW-823DRU splňuje základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
 Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-823DRU tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-823DRU står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2006/95/EG och 2009/125/EG.

Specifications

Item	Specifications
Standards	- IEEE 802.11b/g/n Wireless LAN 2.4GHz - IEEE 802.11a/n/ac Wireless LAN 5GHz - IEEE 802.3/IEEE 802.3z Gigabit Ethernet - ANSI/IEEE 802.3 Auto negotiation
Radio Technology	- IEEE 802.11g / IEEE 802.11n / IEEE 802.11a/n/ac Orthogonal Frequency Division Multiplexing (OFDM) - IEEE 802.11b: Direct Sequence Spread Spectrum (DSSS)
Transmission Rate	802.11ac: up to 1300Mbps 802.11an: up to 450Mbps 802.11a: up to 54Mbps 802.11n: up to 450Mbps 802.11g: up to 54Mbps 802.11b: up to 11Mbps
Receiver Sensitivity	11ac VHT80 MCS9: Typical - 51dBm @ 10% PER 11ac VHT40 MCS9: Typical - 54dBm @ 10% PER 11ac VHT20 MCS9: Typical - 57dBm @ 10% PER 11a/n HT40 MCS7/15/23: Typical - 61dBm @ 10% PER 11a/n HT20 MCS7/15/23: Typical - 64dBm @ 10% PER 11a/g 54Mbps: Typical - 65dBm @ 10% PER 11b 11Mbps: Typical - 83dBm @ 8% PER
Wireless LAN Frequency Range	2.4GHz: 2412 ~ 2472 MHz ISM band (channels 1 ~ 13) 5GHz: 5180 ~ 5825 MHz ISM band (channels 36 ~ 165)
Modulation Schemes	- DBPSK/DQPSK/CCK for DSSS technique - BPSK/QPSK/16-QAM/64-QAM/256-QAM for OFDM technique
Media Access Protocol	CSMA/CA with ACK

Item	Specifications
Transmit Power (RF Output Power at each RF chain)	2.4GHz Mode - FCC:18dBm,ETSI:16dBm (max) @ 802.11b - FCC:22dBm,ETSI:15dBm (max) @ 802.11g - FCC:22dBm,ETSI:15dBm (max) @ 802.11n HT20 - FCC:18dBm,ETSI:16dBm (max) @ 802.11n HT40 5GHz Mode - FCC:20dBm,ETSI:20dBm (max) @ 802.11a - FCC:20dBm,ETSI:20dBm (max) @ 802.11n HT20 / 802.11ac VHT20 - FCC:20dBm,ETSI:20dBm (max) @ 802.11n HT40 / 802.11ac VHT40 - FCC:14dBm,ETSI:20dBm (max) @ 802.11ac VHT80
Antenna Type	2.4 GHz: 3 x 2dBi (Peak) PCB Antenna's internal 5 GHz: 3 x 3dBi (Peak) PCB Antenna's internal
Protocol	TCP/IP
Interface	- LAN: 4 x 10/100/1000Mbps Auto-MDIX Gigabit Ethernet ports - WAN: 1 x 10/100/1000Mbps Auto-MDIX Gigabit Ethernet port - Reset button - WPS button - On/off power switch - Power Jack
Supported Network Protocols	- TCP/IP - NAT - PPPoE/PPTP/L2TP - HTTP
DHCP Server/Client Network Management	Web base configuration utility via Ethernet
Channel	2.4GHz: Channel 1 ~ 11(FCC), Channel 1 ~ 13(ETSI) 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161 and 165 (FCC), 36, 40, 44, 48,52,56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 (ETSI)

Item	Specifications
Security	• 64/128-bits WEP Encryption • WPA, WPA2 • WPA-PSK, WPA2-PSK • MAC address filtering (Up to 24 entries) • Protocol filtering • Domain filtering
Range Coverage	• Indoor: Up to 100 meters (depends on environment) • Outdoor: Up to 300 meters (depends on environment)
Diagnostic LEDs	• Power • Internet (WAN port)
Power Adapter	12VDC / 2A external power adapter
Power Consumption	1500 mA(max.)
Operation Temperature	0 ~ 40°C
Storage Temperature	-10 ~ 70°C
Humidity	10% ~ 95% RH, no condensation
Certifications	• FCC certificate for USA • CE certificate for Europe
Dimensions (W x H x D)	151 x 191 x 45.5 mm
Weight	413g

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



Product 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