User's Guide

TRENDNET®

N600 Dual Band Wireless Access Point

TEW-750DAP

Table of Contents

Product Overview

TEW-750DAP

Package Contents

In addition to your access point, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Multi-Language Quick Installation Guide
- 1 x Network cable (1.5m / 5ft.)
- Power Adapter (12V, 1A)

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

Features

TRENDnet's N600 Dual Band Wireless Access Point, model TEW-750DAP, supports Access Point (AP), Wireless Distribution System (WDS) Bridge, AP + WDS, Repeater, and Client Bridge mode functionality. A convenient wireless scan feature streamlines the WDS setup process. Embedded GREENnet technology reduces power consumption by up to 50%. Multiple SSIDs are supported for each band.

Ease of Use

Multi-Mode Support

Supports Access Point (AP), WDS Bridge, and WDS Bridge + Access Point, Repeater, and Client Bridge modes

WDS Wireless Scan

Wireless Scan support for WDS setup automatically populates MAC address

One Touch Connection

Securely connect to the wireless network at the touch of the Wi-Fi Protected Setup (WPS) button

Multi Language

Multi Language Interface: English, Spanish, French, German, and Russian

Logs

Real time logs and statistics help trouble shooting

Security

Encrypted Wireless

Support for wireless encryption of up to WPA2

Multiple SSIDs

Create multiple SSIDs per wireless band

Performance

N600 Wireless

Proven concurrent dual band 300 Mbps Wireless N

Wireless Coverage

Extended wireless coverage with MIMO antenna technology

Compatibility

Compatible with legacy wireless devices

Energy Savings

Embedded GREENnet technology reduces power consumption by up to 50%

IPv6

IPv6 network support

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

Product Hardware Features

Rear View
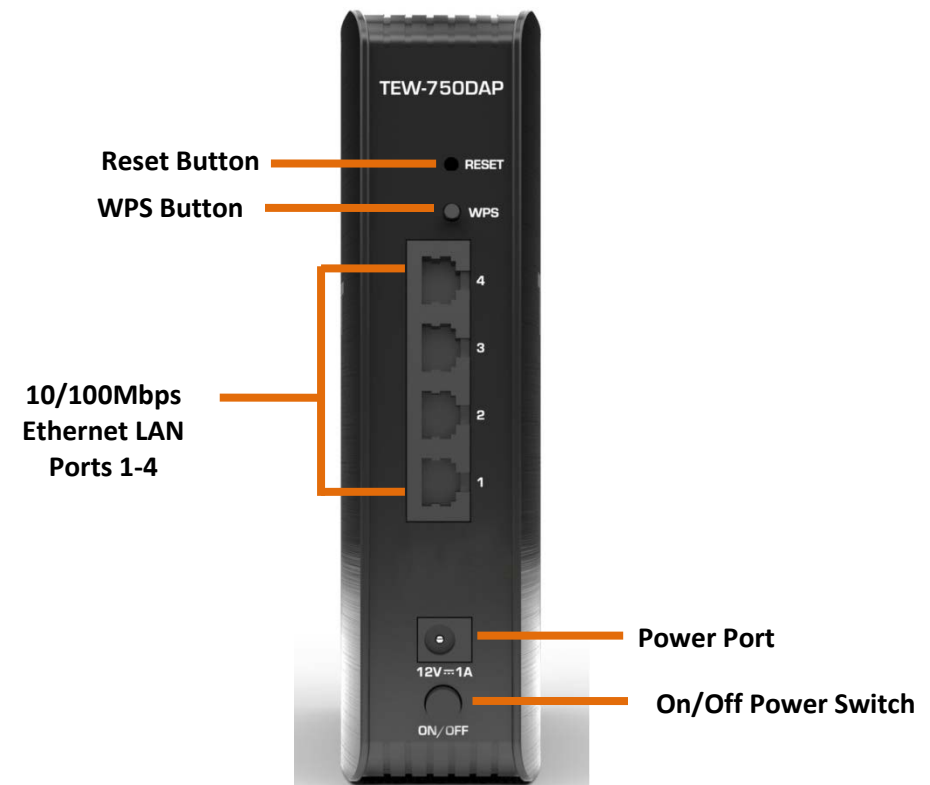
- **Reset Button** – Press and hold this button for 10 seconds to reset the access point.
- **WPS Button (Wi-Fi Protected Setup)** – Push and hold this button for 5 seconds to activate WPS. The Power LED will blink when WPS is activated. *Note: WPS is only available when the device is in Access Point mode.*
- **Ethernet LAN Ports 1-4** – Connect Ethernet cables (also called network cables) from your access point to your router and wired network devices.
- **Power Port** – Connect the included power adapter from your access point power port and to an available power outlet.
- **On/Off Power Switch** – Push the access point On/Off power switch to turn your access point "On" (Inner position) or "Off" (Outer position).

Front View

WPS LED

Wireless LED

LAN Ports 1-4 LEDs

Power LED
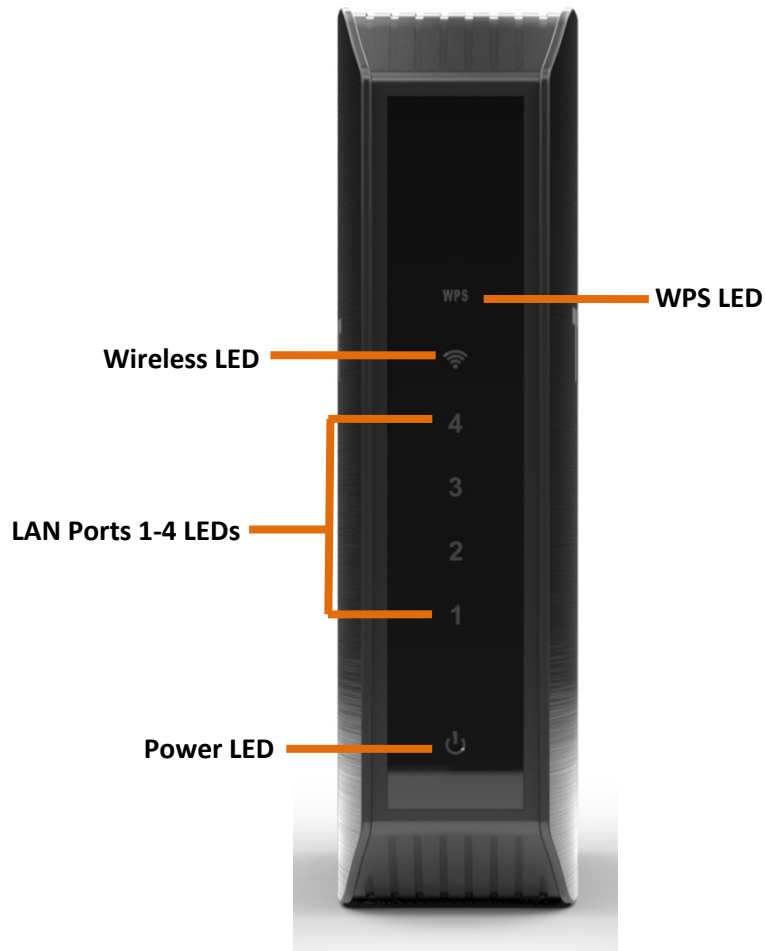
- **WPS LED:** The indicator will blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.
- **Wireless (Link/Activity) LED:** The indicator turns on solid green when wireless is enabled on your access point. The indicator will blink during when data is transmitted or received by your wireless client devices connected to your access point.
- **Ethernet LAN Ports 1-4 (Link/Activity) LED:** These LED indicators are solid green when the LAN ports 1-4 are physically connected to your wired network devices (which are turned on) with a network or Ethernet cable. These LED indicators will blink green while data is transmitted or received through your access point's Ethernet LAN ports.
- **Power LED:** The indicator is solid green when your access point is powered on. Otherwise if this LED indicator is off, there is no power to your access point. The indicator will also blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.

Application Diagram
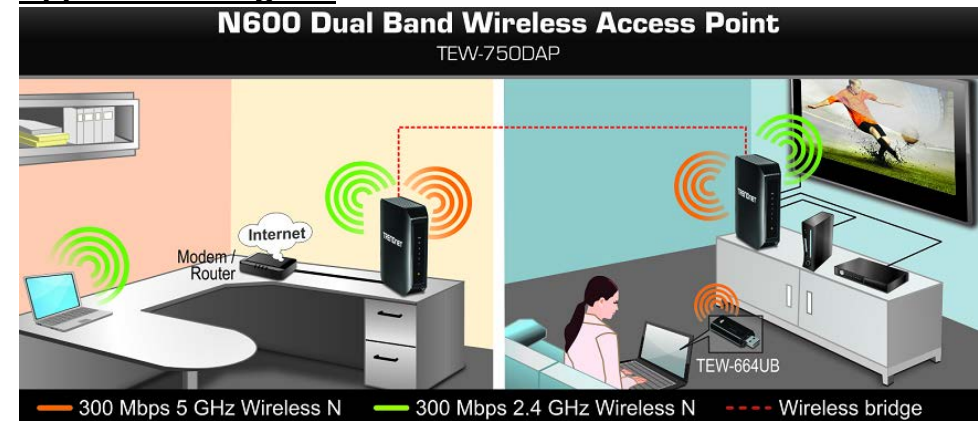
The first access point is installed near your modem/router (typically supplied by your ISP "Internet Service Provider") and physically connected using one of your access point's Ethernet LAN ports. The access point is configured to create a WDS (Wireless Distribution System) Bridge or wireless bridge to a second access point installed in your entertainment center extending wireless coverage as well as wired network connectivity to media devices (TVs, game consoles, or media bridges) using the four Ethernet LAN ports. In addition, 2.4GHz and 5GHz wireless signals from both access points are broadcasted to wireless clients such as laptops (with wireless capability), thereby providing network connectivity and Internet access for all wireless client devices and extending network connectivity.

Basic Access Point Setup

Expanding a Home Network

What is a network?

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

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

- **Modem** – Connects a computer or router to the Internet or ISP (Internet Service Provider).
- **Router** – Connects multiple devices to the Internet.
- **Switch** –Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to add more wired connections.

How to expand a home network

The access point provides multiple modes to extend your current network.

The access point offers the following modes:

- **Access Point (Default)**
- **Wireless Bridge (also known as WDS mode)**
- **Wireless Range Extender (also known as repeater mode)**
- **Wireless Client Bridge (also known as wireless client adapter mode)**

For detailed information on these modes and how to use them, please refer to the following section Choosing your device mode on page 9.

Where to find more help

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

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

Basic Installation

1. Connect the power adapter to the access point and then to a power outlet. Connect your computer to one of the access point's LAN ports (1-4). Push the ON/OFF switch on the TEW-750DAP to power up the access point.

2. Assign a static IP address to your computer's network adapter in the subnet of 192.168.10.x (ex. 192.168.10.25) and a subnet mask of 255.255.255.0. (Please refer to the Appendix on page 60 on how to assign static IP address to your computer)

3. Open your web browser and enter http://tew-750dap.

Note: You can also access the device using the default IP address (192.168.10.100)
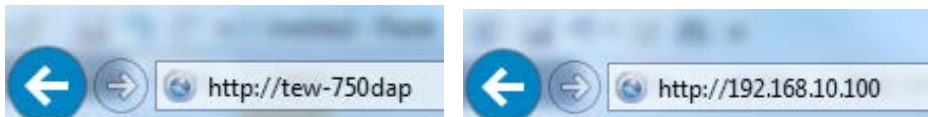
4. Enter the User Name and Password. By default

User Name: **admin**

Password: **admin**

5. Enter a new password, verify the new password and click **Next**.

*Note: The Wizard should automatically appear. If the wizard does not appear automatically, click **Main** and then click **Wizard.***

6. Select **Access Point** and then click **Next**.

Select Your Wireless Mode

Please select wireless mode. Please note that the selected mode will be applied to both 2.4GHz and 5GHz bands.

Wireless Mode   :   Access Point

Prev   Next   Cancel

7. For added security, we have pre-encrypted each TEW-750DAP with a unique Wi-Fi Name (SSID) and Wi-Fi Key. You can find these pre-configured settings on the labels at the front and back of the TEW-750DAP. You will use this information to connect wirelessly to the access point. To change the Wi-Fi key, please refer to Secure your Wireless Network on page 13. If the access point is reset, the Wi-Fi Key and Wi-Fi Name will also reset to factory defaults click **Next**.

Confirm Wi-Fi Settings

Below is a detailed summary of your Wi-Fi security settings. Please print this page out or write the information on a piece of paper so that you can configure the correct settings on your Wi-Fi devices.

Access Point IP address   :   192.168.10.100

Access Point's MAC address   :   d0:ae:ec:51:bf:f0

Wi-Fi Network Name (SSID) 2.4GHz   :   TRENDnet750_2.4GHz_0020

Wireless Encryption   :   WPA-Personal / WPA2 Only

Wi-Fi Network Name (SSID) 5GHz   :   TRENDnet750_5GHz_0020

Wireless Encryption   :   WPA-Personal / WPA2 Only

Prev   Next   Cancel

Preset
Wireless Settings
Wi-Fi Name/SSID
XXXXXXXXXXXX
Wi-Fi Key
XXXXXXXXXXXX
Management Login
http://tew-750dap
    username: admin
    password: admin

8. Please wait while the settings are being applied. Setup is complete. Connect the access point to your router and connect your network ready devices to the access point's LAN ports.

Note: To configure additional modes, please refer to the Choosing your device mode on page 9.

The settings are being saved and are taking effect.

Please wait ...

Connect additional wired devices to your network

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

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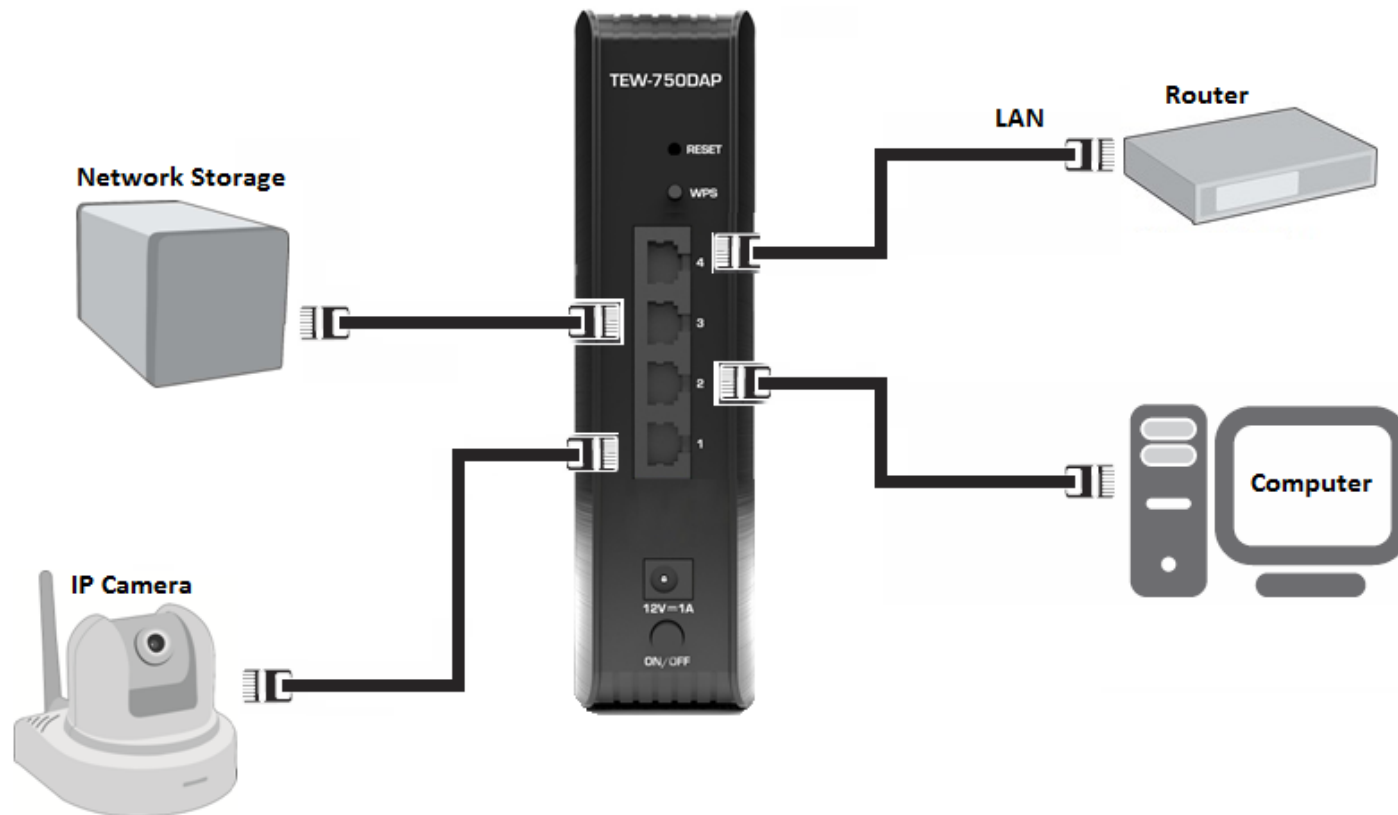
Access your access point management page

Note: Your access point management page URL/domain name http://tew-750dap or default IP address http://192.168.10.100 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.

If you have changed the default IP address, you will need to ensure that your computer is configured with IP address settings in the same subnet as the as the access point in order to access the access point management page. (Ex. Access Point IP address changed to 192.168.0.100 / 255.255.255.0, example computer address 192.168.0.25 / 255.255.255.0).

1. Open your web browser and go to URL/domain name http://tew-750dap or IP address http://192.168.10.100. Your access point will prompt you for a user name and password.
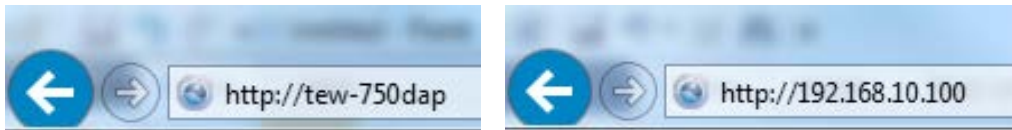
2. By default, the user name is *admin* and password is *admin*. You can also find the **Password** on a sticker on the side of the access point and on the label on the bottom of the access point. Enter your **Username** and **Password**, select your preferred language, then click **Login**.

Note: If you have changed the password already such as in the Setup Wizard, you will need to login using the new password.

Default User Name: **admin**
Default Password: **admin**
Note: User Name and Password are case sensitive.
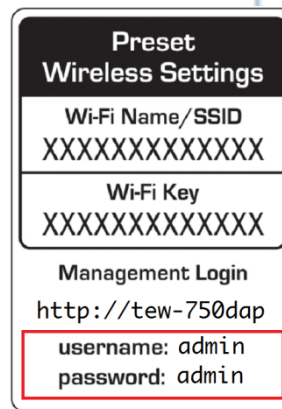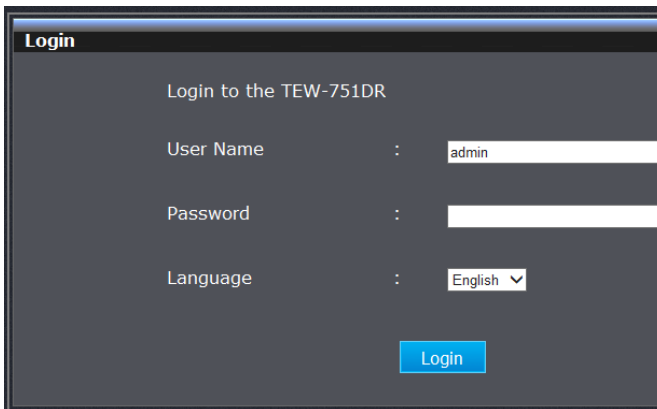
Choosing your device mode

Access Point (AP) Mode

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

The diagram below shows your access point connected to one of your router LAN ports and functioning in Access Point mode allowing wireless clients (ex. laptops, game consoles, DVRs, Smart TVs, and mobile devices, etc.) to wirelessly connect to your access point to establish network and Internet connectivity.

Note: The TEW-750DAP has dual band wireless capability allowing the access point to broadcast a wireless network name on two separate bands, 2.4GHz and 5GHz. Wireless clients can connect to your access on either band depending on the wireless band supported by your wireless client. The 2.4GHz band is more commonly used and supported for general applications such as Internet access and web browsing. The 5GHz band is less commonly used and supported which can be more useful for higher or stable bandwidth application requirements such as media streaming as this band may be less likely affected by neighboring wireless networks operating on the 5GHz band.

Set the device to access point mode

Main > Device Mode

Note: By default, the device is set to function in access point mode.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, click on **Device Mode.**

3. Click the **Device Operation Mode** drop-down list and select **Access Point**.
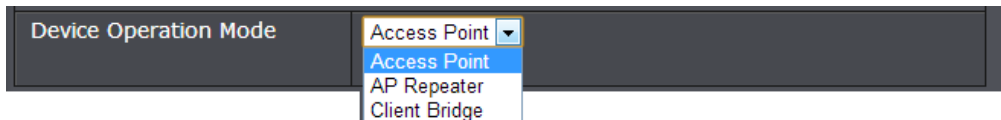
Device Operation Mode | Access Point
Access Point
AP Repeater
Client Bridge

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings   Don't Save Settings

Using access point mode

Wireless > Basic

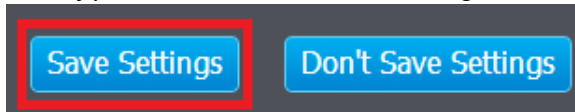This section outlines available management options under basic wireless sub tab for both 2.4GHz and 5GHz wireless sections.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, click on **Basic** scroll down to **Wireless Network Settings** (2.4GHz or 5GHz)

3. Review the settings, click **Save Settings** when finished.

- **Enable Wireless –** Check the option to enable the wireless network/band or uncheck to disable. *Note: It is recommended to leave this setting checked.*
  o **New Schedule –** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **New Schedule** and refer to page 45 Create Schedules. After you have created a new schedule, click the drop-down list and the new schedule will be available for selection.

Enable Wireless | ☑ Always ▼ New Schedule
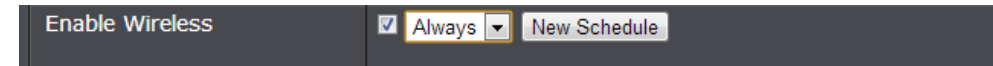
- **Wireless Network Name (SSID):** Enter the wireless name (SSID) for your wireless network. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the access point's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.

Wireless Network Name | TRENDnet750_2.4GHz_0((This is also called the SSID.)
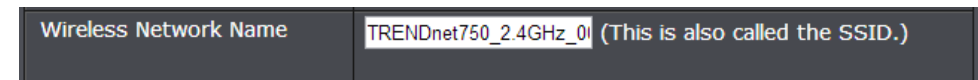
When applying the 802.11 Mode setting, please keep in mind the following:
- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g, 802.11b, or 802.11a.
- Connecting at 802.11b, 802.11g, or 802.11a will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b, 802.11g, or 802.11a devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b, 802.11g, or 802.11a 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.

- **Enable Auto Channel Scan –** Check this option to set your access point to scan for which wireless channels to use automatically.
- **Wireless Channel** – Unchecking the **Enable Auto Channel Scan** option will you to manually set the channel on which the access point will broadcast. Click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.

- **Transmission Rate** – Allows you to lock down the wireless transmission rate.
  Note: This feature is only available when using 802.11 n only mode.

- **Channel Width:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n. For greater 802.11n performance, select **20/40MHz (Auto)** (Options: 20MHz or 20/40MHz (Auto)). It is recommended to use the default channel bandwidth settings.
  Note: Please note that this setting may provide more stability than the higher channel bandwidth settings such as 20/40MHz (Auto) *for connectivity in busy wireless environments where there are several wireless networks in the area.*
  o **20 MHz** – 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 neighboring wireless networks in the area.
  o **20/40MHz (Auto)** –When 20/40MHz (Auto) is active, this mode is capable of providing higher performance only if the wireless devices support the channel bandwidth settings. Enabling 20/40MHz (Auto) typically results in substantial performance increases when connecting an 802.11n client.

- **Visibility Status**
  o **Visible -** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your access point.
  o **Invisible -** 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.

- **WMM:** Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your access point. *Note: This feature can only be disabled in 802.11a/b/g modes.*

Wireless Networking and Security

How to choose the type of security for your wireless network

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

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 access point to WEP to allow the old adapters to connect to the access point.
  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 access point 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 access point to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your access point to either WPA or WPA-Auto encryption.

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

| Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (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
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 300Mbps
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

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

Secure your wireless network

Wireless > Basic

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

Note: By default, your access point is configured with a predefined wireless network name (SSID) and security key using WPA2-Personal. The predefined wireless network name and security can be found on the sticker on the side of the access point or on the device label at the bottom of the access point.
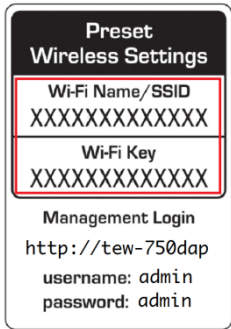
1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, and click on **Basic**.

4. Under **Wireless Security Mode (2.4GHz or 5GHz)**, click on the **Security Mode** drop-down list to select your wireless security type.
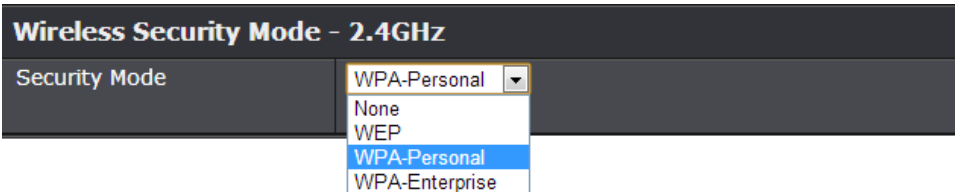
Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Save Settings** to save the changes.
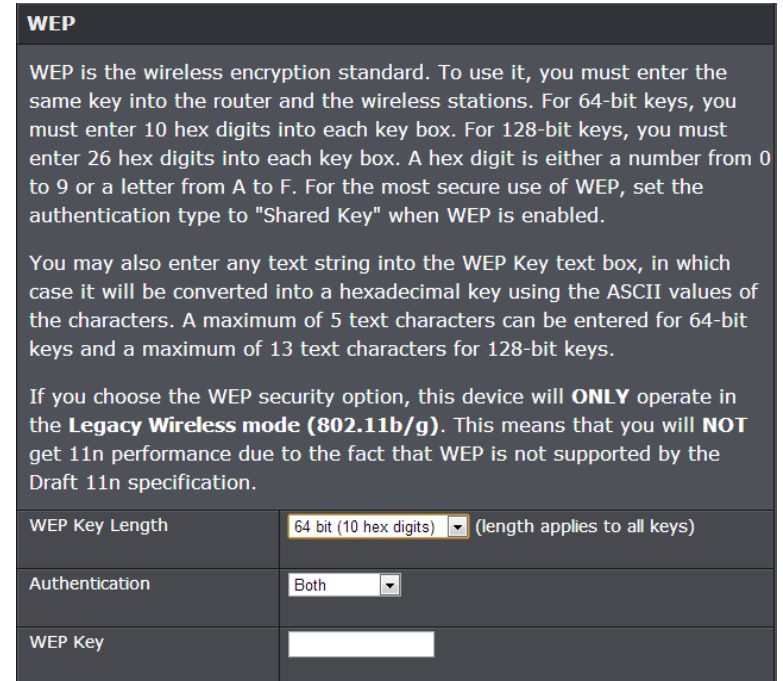
- **WEP Key Length:** Choose the key length **64-bit** or **128-bit** .
  Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.
- **Authentication:** Choose **Both** or **Shared.**
  Note: It is recommended to use Both which includes both Open and Shared. Open is known to be more secure than Shared Key.
- o **WEP Key:** Enter the WEP key. This is the password or key that is used to connect your computer to this access point wirelessly.

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-Personal with Auto (WPA or WPA2)/WPA Only/WPA2 Only
(WPA2 Only recommended):**

In the **Security Mode** drop-down list, select **WPA-Personal.** Please review the WPA-
Personal settings to configure and click **Save Settings** to save the changes.

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best
compatibility. This mode uses WPA for legacy clients while maintaining
higher security with stations that are WPA2 capable. Also the strongest
cipher that the client supports will be used. For best security, use **WPA2
Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not
allowed access with WPA security. For maximum compatibility, use **WPA
Only**. This mode uses TKIP cipher. Some gaming and legacy devices work
only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or
in other words AES cipher).

WPA Mode	WPA2 Only
Cipher Type	AES
Group Key Update Interval	3600 (seconds)

Pre-Shared Key

Enter an 8 to 63 ASCII or 8 to 64 HEX alphanumeric pass-phrase. For good
security it should be of ample length and should not be a commonly known
phrase.

Pre-Shared Key	75112345678

**Selecting WPA-Enterprise with Auto (WPA or WPA2)/WPA Only/WPA2 Only
(WPA2 Only recommended):**

EAP (802.1x)

**When WPA enterprise is enabled, the router uses EAP (802.1x) to
authenticate clients via a remote RADIUS server.**

RADIUS server IP Address	
RADIUS server Port	1812
RADIUS server Shared Secret	
Advance Setting	Advanced >>

The following section outlines options when selecting **WPA-Enterprise** (EAP or RADIUS)**.**
This security type is also known as EAP (Extensible Authentication Protocol) or Remote
Authentication Dial-In User Service or RADIUS.

*Note: This security type requires an external RADIUS server, Pre-Shared Key only requires
you to create a passphrase.*
- **RADIUS Server Address:** Enter the IP address of the RADIUS server. (e.g.
  192.168.10.250)
- **RADIUS Port:** Enter the port your RADIUS server is configured to use for RADIUS
  authentication.
  Note: It is recommended to use port 1812 which is typical default RADIUS port.
- **RADIUS Server Shared Secret:** Enter the shared secret used to authorize your
  access point with your RADIUS server.
- **Advance Setting** – Click this option to set up an additional backup RADIUS server.

Connect wireless devices to your access point

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

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

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this access point's wireless network.

See the "Appendix" on page 60 for general information on connecting to a wireless network.

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. Please note that WPS functionality will only be available when the Device Mode is set to Access Point mode under Main > Device Mode.*

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

- Push Button Configuration (PBC) method
  - o (RECOMMENDED) Hardware Push Button method–with an external button located physically on your access point and on your client device
  - o WPS Software/Virtual Push Button - located in access point management page
- PIN (Personal Identification Number) Method - located in access point management page
  Note: *Refer to your wireless device documentation for details on the operation of WPS.*

Recommended Hardware Push Button (PBC) Method

- **Note:** It is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. By default your access point is preconfigured with a wireless encryption key. If no wireless key is defined when connecting via PBC, the access point 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 access point 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 access point for 3 seconds and release it. The WPS LED will blink to indicate WPS has been activated on your access point. (See "Product Hardware Features" on page 2)

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

PBC (Software/Virtual Push Button)

Wireless > Wi-Fi Protected Setup

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

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, and click on **Wi-Fi Protected Setup**.

3. To add a wireless device to your network, click the **Connect** button in the access point management page.

Add Wireless Station

Connect your Wireless Device
Connect

4. Make sure **Auto** is selected and click **Next**.

Step 1: Select Configuration Method for your Wireless Network

Please select one of following configuration methods and click next to continue.

- ⊙ **Auto:** Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)
- ○ **Manual:** Select this option will display the current wireless settings for you to configure the wireless device manually

Prev　Next　Cancel　Connect

5. Select **PBC** and click **Connect**. Then push the WPS button on the wireless device (consult wireless device's User's Guide for length of time) you are connecting.

Step 2: Connect your Wireless Device

There are two ways to add wireless device to your wireless network:
-PIN (Personal Identification Number)
-PBC (Push Button Configuration)

○ PIN : [_____]

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

⊙ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Prev　Next　Cancel　Connect

6. Wait for your access point to finsh the WPS process.

Press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network.
Remain time in seconds.: 110

Adding wireless device.: Started.

Prev　Next　Cancel　Connect

7. If successful, you will receive the message below. Click on **Wireless Status** to view the information about the current wireless client devices connected to your access point.

Adding wireless device.: Succeeded. To add another device click on the Cancel button below or click on the Wireless Status button to check the wireless status.

Prev　Next　Cancel　Wireless Status

PIN (Personal Identification Number)

Wireless > Wi-Fi Protected Setup

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

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, and click on **Wi-Fi Protected Setup**.

3. To add a wireless device to your network, click the **Connect** button in the access point management page.

4. Make sure **Auto** is selected and click **Next**.

5. Select **PIN** and enter the 8-digit numeric PIN number of the wireless client device and click **Connect**.

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

6. Wait for your access point to finsh the WPS process.

7. If successful, you will receive the message below. Click on **Wireless Status** to view the information about the current wireless client devices connected to your access point.

Steps to improve wireless connectivity

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

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
    a. For the widest coverage area, install your access point near the center of your home, and near the ceiling, if possible.
    b. Avoid placing the access point on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.

    c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the access point and the wireless device, the better.

    d. Place the access point in a location away from other electronics, motors, and fluorescent lighting.

    e. Many environmental variables can affect the access point's performance, so if your wireless signal is weak, place the access point in several locations and test the signal strength to determine the ideal position.

2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.

3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.

4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n 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.

Multiple SSID

Access > Multi-SSID

The multiple SSID feature allows you to broadcast up to 3 additional SSIDs (or wireless network names) per band (2.4GHz and 5GHz). 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. Each SSID 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.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Advanced**, and click on **Multi-SSID**.

3. Click the **Multi-SSID Index** drop-down list and select the SSID to configure.

4. Check the **Enable SSID** option to enable the selected SSID or uncheck to disable.

    o **New Schedule –** The schedule function allows you to define a schedule when the wireless SSID should be turned on. To define a new schedule, click **New Schedule** and refer to page 45 Create Schedules. After you have created a new schedule, click the drop-down list and the new schedule will be available for selection.
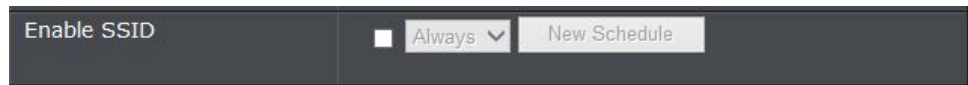
5. In the **Wireless Network Name (SSID)** field, enter the wireless name (SSID) to broadcast for the additional SSID.
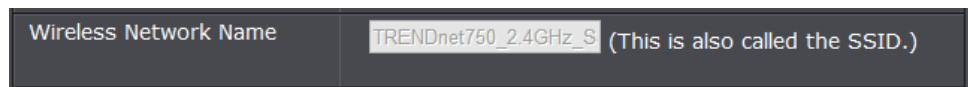
6. Configure the wireless security for the selected SSID. See page 13 Securing your wireless network for details on configuring wireless security.

7. Click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***
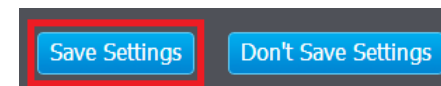
Repeat these steps 2-7 to configure the additional SSIDs.

Note: To verify that the multiple SSIDs are active, using a wireless device, scan for available wireless networks and check if the wireless device is able to discover the SSIDs. To check connectivity, using a wireless device, connect to these SSIDs using the wireless security types you have configured.

Allow/deny multicast streaming

Access > Advanced Network

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Access**, and click on **Advanced Network**.

3. Under **Enable IPv4 Multicast Streams** next to **Wireless Enhanced Mode**, check the option to enable or uncheck to disable.

Enable IPv4 Multicast Streams	☐

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Advanced wireless settings

Wireless > Advanced

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

- **Transmit 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 neighboring wireless networks.

- **Beacon Period:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the access point's wireless network. The interval is the amount time between each beacon transmission.

    Default Value: 100 milliseconds (range: 20-1000)

- **Preamble Type:** Select the option that works best for your installation. It may be best to keep this option at its default setting.
    - **Short Preamble -** Using a short guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections.
    - **Long Preamble –** Using a long preamble can help to decrease the error rate in wireless data transmission and receiving.

Advanced Wireless Settings - 2.4GHz

Transmit Power	100%
Beacon Period	100 (milliseconds, Range: 20~1000, default: 100)
Preamble Type	○ Short Preamble ⊙ Long Preamble

Advanced Wireless Settings - 5GHz

Transmit Power	100%
Beacon Period	100 (milliseconds, Range: 20~1000, default: 100)
Preamble Type	○ Short Preamble ⊙ Long Preamble

Wireless Bridge (WDS) Mode

Wireless bridging using WDS (Wireless Distribution System) 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. Network enabled devices can be plugged into one of the four available Ethernet LAN ports. WDS is subset option of Access Point mode.

There are 2 types of WDS modes,

- WDS (pure WDS) – Strictly for establishing wireless bridging only and will not function in access point simultaneously, 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. The diagram below illustrates examples of pure WDS.

- WDS+AP - Allows the device to establish wireless bridging and function as access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect to the access point in order to access network resources from multiple groups of network devices as well as the Internet. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 23 for details on this mode.

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.

The diagram below illustrates an example of multiple WDS wireless bridge links.

Wireless Bridge (WDS) with Access Point (AP) Mode

Wireless bridging using WDS (Wireless Distribution System) 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. Network enabled devices can be plugged into one of the four available Ethernet LAN ports. WDS is subset option of Access Point mode.
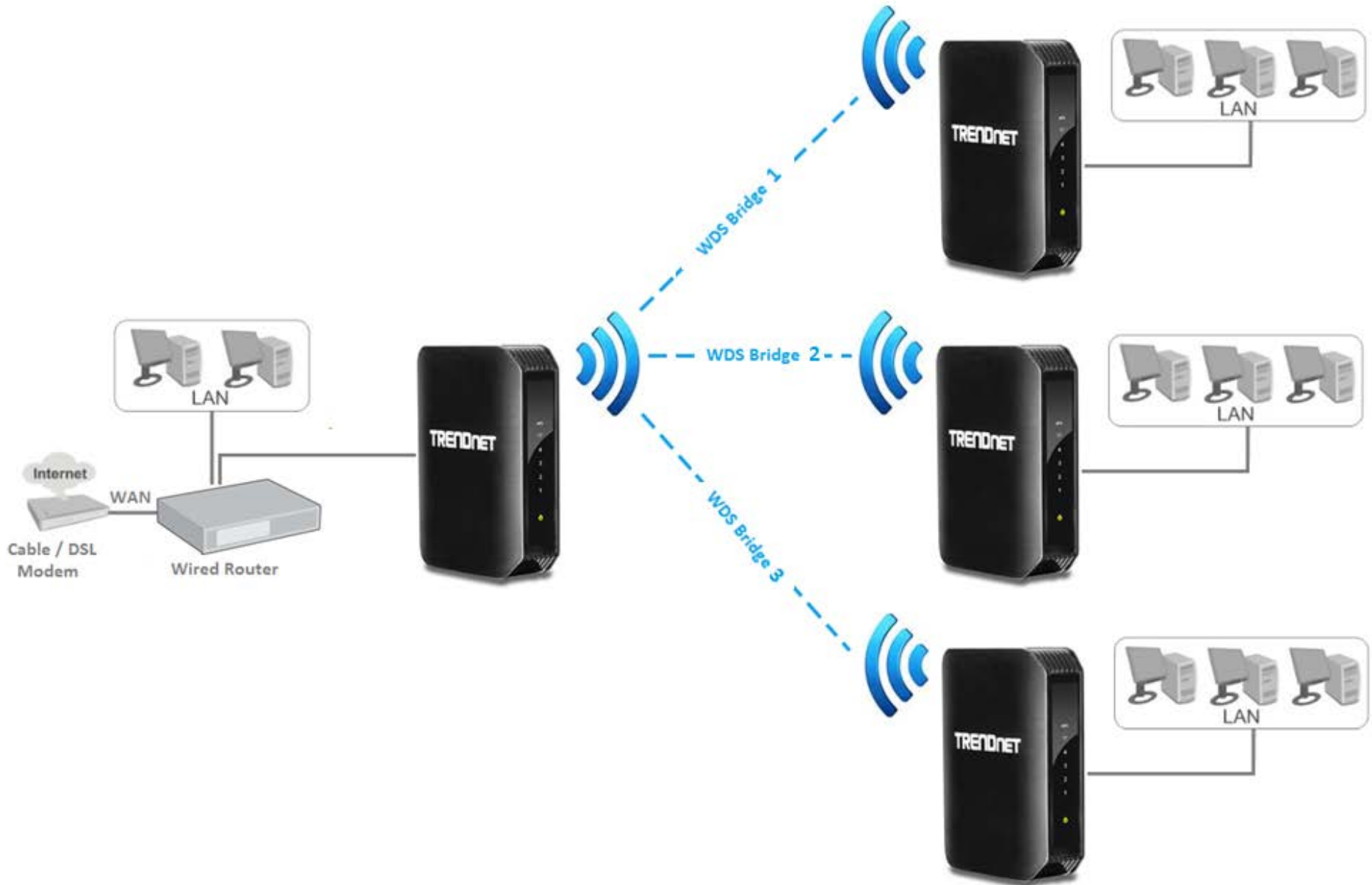
There are 2 types of WDS modes,

- WDS+AP - Allows the device to establish wireless bridging and function as access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect to the access point in order to access network resources from multiple groups of network devices as well as the Internet. The diagrams below illustrate examples of WDS with Access Point.

- WDS (pure WDS) – Strictly for establishing wireless bridging only and will not function in access point simultaneously, 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. Please refer to the section Wireless Bridge (WDS) Mode page 21 for details on this mode.

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.

The diagram below illustrates an example of multiple WDS wireless bridge links with access point functionality.
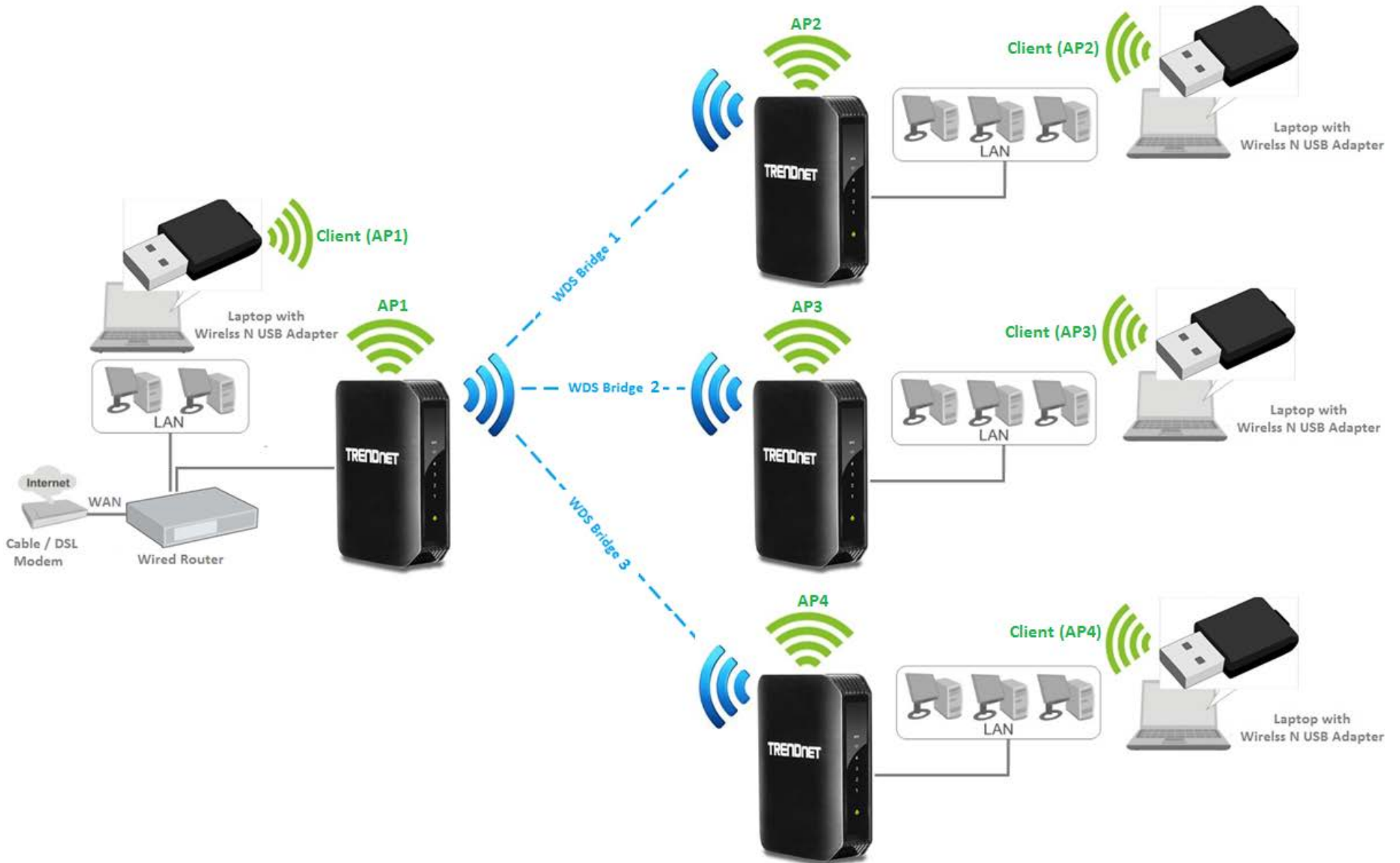
Planning for Wireless Bridging (WDS)

Note: By default, the device is set to function in access point mode. WDS is a subset option of Access Point Mode. You must set your access point device mode to operate in Access Point first in order to configure WDS. Please ensure the Device Mode is set to Access Point under Main > Device Mode.

Before configuring WDS, please ensure the following items first:

1. Choose which band to use for bridging (2.4GHz or 5GHz). If all of your WDS supported devices do not the 5GHz band, you may need to choose the 2.4GHz.

2. Make sure different IP addresses are assigned to each WDS supported wireless device used for bridging. (ex. 192.168.10.100,192.168.10.99,192.168.10.98, etc.) to avoid IP address conflicts. See the section Change your access point IP address page 40 for changing the access point IP address.

3. Please ensure that only one DHCP server is assigning IP addresses on your network to avoid IP address conflicts. Typically, most routers used in a home environment include a built-in DHCP server (typically enabled by default) to assign IP addresses to local client devices automatically. Please make sure that only one device on your network has DHCP server enabled and disabled on all others to avoid IP address conflicts.

4. WDS bridging requires all WDS supported devices to use the same wireless network name (SSID), wireless channel, and wireless security settings on all WDS supported wireless devices. Refer to page 10 "Using access point mode" to configure wireless network name (SSID) and wireless channel settings. Refer to page 12 "Wireless Networking and Security" to configure wireless security settings.

5. You will require the wireless MAC address of each WDS supported device. On any network, each network device has a unique 6-digit MAC (Media Access Control) address. *For each WDS supported device, all of the remote wireless MAC addresses of the other WDS supported device you are bridging. (Ex. In diagram on the next page, AP1 needs to enter the remote MAC addresses (red text) of AP2, AP3, and AP4. AP2 needs to enter the remote MAC address of AP1 only, AP3 and AP4 also need to enter the remote MAC address of AP1 only). You can find the wireless MAC address of the access point in the management page under Status > Device Information.*
Note: Please note that 2.4GHz and 5GHz bands will have two different MAC addresses.

The diagram below illustrates an example of the parameters configured when planning for WDS bridging. Each WDS supported access point is configured with a different IP address **(blue)** to prevent IP address conflict. The "wired router" is the only single DHCP server **(gray)** providing automatic IP address assignment for all client devices in the network. The WDS parameters required to match on all WDS supported access points in order to establish WDS wireless bridging is configured **(blue)**. The wireless MAC of all devices is noted **(red)**.
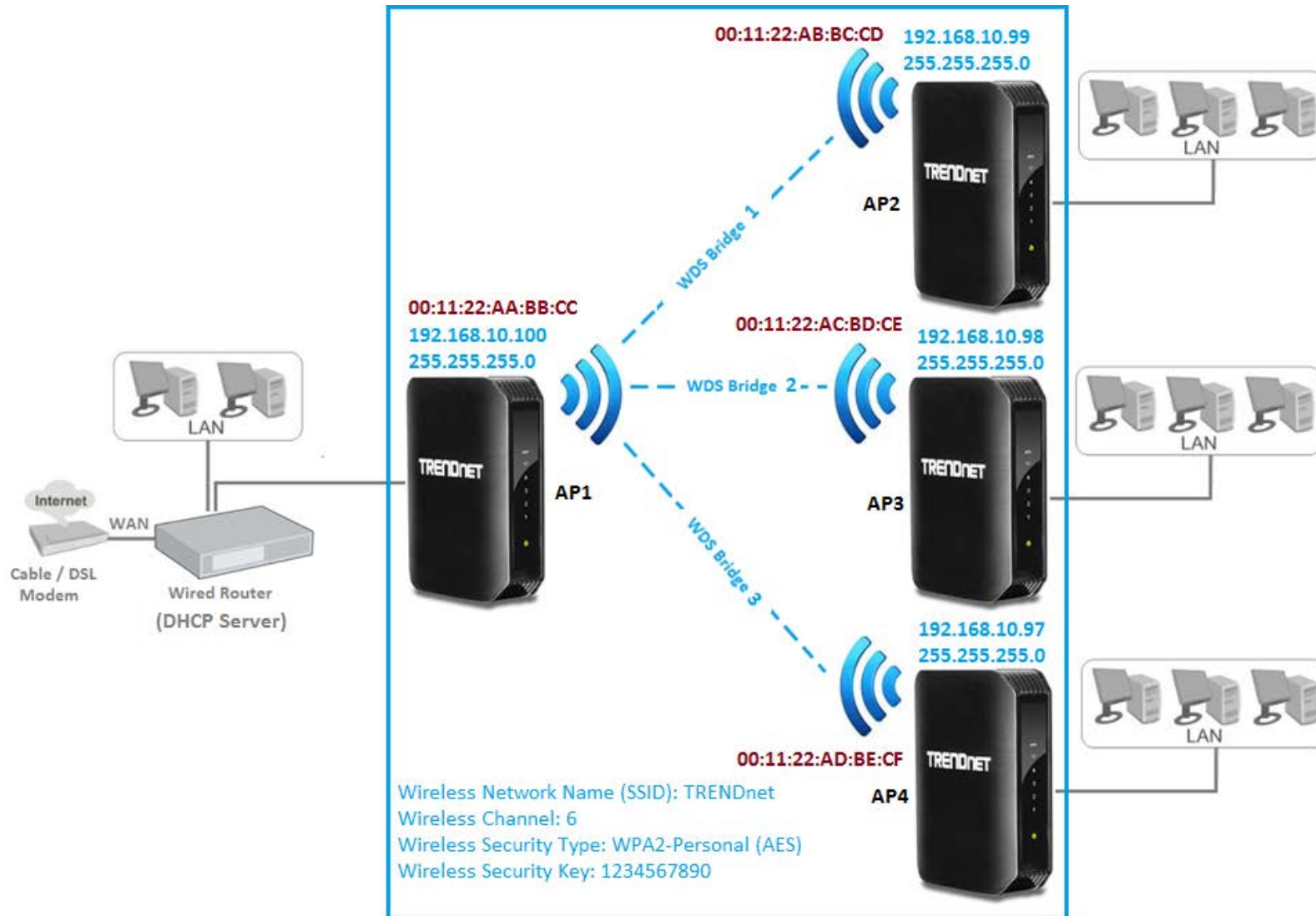
Creating a Wireless Bridge (WDS)

Wireless > Basic

Note: *Since wireless bridge (WDS) is a subset of Access Point mode, please make sure that Access Point mode is selected under Main > Device Mode for all access points. See page 13 "Set your device to access point mode." This procedure can apply for both WDS and WDS+AP modes.*

To configure a wireless bridge (WDS) between two TEW-750DAP access points:

- Make note of the wireless MAC address of both access points. See page XX for checking the status page.

  Note: *Please note that 2.4GHz and 5GHz bands will have two different MAC addresses. If using the 2.4GHz band wireless MAC address, please use the 2.4GHz wireless MAC address for all other WDS supported devices to bridge and if using the 5GHz band wireless MAC address, use the 5GHz wireless MAC address for all other WDS supported devices to bridge.*

  Example:

  *AP1 (Access Point 1) 2.4GHz Wireless MAC Address: 00:11:22:AA:BB:**C1***

  *AP1 (Access Point 1) 5GHz Wireless MAC Address: 00:11:22:AA:BB:**C2***

  *AP2 (Access Point 2) 2.4GHz Wireless MAC Address: 00:11:22:AA:BB:**C3***

  *AP2 (Access Point 2) 5GHz Wireless MAC Address: 00:11:22:AA:BB:**C4***

- Make sure the IP address on each WDS supported access is point is different and on the same IP network/subnet. See page XX for changing access point IP address.

  Example:

  *AP1 (Access Point 1) IP Address Settings: 192.168.10.**100** / 255.255.255.0*

  *AP2 (Access Point 2) IP Address Settings: 192.168.10.**99** / 255.255.255.0*

AP1 Configuration
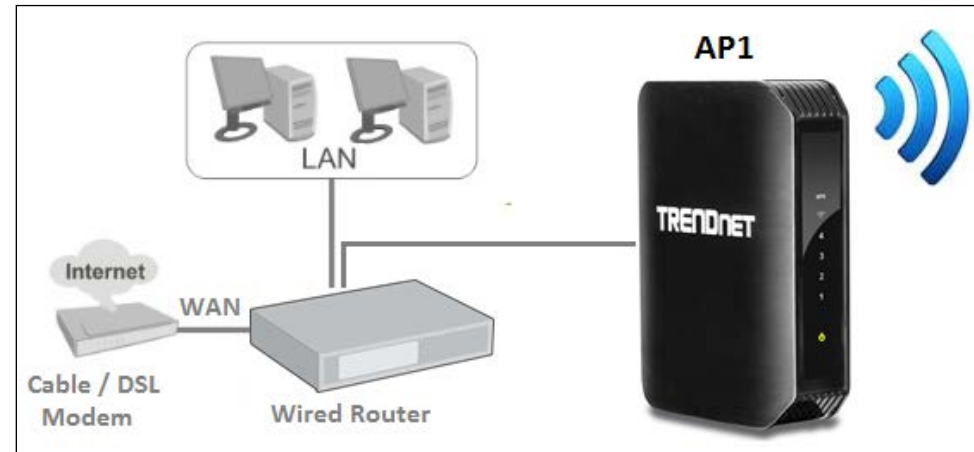
1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, click on **Basic** and scroll down to **Wireless Network Settings -** (2.4GHz or 5GHz). **Note:** *For this example, 2.4GHz band will be used.*

3. Click the **Device Operation Mode** drop-down list and select one of following WDS options.

- **WDS –** Select this option to establish wireless bridging only without broadcasting your wireless network name for client devices to connect. Please refer to the section Wireless Bridge (WDS) Mode page 21 for details on this mode.

- **WDS+AP (Recommended)** – Select this option to establish wireless bridging and broadcast your wireless network name for client devices to connect simultaneously. See page 23 for details. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 23 for details on this mode.
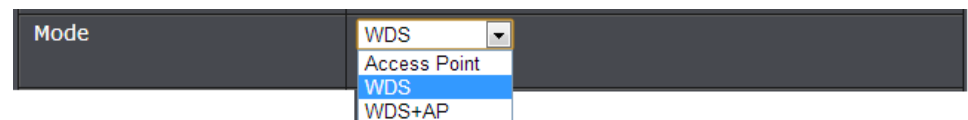
4. Next to **Wireless Network Name**, enter the wireless network name (SSID).

(ex. TRENDnet750_2.4GHz)

Wireless Network Name	TRENDnet750_2.4GHz	(This is also called the SSID.)

5. Click the **Wireless Channel** drop-down list and select a specific wireless channel.

(ex. 2.462GHz - CH 11)

Wireless Channel	2.462 GHz - CH 11 ▾

6. Under the **WDS** section, next to **Remote AP MAC Address1**, enter the wireless MAC address of the remote WDS supported access point or router.

Remote AP MAC Address1		Site Survey

Note: Based on the example, enter the remote 2.4GHz wireless MAC address of AP2.

(00:11:22:AA:BB:C3)

Remote AP MAC Address1	00:11:22:AA:BB:C3	Site Survey **AP2 2.4GHz MAC Address**

Note: You can also use the site survey option to scan for your remote WDS supported device broadcasting (AP or WDS+AP), then select and connect to copy the wireless MAC addresses of your other WDS supported devices. This simplifies the process of having to write down the wireless MAC addresses of all devices and manually enter.

7. Configure the wireless security settings and wireless key.

Note: Please refer to page 12 "Wireless Networking and Security" for details on configuring wireless security settings.

8. Click **Save Settings**.
*Note: If you would like to discard the changes, click **Don't Save Settings.***

[Save Settings] [Don't Save Settings]

AP2 Configuration
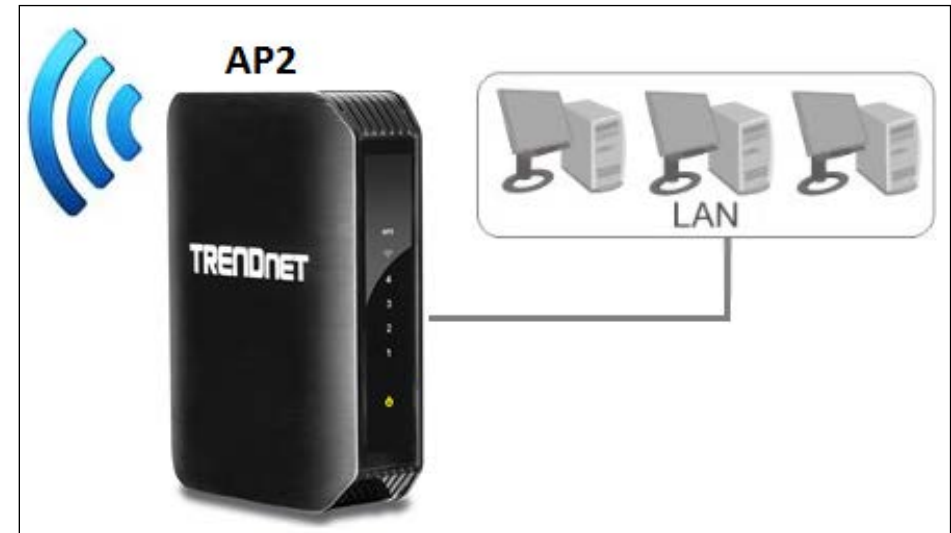
1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless**, click on **Basic** and scroll down to **Wireless Network Settings -** (2.4GHz or 5GHz). *Note: For this example, 2.4GHz band will be used which also matches the band used for AP1.*

3. Click the **Device Operation Mode** drop-down list and select one of following WDS options. *Note: WDS or WDS+AP modes can work with each other between WDS support devices.*

- **WDS –** Select this option to establish wireless bridging only without broadcasting your wireless network name for client devices to connect. Please refer to the section Wireless Bridge (WDS) Mode page 21 for details on this mode.
- **WDS+AP** (Recommended) – Select this option to establish wireless bridging and broadcast your wireless network name for client devices to connect simultaneously. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 23 for details on this mode.

Mode   WDS
        Access Point
        WDS
        WDS+AP

4. Next to **Wireless Network Name**, enter the wireless network name (SSID).

Note: For this example, the wireless network name (SSID) is required to match the wireless network name (SSID) configured on AP1.

(ex. TRENDnet750_2.4GHz)

Wireless Network Name   TRENDnet750_2.4GHz   (This is also called the SSID.)

5. Click the **Wireless Channel** drop-down list and select a specific wireless channel.

Note: For this example, the wireless channel is required to match the wireless channel configured on AP1.

(ex. 2.462GHz - CH 11)

Wireless Channel   2.462 GHz - CH 11

6. Under the **WDS** section, next to **Remote AP MAC Address1**, enter the wireless MAC address of the remote WDS supported access point or router.

Remote AP MAC Address1   [   ]   Site Survey

Note: Based on the example, enter the remote 2.4GHz wireless MAC address of AP1.

(00:11:22:AA:BB:**C1**)

Remote AP MAC Address1   00:11:22:AA:BB:C1   Site Survey   **AP1 2.4GHz MAC Address**

Note: You can also use the site survey option to scan for your remote WDS supported device broadcasting (AP or WDS+AP), then select and connect to copy the wireless MAC addresses of your other WDS supported devices. This simplifies the process of having to write down the wireless MAC addresses of all devices and manually enter.

7. Configure the wireless security settings and wireless key.

Note: Please refer to page 12 "Wireless Networking and Security" for details on configuring wireless security settings.

8. Click **Save Settings**.

Note: If you would like to discard the changes, click **Don't Save Settings.**

Save Settings   Don't Save Settings

Bridging additional WDS supported devices

For a point-to-multipoint (hub and spoke) WDS configuration, the AP2 (spoke) configuration procedure in the previous section "Creating a Wireless Bridge" page 28 can be used when creating additional WDS bridges to AP1 (hub).

For multiple point-to-point wireless WDS bridge links, you can follow the entire configuration procedure in the previous section "Creating a Wireless Bridge" on page 28.

The TEW-750DAP can support up to 4 wireless WDS bridges per band (2.4GHz and 5GHz) for a total of 8 wireless WDS bridge connections.

Additional WDS Options

The TEW-750DAP access point provides 2 methods to simplify the entering the remote wireless MAC addresses when configuring WDS mode.

- **Lazy WDS**

  Wireless > Basic > Wireless Network Settings - (2.4GHz or 5GHz) > WDS

  This option simplifies the configuration of MAC address in WDS by only requiring one side of a WDS bridge to add remote wireless MAC addresses. For example, if the wireless MAC address of AP2 has been added to AP1, the wireless MAC address of AP1 does not need to be added to AP2. On AP2, you would need to simply enable (check) Lazy WDS to establish the bridge connection. This option is only available when using Wireless Bridge with Access Point.

Enable Lazy Mode	☐
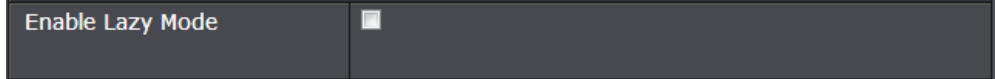
- **WDS Site Survey**

  Wireless > Basic > Wireless Network Settings - (2.4GHz or 5GHz) > WDS

  This option allows you to scan for your remote WDS supported devices broadcasting (WDS+AP mode), then select and connect to copy the wireless MAC addresses of your other WDS supported device. This simplifies the process of having to write down the wireless MAC addresses of all other WDS supported devices. This option is most useful when using Wireless Bridge with Access Point.

Remote AP MAC Address1		Site Survey

SITE SURVEY

Wireless Network Name	BSSID	Channel	Type	Auth	Encrypt	Signal	Select
TRENDnet735_2.4GHz_9ELS	00:02:6f:e8:7f:6c	11(b/g/n)	AP	WPA2PSK	AES	100%	●
Samsung Test	d8:eb:97:a8:4d:bc	11(b/g/n)	AP	WPA2PSK	AES	86%	●
QH Wifi	58:6d:8f:d6:de:c2	11(b/g/n)	AP	WPA2PSK	AES	15%	●
TrendnetSkyN	00:14:d1:cf:3f:0c	11(b/g/n)	AP	WPA2PSK	AES	91%	●
Wally World	00:14:d1:9b:b3:74	11(b/g/n)	AP	WPA2PSK	AES	70%	●
TRENDnet8128445	d8:eb:97:a4:fe:5f	11(b/g/n)	AP	WPA2PSK	AES	65%	●

| Refresh | Connect | Cancel |

- **Spanning Tree Protocol**

  Wireless > Advanced > Spanning Tree Protocol (STP)

  This option allows the device to create redundant wireless WDS bridge links to provide fault tolerance in case the primary wireless WDS bridge link fails. When creating redundant wireless WDS bridge links, STP must be enabled to prevent loops and broadcast storms to occur across the network which may cause slow network connectivity and even intermittent loss of connectivity over the wireless bridged network. This option is only available when the device is set to WDS or WDS+AP modes.

  The diagram below illustrates 2 additional redundant/backup wireless WDS bridged links (WDS Bridge 4 between AP2 & AP3 and WDS Bridge 5 between AP3 & AP4) created which would require the STP option to be enabled.

Spanning Tree Protocol(STP)

Enable Spanning Tree	☐
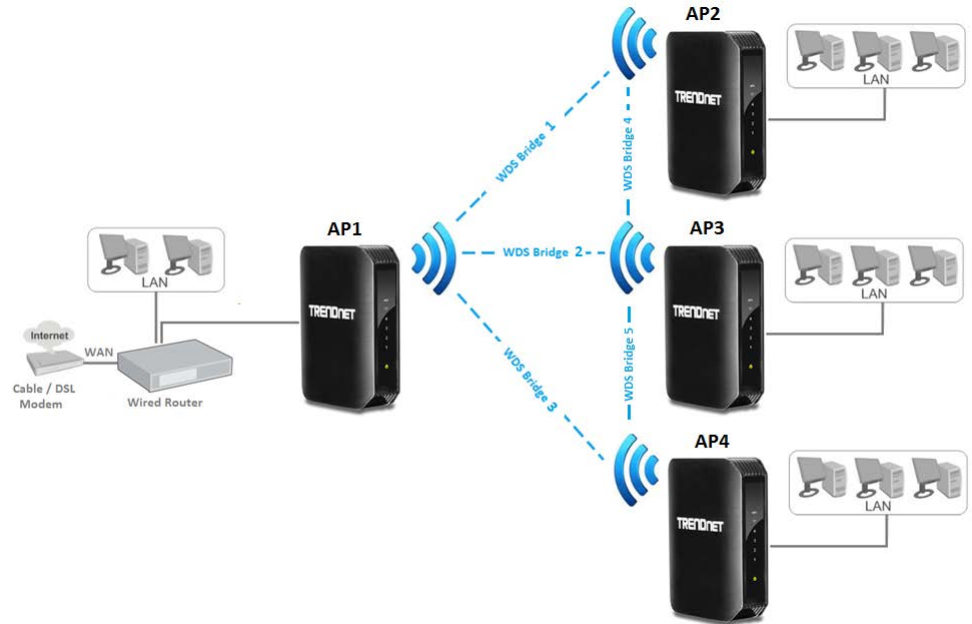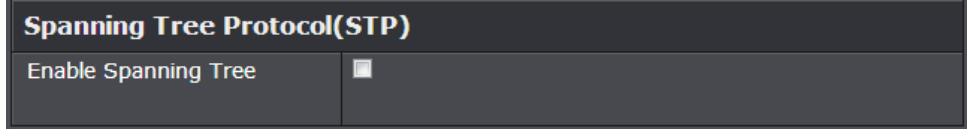
Wireless Range Extender (AP Repeater)

Wireless range extender or repeater mode allows the device to extend the range of an existing wireless network. The existing wireless signal can be broadcasted from your wireless router or other access point. In addition, other network enabled devices can connect to your network using the Ethernet LAN ports. The functionality of this mode is similar to WDS with Access Point however, wireless range extender mode does not require the other wireless device to support repeater or WDS and can only function using one band at a time, 2.4GHz or 5GHz and other modes cannot be used simultaneously. The diagram illustrates an example of the device repeating the signal of an existing access point. Wireless client devices can connect to which ever signal is stronger.

Set the device to wireless range extender (repeater) mode

Main > Device Mode

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, click on **Device Mode.**

3. Click the **Device Operation Mode** drop-down list and select **AP Repeater**.
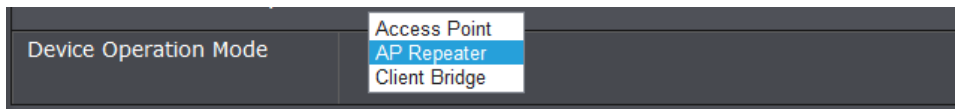
Device Operation Mode	Access Point
	AP Repeater
	Client Bridge

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings	Don't Save Settings
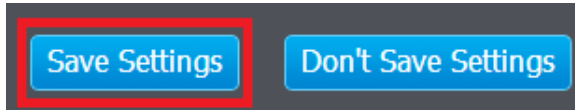
Using wireless range extender (repeater) mode

Wireless > Site Survey

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless** and click on **Site Survey.**

3. Search for your wireless network to extend or repeat in the wireless network list. In the **Select** column, click the radio button to select your wireless network.

SITE SURVEY

Select your wireless network using the Select column and click the Connect button below.

Wireless Network Name	BSSID	Channel	Type	Auth	Encrypt	Signal	Select
TRENDnet753_2.4GHz_5RL2	00:02:6f:e8:f7:d9	6(b/g/n)	AP	WPA2PSK	AES	100%	○
TrendnetSkyN	00:14:d1:c5:7d:44	1(b/g/n)	AP	WPA2PSK	AES	39%	○
TrendnetOp	00:14:d1:9d:9a:1c	1(b/g/n)	AP	WPA2PSK	AES	29%	○
TRENDnet711	00:14:d1:b8:0b:64	1(b/g)	AP	WPAPSK	TKIP	100%	○
TRENDnet812b2fa	00:11:e0:04:96:4d	1(b/g/n)	AP	WPA2PSK	AES	91%	○
TRENDnet812acb2fa	00:11:e0:04:96:51	149(a/n)	AP	WPA2PSK	AES	100%	○
TRENDnet753_5GHz_5RL2	00:02:6f:e8:f7:d8	149(a/n)	AP	WPA2PSK	AES	100%	○
TRENDnet810AC6H4Z	d8:e8:97:1e:34:aa	157(a/n)	AP	WPA+2PSK	TKIPAES	60%	○
TRENDnet812ac9750	d8:eb:97:a5:18:6b	157(a/n)	AP	WPA2PSK	AES	100%	○

4. At the bottom, click **Connect** to connect and copy the settings of the selected wireless network.

*Note: If you are unable to find your wireless network in the list, you can click **Refresh** to rescan the available wireless networks.*

Refresh	Connect	Cancel

5. If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your **Wireless Key** required to connect to your existing wireless network and click **Next.**

Note: If you wireless network does not require wireless security, skip to the next step.

ENTER WIRELESS KEY

Please enter Wireless key to establish wireless connection.

Wireless Key   :   [_____] ■ Display Characters

[Prev]   [Next]   [Cancel]

6. Click **Save Settings** to apply the changes.

SAVE SETTINGS

Click Save Settings to apply the changes.

[Save Settings]

7. Wait for the device to apply the settings.

Saving

The settings are being saved and are taking effect.

Please wait …

8. To verify the access point has successfully copied the settings and repeated the signal of your wireless network, wait for the Link Status to display **Connected**.

It may take up to 1 minute for your device to verify and display the connection status.

Note: If the Link Status does not display a Connected status after 1 min, please re-attempt the procedure.

Link Status	
Status	Connected
Tx Link Speed	130.0 (Mbps)
Rx Link Speed	130.0 (Mbps)
Signal Strength	100%

Status > Link Status

- **Status** – Displays the connection status of the device either **Connected** or **Disconnected.**
- **Tx Link Speed** – Displays the estimated wireless transmission speed established to the wireless network.
- **Rx Link Speed** – Displays the estimated wireless receive speed established to the wireless network.
- **Signal Strength** – Displays the estimated signal strength of the wireless network detected by the device.

9. Once your wireless signal has been successfully verified, unplug the device and plug into an available power outlet in the area you would like to repeat or extend signal coverage of your existing wireless network.

Note: You can also connect additional wired network devices to the available LAN ports 1-4 on the back of the device via Ethernet to connect these devices to your network.

Client Bridge

Client Bridge mode allows the device to act as a wireless client device to connect to your wireless network and bridge the wireless connection from the wireless network to the four LAN ports (1-4) located on the back of the device. Client devices with wired network capability such as in a media or entertainment center (ex. Smart TV, Game Console, DVR, etc.) can connect to one of the available LAN ports using an Ethernet cable to establish wired connectivity to your network. When using this mode, please note that Client Bridge mode can only function using one band at a time, 2.4GHz or 5GHz and other modes cannot be used simultaneously.
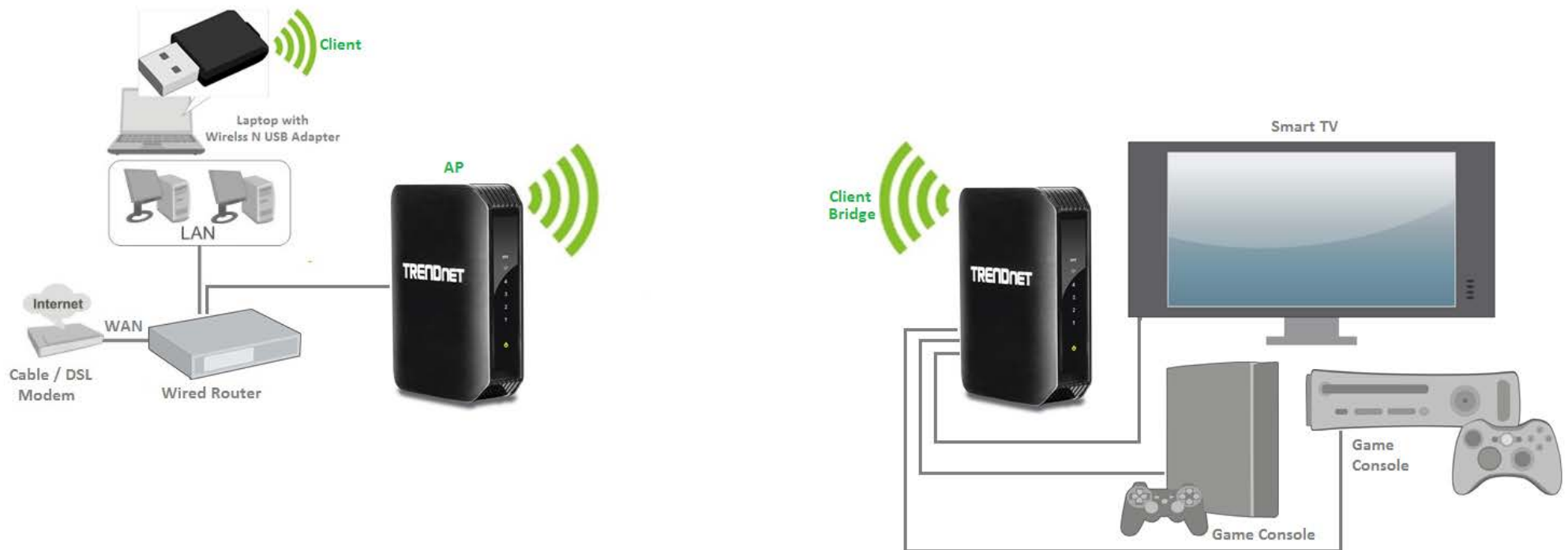
Set the device to client bridge mode

Main > Device Mode

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, click on **Device Mode.**

3. Click the **Device Operation Mode** drop-down list and select **Client Bridge**.
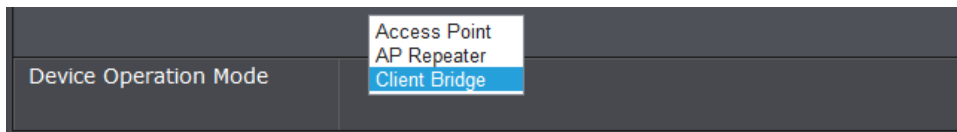
4. To save changes, click **Save Settings**.

Note: *If you would like to discard the changes, click **Don't Save Settings.***
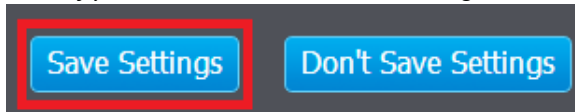
Using client bridge mode

Wireless > Site Survey

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Wireless** and click on **Site Survey.**

3. Search for your wireless network to connect to in the wireless network list. In the **Select** column, click the radio button to select your wireless network.

SITE SURVEY

Select your wireless network using the Select column and click the Connect button below.

Wireless Network Name	BSSID	Channel	Type	Auth	Encrypt	Signal	Select
TRENDnet753_2.4GHz_5 RL2	00:02:6f:e8:f7:d9	6(b/g/n)	AP	WPA2PSK	AES	100%	●
TrendnetSkyN	00:14:d1:c5:7d:44	1(b/g/n)	AP	WPA2PSK	AES	39%	●
TrendnetOp	00:14:d1:9d:9a:1c	1(b/g/n)	AP	WPA2PSK	AES	29%	●
TRENDnet711	00:14:d1:b8:0b:64	1(b/g)	AP	WPAPSK	TKIP	100%	●
TRENDnet812b2fa	00:11:e0:04:96:4d	1(b/g/n)	AP	WPA2PSK	AES	91%	●
TRENDnet812acb2fa	00:11:e0:04:96:51	149(a/n)	AP	WPA2PSK	AES	100%	●
TRENDnet753_5GHz_5RL 2	00:02:6f:e8:f7:d8	149(a/n)	AP	WPA2PSK	AES	100%	●
TRENDnet810AC6H4Z	d8:e8:97:1e:34:aa	157(a/n)	AP	WPA+2P SK	TKIPAES	60%	●
TRENDnet812ac9750	d8:eb:97:a5:18:6b	157(a/n)	AP	WPA2PSK	AES	100%	●

4. At the bottom, click **Connect** to connect to the selected wireless network.

Note: *If you are unable to find your wireless network in the list, you can click **Refresh** to rescan for the available wireless networks.*

5. If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your **Wireless Key** required to connect to your existing wireless network and click **Next.**

Note: If you wireless network does not require wireless security, skip to the next step.

ENTER WIRELESS KEY
Please enter Wireless key to establish wireless connection.

Wireless Key   :   [   ] ■ Display Characters

[Prev]   [Next]   [Cancel]

6. Click **Save Settings** to apply the changes.

SAVE SETTINGS
Click Save Settings to apply the changes.

[Save Settings]

7. Wait for the device to apply the settings.

Saving

The settings are being saved and are taking effect.

Please wait …

8. To verify the access point has successfully connected to your wireless network, wait for the Link Status to display **Connected**.

It may take up to 1 minute for your device to verify and display the connection status.

Note: If the Link Status does not display a Connected status after 1 min, please re-attempt the procedure.

Link Status	
Status	Connected
Tx Link Speed	130.0 (Mbps)
Rx Link Speed	130.0 (Mbps)
Signal Strength	100%

Status > Link Status

- **Status** – Displays the connection status of the device either **Connected** or **Disconnected.**
- **Tx Link Speed** – Displays the estimated wireless transmission speed established to the wireless network.
- **Rx Link Speed** – Displays the estimated wireless receive speed established to the wireless network.
- **Signal Strength** – Displays the estimated signal strength of the wireless network detected by the device.

9. Once your wireless signal has been successfully verified, unplug the device and plug into an available power outlet in the area extend or bridge connectivity to your wireless network to wired client devices such as computers, Smart TVs, Game Consoles, DVRs, etc..

Note: A typical application for this would be a media or entertainment center where multiple devices with wired network capability can connect using an Ethernet cable.

Access Control Filters

MAC Address Filters

Access > MAC Filters

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this access point's wireless network. You can enter up to 24 MAC address entries.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Access**, click on **MAC Filters.**

3. Review the MAC Filter options, click **Save Settings** to save settings.

Click the **Configuring MAC Filtering below** drop-down list to choose the MAC filter function.
- **Turn MAC Filtering OFF** – disables the MAC address filter.
- **Turn MAC Filtering ON and ALLOW computers listed to access the network**
  Only **Allow** computers/devices with MAC addresses listed to access the access point management page and the Internet. Deny all others. **Turn MAC Filtering ON and DENY computers listed to access the network**

  Only **Deny** computers/devices with MAC addresses listed to access to the access point management page and the Internet. Allow all others.

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

Before saving settings, add the MAC addresses to the MAC Table and configure the options first.

- **MAC Address –** Check the box next to the entry to enable and in the empty field, enter the MAC address of the devices you would like to filter.
  (e.g. 00:11:22:AA:BB:CC)
- **DHCP Client List** – Click the drop-down list to select from the list of client devices connected to your access point. Once selected, click **<<** to copy the MAC address of the selected device to MAC Address field.
  Note: DHCP Client List will only be active if using the access point's built in DHCP server functionality. See page 41 "Setup the DHCP Server on your access point " for DHCP server options.
- **New Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 45).
  Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 44 to configure Time Settings and see page 45 to create a schedule.

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

Advanced Access Point Setup

Change your access point login password

Main > Password

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, and click on **Password**.

3. Under the **Admin Password** section, in the **Password** field, enter the new password and enter the password again in the **Verify Password** field to confirm.

3. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Note: If you change the access point login password, you will need to access the access point management page using the User Name "admin" and the new password.

Change your device name

Main > Password

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, and click on **Password**.

3. Under the **System Name** section, in the **Device Name** field, enter the new device name to display on your network to identify the access point.

3. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

IPv6 Connection Settings

Main > IPv6

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

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, and click on **IPv6**.

3. Select the IPv6 connection type used to assigned IPv6 addressing to the access point.

- Static IPv6
- Auto-configuration (SLAAC/DHCPv6)
- Link-Local Only

Change your access point IP address

Main > Network Settings

Typically, the access point IP address settings only needs to be changed when connecting the access point to your network and configuring to the device to be in the same IP network as your existing network.

Default Access Point IP Address Settings: 192.168.10.100 / 255.255.255.0

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, and click on **Network Settings**.

3. Under **Connection Type**, click the drop-down list to select the access point IP address settings.
   - **Dynamic IP (DHCP):** Choose the option to set the access point to automatically obtain IP address settings from a DHCP server
   Note: Typically, your network router has a built-in DHCP server.
   - **Static IP:** Choose this option to manually configure the IP address settings of the access point.
     o **IP Address:** Enter the new access point IP address. (e.g. *192.168.0.100*)
     o **Subnet Mask:** Enter the new access point subnet mask. (e.g. *255.255.255.0*)
     o **Gateway Address:** Enter the default gateway address of your network. This parameter is required for the access point to access Internet for functions such as e-mail notifications.
     Note: Typically, your network router IP address is used as the default gateway address to access the Internet e.g. 192.168.10.1)
     o **Primary/Secondary DNS Server:** Enter the primary and secondary DNS server addresses. This parameter is required for access point to resolve web addresses/domain names to IP address for functions such as e-mail notifications.
     Note: Typically, your network IP address is used as the DNS server address.

Connection Type

Choose the mode to be used by the Access Point

My Connection is	Dynamic IP (DHCP) ▾
	Static IP
	Dynamic IP (DHCP)

Static IP Address Connection Type

Enter the static address information.

IP Address	
Subnet Mask	
Gateway Address	
Primary DNS Server	
Secondary DNS Server	

4. To save changes, click **Save Settings**.

 Note: You will need to access your access point management page using your new access point IP address. (e.g. Instead of using the default http://192.168.10.100 your new access point IP address will use the following format using your new IP address http://(new.ipaddress.here) to access your access point management page. You can also use the default login URL http://tew-750dap

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings   Don't Save Settings

Set up the DHCP server on your access point

Main > Network Settings

Your access point 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 disabled by default on your access point. In most cases your network router has a built-in DHCP server that is typically enabled and used as your network DHCP server. If you already have a DHCP server on your network, leave this settings disabled.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, click on **Network Settings,** and click on the link **DHCP Server Settings.**

3. Review the DHCP Server settings. Click **Save Settings** to save settings.

- **Enable DHCP Server:** Enable or Disable the DHCP server.
- **DHCP IP Address Range:** Enter the starting IP address and ending IP address for the DHCP server range. (e.g.*192.168.10.20* to *192.168.10.30*)
  ***Note:** The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*
- **Default Subnet Mask**: Enter the subnet mask to automatically assign to computers or devices on your network. *(e.g. 255.255.255.0)*
- **Default Gateway:** Enter the default gateway IP address to automatically assign to computers or devices on your network. *(e.g. 192.168.10.1)*
- **Default WINS:** Enter the WINS server IP address to automatically assign to computers or devices on your network.
- **Default DNS:** Enter the DNS server IP address to automatically assign to computer or devices on your network. *(e.g. 192.168.10.1)*
- **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 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 Settings

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server	☐
DHCP IP Address Range	192.168.10.101 to 199
Default Subnet Mask	255.255.255.0
Default Gateway	
Default WINS	
Default DNS	
DHCP Lease Time	10080 (minutes)
Always Broadcast	☐ (Compatibility for some DHCP clients.)

You can also view the current DHCP clients in the **Number of Dynamic DHCP Clients** list.

Number of Dynamic DHCP Clients

Host Name	IP Address	MAC Address	Expired Time
	192.168.10.102	68:09:27:66:50:14	6 Days 23 Hours 46 Minutes

Add a DHCP reservation

Main > LAN

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your access point 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.

Note: *This function can only be used when the access point built-in DHCP server is used.*

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, click on **Network Settings,** and click on the link **DHCP Server Settings.**

3. Review the DHCP reservation settings.

- **Enable** – Enable or Disable the DHCP reservation.

- **Computer Name** – Enter a name of the device you will assign the DHCP reservation. **Note:** *You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.*

- **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
  Note: *You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.*

- **MAC Address** – Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC*)
  Note: *You can click Clone your PC's MAC Address to copy the current computer's MAC address into the MAC address field.*

Add DHCP Reservation

Enable	☐
Computer Name	[_____] [<<] [Computer Name ▾]
IP Address	[_____]
MAC Address	[_____]
Clone Your PC's MAC Address	[Clone Your PC's MAC Address]

Click **Add/Update** - Saves the reservation.
Note: Click Clear discards and erases the current information.

[Add / Update] [Clear]
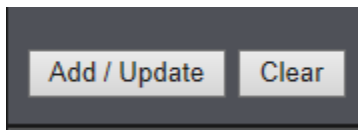
You will see the new reservation added to the DHCP Reservation List.

You can check the **Enable** option to enable the reservation or uncheck to disable.

You can click the 📝 icon to edit the reservation or 🗑 to delete the reservation.

DHCP Reservations List

Enable	Host Name	IP Address	MAC Address		
☑		192.168.10.101	d4:be:d9:03:7f:9f	📝	🗑

To save changes, click **Save Settings**.
*Note: If you would like to discard the changes, click **Don't Save Settings.***

[Save Settings] [Don't Save Settings]

Allow/deny multicast streaming

Access > Advanced Network

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Access**, and click on **Advanced Network**.

3. Next to **Enable IPv4 Multicast Streams**, check the option to enable or uncheck to disable.

Enable IPv4 Multicast Streams	☐

4. To save changes, click **Save Settings**.
*Note: If you would like to discard the changes, click **Don't Save Settings.***

[Save Settings] [Don't Save Settings]

Set your access point date and time

Main > Time

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Main**, and click on **Time**.

3. Review the Time settings. Click **Save Settings** to save settings.

- **Time:** Displays the current device time and date information.

Time	2000/01/01 01:23:11

- **Time Zone –** Click the drop-down list and select your time zone.

Time Zone	(GMT+08:00) Ulaan Bataar ▾

- **Enable Daylight Saving:** Check the option to enable daylight savings time and set the annual range when daylight saving is activated.

Enable Daylight Saving	■			
Daylight Saving Offset	+01:00 ▾			
Daylight Saving Dates		Month	Week	Day of Week	Time
	DST Start	Jan ▾	1st ▾	Sun ▾	12:00 AM ▾
	DST End	Jan ▾	1st ▾	Sun ▾	12:00 AM ▾

- **Automatically synchronize with Internet Time Server –** Check the **optionerver** option to set your access point date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to Default NTP server, (e.g. pool.ntp.org). Click the **Time Zone** drop-

down list to select the appropriate zone and you can optionally change your NTP Sync period.

> *Note: NTP servers are used for computers and other network devices to synchronize time across an entire network.*

Automatic Time and Date Configuration		
■ Automatically synchronize with Internet time server.		
NTP Server Used		Update Now

- **Manually set time –** Set your access point date and time manually in the Date and Time Settings section. **Note:** *Time is specified in 24-hour format. In addition, you can click Synchronize with Your Computer's Time Settings to copy the time and date settings from your computer.*

Set the Time and Date manually.					
Year	2013 ▾	Month	Jan ▾	Day	1 ▾
Hour	1 ▾	Minute	22 ▾	Second	54 ▾
Synchronize with Your Computer's Time Settings					

Create schedules

Tools > Schedules

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

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

- *Wireless (2.4GHz and 5GHz)*
- *Wireless Multiple SSID (2.4GHz and 5GHz)*
- *MAC Filters*

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Schedules**.

3. Review the Schedule settings. Click **Save Settings** to save settings.

- **Name:** Enter a name for the schedule you would like to apply.
- **Day(s)/Select Day(s):** Check **Select Day(s)** to select the days in the **Select Day(s)** section or select **All Week** to set the schedule for all days.
- **All Day – 24 Hours –** Check the option to set the schedule to 24 hours or define the schedule under **Start Time** and **End Time.**
- **Start/End Time:** Select the start and end time you would like the schedule to follow.
  Note: The schedule defined will define the time/day the feature will be activated.

10 -- Add Schedule Rule	
Name	
Day(s)	● All Week ○ Select Day(s)
Select Day(s)	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
All Day - 24 Hours	☐
Time Format	12-hour ▼
Start Time	12 : 0 AM ▼ (hour:minute)
End Time	11 : 59 PM ▼ (hour:minute)

Access Point Maintenance & Monitoring

Reset your Access Point to factory defaults

Tools > Restart

You may want to reset your access point to factory defaults if you are encountering difficulties with your access point and have attempted all other troubleshooting. Before you reset your access point to defaults, if possible, you should backup your access point configuration first, see "Backup and restore your access point configuration settings" on page 47.

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

- **Reset Button** – Located on the rear panel of your access point, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your access point management page.

  OR

- **Access Point Management Page**

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Restart**.

3. Next to **Restore to Factory Default Settings**, click **Restore to Factory Defaults**. When prompted to confirm this action, click **OK**.

Restore To Factory Default Settings	Restore Factory Defaults

Access Point Default Settings

Administrator User Name	admin
Administrator Password	admin
Access Point Default URL	http://tew-750dap
Access Point IP Address	192.168.10.100
Access Point Subnet Mask	255.255.255.0
Mode	Access Point
Wireless 2.4GHz & 5GHz	Enabled
Wireless 2.4GHz Network Name/Encryption	Please refer to sticker or device label
Wireless 2.4GHz & 5GHz Multiple SSID	Disabled

Backup and restore your access point configuration settings

Tools > Restart

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

To backup your access point configuration:

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Restart**.

3. Next to **Save Settings to Local Hard Drive** section, click **Save Configuration**.

Save Settings to Local Hard Drive	Save Configuration

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

To restore your access point configuration:

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Restart**.

3. Next to **Load Settings From Local Hard Drive,** depending on your web browser, click on **Browse** or **Choose File**.

Load Settings From Local Hard Drive		Browse...

4. A separate file navigation window should open.

5. Select the access point configuration file to restore and click **Import**. (Default Filename: *config.bin*). If prompted, click **Yes** or **OK**.

6. Wait for the access point to restore settings.

Reboot your access point

Tools > Restart

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

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

- **Turn the access point** off for 10 seconds using the access point On/Off switch located on the rear panel of your access point or disconnecting the power port, see "Product Hardware Features" on page 2.
  Use this method if you are encountering difficulties with accessing your access point management page. This is also known as a hard reboot or power cycle.
  OR
- **Access Point Management Page** – This is also known as a soft reboot or restart.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Restart**.

3. Next to **Reboot The Device**, click **Reboot the device**.

Reboot The Device	Reboot the Device

4. Wait for the device to reboot.

Upgrade your access point firmware

Tools > Firmware

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet access point 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 access point is currently running. To identify the firmware that is currently loaded on your access point, log in to the access point, click on the Administrator section and then on the Status. The firmware used by the access point 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.

1. If a firmware upgrade is available, download the firmware to your computer.

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

1. 1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Firmware**.

3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.

4. Navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.

5. Click **Upload**. If prompted, click **Yes** or **OK**.

Wireless Client List

Status > Wireless

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

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status**, and click on **Wireless.**

Number Of Wireless Clients - 2.4GHz Band : 1				
MAC Address	**IP Address**	**Mode**	**Rate (Mbps)**	**Signal (%)**
68:09:27:66:50:14	192.168.10.102	11n	65	100
Number Of Wireless Clients - 5GHz Band : 0				
MAC Address	**IP Address**	**Mode**	**Rate (Mbps)**	**Signal (%)**

.

- **MAC Address:** Displays the current MAC address of your wireless client.
- **IP Address:** Displays the current IP address of your wireless client.
- **Mode:** Displays the current mode your wireless client is connected (11a/b/g/n)
- **Rate:** Displays the current rate your wireless client has established.
- **Signal:** Displays the signal strength of your wireless client.

.

Check the access point system information

Status > Device Information

You may want to check the system information of your access point such as IP address settings, access point mode, wireless and wired network settings, access point wireless MAC addresses, and firmware version.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status** and click on **Device Information**.

System Information

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

General	
Time	2000/01/01 03:48:26
System Up Time	0 Day 3 Hour 48 Min 28 Sec
Firmware Version	1.00 Wed 15 May 2013

Ethernet Information

- **Connection Type:** Displays IP address connection type.
- **MAC Address:** Displays the current Ethernet wired interface MAC address.
- **IP Address** – The current IP address settings assigned to your access point.
- **Subnet Mask** - The current subnet mask assigned to your access point.
- **Default Gateway** – The current gateway assigned to your access point.
- **Primary/Secondary DNS (Domain Name System) Server** – The current DNS address(es) assigned to your access point.

Ethernet	
Connection Type	Static IP
MAC Address	d0:ae:ec:51:bf:f0
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

Wireless LAN - 2.4GHz

- **Wireless Radio:** Displays if the current status if the 2.4GHz radio is enabled or disabled.
- **MAC Address:** The MAC address of your access point's 2.4GHz wireless LAN or interface configuration.
- **Wireless Mode:** Displays the current device mode for the 2.4GHz radio.
- **802.11 Mode:** Displays the current 802.11 Mode of the 2.4GHz radio.
- **Channel Width**– Displays the current channel width configuration of the 2.4GHz radio.
- **Channel** – Displays the current 2.4GHz wireless channel your access point is operating.
- **Network Name (SSID):** Displays the current 2.4GHz wireless network name assigned to your access point.
- **Wi-Fi Protected Setup:** Displays the current 2.4GHz WPS status.
- **Security:** Displays the wireless security type applied to 2.4GHz primary SSID.
- **Multiple SSID(1/2/3)/Security Mode:** Displays the current wireless network names assigned and wireless security type assigned to each 2.4GHz multiple SSID.

Wireless LAN - 5GHz

- **Wireless Radio:** Displays if the current status if the 5GHz radio is enabled or disabled.
- **MAC Address:** The MAC address of your access point's 5GHz wireless LAN or interface configuration.
- **Wireless Mode:** Displays the current device mode for the 5GHz radio.
- **802.11 mode:** Displays the current 802.11 Mode of the 5GHz radio.
- **Channel Width**– Displays the current channel width configuration of the 5GHz radio.
- **Channel** – Displays the current 5GHz wireless channel your access point is operating.
- **Network Name (SSID):** Displays the current 5GHz wireless network name assigned to your access point.
- **Wi-Fi Protected Setup:** Displays the current 5GHz WPS status.
- **Security:** Displays the wireless security type applied to 5GHz primary SSID.
- **Multiple SSID(1/2/3)/Security Mode:** Displays the current wireless network names assigned and wireless security type assigned to each 5GHz multiple SSID.

Wireless LAN - 2.4GHz Band

Wireless Radio	Enabled
MAC Address	d0:ae:ec:51:bf:f0
Wireless Mode	Access Point
802.11 Mode	Mixed 802.11n, 802.11g and 802.11b
Channel Width	20MHz
Channel	6
Network Name (SSID)	TRENDnet750_2.4GHz_0020
Wi-Fi Protected Setup	Enabled/Configured
Security	WPA2-PSK
Multiple SSID1/Security Mode	TRENDnet750_2.4GHz_SSID1/WPA2-PSK
Multiple SSID2/Security Mode	TRENDnet750_2.4GHz_SSID2/WPA2-PSK
Multiple SSID3/Security Mode	TRENDnet750_2.4GHz_SSID3/WPA2-PSK

Wireless LAN - 5GHz Band

Wireless Radio	Enabled
MAC Address	d0:ae:ec:51:bf:f4
Wireless Mode	Access Point
802.11 Mode	Mixed 802.11n and 802.11a
Channel Width	20/40MHz
Channel	36
Network Name (SSID)	TRENDnet750_5GHz_0020
Wi-Fi Protected Setup	Enabled/Configured
Security	WPA2-PSK
Multiple SSID1/Security Mode	TRENDnet750_5GHz_SSID1/WPA2-PSK
Multiple SSID2/Security Mode	TRENDnet750_5GHz_SSID2/WPA2-PSK
Multiple SSID3/Security Mode	TRENDnet750_5GHz_SSID3/WPA2-PSK

IPv6 Status

Status > IPv6

You can view the current IPv6 status on your access point.

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status**, and click on **IPv6 Status**
   - **IPv6 Connection Type:** Displays the IPv6 connection type assigned to your access point.
   - **LAN IPv6 Address:** Displays the IPv6 IP address assigned to your access point.
   - **IPv6 Default Gateway:** Displays the IPv6 default gateway assigned to your access point.
   - **LAN IPv6 Link-Local Address:** Displays the link-local address of the access point.
   - **Primary/Secondary IPv6 DNS Server:** Displays the IPv6 DNS server addresses assigned to your access point.

IPv6 Connection Information	
IPv6 Connection Type	Link-local Only
LAN IPv6 Address	none
IPv6 Default Gateway	none
LAN IPv6 Link-Local Address	fe80::d2ae:ecff:fe51:bff0/64
Primary IPv6 DNS Server	none
Secondary IPv6 DNS Server	none

View your access point log

Status > Log

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

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status**, and click on **Log**.

- **Time** – Displays the time of the log entry. If the time is inaccurate, make sure to set the access point date and time correctly. (See "Set your access point date and time" on page 44)
- **Message** – Displays the log message.

Time	Message
Sat Jan 1 06:38:38 2000	DHCP: Server sending ACK to 192.168.10.102. (Lease time = 604800)
Sat Jan 1 06:38:38 2000	DHCP: Server receive REQUEST from 68:09:27:66:50:14.

Access Point Log Navigation

- **First Page** – Displays the first page of the log.
- **Last Page** – Displays the last page of the log.
- **Previous –** Display the log page previous to the current.
- **Next** – Displays the log page next to the current.
- **Clear**   - Clears all logging

First Page	Last Page	Previous	Next	Clear

1/13

Configure your access point log

Status > Log

You may want to only see specific categories of logging for troubleshooting purposes.

Set the types or categories to include in logging

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status** and click on **Log**.

3. Next to Log **Level**, select the category to view in logging.

Log Type & Level	
Log Type	◉ System
Log Level	● Critical ◉ Warning ◉ Information

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings	Don't Save Settings

Save your access point log

You may want send your access point log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to save the access point logging to a local text file for troubleshooting purposes.

Save access point logs to your hard drive

Status > Log

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Status** and click on **Log.**

3. Next **Save Log File to Local Hard Drive**, click **Save.** (Default Filename: log.txt)

Note: Browse for a location on your local hard drive to save the log file.

Save Log File

Save Log File To Local Hard Drive. Save

Send access point logs to your e-mail address

Tools > Email Settings

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Email Settings.**

3. Review the e-mail log settings.
- **Enable Email Notification –** Check the option to enable email log notification.
- **From Email Address** – Enter a sender e-mail address. (e.g. *access point@trendnet.com*)
  Note: *This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.*
- **To Email Address** – Enter your e-mail address.
- **Email Subject** – Enter the subject for your email.
- **SMTP Server Address** – Enter the IP address (e.g. *10.10.10.10*) or domain name (e.g. *mail.trendnet.com*) of your e-mail server.
- **SMTP Server Port** – Enter the port used by your e-mail service. (e.g. *Default SMTP Server Port: 25*)
- **Enable Authentication** – Check this option if your e-mail service requires authentication. If not, leave this settings disabled (unchecked)
  Note: If you are unsure of this setting check with your e-mail service provider if authentication is required.
- **Account Name**– Enter your account user name for your e-mail service.
- **Password** – Enter your password for your e-mail service.
- **Send Mail Now** – Click this option to send an e-mail with the current access point log using your email settings.
- **Email Logs When Fulll –** The access point log will be e-mailed to your e-mail address when access point internal log is full.

Email Notification	
Enable Email Notification	☐

Email Settings	
From Email Address	
To Email Address	
Email Subject	
SMTP Server Address	
SMTP Server Port	25
Enable Authentication	☐
Account Name	
Password	
Verify Password	Send Mail Now

Email Log When Full	
Enable Log When Full :	☐

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings   **Don't Save Settings**

Send access point logs to an external log server

Tools > Syslog

1. Log into your access point management page (see "Access your access point management page" on page 11).

2. Click on **Tools** and click on **Syslog.**

3. Next to **Enable Logging to Syslog Server**, check the option to enable Syslog. Enter the IP address of the local syslog server to forward the logs.

*Note: You can also click the **Computer Name** drop-down list and select from the DHCP server list. Click **<<** to copy the IP address information to the **Syslog Server IP Address** field. This feature can only be used if using the access point's built-in DHCP server.*

Syslog Settings	
Enable Logging to SysLog Server	☑
Syslog Server IP Address	<< Computer Name ∨

4. To save changes, click **Save Settings**.

*Note: If you would like to discard the changes, click **Don't Save Settings.***

Save Settings   **Don't Save Settings**

Access Point Mode Management Page Structure

Main

- Wizard
- Device Mode
    - Access Point
    - AP Repeater
    - Client Bridge
- Network Settings
    - IP Address Settings
    - Optional DHCP Server Settings
- Password
    - Device Name
- Time
- IPv6

Wireless

- Basic
    - 2.4GHz Settings & Security
    - 5GHz Settings & Security
    - WDS
- Advanced
- WPS (Wi-Fi Protected Setup)

Status

- Device Information
- Log
- Statistic
- Wireless
- IPv6

Access

- MAC Filters
- Advanced Network
    - UPnP
    - Multicast Streaming

Tools

- Restart
    - Backup Configuration
    - Restore Configuration
    - Restore to Factory Defaults
    - Reboot Device
- Firmware
    - Upgrade Firmware
- Ping Test
- Email Settings
- Syslog
- Schedules

AP Repeater/Client Bridge Mode Management Page Structure

Main

- Wizard
- Device Mode
    - o Access Point
    - o AP Repeater
    - o Client Bridge
- Network Settings
    - o IP Address Settings
    - o Optional DHCP Server Settings
- Password
    - o Device Name
- Time
- IPv6

Wireless

- Site Survey

Status

- Device Information
- Log
- Statistic
- Link Status
- IPv6

Tools

- Restart
    - o Backup Configuration
    - o Restore Configuration
    - o Restore to Factory Defaults
    - o Reboot Device
- Firmware
    - o Upgrade Firmware
- Ping Test
- Email Settings
- Syslog
- Schedules

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), Wireless: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.11a
Internet Protocol	IPv4 and IPv6
Ports	4 x 10/100 Mbps Ethernet (Auto-MDIX)
WPS Button	Wi-Fi Protected Setup (WPS) connects with other WPS compliant devices
Reset Button	Reset unit back to factory default (press and hold for 10 seconds)
Network Protocols / Features	Static IP, DHCP Server/Client, NTP, IPv6
Management / Monitoring	Local / remote configuration, upgrade firmware, backup / restore configuration via web browser, internal system log (Categories: System, Access Point Status: Critical, Warning, Information), syslog, email log, wireless client list
Supported Web Browser	Internet Explorer 8.0 or above, Firefox, Chrome, Opera, Safari
LED Indicator	Power, Ethernet 1-4, Wireless (2.4GHz/5GHz), WPS
Power Adapter	Input: 100 ~ 240 V, 50~60 Hz, 0.4 A Output: 12 V DC, 1 A external power adapter
Power Consumption	10.1 watts (max.)
Dimension (L x W x H)	45 x 118 x 164 mm (1.8 x 4.6 x 6.5 in.)
Weight	238 g (8.4 oz)
Temperature	Operation: 0° ~ 40°C (32°F ~ 104°F) Storage: -20° ~ 65°C (-4°F ~ 149°F)
Humidity	Max. 95% (non-condensing)

Certifications	CE, FCC
Wireless	
Frequency	2.4 GHz: 2.412~2.462 (FCC) and 2.412~2.483 (ETSI) 5 GHz: 5.15 ~ 5.35 / 5.725~5.825 GHz (FCC) and 5.15 ~ 5.35 / 5.47 ~ 5.725 (ETSI)
Modes	Access Point (AP), AP+WDS, WDS only, Repeater, Client Bridge
Antenna	2.4 GHz: 2 x 1.5 dBi PIFA internal 5 GHz: 2 x 4 dBi PIFA internal
Modulation	CCK, DQPSK, DBPSK, OFDM, BPSK, QPSK, 16/64-QAM
Data Rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps (for both 2.4 & 5 GHz)
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
SSIDs	4 SSIDs per band
WDS	Up to 4 WDS bridge connections per band
Output Power	802.11a: 18 dBm (typical) 802.11b: 18 dBm (typical) 802.11g: 18 dBm (typical) 802.11n: 15 dBm (typical) (for 2.4 & 5GHz)
Receiving Sensitivity	802.11a: -65 dBm (typical) @ 54 Mbps 802.11b: -76 dBm (typical) @ 11 Mpbs 802.11g: -65 dBm (typical) @ 54 Mbps 802.11n: -61 dBm (typical) @ 300 Mbps (for 2.4 & 5 GHz)
Channels	2.4 GHz: 1~11 (FCC), 1~13 (ETSI) 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161, 165 (FCC) 36, 40, 44, 48 (ETSI)

*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.

Troubleshooting

Q: I typed http://tew-750dap in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the access point management page?
Answer:
Assign your computer a static IP address in the subnet of 192.168.10.x (ex. 192.168.10.25) and access the access point using the default IP address 192.168.10.100.
http://192.168.10.100

Q: I typed http://192.168.10.100 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the access point management page?
Answer:
1. Check your hardware settings again. See "Basic Installation" on page 8.
2. Make sure the LAN port you are connected to is on.
3. Make sure your network adapter TCP/IP settings are set to *Obtain an IP address automatically* or *DHCP* (see the steps below).
4. Make sure your computer is connected to one of the access point's LAN ports
5. Press on the factory reset button for 15 seconds, the release.
Windows 7

      a. Go into the **Control Panel**, click **Network and Sharing Center**.

      b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

      c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

      d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

      a. Go into the **Control Panel**, click **Network and Internet**.
      b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
      c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
      d. Then click **Obtain an IP address automatically** and click **OK**.
Windows XP/2000

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

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

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

Q: I cannot connect wirelessly to the access point. What should I do?
Answer:
1. Double check that the Wireless LED on the access point is on.
2. Power cycle the router. Unplug the power to the access point. Wait 15 seconds, then plug the power back in to the access point.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The default predefined SSID is printed on the device label on the bottom or on the sticker on the side of the unit.
4. To verify whether or not wireless is enabled, login to the access point management page, click on *Basic and Wireless*.
5. Please see "Steps to improve wireless connectivity" on page 18 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.

2. In the dialog box, type *cmd* to bring up the command prompt.

3. In the command prompt, type *ipconfig /all* to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.

2. Double-click on **Terminal** to launch the command prompt.

3. In the command prompt, type *ipconfig getifaddr <en0 or en1>* to display the wired or wireless IP address settings.

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

Graphical Method

MAC OS 10.6/10.5
1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4
1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

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

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

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

Windows 7/8
   a. Go into the **Control Panel**, click **Network and Sharing Center**.
   b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
   c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
   d. Then click **Obtain an IP address automatically** and click **OK**.

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

Windows XP/2000
   a. Go into the **Control Panel**, double-click the **Network Connections** icon
   b. Right-click the **Local Area Connection** icon and the click **Properties**.
   c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
   d. Then click **Obtain an IP address automatically** and click **OK**.

MAC OS 10.4/10.5/10.6
   a. From the **Apple**, drop-down list, select **System Preferences**.
   b. Click the **Network** icon.
   c. From the **Location** drop-down list, select **Automatic**.
   d. Select and view your Ethernet connection.
       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**.

e. Configure TCP/IP to use DHCP.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

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

How to configure your network settings to use a static IP address?

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

Windows 7/8

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.

b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.

c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.

c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.
b. Click the **Network** icon.
c. From the **Location** drop-down list, select **Automatic**.
d. Select and view your Ethernet connection.

How to find your MAC address?

In Windows 2000/XP/Vista/7/8,

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

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**

2. From the **Show** menu, select **Built-in Ethernet**.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**

2. Select **Ethernet** from the list on the left.

3. Click the **Advanced** button.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

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

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

Windows 7/8

1. Open Connect to a Network by clicking the network icon (or) in the notification area.

2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**. and then click **Connect To.**

2. In the **Show** list, click **Wireless**.

3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.

2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.

3. You may be prompted to enter a security key in order to connect to the network.

4. Enter in the security key corresponding to the wireless network, and click **Connect**.

Federal Communication Commission Interference Statement

This 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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

FCC Radiation Exposure Statement:

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

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 50385 : 2002
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
EN 300 328 V1.7.1 : (2006-10) 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 V2.1.1 : (2009-05)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems
**EN 301 893 V1.6.1 : (2011-11)**
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.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-750DAP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.			Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-TEW-750DAP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.		**nl** Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-750DAP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-750DAP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.		**mt** Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-750DAP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-750DAP vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.		**hu** Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-750DAP megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb elõírásainak.
en English	Hereby, TRENDnet, declares that this TEW-750DAP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.		**pl** Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-750DAP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-750DAP 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.		**pt** Português [Portuguese]	TRENDnet declara que este TEW-750DAP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑTRENDnet ΔΗΛΩΝΕΙ ΟΤΙ TEW-750DAP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ, 2006/95/ΕΚ, 2009/125/ΕΚ και.		**sl** Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-750DAP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES in 2009/125/ES.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-750DAP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.		**sk** Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TEW-750DAP spíňazákladnépožiadavky a všetkypríslušnéustanoveniaSmernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
it Italiano[Italian]	Con la presente TRENDnet dichiara che questo TEW-750DAP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.		**fi** Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-750DAP tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
lv Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-750DAP atbilstDirektīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.		**sv** Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-750DAP 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.
lt Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-750DAP atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB			

Limited Warranty

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

TEW-750DDAP – 3 Years Warranty

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

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

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

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

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

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

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

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

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

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

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

PWP05202009v2   2013/09/10

TRENDNET®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA