TRENDnet®

User's Guide

TEW-653AP

1.02

Table of Content

Introduction

TEW-653AP is a powerful and multi-functioned 11n Access Point and it can act three modes AP/WDS/Universal Repeater. Smoke detector appearance will minimize visibility. So this model can work properly at Hotel or public area.

TEW-653AP is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11g devices. Product's RF performance is finely tuned so it will bring best wireless signal for each client. TEW-653AP supports home network with superior throughput, performance and unparalleled wireless range. To protect data during wireless transmissions, TEW-653AP encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2. Its MAC address filter allows users to select stations with access to connect network. TEW-653AP thus is the best product to ensure network quality for hotspots.

Features and Benefits

- Wi-Fi compliant with IEEE 802.11n and IEEE 802.11b/g standards
- Power device by an Ethernet cable using standard IEEE802.3af Power over Ethernet (PoE) protocol
- Functional Access Point, WDS and Universal Repeater modes provide network flexibility
- Advance wireless security with 64/128-bit WEP, WPA/WPA2 Radius and WPA-PSK/WPA2-PSK
- Supports multiple SSID (up to 4 SSIDs) with 802.1q VLAN tagging (AP mode)
- High-speed up to 300Mbps data rate using 802.11n connection
- Monitor bandwidth allocation through graphical interface
- Support Wi-Fi Protected Setup (WPS) for easy configuration
- 802.1x Authentication protocol support
- Support for Wireless Multimedia (WMM) QoS
- Easy web management via web browser
- Remote network management and SNMP support (v1, v2c)
- 3-year limited warranty

Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. 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.
3. 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.
4. 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.
5. 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.
6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

Package Contents

The package contains the following items. In case of return, please keep the original box set, and the complete box set must be included for full refund.

- TEW-653AP
- 12V/1A 100V~240V Power Adapter
- Quick Installation
- CD-Rom (User's Guide)
- Mounting Kit

System Requirement

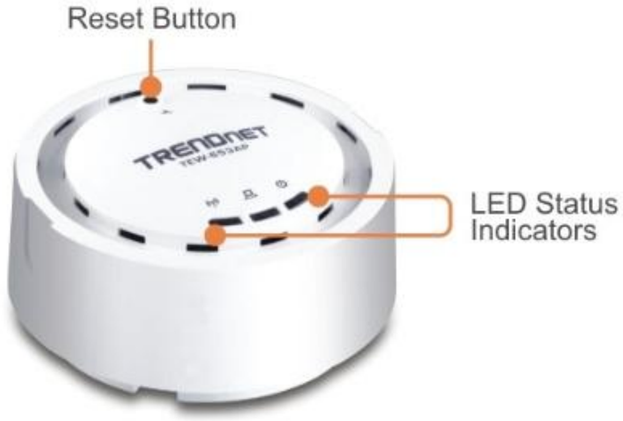
The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

Hardware Installation

Front Panel

The image below shows the front panel of the TEW-653AP



Reset Button: This button will reset the TEW-653AP to its factory default settings. To do this, press and hold the Reset button for 10seconds.

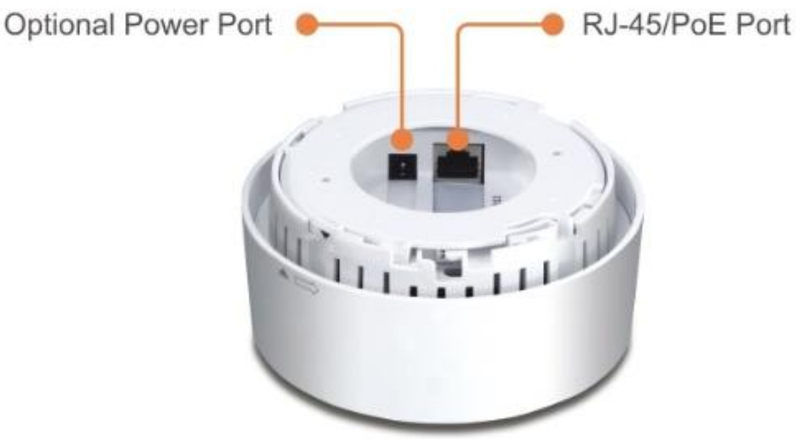
Power LED: On - Power on
Off - No Power

LAN LED: On - The LAN port is active
Off- No active connection on the LAN port.
Flashing – Data is being transmitted or received on the LAN port

WLAN LED: Flashing – Data is being transmitted or received through the wireless access point

Rear Panel

The image below shows the rear panel of the TEW-653AP



Power Port: Connect the supplied power adapter here, power port is not required when using PoE port.

RJ-45/PoE Port: Plug standard LAN cables (RJ45 connectors) to connect into a network or to a PoE powering device.

1 Place the unit in an appropriate place after conducting a site survey.
2 Plug one end of the Ethernet cable into the RJ-45 port on the rear panel of the device and another end into your PC/Notebook.
3 Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

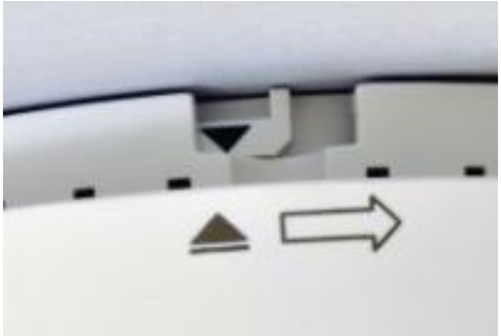
Mounting Installation

1 Use the mounting plate as a template and mark the wall or ceiling for the correct screw position

2 Drill holes for the screws at the marked positions.

3 Align the TEW-653AP with the mounting plate

4 Follow the arrow to secure the TEW-653AP to the mounting plate



Modes

You are allowed to configure TEW-653AP into different modes: AP, WDS Bridge and Repeater.

AP/WDS/Universal Repeater

Access Point

In AP (Access Point) mode, your device acts as a communication hub for users with a wireless device to connect to a wired LAN/WAN.

WDS Bridge

⚠ You can only connect to the device via Ethernet Port

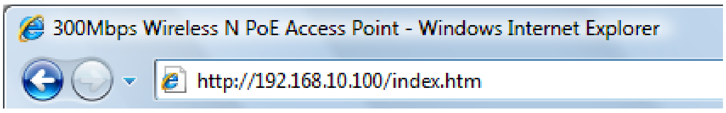
WDS (Wireless Distribution System) allows AP to communicate with one another wirelessly. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks.

Repeater

Repeater is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances and through areas with high levels of electromagnetic interference (EMI). Repeater (AP) mode on one radio channel is usually configured along with Universal (STA) mode on AP channel.

Using the Web Browser

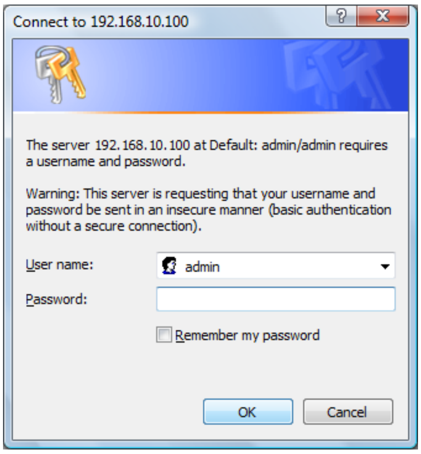
1. Open Internet Explorer 5.0 or above Internet browser.
2. Enter IP address ***http://192.168.10.100*** (the factory-default IP address setting) to the URL web address location.



300Mbps Wireless N PoE Access Point - Windows Internet Explorer

http://192.168.10.100/index.htm

3. When the following dialog box appears, enter the user name and password to login to the main configuration window, the default username and password is "***admin***".



Connect to 192.168.10.100

The server 192.168.10.100 at Default: admin/admin requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

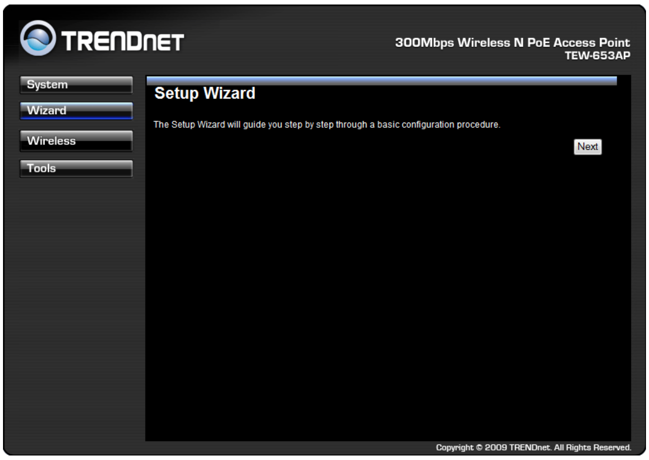
User name: admin

Password:

□ Remember my password

Setup Wizard

Setup wizard is provided as part of the web configuration utility. User can simply follow the step-by-step process to get the wireless Access Point configuration ready to run in these easy steps by clicking on` the “Wizard” button on the function menu. The following screen will appear. Please click “Next” to continue.

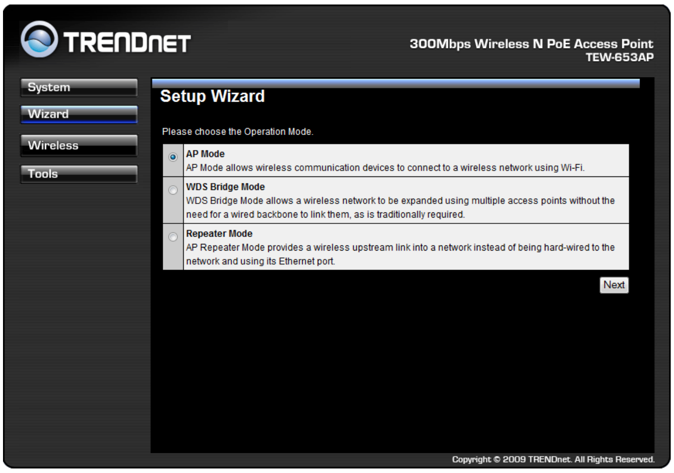


TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
Tools
Next
Copyright © 2009 TRENDnet. All Rights Reserved.

Setup Wizard

The Setup Wizard will guide you step by step through a basic configuration procedure.

Step 1: Set the Operation Mode of the Access Point by selecting AP Mode, WDS Bridge Mode or Repeater Mode. Please click “Next” to continue.



TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
Tools
Next
Copyright © 2009 TRENDnet. All Rights Reserved.

Setup Wizard

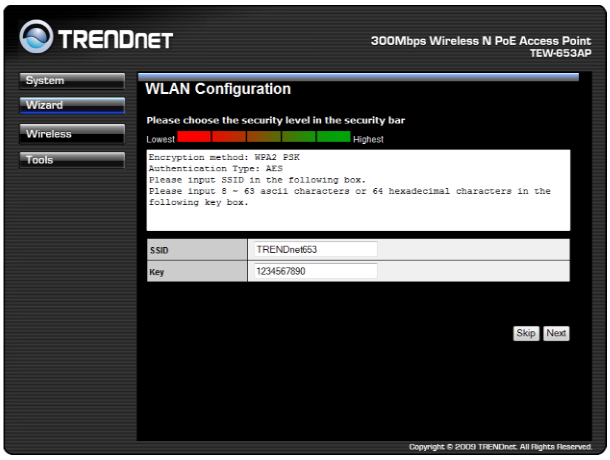
Please choose the Operation Mode.

● **AP Mode**
AP Mode allows wireless communication devices to connect to a wireless network using Wi-Fi.

○ **WDS Bridge Mode**
WDS Bridge Mode allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required.

○ **Repeater Mode**
AP Repeater Mode provides a wireless upstream link into a network instead of being hard-wired to the network and using its Ethernet port.

Step 2: Select the level of security you would like to apply on the Access Point between Lowest to Highest. You can type in your personal settings by entering in the SSID and KEY information. Please click “Next” to continue.



TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
Tools
Lowest
Highest
Skip
Next
Copyright © 2009 TRENDnet. All Rights Reserved.

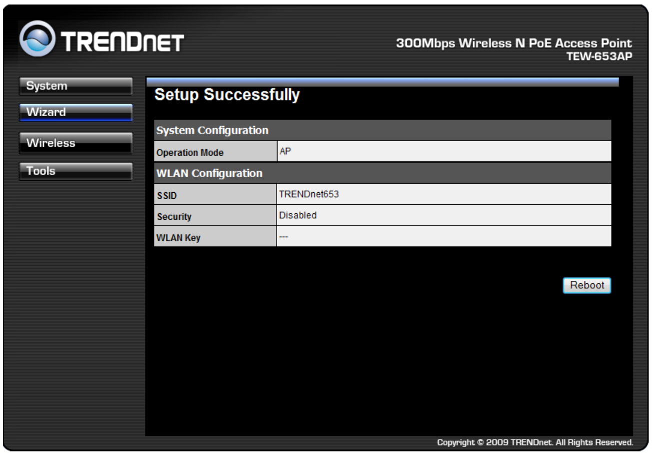
WLAN Configuration

Please choose the security level in the security bar

```
Encryption method: WPA2 PSK
Authentication Type: AES
Please input SSID in the following box.
Please input 8 ~ 63 ascii characters or 64 hexadecimal characters in the
following key box.
```

SSID	TRENDnet653
Key	1234567890

Step 3: Your settings will appear and click Reboot to apply settings.


TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
Tools
Reboot
Copyright © 2009 TRENDnet. All Rights Reserved.

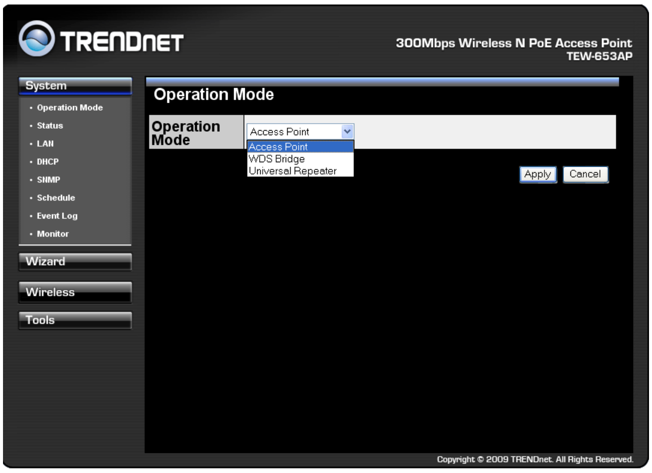
Setup Successfully

System Configuration	
Operation Mode	AP
WLAN Configuration	
SSID	TRENDnet653
Security	Disabled
WLAN Key	---

System

Operation Mode

This window allows you to configure the TEW-653AP into different operating modes: AP, WDS Bridge and Repeater.

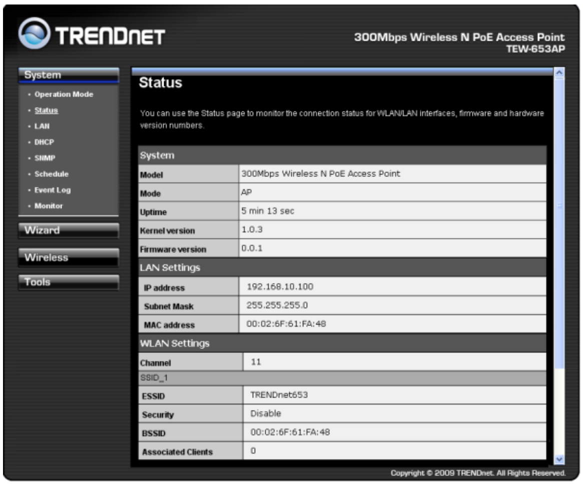


Operation Mode

Operation Mode: Access Point

Status

This selection displays the current applied settings of the Access Point.



Status

You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.

System	
Model	300Mbps Wireless N PoE Access Point
Mode	AP
Uptime	5 min 13 sec
Kernel version	1.0.3
Firmware version	0.0.1
LAN Settings	
IP address	192.168.10.100
Subnet Mask	255.255.255.0
MAC address	00:02:6F:61:FA:48
WLAN Settings	
Channel	11
SSID_1	
ESSID	TRENDnet653
Security	Disable
BSSID	00:02:6F:61:FA:48
Associated Clients	0

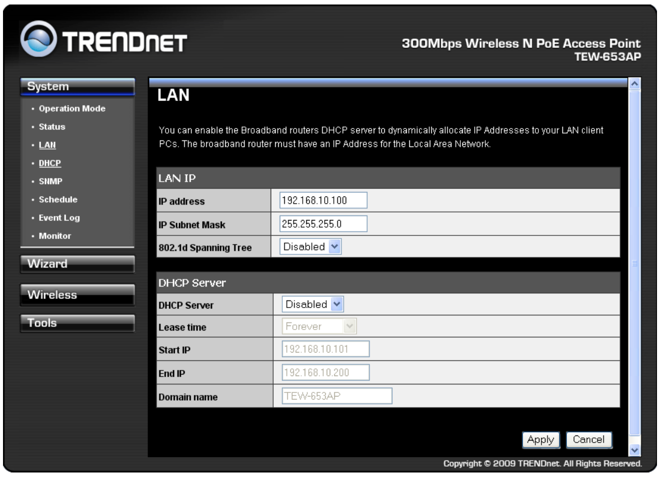
System: Basic information of the device.

WLAN Settings: WLAN channel.

SSID_1: SSID information.

LAN

This screen allows users to configure the LAN settings of the access point and to configure the DHCP settings.



LAN

You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP	
IP address	192.168.10.100
IP Subnet Mask	255.255.255.0
802.1d Spanning Tree	Disabled

DHCP Server	
DHCP Server	Disabled
Lease time	Forever
Start IP	192.168.10.101
End IP	192.168.10.200
Domain name	TEW-653AP

Bridge Type: Select Static IP or Dynamic IP from the drop-down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server.

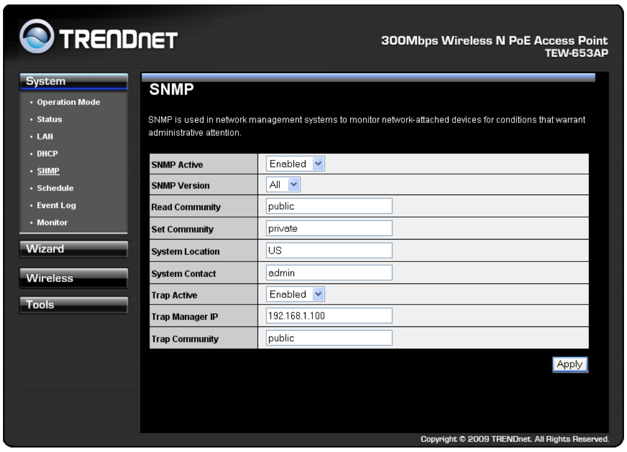
IP Address: Specify an IP address.

IP Subnet Mask: Specify a subnet mask for the IP address.

802.1d Spanning Tree: Select Enable or Disable from the drop-down list. Enabling spanning tree will avoid redundant data loops.

SNMP

Allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.



SNMP

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP Active	Enabled
SNMP Version	All
Read Community	public
Set Community	private
System Location	US
System Contact	admin
Trap Active	Enabled
Trap Manager IP	192.168.1.100
Trap Community	public

SNMP Active: Choose to enable or disable the SNMP feature.

SNMP Version: You may select a specific version or select All from the drop-down list.

Read Community Name: Specify the password for access the SNMP community for read only access.

Set Community Name: Specify the password for access to the SNMP community with read/write access.

System Location: Specify the location of the device.

System Contact: Specify the contact details of the device.

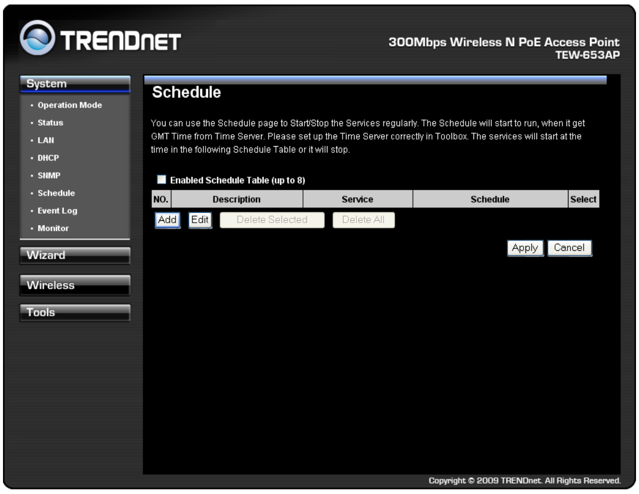
Trap Active: Choose to enable or disable the SNMP trapping feature. .

Trap Manager IP: Specify the password for the SNMP trap community.

Trap Community: Specify the name of SNMP trap community.

Schedule

This screen allows users to set schedules on the access point and also to schedule the time for Power Saving Mode.



Schedule

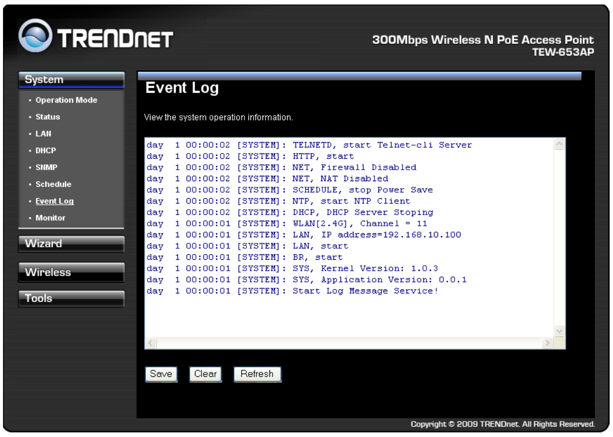
You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

□ Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select

Event Log

This screen allows users to view a running log of the access point system statistics, events and activities.



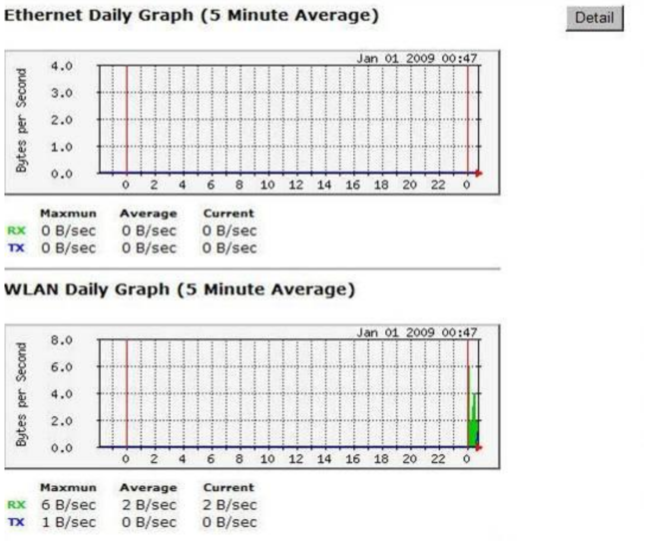
Event Log

View the system operation information.

```
day  1 00:00:02 [SYSTEM]: TELNETD, start Telnet-cli Server
day  1 00:00:02 [SYSTEM]: HTTP, start
day  1 00:00:02 [SYSTEM]: NET, Firewall Disabled
day  1 00:00:02 [SYSTEM]: NET, NAT Disabled
day  1 00:00:02 [SYSTEM]: SCHEDULE, stop Power Save
day  1 00:00:02 [SYSTEM]: NTP, start NTP Client
day  1 00:00:02 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:00:01 [SYSTEM]: WLAN[2.4G], Channel = 11
day  1 00:00:01 [SYSTEM]: LAN, IP address=192.168.10.100
day  1 00:00:01 [SYSTEM]: LAN, start
day  1 00:00:01 [SYSTEM]: BR, start
day  1 00:00:01 [SYSTEM]: SYS, Kernel Version: 1.0.3
day  1 00:00:01 [SYSTEM]: SYS, Application Version: 0.0.1
day  1 00:00:01 [SYSTEM]: Start Log Message Service!
```

Monitor

This screen provides users to view a graphical diagram of the data rates running through the access point.



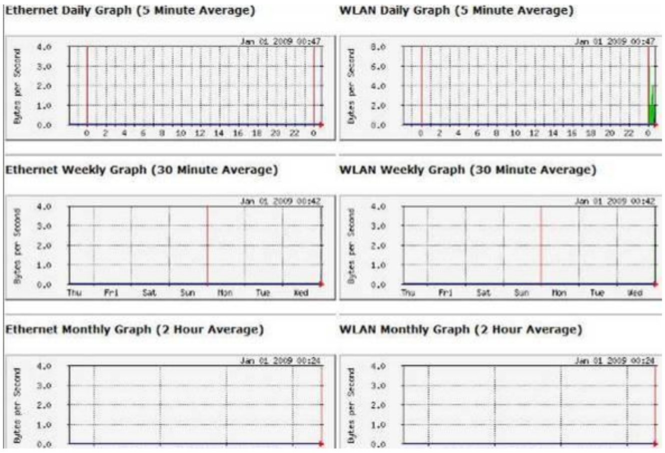
Ethernet Daily Graph (5 Minute Average)

	Maxmun	Average	Current
RX	0 B/sec	0 B/sec	0 B/sec
TX	0 B/sec	0 B/sec	0 B/sec

WLAN Daily Graph (5 Minute Average)

	Maxmun	Average	Current
RX	6 B/sec	2 B/sec	2 B/sec
TX	1 B/sec	0 B/sec	0 B/sec

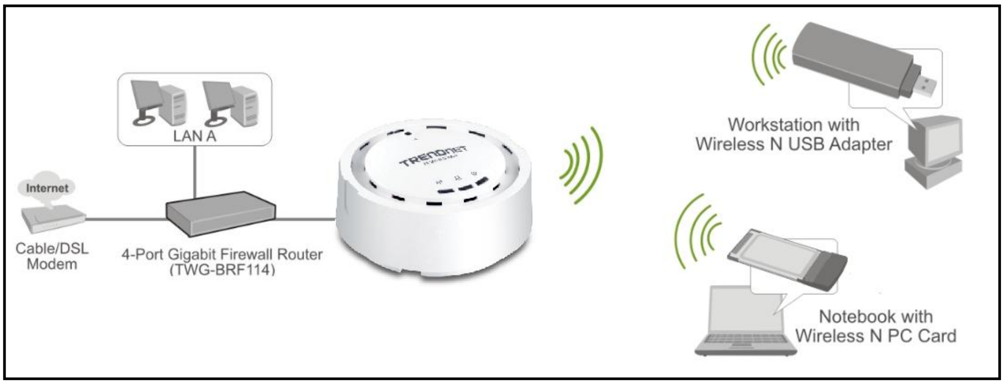
Detail: Displays a historical record of the access point's data rates.



Ethernet Daily Graph (5 Minute Average)
WLAN Daily Graph (5 Minute Average)
Jan 01 2009 00:47
Bytes per Second
4.0
3.0
2.0
1.0
0.0
8.0
6.0
4.0
2.0
0.0
0 2 4 6 8 10 12 14 16 18 20 22 0
Ethernet Weekly Graph (30 Minute Average)
WLAN Weekly Graph (30 Minute Average)
Jan 01 2009 00:42
Thu Fri Sat Sun Mon Tue Wed
Ethernet Monthly Graph (2 Hour Average)
WLAN Monthly Graph (2 Hour Average)
Jan 01 2009 00:24

Wireless Access Point Mode

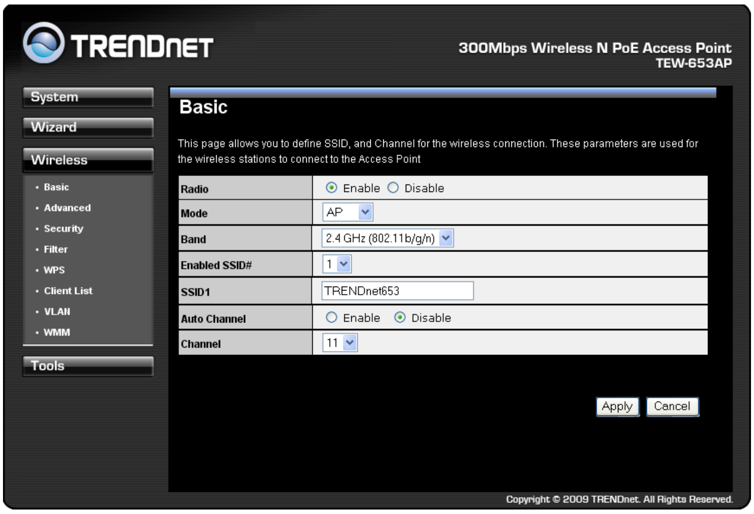
The wireless section is used to configure the wireless settings for your Access Point. Note that changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network.



LAN A
Internet
Cable/DSL Modem
4-Port Gigabit Firewall Router (TWG-BRF114)
TRENDnet
Workstation with Wireless N USB Adapter
Notebook with Wireless N PC Card

Basic

When Access point is selected this screen allows users configure the wireless settings of the access point.



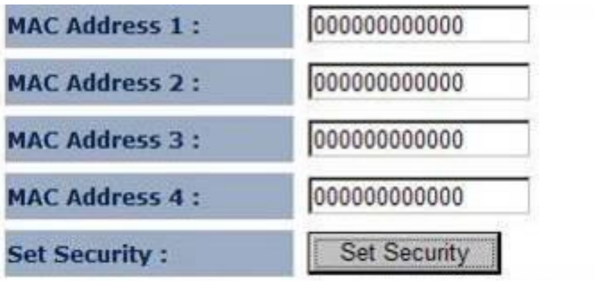
Basic

This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point

Radio	● Enable ○ Disable
Mode	AP
Band	2.4 GHz (802.11b/g/n)
Enabled SSID#	1
SSID1	TRENDnet653
Auto Channel	○ Enable ● Disable
Channel	11

Radio: To enable/disable wireless signal.

Mode: Select AP or WDS mode. When WDS is selected the access point becomes a AP+ WDS mode allowing the access point to interlink with other AP devices through WDS connection, while maintaining the AP feature to be enabled.



MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000
MAC Address 4 :	000000000000
Set Security :	Set Security

Band: Configure the device into different wireless modes.

- 2.4 GHz (B)
- 2.4 GHz (N)
- 2.4 GHz (B+G)
- 2.4 GHz (G)
- 2.4 GHz (B+G+N)

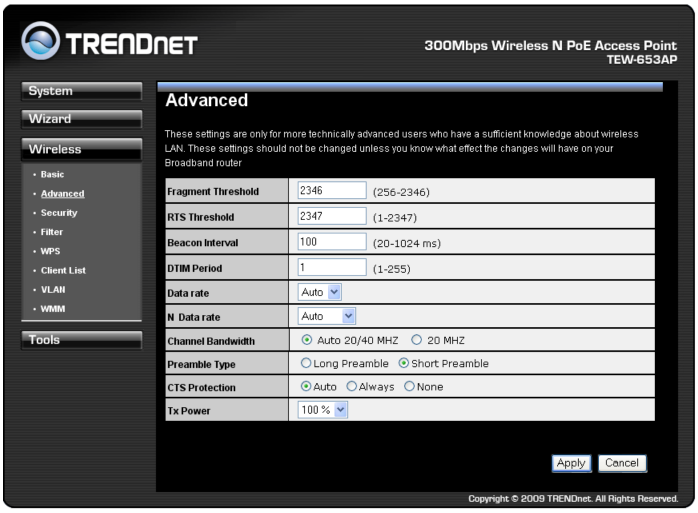
Enabled SSID#: The device allows you to add up to 4 unique SSID

ESSID#: Description of each configured SSID

MAC Address 1~4: When WDS is selected enter the MAC address of the access points you would like to establish a WDS connection with.

Advanced

This screen allows users to configure advance settings of the access point.



Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router

Fragment Threshold	2346 (256-2346)
RTS Threshold	2347 (1-2347)
Beacon Interval	100 (20-1024 ms)
DTIM Period	1 (1-255)
Data rate	Auto
N Data rate	Auto
Channel Bandwidth	● Auto 20/40 MHZ ○ 20 MHZ
Preamble Type	○ Long Preamble ● Short Preamble
CTS Protection	● Auto ○ Always ○ None
Tx Power	100 %

Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 24 and 1024. The default value is set to 100 milliseconds.

DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

Data rate: You may select a data rate from the drop-down list, however, it is recommended to select auto. This is also known as auto-fallback.

N Data Rate: You may select N data rate from the drop-down list, however, it is recommended to select auto.

Channel Bandwidth: Select channel bandwidth.

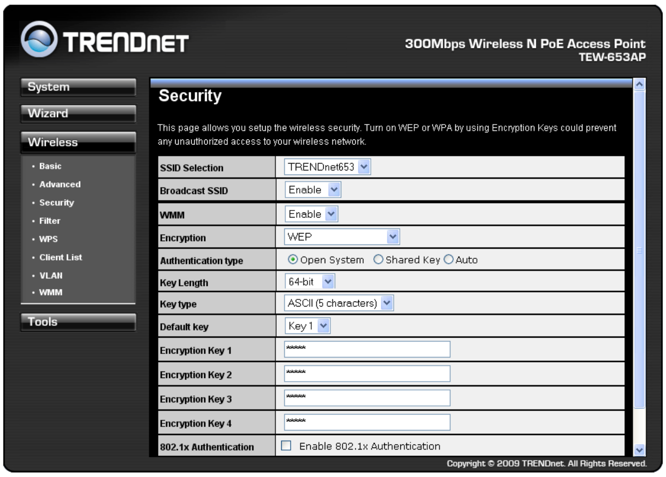
Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a ‘clear’ signal before transmitting. It is recommended to select auto.

Security

This screen allows users to configure the wireless security settings of the access point. Enabling security prevents any unauthorized wireless clients to connect into your network.

Encryption: WEP



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection	TRENDnet653
Broadcast SSID	Enable
WMM	Enable
Encryption	WEP
Authentication type	● Open System ○ Shared Key ○ Auto
Key Length	64-bit
Key type	ASCII (5 characters)
Default key	Key 1
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****
802.1x Authentication	□ Enable 802.1x Authentication

Copyright © 2009 TRENDnet. All Rights Reserved.

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to Enable or Disable WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in WMM under the Wireless drop-down menu.

Encryption: Select WEP from the drop-down list.

Authentication Type: Select Open System, Shared Key, or auto. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

Key Length: Select a 64-bit or 128-bit WEP key length from the drop-down list.

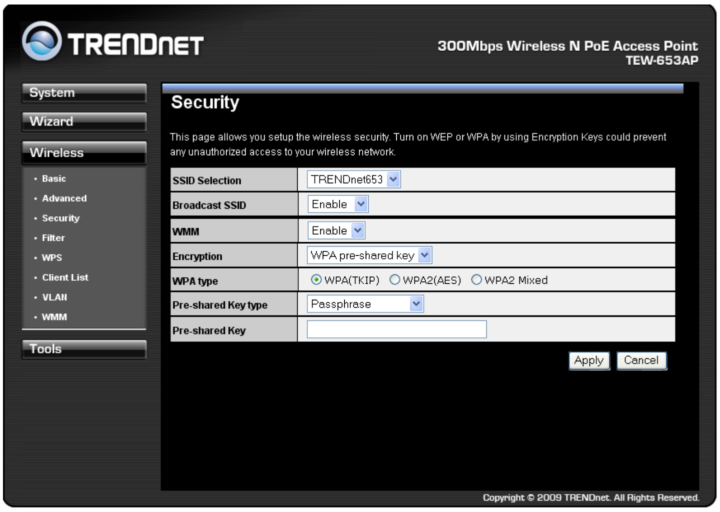
Key Type: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

Default Key: You may choose one of your 4 different WEP keys from below.

Encryption Key 1-4: You may enter four different WEP keys.

Enable 802.1x Authentication: Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

Encryption: WPA pre-shared key



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection	TRENDnet653
Broadcast SSID	Enable
WMM	Enable
Encryption	WPA pre-shared key
WPA type	● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
Pre-shared Key type	Passphrase
Pre-shared Key	

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to Enable or Disable WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in WMM under the Wireless drop-down menu.

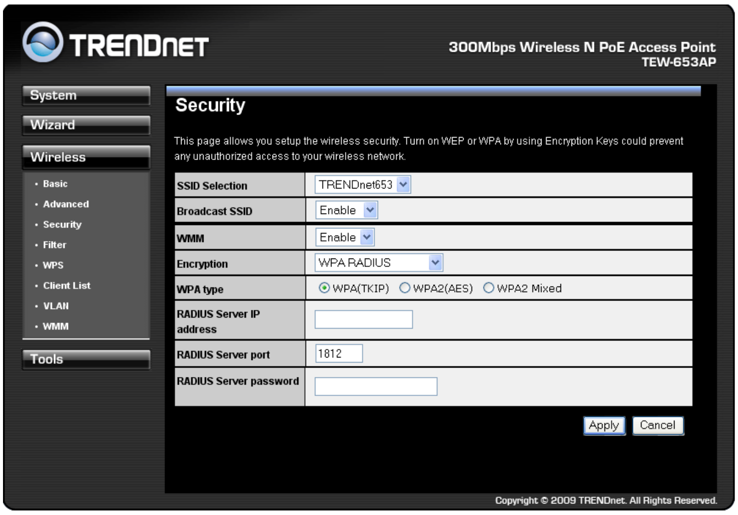
Encryption: Select WPA pre-shared key from the drop-down list.

WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

Pre-shared Key Type: The Key Type can be passphrase or Hex format.

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Encryption: WPA RADIUS



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection	TRENDnet653
Broadcast SSID	Enable
WMM	Enable
Encryption	WPA RADIUS
WPA type	● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
RADIUS Server IP address	
RADIUS Server port	1812
RADIUS Server password	

Copyright © 2009 TRENDnet. All Rights Reserved.

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to Enable or Disable WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in WMM under the Wireless drop-down menu.

Encryption: Select WPA RADIUS from the drop-down list.

WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

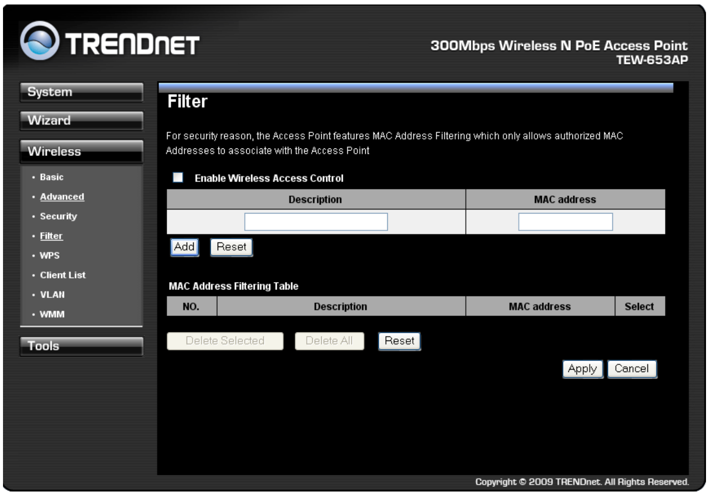
RADIUS Server IP Address: Specify the IP address of the RADIUS server.

RADIUS Server Port: Specify the port number of the RADIUS server, the default port is 1812.

RADIUS Server Password: Specify the pass-phrase that is matched on the RADIUS Server.

Filter

The filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter, up to 32 entries. It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacture of the network adapter.



Filter

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point

□ Enable Wireless Access Control

Description	MAC address

Add Reset

MAC Address Filtering Table

NO.	Description	MAC address	Select

Delete Selected Delete All Reset

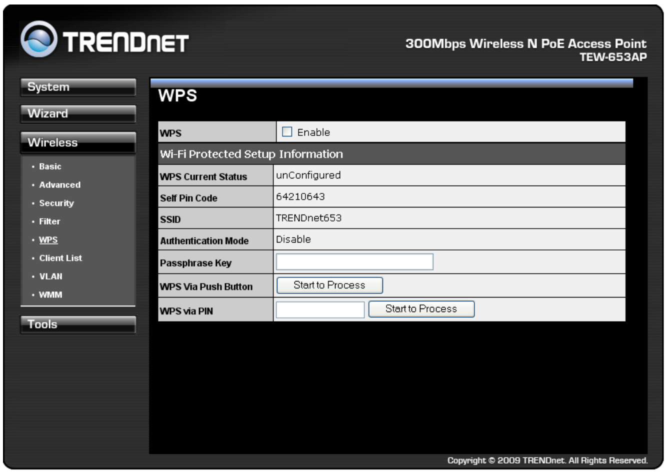
Apply Cancel

Enable Wireless Access Control: Check box to enable feature
Description: Enter the name of the device
MAC address: Enter the device’s MAC address
ADD: Click to add MAC address into table
Reset: Click to reset entry
Delete Selected: Allows you to delete selected entry
Delete All: Deletes all entries in the MAC address table
Reset: Reset all entries
Apply: Click to apply changes made
Cancel: Click to cancel any new setting changes made.

WPS

WPS is the simplest way to establish a connection between the wireless clients and the wireless router. You don’t have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the ‘Start to Process’ button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.



WPS

WPS	☐ Enable
Wi-Fi Protected Setup Information	
WPS Current Status	unConfigured
Self Pin Code	64210643
SSID	TRENDnet653
Authentication Mode	Disable
Passphrase Key	
WPS Via Push Button	Start to Process
WPS via PIN	Start to Process

WPS: Place a check in this box to enable this feature.

WPS Current Status: Displays the current status of the WPS configuration.

Self Pin Code: Displays the current PIN.

SSID: Displays the current SSID.

Authentication Mode: Displays the current authentication mode.

Passphrase Key: Displays the current passphrase.

Interface: Displays the current interface.

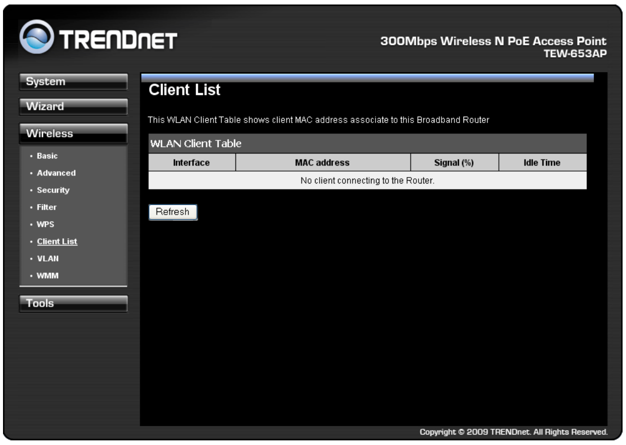
WPS Via Push Button: Click on the **Start to Process** button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click on the **OK** button in the dialog box.

WPS via PIN: Specify a PIN, which unique number that can be used to add the router to an existing network or to create a new network. Then click on the **Start to Process** button.

Apply: Click on the button to save the changes.

Client List

This screen displays all wireless client's currently connected to the access point.



Client List

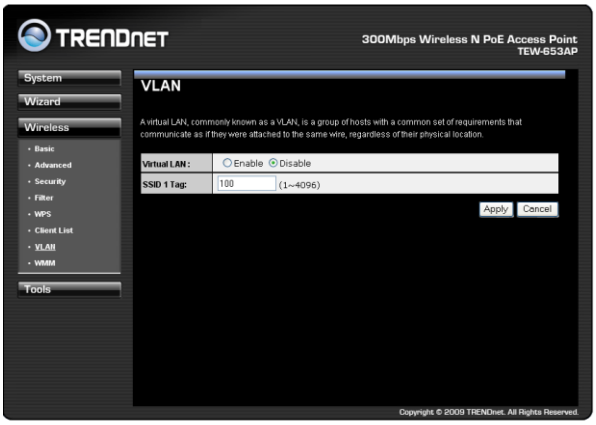
This WLAN Client Table shows client MAC address associate to this Broadband Router

WLAN Client Table

Interface	MAC address	Signal (%)	Idle Time
No client connecting to the Router.			

VLAN

This feature is only available under AP mode and allows users to configure the VLAN settings of the access point.



VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

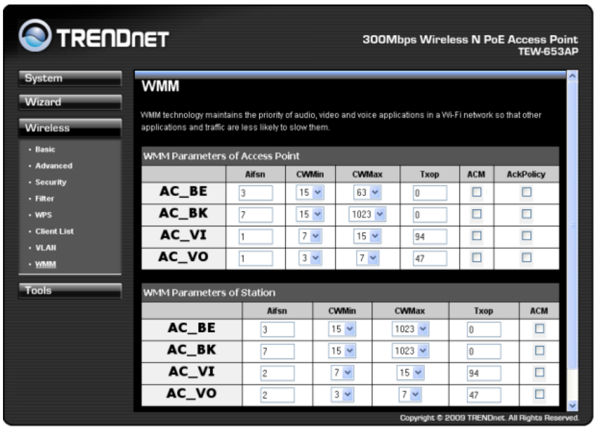
Virtual LAN :	○ Enable ● Disable
SSID 1 Tag:	100 (1~4096)

Virtual LAN: Choose to Enable or Disable the VLAN features.

SSID1 Tag: Specify the VLAN tag.

WMM

This screen allows users to configure the WMM (Wireless Multi-Media) settings of the access point under AP mode.



WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point

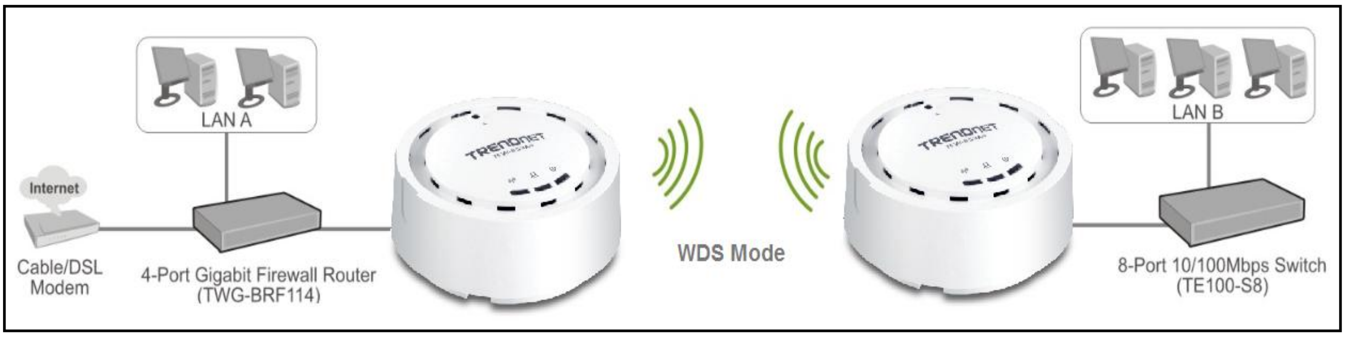
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

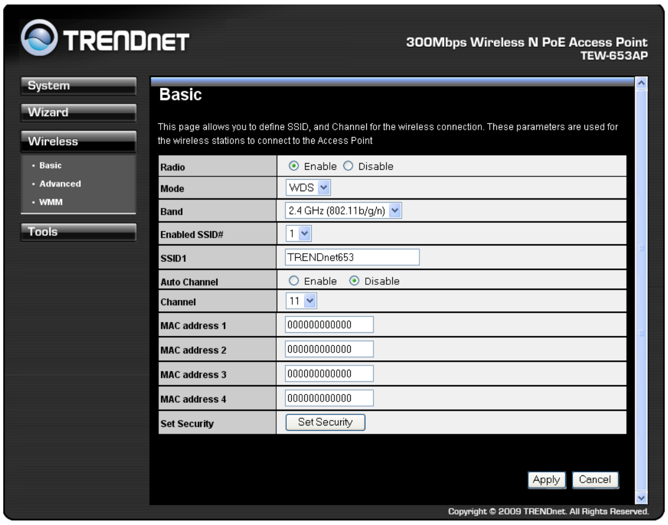
Wireless WDS Bridge Mode

When WDS mode is selected, the access point functions as a wireless bridge and is able to wirelessly communicate with other access points via WDS links. A WDS link is bidirectional; both end points must support WDS and each access point must know the MAC Address of the other. Each access point will be configured with the remote access point's MAC address and vice versa. Make sure all access points are configured with the same SSID, channel and wireless encryption settings.



Basic

When WDS (Wireless Distribution System) is selected this screen allows users configure the wireless settings of the device.


TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
• Basic
• Advanced
• WMM
Tools
Apply
Cancel
Copyright © 2009 TRENDnet. All Rights Reserved.

Basic

This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point

Radio	● Enable ○ Disable
Mode	WDS
Band	2.4 GHz (802.11b/g/n)
Enabled SSID#	1
SSID1	TRENDnet653
Auto Channel	○ Enable ● Disable
Channel	11
MAC address 1	000000000000
MAC address 2	000000000000
MAC address 3	000000000000
MAC address 4	000000000000
Set Security	Set Security

Radio: To enable/disable radio frequency.

Mode: WDS mode allows you to interlink with other AP devices. Setting MAC address and encryption algorithm

Band: Configure the device into different wireless modes.

2.4 GHz (B)

2.4 GHz (N)

2.4 GHz (B+G)

2.4 GHz (G)

2.4 GHz (B+G+N)

Enabled SSID#: The device allows you to add up to 4 unique SSID

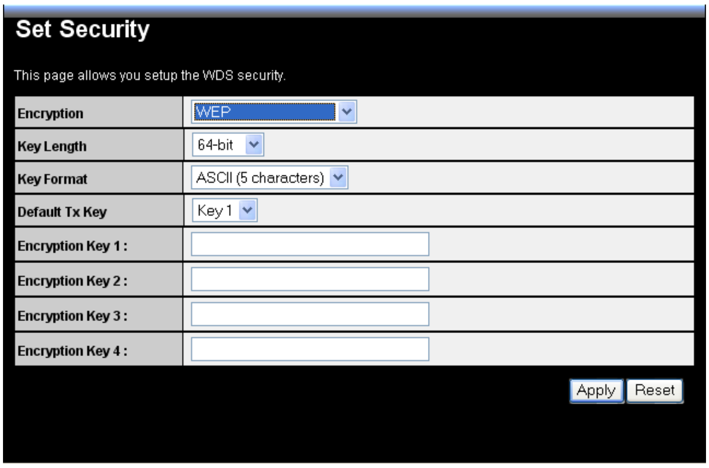
ESSID#: Description of each configured SSID

Channel: You can manually configure a channel to be used.

MAC Address 1~4: To specify MAC address of other AP devices.

⚠ MAC address will only show when configured in WDS AP mode.

Security: WEP



Set Security

This page allows you setup the WDS security.

Encryption	WEP
Key Length	64-bit
Key Format	ASCII (5 characters)
Default Tx Key	Key 1
Encryption Key 1 :	
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

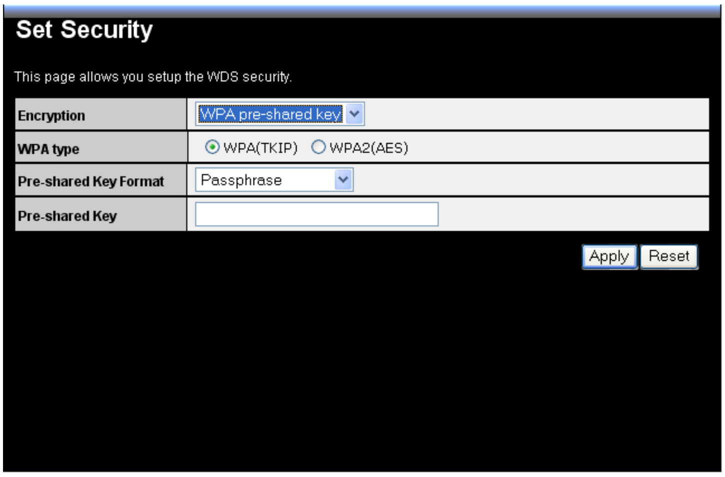
Key Length: Select a 64-bit or 128-bit WEP key length from the drop-down list.

Key Format: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

Default Tx Key: You may choose one of your 4 different WEP keys from below.

Encryption Key 1-4: You may enter four different WEP keys.

Security: WPA pre-shared key



Set Security

This page allows you setup the WDS security.

Encryption	WPA pre-shared key
WPA type	● WPA(TKIP) ○ WPA2(AES)
Pre-shared Key Format	Passphrase
Pre-shared Key	

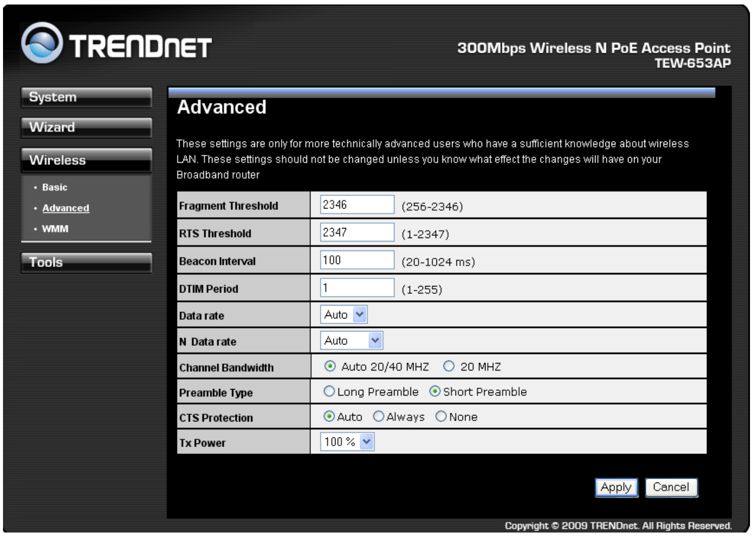
WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

Pre-shared Key Type: The Key Type can be passphrase or Hex format.

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Advanced

This screen allows users to configure the advance wireless settings of the devicein WDS mode.


TRENDnet
300Mbps Wireless N PoE Access Point
TEW-653AP
System
Wizard
Wireless
Basic
Advanced
WMM
Tools
Apply
Cancel
Copyright © 2009 TRENDnet. All Rights Reserved.

Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router

Fragment Threshold	2346 (256-2346)
RTS Threshold	2347 (1-2347)
Beacon Interval	100 (20-1024 ms)
DTIM Period	1 (1-255)
Data rate	Auto
N Data rate	Auto
Channel Bandwidth	● Auto 20/40 MHZ ○ 20 MHZ
Preamble Type	○ Long Preamble ● Short Preamble
CTS Protection	● Auto ○ Always ○ None
Tx Power	100 %

Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

Data rate: You may select a data rate from the drop-down list, however, it is recommended to select auto. This is also known as auto-fallback.

N Data Rate: You may select N data rate from the drop-down list, however, it is recommended to select auto.

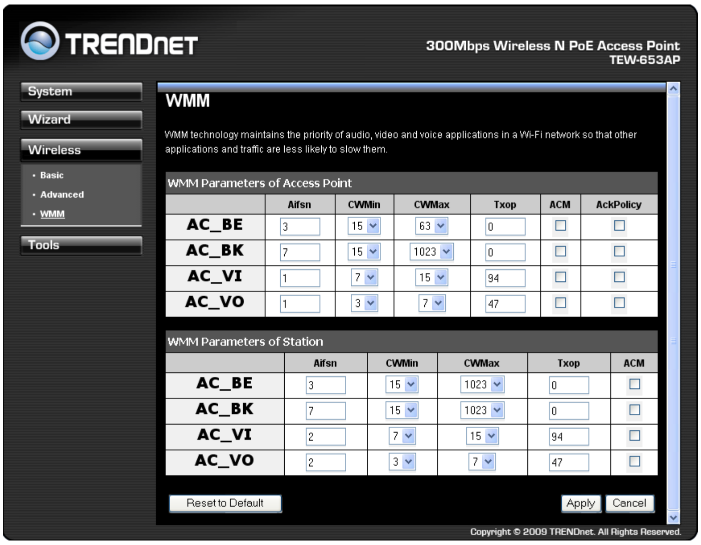
Channel Bandwidth: Select channel bandwidth.

Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select auto.

WMM

This screen allows users to configure the WMM (Wi-Fi Multi-Media) settings of the access point in WDS mode.



WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point

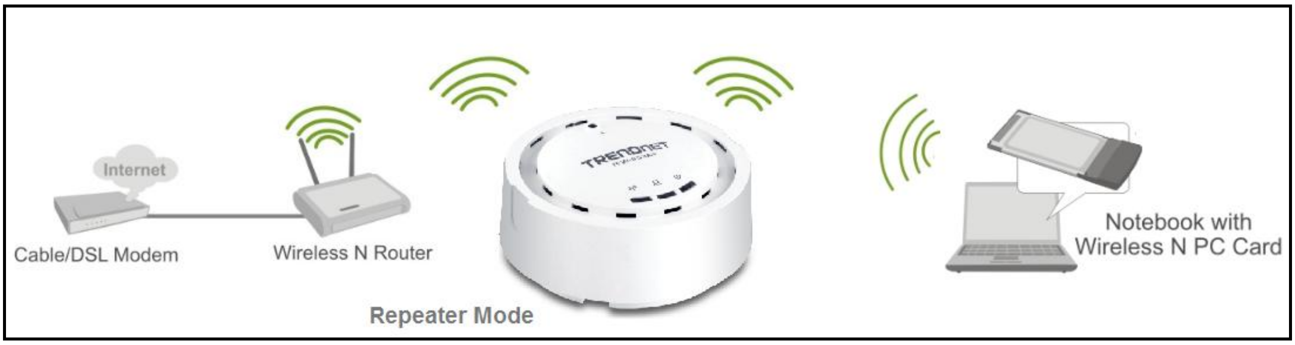
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

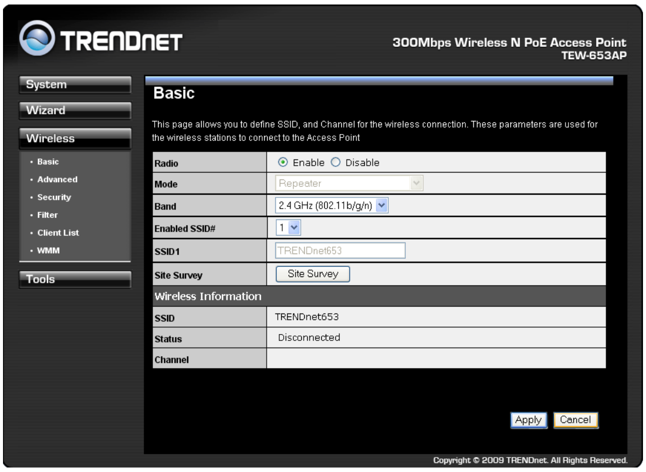
Repeater Mode

When Repeater Mode is selected, the access point functions as a wireless repeater and is able to repeat the wireless signal of an access point. This feature is used to expand your existing wireless network on places your current access point is unable to reach. Make sure all the settings of the TEW-653.AP matches your wireless access points wireless settings same SSID, channel and wireless encryption settings.



Wireless Basic

When Repeater mode is selected the following screen allows user’s to configure the wireless settings of the access point.



Basic

This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point

Radio	● Enable ○ Disable
Mode	Repeater
Band	2.4 GHz (802.11b/g/n)
Enabled SSID#	1
SSID1	TRENDnet653
Site Survey	Site Survey
Wireless Information	
SSID	TRENDnet653
Status	Disconnected
Channel	

Copyright © 2009 TRENDnet. All Rights Reserved.

Radio: To enable/disable radio frequency.

Mode: Universal Repeater

Band: Configure the device into different wireless modes.

2.4 GHz (B)

2.4 GHz (N)

2.4 GHz (B+G)

2.4 GHz (G)

2.4 GHz (B+G+N)

Enabled SSID#: The device allows you to add up to 4 unique SSID

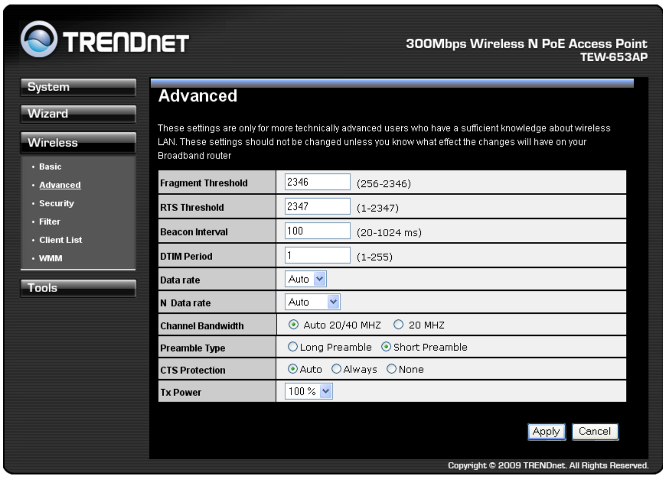
ESSID#: Description of each configured SSID

Channel: You can manually configure a channel to be used.

Site Survey: List out all connected devices.

Advanced

This screen allows users to configure the advance wireless settings of the access point in Repeater mode.



Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router

Fragment Threshold	2346 (256-2346)
RTS Threshold	2347 (1-2347)
Beacon Interval	100 (20-1024 ms)
DTIM Period	1 (1-255)
Data rate	Auto
N Data rate	Auto
Channel Bandwidth	● Auto 20/40 MHZ ○ 20 MHZ
Preamble Type	○ Long Preamble ● Short Preamble
CTS Protection	● Auto ○ Always ○ None
Tx Power	100 %

Copyright © 2009 TRENDnet. All Rights Reserved.

Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.

RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

Beacon Interval: Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.

DTIM Period: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.

Data rate: You may select a data rate from the drop-down list, however, it is recommended to select auto. This is also known as auto-fallback.

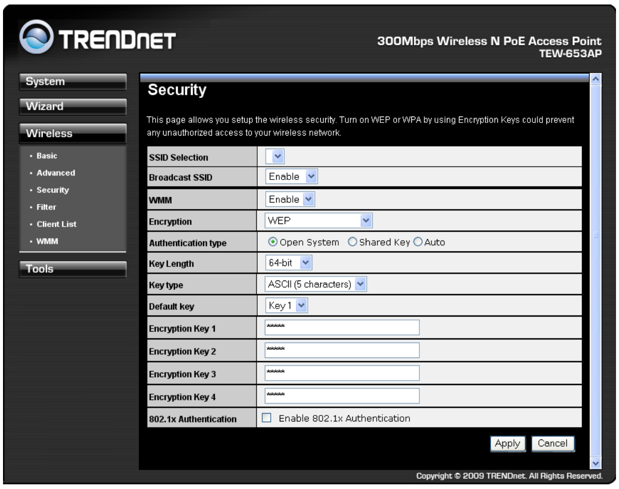
Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.

CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select auto.

Repeater Mode Security

This screen allows users to configure the wireless security settings of the access point in Repeater mode.

WEP



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection	
Broadcast SSID	Enable
WMM	Enable
Encryption	WEP
Authentication type	● Open System ○ Shared Key ○ Auto
Key Length	64-bit
Key type	ASCII (5 characters)
Default key	Key 1
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****
802.1x Authentication	□ Enable 802.1x Authentication

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to Enable or Disable WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in WMM under the Wireless drop-down menu.

Encryption: Select WEP from the drop-down list.

Authentication Type: Select Open System, Shared Key, or auto. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

Key Length: Select a 64-bit or 128-bit WEP key length from the drop-down list.

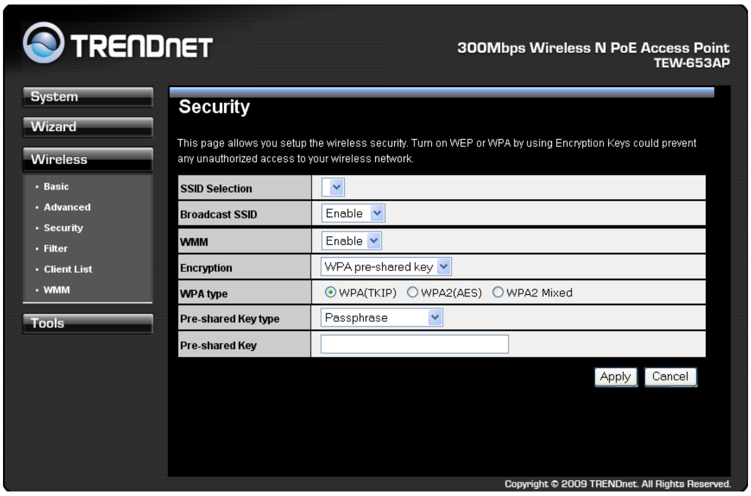
Key Type: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

Default Key: You may choose one of your 4 different WEP keys from below.

Encryption Key 1-4: You may enter four different WEP keys.

Enable 802.1x Authentication: Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

WPA pre-shared key



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection	
Broadcast SSID	Enable
WMM	Enable
Encryption	WPA pre-shared key
WPA type	● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
Pre-shared Key type	Passphrase
Pre-shared Key	

ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.

Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

WMM: Choose to Enable or Disable WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in WMM under the Wireless drop-down menu.

Encryption: Select WPA pre-shared key from the drop-down list.

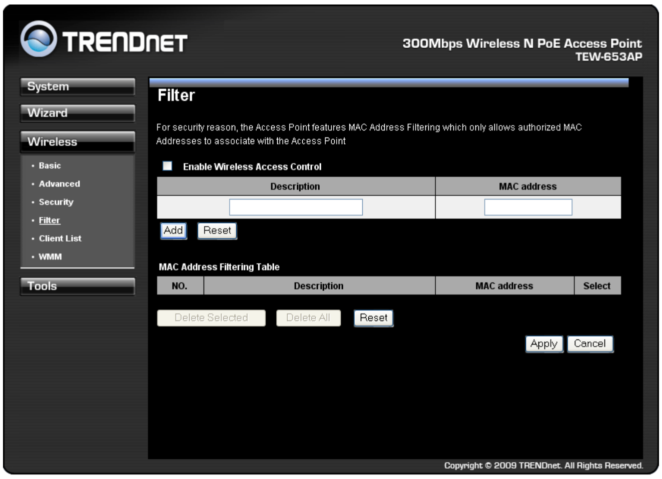
WPA Type: Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

Pre-shared Key Type: The Key Type can be passphrase or Hex format.

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Filter

The filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter, up to 32 entries. It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacture of the network adapter.



Filter

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point

□ Enable Wireless Access Control

Description	MAC address

MAC Address Filtering Table

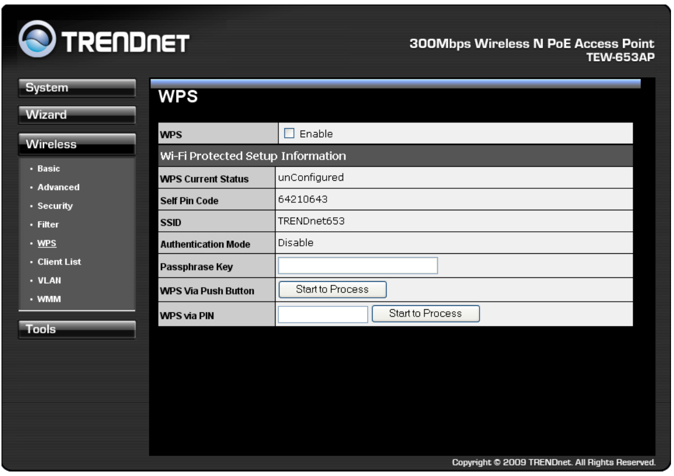
NO.	Description	MAC address	Select

Copyright © 2009 TRENDnet. All Rights Reserved.

WPS

WPS is the simplest way to establish a connection between the wireless clients and the wireless router. You don’t have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the ‘Start to Process’ button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.



WPS

WPS	□ Enable
Wi-Fi Protected Setup Information	
WPS Current Status	unConfigured
Self Pin Code	64210643
SSID	TRENDnet653
Authentication Mode	Disable
Passphrase Key	
WPS Via Push Button	Start to Process
WPS via PIN	Start to Process

WPS: Place a check in this box to enable this feature.

WPS Current Status: Displays the current status of the WPS configuration.

Self Pin Code: Displays the current PIN.

SSID: Displays the current SSID.

Authentication Mode: Displays the current authentication mode.

Passphrase Key: Displays the current passphrase.

Interface: Displays the current interface.

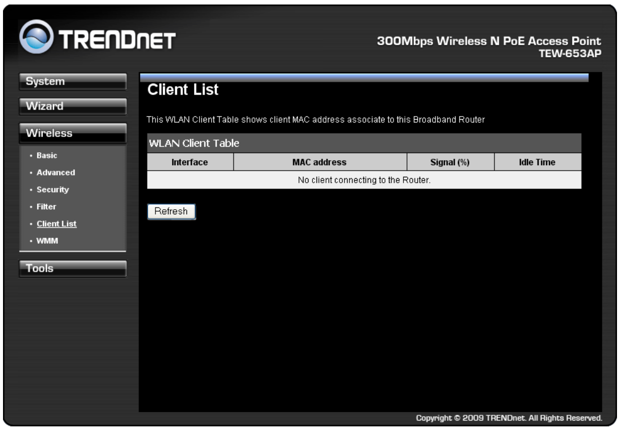
WPS Via Push Button: Click on the **Start to Process** button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click on the **OK** button in the dialog box.

WPS via PIN: Specify a PIN, which unique number that can be used to add the router to an existing network or to create a new network. Then click on the **Start to Process** button.

Click on the **Apply** button to save the changes.

Client List

This screen allows users to view a list of connected clients.



Client List

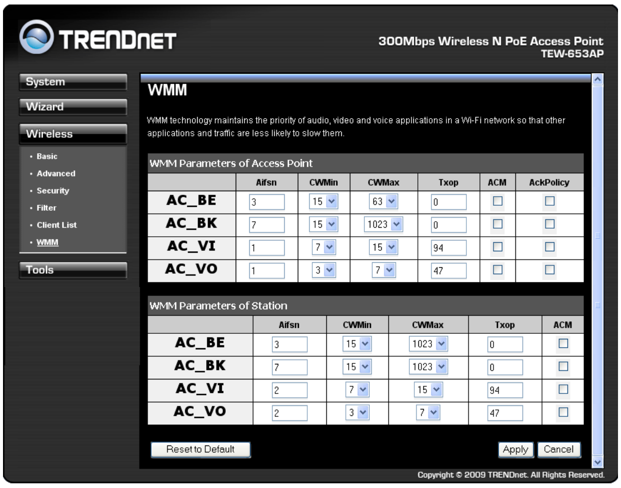
This WLAN Client Table shows client MAC address associate to this Broadband Router

WLAN Client Table

Interface	MAC address	Signal (%)	Idle Time
No client connecting to the Router.			

WMM

This screen allows users to configure the WMM (Wi-Fi Multi-Media) settings in Repeater mode.



WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

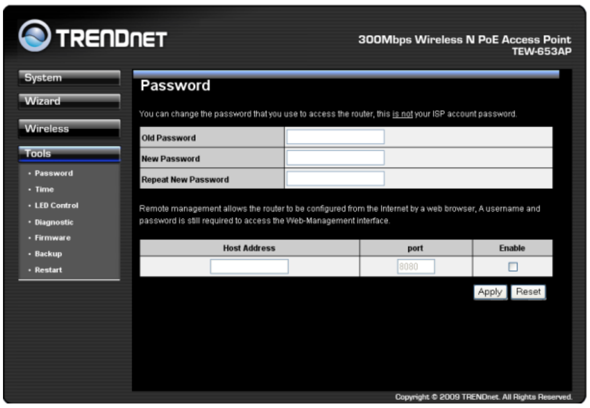
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

Copyright © 2009 TRENDnet. All Rights Reserved.

Tools

Admin

You can change the password required to log into the access point's web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.



Password

You can change the password that you use to access the router, this is not your ISP account password.

Old Password	
New Password	
Repeat New Password	

Remote management allows the router to be configured from the Internet by a web browser, A username and password is still required to access the Web-Management interface.

Host Address	port	Enable
	8080	□

Copyright © 2009 TRENDnet. All Rights Reserved.

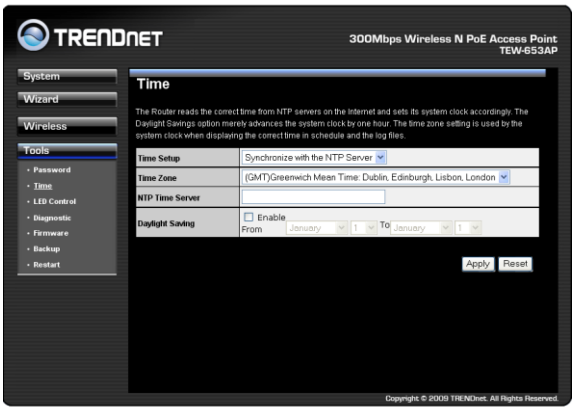
Current Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and type it again in **Repeat New Password** for verification purposes

Time Setting

The Time Zone allows your access point to reference or base its time on the settings configured here, which will affect functions such as Log entries and Power Saving mode.

⚠ If the device losses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.



Time

The Router reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

Time Setup	Synchronize with the NTP Server
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
NTP Time Server	
Daylight Saving	□ Enable From January 1 To January 1

Time Zone: Select the time zone of the country you are currently in. The router will set its time based on your selection.

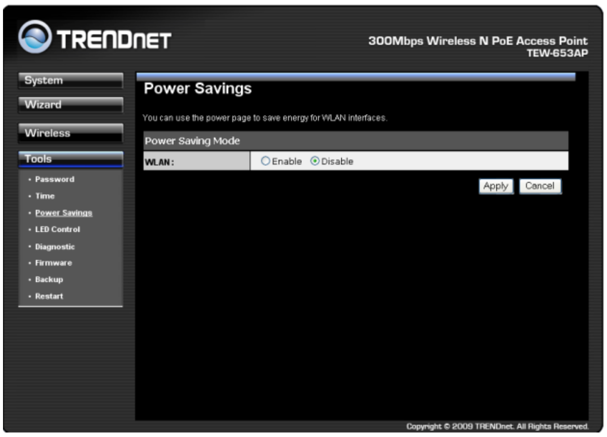
NTP Time Server: The router can set up external NTP Time Server.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **Apply** at the bottom of the screen to save the above configurations.

Power Saving

This screen allows users to enable the Power Saving feature of the access point. Please note that users must enable the power saving schedule.



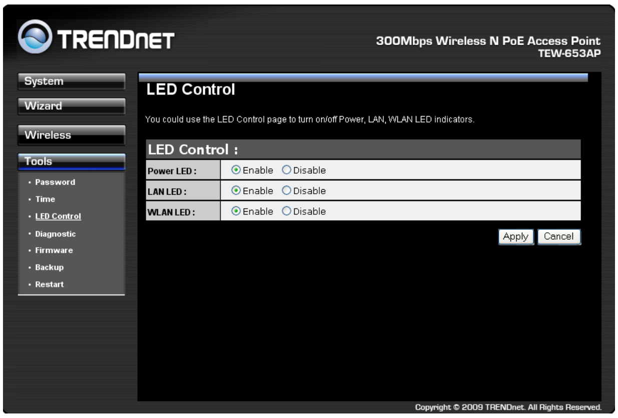
Power Savings

You can use the power page to save energy for WLAN interfaces.

Power Saving Mode	
WLAN :	○ Enable ● Disable

LED Control

This screen allows users to control the LED behavior of the access point.



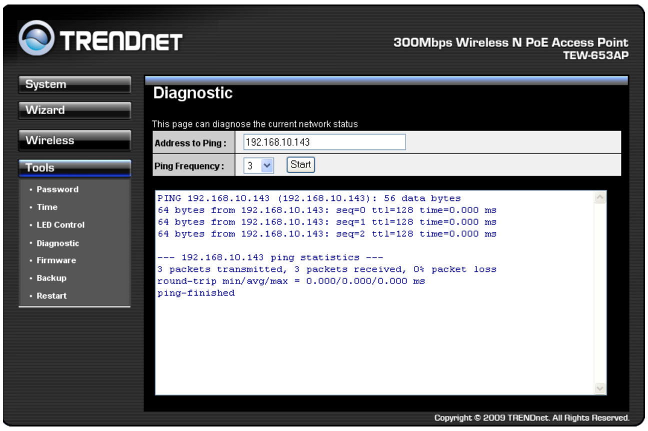
LED Control

You could use the LED Control page to turn on/off Power, LAN, WLAN LED indicators.

LED Control :	
Power LED :	● Enable ○ Disable
LAN LED :	● Enable ○ Disable
WLAN LED :	● Enable ○ Disable

Diagnosis

Diagnosis screen allows users to check whether a network destination is reachable with ping service.



Diagnostic

This page can diagnose the current network status

Address to Ping : 192.168.10.143

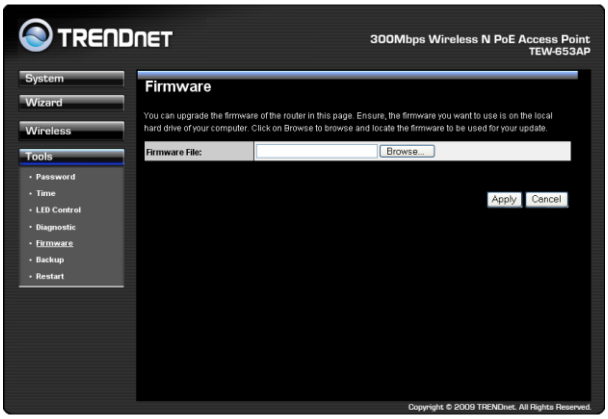
Ping Frequency : 3

```
PING 192.168.10.143 (192.168.10.143): 56 data bytes
64 bytes from 192.168.10.143: seq=0 ttl=128 time=0.000 ms
64 bytes from 192.168.10.143: seq=1 ttl=128 time=0.000 ms
64 bytes from 192.168.10.143: seq=2 ttl=128 time=0.000 ms

--- 192.168.10.143 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
ping-finished
```

Firmware

This page allows you to upgrade the access point’s firmware. To upgrade the firmware of your you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.



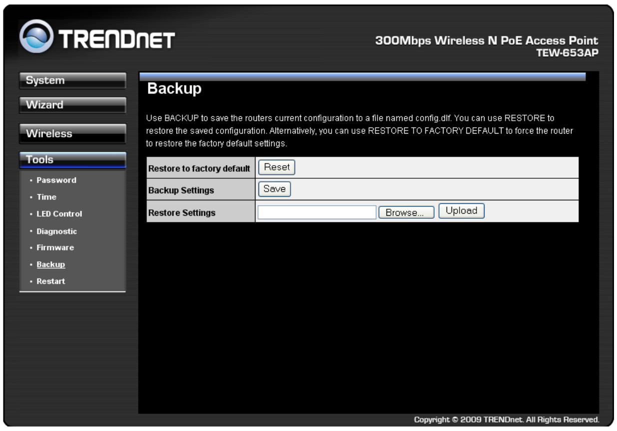
Firmware

You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.

Firmware File:

Backup

This page allows you to save the current configurations. When you save the configurations, you also can re-load the saved configurations into the access point through the **Restore Settings**. If extreme problems occur you can use the **Restore to Factory Defaults** to set all configurations to its original default settings.



Backup

Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings.

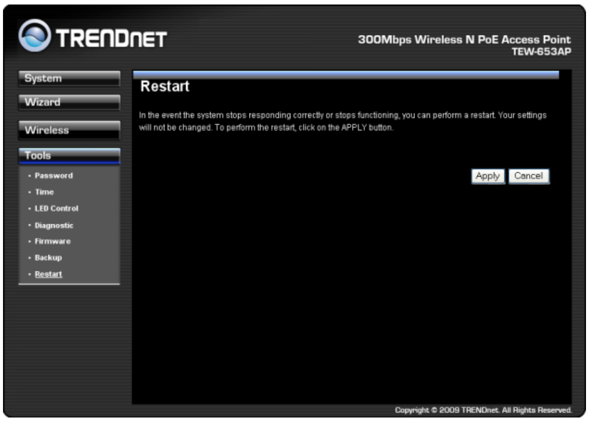
Restore to factory default	Reset
Backup Settings	Save
Restore Settings	Browse... Upload

Copyright © 2009 TRENDnet. All Rights Reserved.

Backup Settings: This can save the current configuration to a file named "**config.bin**" on your PC. You can also use the **Upload** button to restore the saved configuration to the Broadband router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Restart

Restart allows user to restart or reboot the device, none of the settings applied will be changed.



Restart

In the event the system stops responding correctly or stops functioning, you can perform a restart. Your settings will not be changed. To perform the restart, click on the APPLY button.

Copyright © 2009 TRENDnet. All Rights Reserved.

FCC Interference Statement

Federal Communication Commission Interference Statement

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

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

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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

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

IC Interference Statement

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada 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.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Specifications

Hardware	
Standards	IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0), 802.3af
Interface	1 x 10/100Mbps Auto-MDIX PoE LAN port
LED Indicators	Power/Status, LAN, WLAN
Button	Reset button – restores factory default settings
Power Supply	Active Ethernet (Power over Ethernet, IEEE802.3af)-48VDC/0.375A Power adapter 12V/1A
Power Consumption	6 watts (max)
Dimensions (Diameter/Height)	120mm (4.72in.)/ 50mm (1.97in)
Weight	280g (9.87oz)
Temperature	Operating: 0° ~ 45°C (32° ~ 113°F) Storage: -20°C ~ 70°C (-4° ~ 158° F)
Humidity	5% ~ 95% typical (non-condensing)
Certifications	CE, FCC
Wireless	
Module Technique	OFDM: BPSK, QPSK, 16-QAM, 64-QAM DBPSK, DQPSK, CCK
Modes	Access Point, WDS Bridge, Universal Repeater
Antenna	4dBi Smart Internal Antenna
Frequency	2.412 ~ 2.472 GHz
Management	Web Browser (HTTP); SNMP v1, v2c
Data Rate (Auto Fallback)	802.11n: up to 300Mbps 802.11g: up to 54Mbps 802.11b: up to 11Mbps
Output Power	802.11n: 18dBm (typical) @ 300Mbps 802.11g: 18dBm (typical) @ 54Mbps 802.11b: 17dBm (typical) @ 11Mbps
Receiving Sensitivity	802.11n: -79dBm @ MCS8 / -61dBm @ MCS15 802.11g: -92 @ 6Mbps / -72dBm @ 54Mbps 802.11b: -93dBm @ 1Mbps / -89dBm @ 11Mpbs
Encryption	64/128/152-bit (WEP), WPA-PSK/WPA2-PSK, WPA/WPA2-RADIUS
Channels	1-11 (FCC), 1-13 (ETSI)

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-653AP – 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.

TRENDnet®

Product Warranty Registration

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