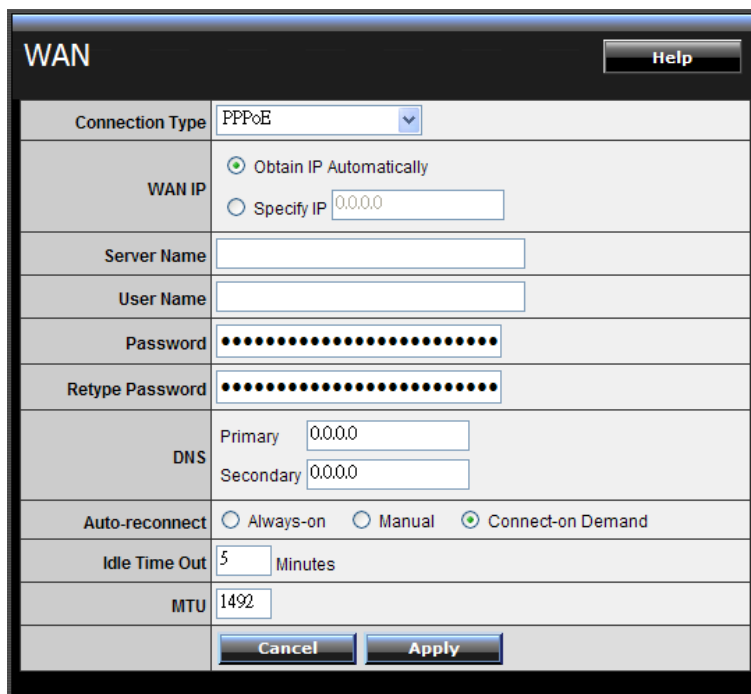


## PPPoE

If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password and User Name, and then the ISP uses PPPoE. Choose this option and enter the required information.



The screenshot shows a 'WAN' configuration window with a 'Help' button in the top right corner. The 'Connection Type' is set to 'PPPoE'. Under 'WAN IP', 'Obtain IP Automatically' is selected. The 'Server Name', 'User Name', 'Password', and 'Retype Password' fields are empty. The 'DNS' section has 'Primary' and 'Secondary' fields both set to '0.0.0.0'. The 'Auto-reconnect' section has 'Connect-on Demand' selected. The 'Idle Time Out' is set to '5' minutes. The 'MTU' is set to '1492'. 'Cancel' and 'Apply' buttons are at the bottom.

Connection Type	PPPoE
WAN IP	<input checked="" type="radio"/> Obtain IP Automatically <input type="radio"/> Specify IP <input type="text" value="0.0.0.0"/>
Server Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
DNS	Primary <input type="text" value="0.0.0.0"/> Secondary <input type="text" value="0.0.0.0"/>
Auto-reconnect	<input type="radio"/> Always-on <input type="radio"/> Manual <input checked="" type="radio"/> Connect-on Demand
Idle Time Out	<input type="text" value="5"/> Minutes
MTU	<input type="text" value="1492"/>
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

**WAN IP:** Select the WAN IP address Obtain from ISP automatically or enter the specified IP address.

**Server Name:** Enter the server name provided by ISP (optional).

**User Name:** Enter the user name provided by ISP.

**Password:** Enter the password provided by ISP.

**Retype Password:** Enter the password again.

**DNS:** Enter the IP address of specified DNS server here, default value 0.0.0.0 is get the DNS settings from ISP.

**Auto-reconnect:** Select the connection type for Always-on, Manual or Connect-on Demand connecting.

**Idle Time Out:** Enter the idle time out for Connect on Daemon, when no Internet access during the idle time, the PPPoE connection will auto disconnect.

**MTU:** Enter the specified MTU (Maximum Transmission Unit). The default value is 1492 bytes.

### PPTP/L2TP with Dynamic IP

If connected to the Internet using a PPTP/L2TP (Dial-up xDSL) with dynamic IP connection, enter the your Server IP, PPTP/L2TP Account and PPTP/L2TP Password, if your ISP has provided you with a DNS IP address, enter it in the DNS field, otherwise, leave it zero.

The image shows two side-by-side screenshots of a WAN configuration interface. Both windows are titled 'WAN' and have a 'Help' button in the top right corner. The left window is configured for PPTP with 'Dynamic IP' selected. The right window is configured for L2TP with 'Dynamic IP' selected. Both windows have the same layout of fields: Connection Type (dropdown), IP Address, Subnet Mask, Gateway, DNS, Server IP, Account, Password, Retype Password, Auto-reconnect (radio buttons), Idle Time Out (minutes), and MTU. At the bottom of each window are 'Cancel' and 'Apply' buttons.

### PPTP/L2TP with Static IP

If connected to the Internet using a PPTP/L2TP (Dial-up xDSL) with static IP connection, enter the your IP Address, Subnet Mask, Gateway IP address, DNS IP address, Server IP address, PPTP Account and PPTP Password.

WAN		Help
Connection Type	PPTP	
	<input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
DNS	0.0.0.0	
Server IP		
PPTP Account		
PPTP Password	.....	
Retype PPTP Password	.....	
Auto-reconnect	<input type="radio"/> Always-on <input type="radio"/> Manual <input checked="" type="radio"/> Connect-on Demand	
Idle Time Out	5 Minutes	
MTU	1400	
MPPE Enable	<input type="checkbox"/> (Only for MSCHAPv2)	
		Cancel Apply

WAN		Help
Connection Type	L2TP	
	<input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
DNS	0.0.0.0	
Server IP		
L2TP Account		
L2TP Password	.....	
Retype L2TP Password	.....	
Auto-reconnect	<input type="radio"/> Always-on <input type="radio"/> Manual <input checked="" type="radio"/> Connect-on Demand	
Idle Time Out	5 Minutes	
MTU	1400	
		Cancel Apply

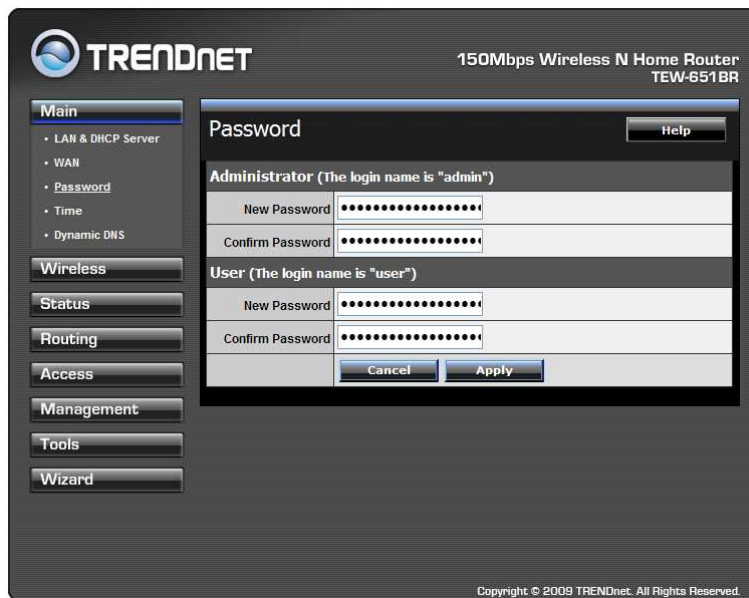
## BigPond Cable

If your ISP is Big Pond Cable, the ISP will provide a User Name, Password, Authentication Server and Login Server IP (Optional). Choose this option and enter the required information.

WAN		Help
Connection Type	BigPond Cable	
User Name		
Password	.....	
Retype Password	.....	
Auth Server	sm-server	
Login Server IP		(optional)
MAC Address	00 - 11 - 22 - 33 - 44 - 56	(optional)
	Clone MAC Address	
		Cancel Apply

## Password

This screen enables users to set administrative and user passwords. These passwords are used to gain access to the WLAN Router interface.



**Administrator:** Type the password the Administrator will use to log into the system. The password must be typed again for confirmation. The Administrator can also authorize users the ability to configure the WLAN Router.

**User:** Type the password the User will use to log in to the system. The password must be typed again for confirmation.

## Time

This screen enables users to set the time and date for the WLAN Router's real-time clock, select properly time zone, and enable or disable daylight saving.

The screenshot displays the 'Time' configuration page of a TRENDNET 150Mbps Wireless N Home Router (TEW-651BR). The interface includes a sidebar with navigation options: Main (LAN & DHCP Server, WAN, Password, Time, Dynamic DNS), Wireless, Status, Routing, Access, Management, Tools, and Wizard. The main content area is titled 'Time' and contains the following fields and controls:

- Local Time:** Sep/9/2009 12:22:41
- Time Zone:** ((GMT-08:00) Pacific Time (US/Canada), Tijuana)
- Synchronize the clock with:** Manual
- Default NTP server:** (Empty text box)
- Set the time:** Year: 2009, Month: Sep, Day: 09, Hour: 12, Minute: 22, Second: 41, Set Time button
- Daylight Saving:** Enabled/Disabled, Start: Mar 3rd, Sun, End: Nov 2nd, Sun, Cancel/Apply buttons

Copyright © 2009 TRENDnet. All Rights Reserved.

**Local Time:** Displays the local time and date.

**Time Zone:** Select the time zone from the drop-down list.

**Synchronize the clock with:** Select the clock adjustment method from the drop-down list.

Automatic: Automatically adjust the system time from NTP Server.

Manual: Manually adjust the system time when you press the **Set Time** button.

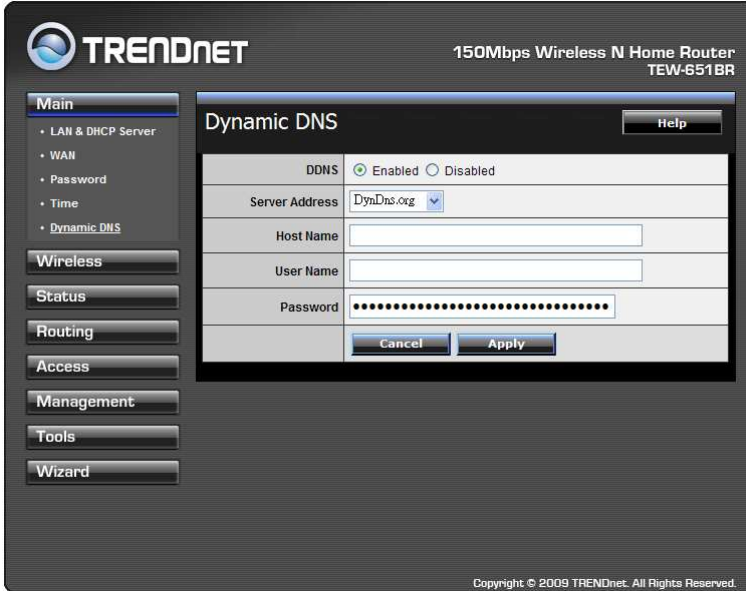
**Default NTP server:** The Simple Network Time Protocol (SNTP) server allows the WLAN Router to synchronize the system clock to the global Internet through the SNTP Server. Specify the NTP domain name or IP address in the text box.

**Set the time:** Manually setting the WLAN Router system time, press the **Set Time** button to update the system time.

**Daylight Saving:** Enables users to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

## Dynamic DNS

This synchronizes the DDNS server with your current Public IP address when you are online. First, you need to register your preferred DNS with the DDNS provider. Then, please select the DDNS address in the Server Address and fill the related information in the below fields: Host Name, User Name and Password.



The screenshot shows the 'Dynamic DNS' configuration page in the Trendnet web interface. The page title is '150Mbps Wireless N Home Router TEW-651BR'. The left sidebar contains a navigation menu with 'Main' selected, and sub-items: LAN & DHCP Server, WAN, Password, Time, and Dynamic DNS. The main content area is titled 'Dynamic DNS' and includes a 'Help' button. The configuration fields are as follows:

DDNS	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Server Address	DynDns.org
Host Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>

Buttons for 'Cancel' and 'Apply' are located at the bottom of the form. A copyright notice 'Copyright © 2009 TRENDnet. All Rights Reserved.' is visible at the bottom of the page.

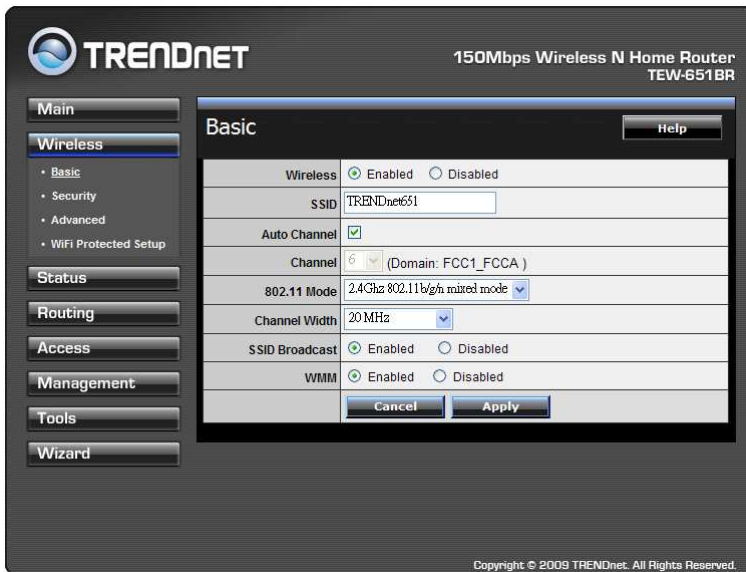
---

## Wireless

This section enables users to configuration the wireless communications parameters for the WLAN Router.

### Basic

This page allow user to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.



The screenshot shows the 'Basic' configuration page in the Trendnet web interface. The page title is '150Mbps Wireless N Home Router TEW-651BR'. The left sidebar contains a navigation menu with 'Wireless' selected, and sub-items: Basic, Security, Advanced, and WiFi Protected Setup. The main content area is titled 'Basic' and includes a 'Help' button. The configuration fields are as follows:

Wireless	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSID	TRENDnet651
Auto Channel	<input checked="" type="checkbox"/>
Channel	6 (Domain: FCC1_FCCA)
802.11 Mode	2.4Ghz 802.11b/g/n mixed mode
Channel Width	20MHz
SSID Broadcast	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
WMM	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Buttons for 'Cancel' and 'Apply' are located at the bottom of the form. A copyright notice 'Copyright © 2009 TRENDnet. All Rights Reserved.' is visible at the bottom of the page.

**Enable/Disable:** Enables or disables wireless LAN via the WLAN Router.

**SSID:** Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the WLAN Router.

**Channel:** Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the WLAN Router.

**802.11 Mode:** Select one of the following:

- **2.4Ghz 802.11b/g mixed mode** - Select if you are using both 802.11b and 802.11g wireless clients.
- **2.4Ghz 802.11b/g/n mixed mode** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.
- **2.4Ghz 802.11n only** - Select if you are using 802.11n wireless clients only.

**Channel Width:** Select the Channel Width:

- **20MHz** – This is the default setting. Select this option if you are not using any 802.11n wireless clients.
- **Auto 20/40 MHz** - Select this option if you are using both 802.11n and non-802.11n wireless devices.

**SSID Broadcast:** While SSID Broadcast is enabled, all wireless clients will be able to view the WLAN Router's SSID.

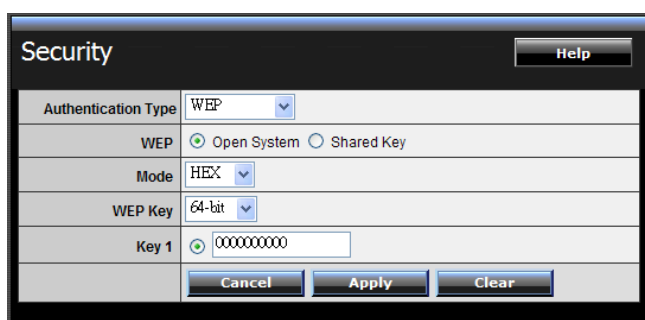
**WMM:** Enable the Wi-Fi Multi-Media will offer Wi-Fi networks stable that improve the user experience for audio, video, and voice applications by prioritizing data traffic.

## Security

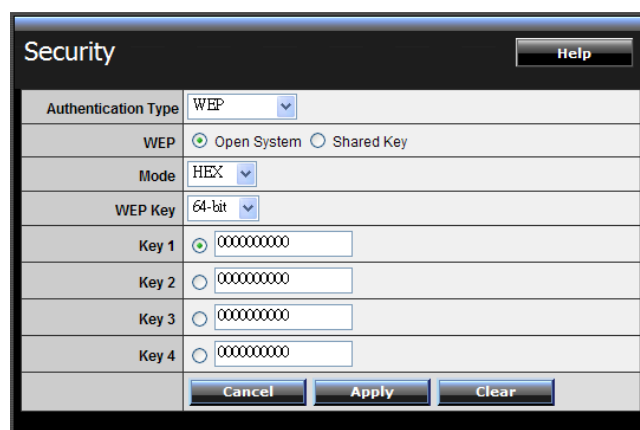


**Authentication Type:** The authentication type default is set to open system. There are four options: Disabled, WEP, WPA, WPA2 and WPA-Auto.

### WEP Encryption



WPS Enabled



WPS Disabled

**WEP:** Open System and Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key.

**Mode:** Select the key type: ASCII or HEX

**WEP Key:** Select the level of encryption from the drop-down list. The WLAN Router supports, 64 and 128-bit encryption.

Key Length	Hex	ASCII
Type	characters 0-9, A-F, a-f	alphanumeric format
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters



**Key 1:** Enables users to create WEP keys with WPS enabled. Manually enter a set of values for Key 1.

**Key 1 ~ Key 4:** Enables users to create up to 4 different WEP keys with WPS disabled. Manually enter a set of values for each key. Select a key to use by clicking the radio button next to the key.

### WPA/WPA2/WPA-Auto Security with EAP

The screenshot shows a 'Security' configuration window with a 'Help' button in the top right. The 'Authentication Type' is set to 'WPA'. Under 'PSK / EAP', the 'EAP' radio button is selected. Under 'Cipher Type', the 'TKIP' radio button is selected. There are two sections for RADIUS servers. 'RADIUS Server 1' has fields for IP (0.0.0.0), Port (1812), and Shared Secret. 'RADIUS Server 2 (Optional)' also has fields for IP (0.0.0.0), Port (1812), and Shared Secret. At the bottom are 'Cancel', 'Apply', and 'Clear' buttons.

If WPA, WPA2 or WPA-Auto EAP is selected, the above screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.

**Cipher Type:** Select the cipher type for TKIP or AES encryption, Selected Auto for auto detects the cipher type.

#### RADIUS Server 1/2:

1. Enter the IP address, Port used and Shared Secret by the Primary Radius Server 1.
2. Enter the IP address, Port used and Shared Secret by the Secondary Radius Server 2. (optional)

### WPA/WPA2/WPA-Auto Security with PSK

The screenshot shows a 'Security' configuration window with a 'Help' button in the top right. The 'Authentication Type' is set to 'WPA'. Under 'PSK / EAP', the 'PSK' radio button is selected. Under 'Cipher Type', the 'TKIP' radio button is selected. There are two fields for 'Passphrase' and 'Confirm Passphrase', both containing masked characters (dots). At the bottom are 'Cancel', 'Apply', and 'Clear' buttons.

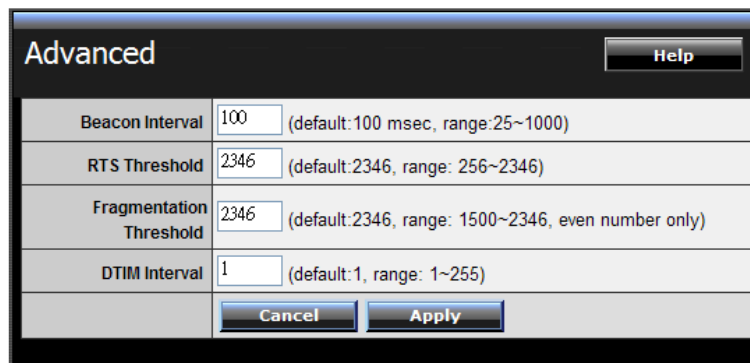
If WPA, WPA2 or WPA-Auto PSK is selected.

**Cipher Type:** Select the cipher type for TKIP or AES encryption, Selected Auto for auto detects the cipher type.

**Passphrase:** The length should be 8 characters at least.

## Advanced

This screen enables users to configure advanced wireless functions.



The screenshot shows a dialog box titled "Advanced" with a "Help" button in the top right corner. It contains four rows of configuration options, each with a label, a text input field, and a description in parentheses:

Beacon Interval	100	(default:100 msec, range:25~1000)
RTS Threshold	2346	(default:2346, range: 256~2346)
Fragmentation Threshold	2346	(default:2346, range: 1500~2346, even number only)
DTIM Interval	1	(default:1, range: 1~255)

At the bottom of the dialog box are two buttons: "Cancel" and "Apply".

**Beacon Interval:** Type the beacon interval in the text box. User can specify a value from 25 to 1000. The default beacon interval is 100.

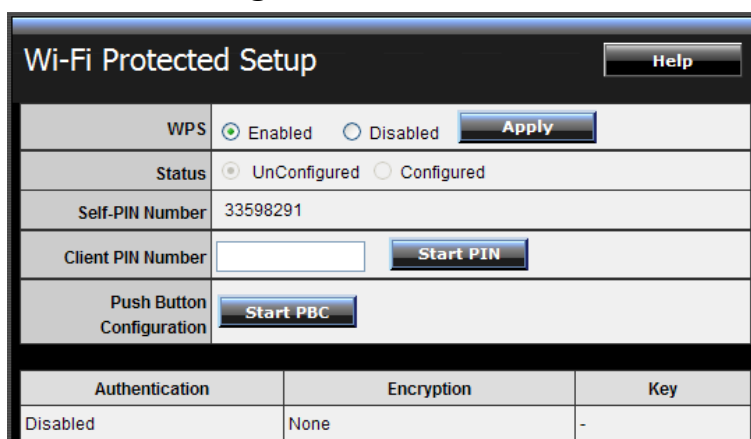
**RTS Threshold:** Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2346 until data flow is normalized.

**Fragmentation Threshold:** Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 1500 and 2346 until packet transfer rates are minimized. (NOTE: set this fragmentation threshold value may diminish system performance.)

**DTIM Interval:** Type a DTIM (Delivery Traffic Indication Message) interval in the text box. User can specify

## Wi-Fi Protected Setup

This screen enables users to configure the Wi-Fi Protected Setup function.



The screenshot shows the 'Wi-Fi Protected Setup' configuration window. At the top right is a 'Help' button. The main area contains several sections:

- WPS:** Radio buttons for 'Enabled' (selected) and 'Disabled', followed by an 'Apply' button.
- Status:** Radio buttons for 'UnConfigured' (selected) and 'Configured'.
- Self-PIN Number:** A text field containing '33598291'.
- Client PIN Number:** An empty text field and a 'Start PIN' button.
- Push Button Configuration:** A 'Start PBC' button.

At the bottom, there is a table with three columns: Authentication, Encryption, and Key.

Authentication	Encryption	Key
Disabled	None	-

**WPS:** Enable or Disable the WPS (Wi-Fi Protected Setup) function

**Status:** Display the status (Un-configured State/Configured State) information of WPS.

**Self-PIN Number:** Display the current PIN number of the WLAN Router.

**Client PIN Number:** Type Client's PIN number the client uses to negotiate with the WLAN Router via WPS connection. It is only used when users want their station to join Router's network.

**Push Button Configuration:** Clicking the **Start PBC** button will invoke the Push Button Configuration (PBC) method of WPS. Push the WPS button on the client side when users want their station to join Router's network.

---

## Status

---

This selection enables users to view the status of the WLAN Router LAN, WAN and Wireless connections, and view logs and statistics pertaining to connections and packet transfers.

### Device Information

This screen enables users to view the WLAN Router's LAN, Wireless and WAN configurations.

The screenshot shows the Trendnet web interface for a 150Mbps Wireless N Home Router (TEW-651BR). The left sidebar contains navigation tabs: Main, Wireless, Status (selected), Routing, Access, Management, Tools, and Wizard. The Status tab is expanded to show 'Device Information', 'Log', 'Log Setting', 'Statistic', and 'Wireless'. The main content area is titled 'Device Information' and includes a 'Help' button. It displays the following information:

- Firmware Version:** 1.00.04
- Router up time:** 0 Day, 2:06:51
- WAN Section:**
  - MAC Address: 00:11:22:33:44:56
  - Connection: DHCP Client Disconnected (with 'DHCP Release' and 'DHCP Renew' buttons)
  - IP: 0.0.0.0
  - Subnet Mask: 0.0.0.0
  - Default Gateway: 0.0.0.0
  - DNS: 0.0.0.0
- Wireless Section:**
  - Connection: 802.11n AP Enable
  - SSID: TRENDnet651
  - Channel: 6
  - Authentication: Disable
- LAN Section:**
  - MAC Address: 00:11:22:33:44:55
  - IP Address: 192.168.10.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Enabled DHCP Table

Copyright © 2009 TRENDnet. All Rights Reserved.

**Firmware Version:** Displays the latest build of the WLAN Router firmware interface. After updating the firmware in Tools - Firmware, check this to ensure that the firmware was successfully updated.

**WAN:** This section displays the WAN interface configuration including the MAC address, Connection status, DHCP client status, IP address, Subnet mask, Default gateway, and DNS.

**Wireless:** This section displays the wireless configuration information, including the MAC address, the Connection status, SSID, Channel and Authentication type.

**LAN:** This section displays the LAN interface configuration including the MAC address, IP Address, Subnet Mask, and DHCP Server Status. Click "DHCP Table" to view a list of client stations currently connected to the WLAN Router LAN interface. Click "DHCP Release" to release all IP addresses assigned to client stations connected to the WAN via the WLAN Router. Click "DHCP Renew" to reassign IP addresses to client stations connected to the WAN.

---

## Log

This screen enables users to view a running log of Router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click *“First Page”* to view the first page of the log

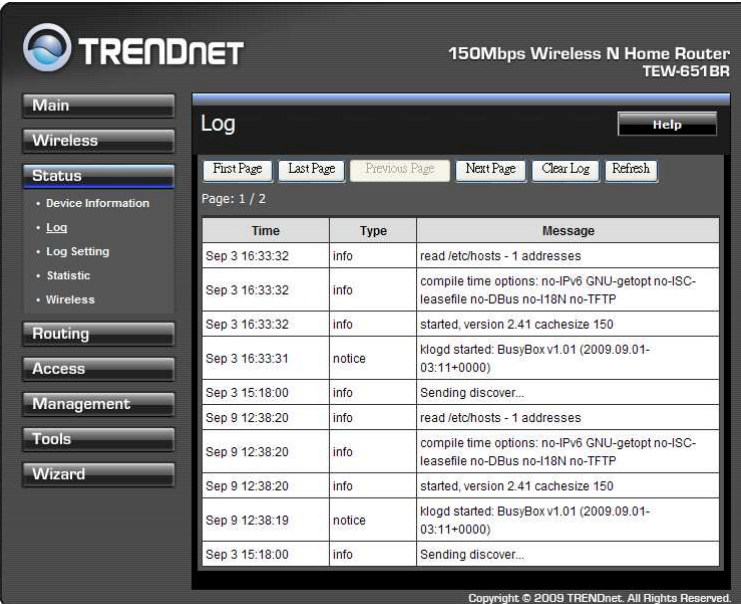
Click *“Last Page”* to view the final page of the log

Click *“Previous Page”* to view the page just before the current page

Click *“Next Page”* to view the page just after the current page

Click *“Clear Log”* to delete the contents of the log and begin a new log

Click *“Refresh”* to renew log statistics



The screenshot shows the TRENDnet web interface for a 150Mbps Wireless N Home Router (TEW-651BR). The 'Log' page is active, displaying a table of system events. The table has three columns: Time, Type, and Message. The log entries are as follows:

Time	Type	Message
Sep 3 16:33:32	info	read /etc/hosts - 1 addresses
Sep 3 16:33:32	info	compile time options: no-IPv6 GNU-getopt no-ISC-leasefile no-DBus no-118N no-TFTP
Sep 3 16:33:32	info	started, version 2.41 cachesize 150
Sep 3 16:33:31	notice	klogd started: BusyBox v1.01 (2009.09.01-03:11+0000)
Sep 3 15:18:00	info	Sending discover...
Sep 9 12:38:20	info	read /etc/hosts - 1 addresses
Sep 9 12:38:20	info	compile time options: no-IPv6 GNU-getopt no-ISC-leasefile no-DBus no-118N no-TFTP
Sep 9 12:38:20	info	started, version 2.41 cachesize 150
Sep 9 12:38:19	notice	klogd started: BusyBox v1.01 (2009.09.01-03:11+0000)
Sep 3 15:18:00	info	Sending discover...

**Time:** Displays the time and date that the log entry was created.

**Message:** Displays summary information about the log entry.

## Log Setting

This screen enables users to set Router Log parameters.

**SMTP Authentication:** Selected the Enabled if the SMTP server need for authentication, fill in account name and password in SMTP Account field and SMTP Password field.

**SMTP Account:** If the SMTP Authentication enabled, fill in the SMTP account name here.

**SMTP Password:** If the SMTP Authentication enabled, fill in the password of the SMTP account here.

**SMTP Server:** Type your SMTP server address here.

**From Email address:** Type an email address for the log to be sent from.

**To Email address:** Type an email address for the log to be sent to. Click “*Email Log Now*” to immediately send the current log.

**E-mail Logs:** Email the logs to specified email receiver.

**When log is full** - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.

**Every day, Every Monday ...** - The log is sent on the interval specified.

- If "Every day" is selected, the log is sent at the time specified.
- If the day is specified, the log is sent once per week, on the specified day.

- Select the time of day you wish the E-mail to be sent.
- If the log is full before the time specified to send it, it will be sent regardless.

**Syslog Server:** Type the IP address of the Syslog Server if user wants the WLAN Router to listen and receive incoming Syslog messages.

**Log Type:** Enables users to select what items will be included in the log:

**System Activity:** Displays information related to WLAN Router operation.

**Debug Information:** Displays information related to errors and system malfunctions.

**Attacks:** Displays information about any malicious activity on the network.

**Dropped Packets:** Displays information about packets that have not been transferred successfully.

**Notice:** Displays important notices by the system administrator.

## Statistic

This screen displays a table that shows the rate of packet transmission via the WLAN Router's LAN, Wireless and WAN ports (in bytes per second).

The screenshot shows the 'Statistic' page of a Trendnet 150Mbps Wireless N Home Router (TEW-651BR). The page features a navigation menu on the left with options: Main, Wireless, Status (selected), Routing, Access, Management, Tools, and Wizard. The 'Status' menu is expanded to show: Device Information, Log, Log Setting, Statistic (selected), and Wireless. The main content area displays a table titled 'Statistic' with a 'Help' button. The table shows utilization in packets for LAN, Wireless, and WAN ports, categorized by Send and Receive. A 'Reset' button is located below the table.

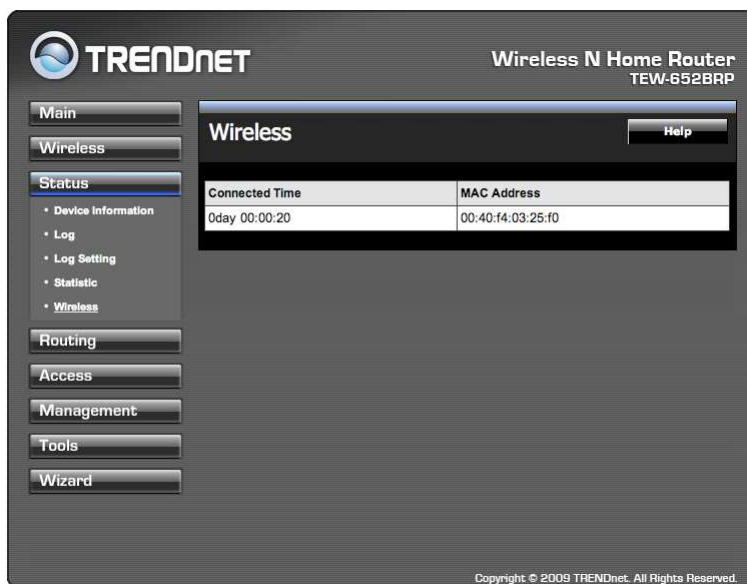
Utilization (packets)		LAN	Wireless	WAN
Send	Peak	2436	7106	9
Receive	Peak	1623	56288	0

Copyright © 2009 TRENDnet. All Rights Reserved.

Click **“Reset”** to erase all statistics and begin logging statistics again.

## Wireless

This screen enables users to view information about wireless devices that are connected to the WLAN Router.



**Connected Time:** Displays the time duration of wireless clients connection to the WLAN Router.

**MAC Address:** Displays the wireless client's MAC address.

---

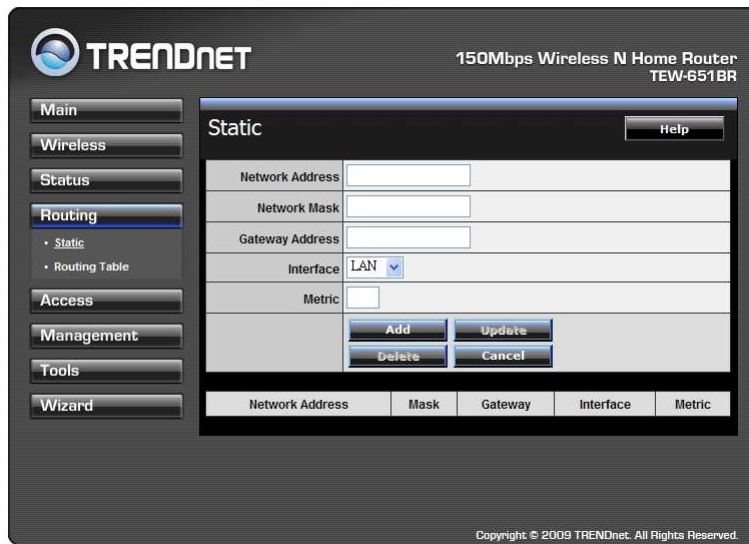
## Routing

This selection enables users to set how the WLAN Router forwards data: Static and Dynamic. Routing Table enables users to view the information created by the WLAN Router that displays the network interconnection topology.

### Static

It enables users to set parameters by which the WLAN Router forwards data to its destination if the network has a static IP address.





**Network Address:** Type the static IP address the network uses to access the Internet. Contact the ISP or network administrator for this information.

**Network Mask:** Type the network (subnet) mask of the network. If this field is left blank, the network mask defaults to 255.255.255.0. Contact the ISP or network administrator for this information.

**Gateway Address:** Type the gateway address of the network. Contact the ISP or network administrator for this information.

**Interface:** Select an interface, WAN or LAN, to connect to the Internet.

**Metric:** Select which metric that the user wants to apply to this configuration.

**Add:** Click to add the configuration to the static IP address table at the bottom of the page.

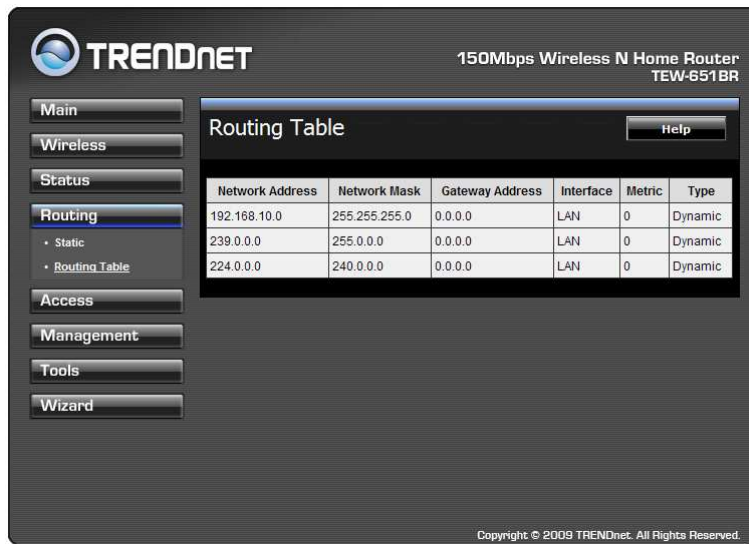
**Update:** Select one of the entries in the static IP address table at the bottom of the page, and after changing parameters, click “Update” to confirm the changes.

**Delete:** Select one of the entries in the static IP address table at the bottom of the page and click “Delete” to remove the entry.

**Cancel:** Click the **Cancel** button to erase all fields and enter new information.

### **Routing Table**

This screen enables users to view the routing table of the WLAN Router. The routing table is a database created by the WLAN Router that displays the network interconnection topology.



**Network Address:** Displays the network IP address of the connected node.

**Network Mask:** Displays the network (subnet) mask of the connected node.

**Gateway Address:** Displays the gateway address of the connected node.

**Interface:** Displays whether the node is connected via a WAN or LAN.

**Metric:** Displays the metric of the connected node.

**Type:** Displays whether the node has a static or dynamic IP address

---

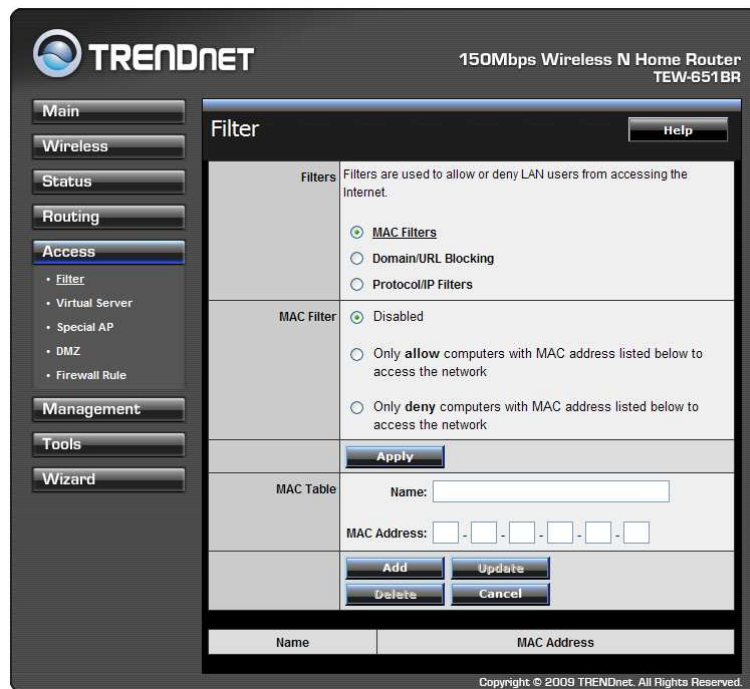
## Access

---

This page enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

### Filters

Using filters to deny or allow the users to access to the internet. Three types of filters can be select: MAC, Domain/URL blocking, and Protocol/IP filter.



## MAC Filters

The screenshot shows a 'Filter' configuration window with a 'Help' button in the top right. The window is divided into several sections:

- Filters:** A section with a description: 'Filters are used to allow or deny LAN users from accessing the Internet.' It contains three radio buttons: 'MAC Filters' (selected), 'Domain/URL Blocking', and 'Protocol/IP Filters'.
- MAC Filter:** A section with three radio buttons: 'Disabled' (selected), 'Only **allow** computers with MAC address listed below to access the network', and 'Only **deny** computers with MAC address listed below to access the network'.
- Buttons:** An 'Apply' button is located below the MAC Filter section.
- MAC Table:** A section with a 'Name:' text input field and a 'MAC Address:' field consisting of six boxes separated by hyphens.
- Actions:** Four buttons are arranged in a 2x2 grid: 'Add', 'Update', 'Delete', and 'Cancel'.
- Table:** At the bottom, a table with two columns: 'Name' and 'MAC Address'.

**MAC Filter:** Enables you to allow or deny accessing the internet.

**Disable:** Disable the MAC filter function.

**Allow:** Only allow computers with MAC address listed in the MAC Table.

**Deny:** Computers in the MAC Table are denied Internet access.

**MAC Table:** Use this section to create a user profile which internet access is denied or allowed. The user profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

**Name:** Type the name of the user to be permitted/denied access.

**MAC Address:** Type the MAC address of the user's network interface.

**Add:** Click to add the user to the list at the bottom of the page.

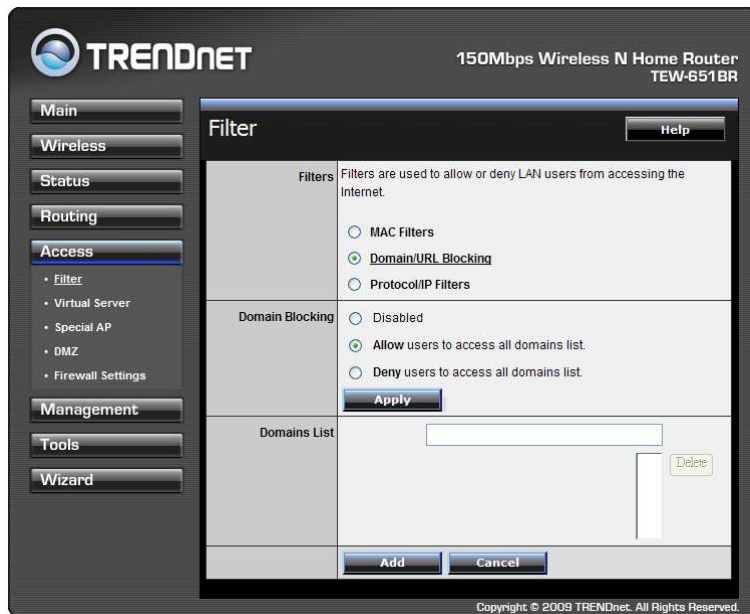
**Update:** Click to update information for the user, if you have changed any of the fields.

**Delete:** Select a user from the table at the bottom of the list and click Delete to remove the user profile.

**Cancel:** Click **Cancel** to erase all fields and enter new information.

## Domain/URL Blocking

You could specify the domains that allow users to access or deny by clicking one of the two items. Also, add the specified domains in the text box.



- **Disable:** Disable the Domain/URL Blocking function.
- **Allow:** Allow users to access all domains except “Domains List”.
- **Deny:** Deny users to access all domains except “Domains List”.

**Domains List:** List Domain/URL you will Denied or Allowed.

- **Delete:** Select a Domain/URL from the table at the bottom of the list and click Delete to remove the Domain/URL.
- **Add:** Click to **Add** button to add domain to the Domains list.
- **Cancel:** Click the **Cancel** button to erase all fields and enter new information.

## Protocol/IP Filters

This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling within the range are not allowed accessing internet. The IP filter profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

	Name	Protocol	Port Range	IP Range
<input type="checkbox"/>	Filter FTP	Any	20-21	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter HTTP	Any	80-80	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter HTTPS	Any	443-443	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter DNS	Any	53-53	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter SMTP	Any	25-25	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter POP3	Any	110-110	0.0.0.0-0.0.0.0
<input type="checkbox"/>	Filter Telnet	Any	23-23	0.0.0.0-0.0.0.0

**Enable:** Click to enable or disable the IP address filter.

**Name:** Type the name of the user to be denied access.

**Protocol:** Select a protocol (TCP or UDP) to use for the virtual server.

**Port:** Type the port range of the protocol.

**IP Range:** Type the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

- **Add:** Click to add the IP range to the table at the bottom of the screen.
- **Update:** Click to update information for the range if you have selected a list item and have made changes.
- **Delete:** Select a list item and click Delete to remove the item from the list.

- **Cancel:** Click the **Cancel** button to erase all fields and enter new information.

## Virtual Server

This screen enables user to create a virtual server via the WLAN Router. If the WLAN Router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The WLAN Router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

	Name	Protocol	LAN Server
<input type="checkbox"/>	Virtual Server FTP	TCP 21/21	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTP	TCP 80/80	0.0.0.0
<input type="checkbox"/>	Virtual Server HTTPS	TCP 443/443	0.0.0.0
<input type="checkbox"/>	Virtual Server DNS	UDP 53/53	0.0.0.0
<input type="checkbox"/>	Virtual Server SMTP	TCP 25/25	0.0.0.0
<input type="checkbox"/>	Virtual Server POP3	TCP 110/110	0.0.0.0
<input type="checkbox"/>	Virtual Server Telnet	TCP 23/23	0.0.0.0
<input type="checkbox"/>	IPSec	UDP 500/500	0.0.0.0
<input type="checkbox"/>	PPTP	TCP 1723/1723	0.0.0.0
<input type="checkbox"/>	NetMeeting	TCP 1720/1720	0.0.0.0

**Enable:** Click to enable or disable the virtual server.

**Name:** Type a descriptive name for the virtual server.

**Protocol:** Select a protocol (TCP or UDP) to use for the virtual server.

**Private Port:** Type the port number of the computer on the LAN that is being used to act as a virtual server.

**Public Port:** Type the port number on the WAN that will be used to provide access to the virtual server.

**LAN Server:** Type the LAN IP address that will be assigned to the virtual server.

- **Add:** Click to add the virtual server to the table at the bottom of the screen.

- **Update:** Click to update information for the virtual server if the user has selected a listed item and has made changes.
- **Delete:** Select a listed item and click **Delete** to remove the item from the list.
- **Cancel:** Click **Cancel** button to erase all fields and enter new information.

## Special AP

This screen enables users to specify special applications, such as games which require multiple connections that are blocked by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

	Name	Trigger Port Range	Incoming Port
<input type="checkbox"/>	Battle.net	Any 6112-6112	Any 6112
<input type="checkbox"/>	Dialpad	Any 7175-7175	Any 51200-51201,51210
<input type="checkbox"/>	ICU II	Any 2019-2019	Any 2000-2038,2025-2051,2069,2085,3010-3030
<input type="checkbox"/>	PC-to-Phone	Any 12053-12053	Any 12120,12122,24150-24220
<input type="checkbox"/>	Quick Time 4	Any 554-554	Any 6970-6999

**Enable:** Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the WLAN Router's WAN connection. Click "Disabled" on a profile to prevent users from accessing the application on the WAN connection.

**Name:** Type a descriptive name for the application.

**Trigger:** Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol (TCP, UDP, or \* for TCP+UDP) that can be used to access the application.
- **Port Range:** Type the port range that can be used to access the application in the text boxes.



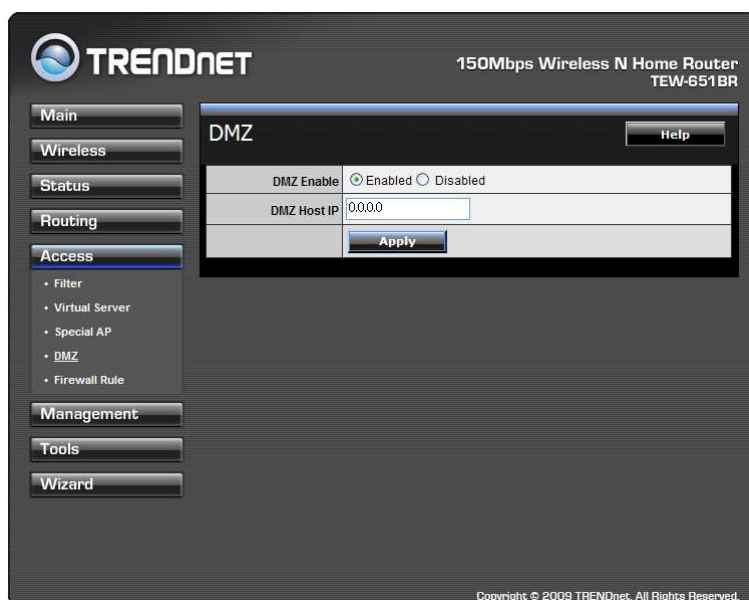
**Incoming:** Defines which incoming communications users are permitted to connect with.

- **Protocol:** Select the protocol (TCP, UDP, or \* for TCP+UDP) that can be used by the incoming communication.
- **Port:** Type the port number that can be used for the incoming communication.
- **Add:** Click to add the special application profile to the table at the bottom of the screen.
- **Update:** Click to update information for the special application if user have selected a list item and have made changes.
- **Delete:** Select a list item and click **Delete** to remove the item from the list.
- **Cancel:** Click **Cancel** button to erase all fields and enter new information.

## DMZ

This screen enables users to create a DMZ for those computers that cannot access Internet applications properly through the WLAN Router and associated security settings.

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



**Enable:** Click to enable or disable the DMZ.

**DMZ Host IP:** Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

**Apply:** Click to save the settings.

## Firewall Settings

This screen enables users to set up the firewall. The WLAN Router provides basic firewall functions, by filtering all the packets that enter the WLAN Router using a set of rules. The rules are listed in sequential order--the lower the rule number, the higher the priority the rule has.

The screenshot shows the 'Firewall Rule' configuration page. The 'Enable' section has 'Enable' selected. The 'Name' field is empty. The 'Action' section has 'Allow' selected. The 'Source' section has 'Interface' set to 'LAN', 'IP Range Start' and 'IP Range End' are empty, and 'Protocol' is 'TCP'. The 'Destination' section has 'Interface' set to 'WAN', 'IP Range Start' and 'IP Range End' are empty, and 'Protocol' is 'ICMP'. Below the form is a table of existing rules:

	Action	Name	Source	Destination	Protocol
<input checked="" type="checkbox"/>	Allow	Allow to Ping WAN port	WAN,*	WAN,*	ICMP,
<input checked="" type="checkbox"/>	Deny	Default	WAN,*	LAN,*	*,*
<input checked="" type="checkbox"/>	Allow	Default	LAN,*	WAN,*	*,*

**Enable:** Click to enable or disable the firewall rule profile.

**Name:** Type a descriptive name for the firewall rule profile.

**Action:** Select whether to allow or deny packets that conform to the rule.

**Source:** Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

**Destination:** Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

**Add:** Click to add the rule profile to the table at the bottom of the screen.

**Update:** Click to update information for the rule if the user has selected a listed item and has made changes.

**Delete:** Select a listed item and click **Delete** button to remove the entry from the list.

**New:** Click “**New**” to erase all fields and enter new information.

**Priority Up:** Select a rule from the list and click “**Priority Up**” to increase the priority of the rule.

**Priority Down:** Select a rule from the list and click “**Priority Down**” to decrease the priority of the rule.

**Update Priority:** After increasing or decreasing the priority of a rule, click “**Update Priority**” to save the changes.

---

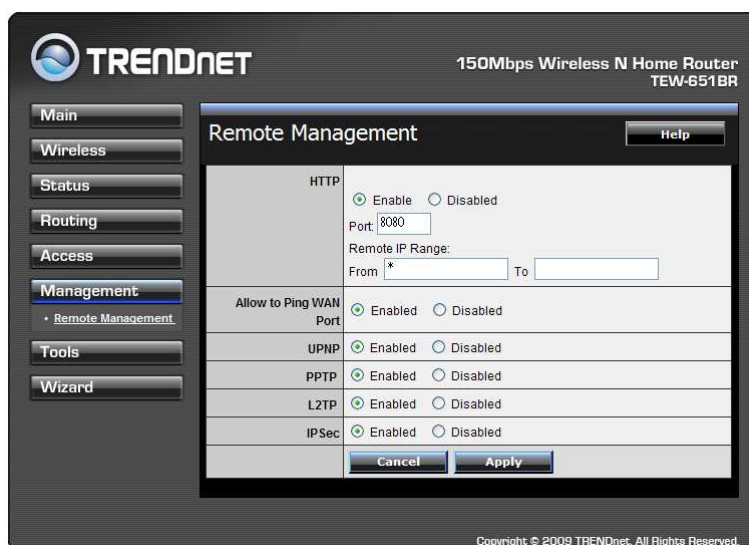
## Management

---

Management enables users to set up the Remote Management feature.

### Remote Management

This screen enables users to set up remote management. Using remote management, the WLAN Router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.



**HTTP:** Enables users to set up HTTP access of the Port number, and Remote IP Range for remote management.

**Allow to Ping WAN Port:** Type a range of Router IP addresses that can be pinged from remote locations

**UPnP Enable:** UPnP is short for Universal Plug and Play that is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The WLAN Router is an UPnP-enabled Router and will only work with other UPnP devices/software. If user does not want to use the UPnP functionality, select “Disabled” to disable it.

**PPTP:** Enables users to set up PPTP access for remote management.

**L2TP:** Enables users to set up L2TP access for remote management.

**IPSec:** Enables users to set up IPSec access for remote management.

---

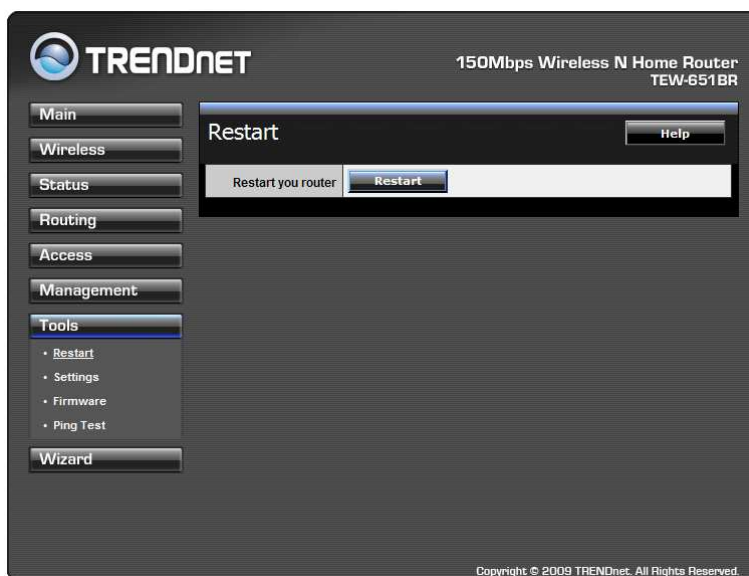
## Tools

---

This page enables users to restart the system, save and load different settings as profiles, restore factory default settings, run a setup wizard to configure WLAN Router settings, upgrade the firmware, and ping remote IP addresses.

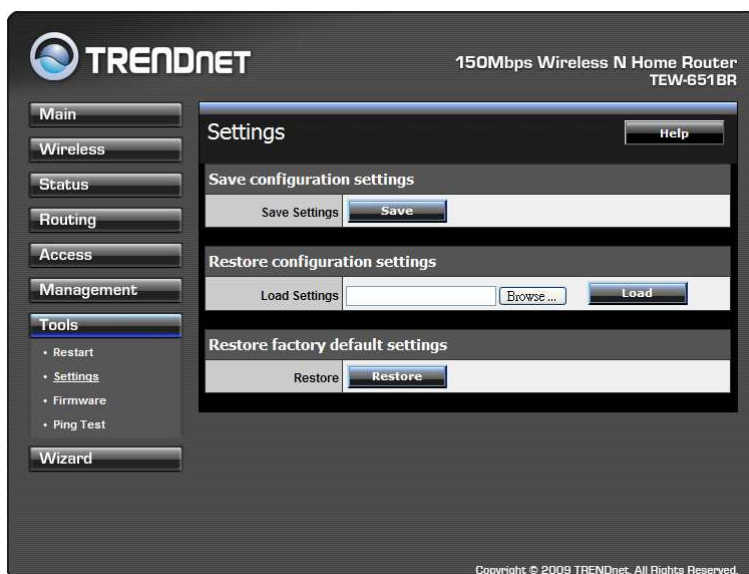
### Restart

Click “Restart” to restart the system in the event the system is not performing correctly.



### Settings

This screen enables users to save settings as a profile and load profiles for different circumstances. User can also load the factory default settings, and run a setup wizard to configure the WLAN Router and Router interface.



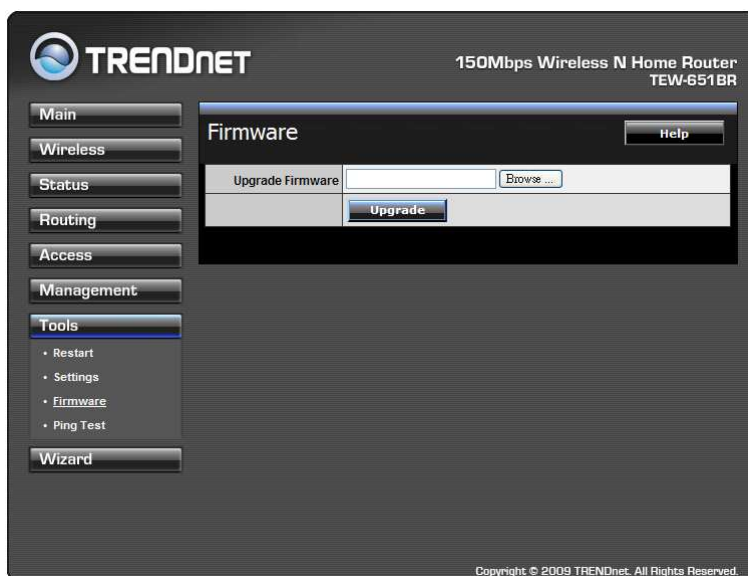
**Save Settings:** Click “Save” to save the current configuration as a profile that can load when necessary.

**Load Settings:** Click “Browse” and go to the location of a stored profile. Click “Load” to load the profile's settings.

**Restore Factory Default Settings:** Click “Restore” to restore the default settings. All configuration changes will lose.

## Firmware

This screen enables users to keep the WLAN Router firmware up to date.



Please follow the below instructions:

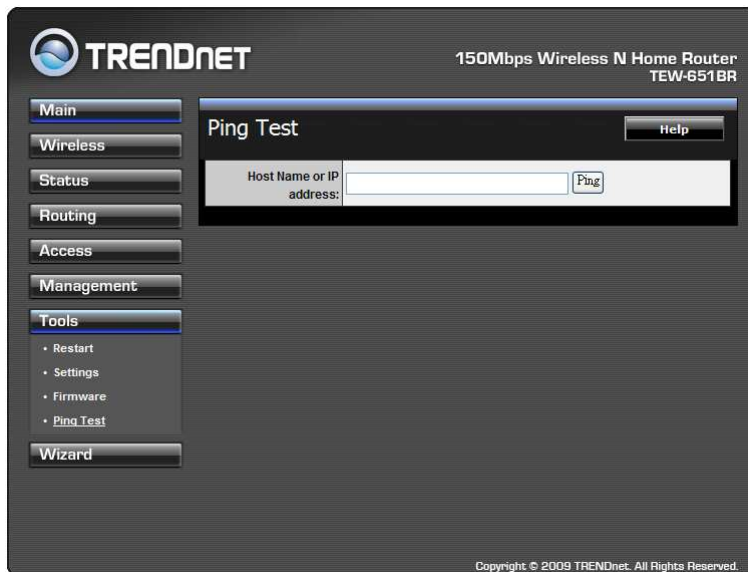
Download the latest firmware from the manufacturer's Web site, and save it to disk.

Click “**Browse**” and go to the location of the downloaded firmware file.

Select the file and click “**Upgrade**” to update the firmware to the latest release.

## Ping Test

The ping test enables users to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click Ping.



The screenshot displays the Trendnet web interface for a 150Mbps Wireless N Home Router (TEW-651BR). The interface features a dark grey background with a navigation menu on the left side. The menu includes options for Main, Wireless, Status, Routing, Access, Management, Tools, and Wizard. The Tools menu is expanded, showing sub-options for Restart, Settings, Firmware, and Ping Test. The main content area is titled "Ping Test" and contains a text input field labeled "Host Name or IP address:" with a "Ping" button next to it. A "Help" button is also visible in the top right corner of the main content area. The copyright notice "Copyright © 2009 TRENDnet. All Rights Reserved." is located at the bottom of the page.

## TECHNICAL SPECIFICATIONS

<b>Hardware</b>	
<b>Standards</b>	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX) Wireless: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n , IEEE 802.11e QoS
<b>WAN</b>	1 x 10/100Mbps Auto-MDIX port (Internet)
<b>LAN</b>	4 x 10/100Mbps Auto-MDIX ports
<b>WPS Button</b>	Enables Wi-Fi Protected Setup (WPS) function
<b>Connection Type</b>	Dynamic IP, Static (Fixed) IP, PPPoE, PPTP, L2TP, Big Pond
<b>UPnP</b>	UPnP IGD 1.0 compliant
<b>DMZ</b>	DMZ host & Virtual Servers
<b>DNS</b>	Static or WAN assigned DNS servers; 3 verified services for DDNS
<b>Internet Access Control</b>	MAC Address Filter, Domain/URL Filter, Protocol/IP Filter
<b>Logging</b>	5 types of event logging; email report
<b>LED Indicator</b>	Power, LAN1~LAN4, WAN, WLAN, Status
<b>Power Adapter</b>	5V DC, 1.2A external power adapter
<b>Power Consumption</b>	3.5watts (max)
<b>Dimension (L x W x H)</b>	150 x 110 x 30mm (5.9 x 4.3 x 1.2in)
<b>Weight</b>	225g (7.8oz)
<b>Temperature</b>	Operation: 0°~ 40°C (32°F~ 104°F); Storage: -10°~ 70°C (14°F~158 °F)
<b>Humidity</b>	Max. 90% (non-condensing)
<b>Certifications</b>	CE, FCC
<b>Wireless</b>	
<b>Frequency</b>	2.412~2.484GHz band
<b>Antenna</b>	1 x 2dBi fixed dipole antennas
<b>Media Access Protocol</b>	CSMA/CA with ACK
<b>Data Rate</b>	802.11b: up to 11Mbps 802.11g: up to 54Mbps 802.11n: up to 150Mbps
<b>Security</b>	WEP(HEX/ASCII): 64/128-bit WPA(AES/TKIP): WPA/WPA2-Radius, WPA-PSK/WPA2-PSK
<b>Output Power</b>	25 dBm
<b>Receiving Sensitivity</b>	802.11b: -85dBm (typical) @ 11Mbps 802.11g: -68dBm (typical) @ 54Mbps 802.11n: -62dBm (typical) @ 150Mbps
<b>Channels</b>	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-651BR – 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, NEGLIGENCE, 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



**TRENDNET<sup>®</sup>**

## Product Warranty Registration

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