TEW-452BRP

108Mbps 802.11g Wireless Firewall Router

User's Guide

TRENDnet®
TRENDware, USA
What's Next in Networking

Contents

1. Overview

1.1 Product Feature

- Compliance with IEEE 802.11g and 802.11b standards
- Highly efficient design mechanism to provide unbeatable performance
- Strong network security with WEP and 802.1X encryption
- Achieving data rate up to 54Mbps for 802.11g and 11Mps for 802.11b with wide range coverage; high performance to deliver up to 108Mbps raw data rate for 802.11g
- Quick and easy setup with Web-based management utility

1.2 System Requirements

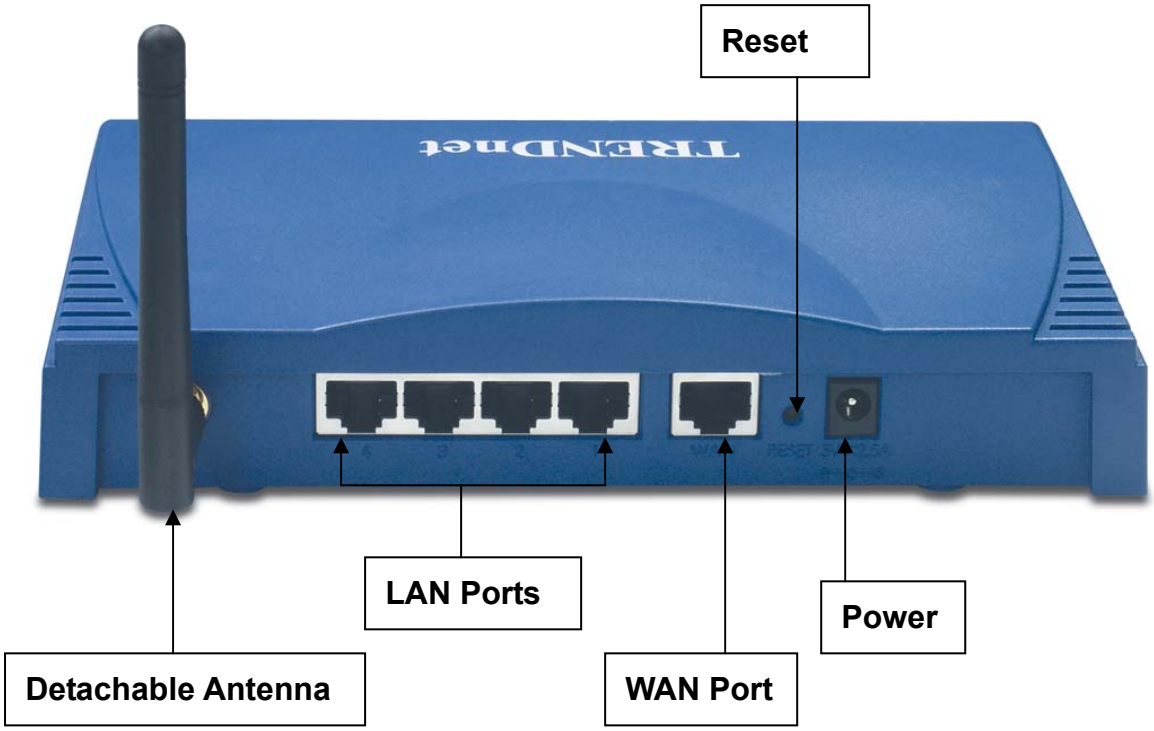
- Windows 98, 98SE, Millennium Edition (ME), 2000 and XP operating systems
- Microsoft Internet Explorer 5.5 or higher
- DSL/ Cable Modem Broadband Internet connection and ISP account
- PCs equipped with 10Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol
- One CD-ROM drive

1.3 Applications

- Home SOHO networking for device sharing and wireless multimedia
- Wireless office provides a wider range for home and SOHO Ethernet
- Enables wireless building-to-building data communication
- Built-in infrastructure mode
- Router provides ideal solution for:
- Difficult-to-wire environments
- Temporary LANs for scenarios such as trade-exhibitions and meetings
- Enables LAN adaptability to frequently changing environments
- Enables remote access to corporate network information, for example e-mail and the company home page

2. Getting Start

2.1 Know the 108Mbps Wireless Router



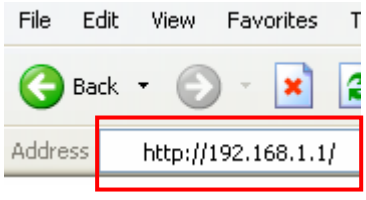
LEDs:

LED	Color	Status	Description
Power	Green	On	Indicates proper connection to power supply.
		OFF	The unit is not receiving power
Status	Green	On	Indicates that the device is connected to the WLAN.
WAN	On		Indicates connection to the WAN port
		Blinking	Data transmission.
WLAN	On		Link is established
	On	Blinking	Packet transmit or receive activity
	Off	—	No Link activity
LAN	On		Indicates connection is established.
	On	Blinking	Data transmissions
	Off	—	No LAN connections

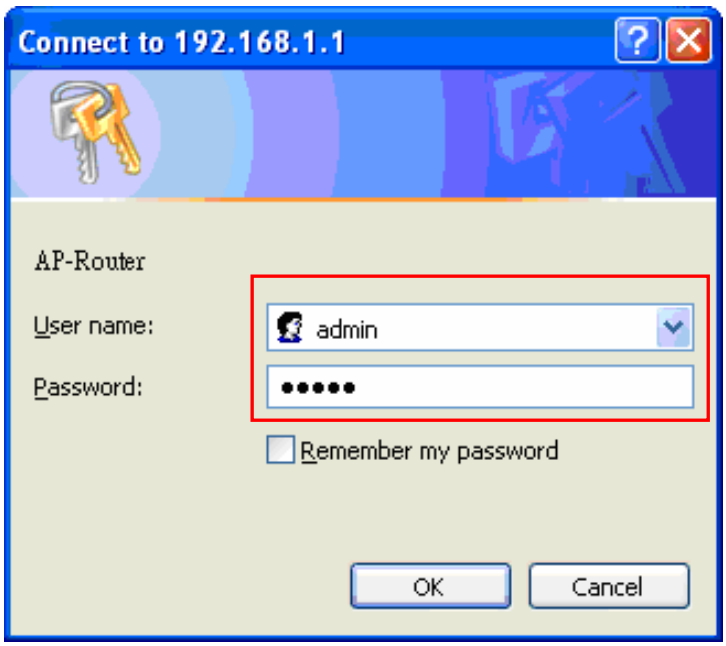
2.2 Connect to the 108Mbps Wireless Router

2.2.1 Access the Setting Menu

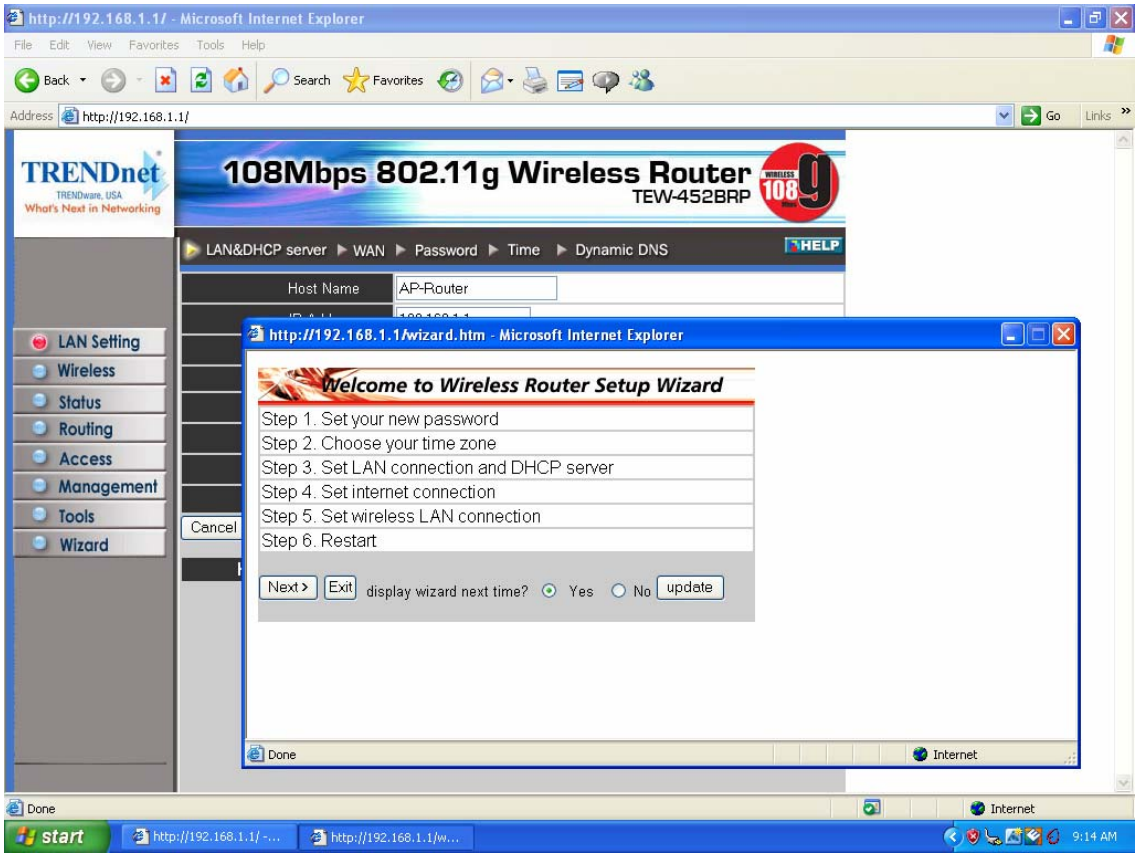
You could start to access the configuration menu anytime by opening a web browser window by typing the IP address of this wireless router. The default IP is 192.168.1.1.



The below window will popup. Please enter the user name and password. Both of the default is “admin”.

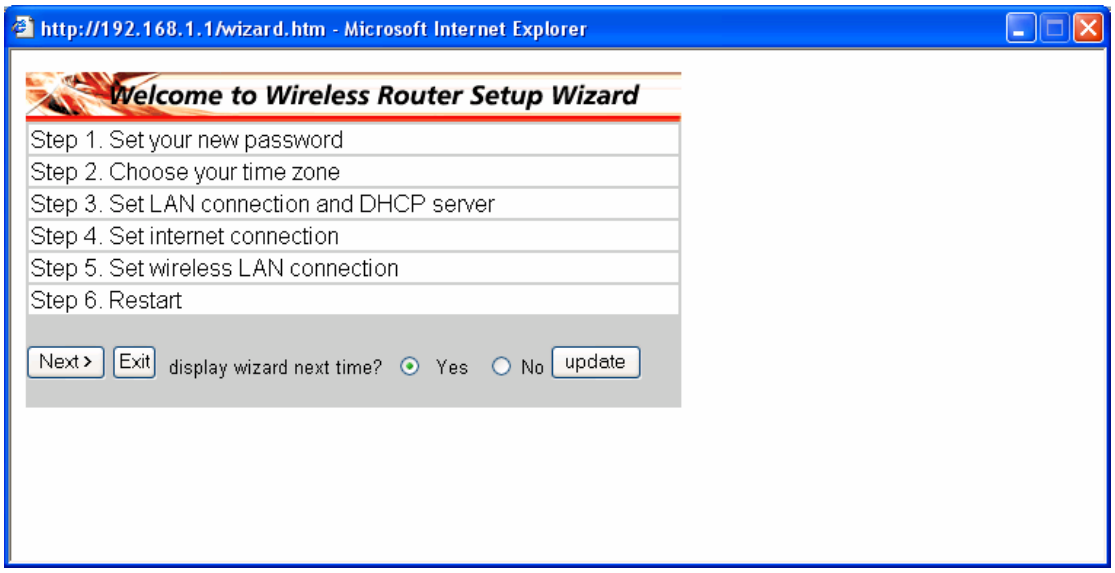


Now, the main menu screen is popup.



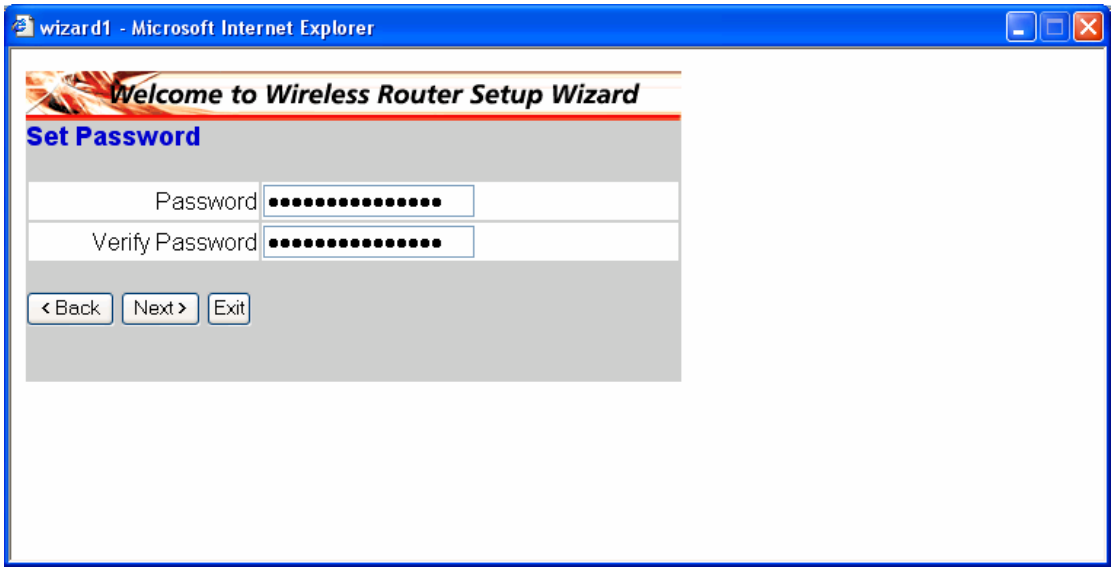
2.2.2 Quick Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. You can simply follow the step-by-step process to get your wireless router configuration ready to run in 6 easy steps by clicking on the "**Wizard**" button on the function menu. The following screen will appear. Please click "**Next**" to continue.



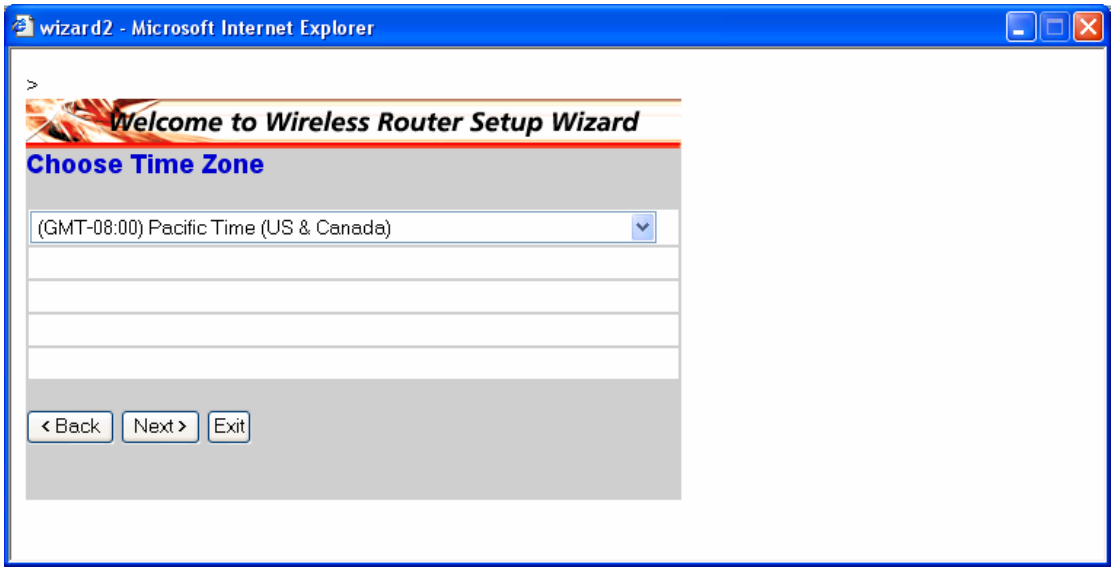
Step 1: Set your new Password

You can change the password as you like and then click "**Next"** to continue.



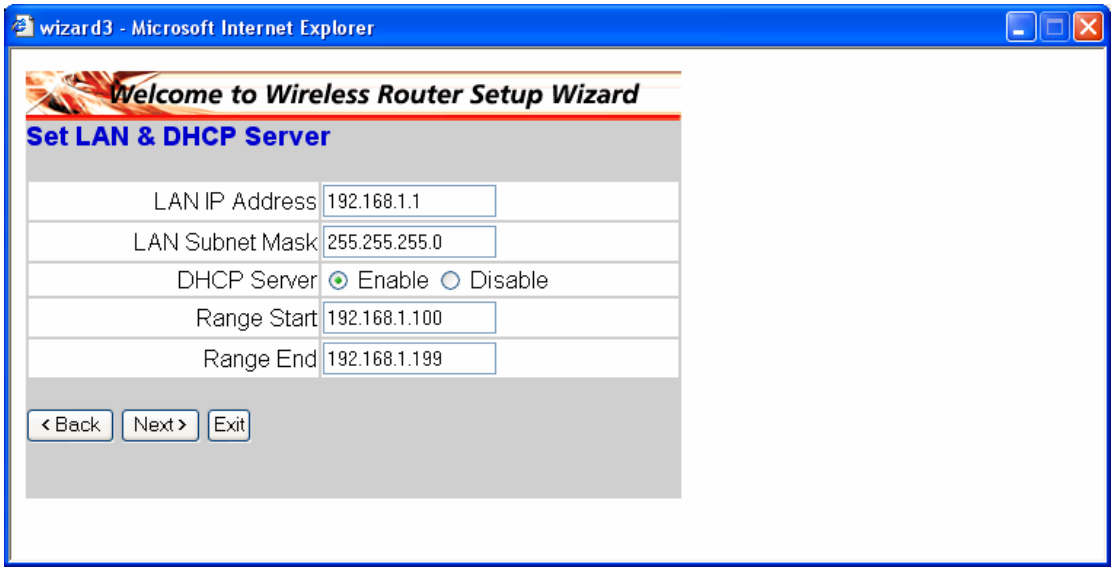
Step2: Choose your time zone

Select your time zone from the drop down list. Please click "**Next"** to continue.



Step 3: Set LAN connection and DHCP server

Set your IP address and mask. The default IP is 192.168.1.1. If you like to enable DHCP, please click "**Enabled**". DHCP enabled is able to automatically assign IP addresses. Please assign the range of IP addresses in the fields of **"Range start"** and **"Range end"**. Please click "**Next"** to continue.

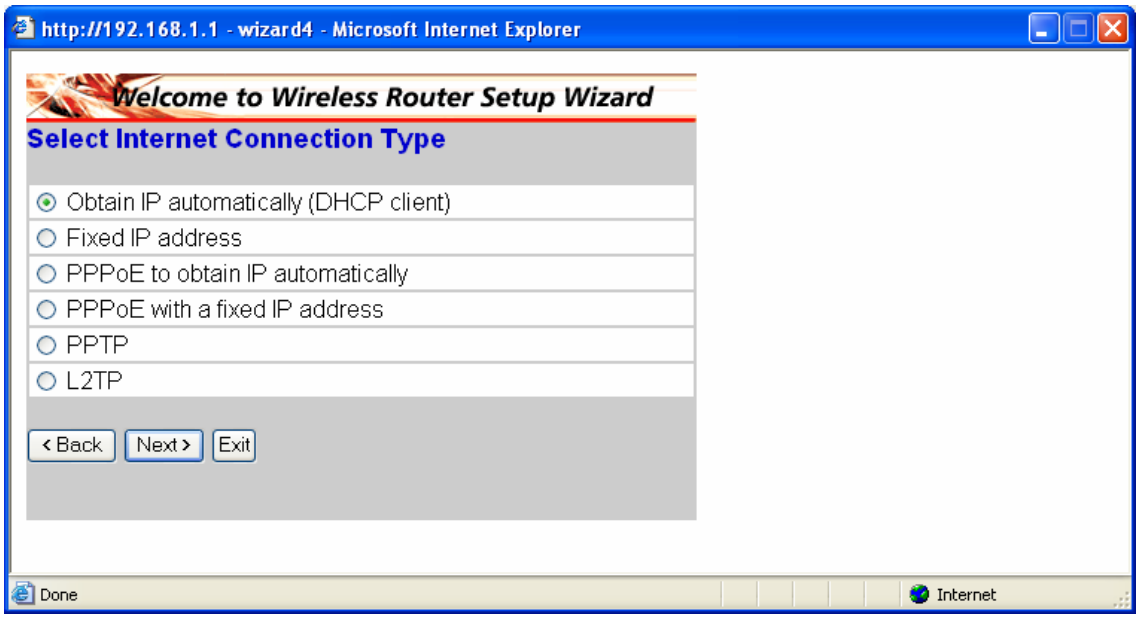


Step 4: Set Internet connection

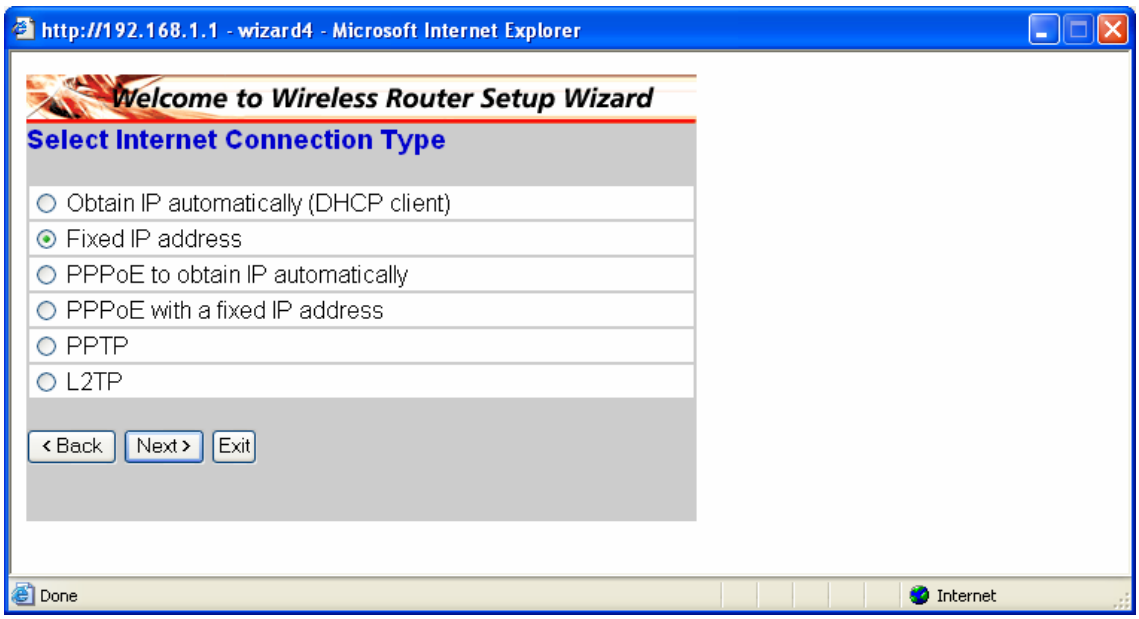
Select how the router will set up the Internet connection: Obtained IP automatically; Fixed IP address; PPPoE to obtain IP automatically; PPPoE with a fixed IP address; PPTP.

Obtain IP automatically (DHCP client):

If you have enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.

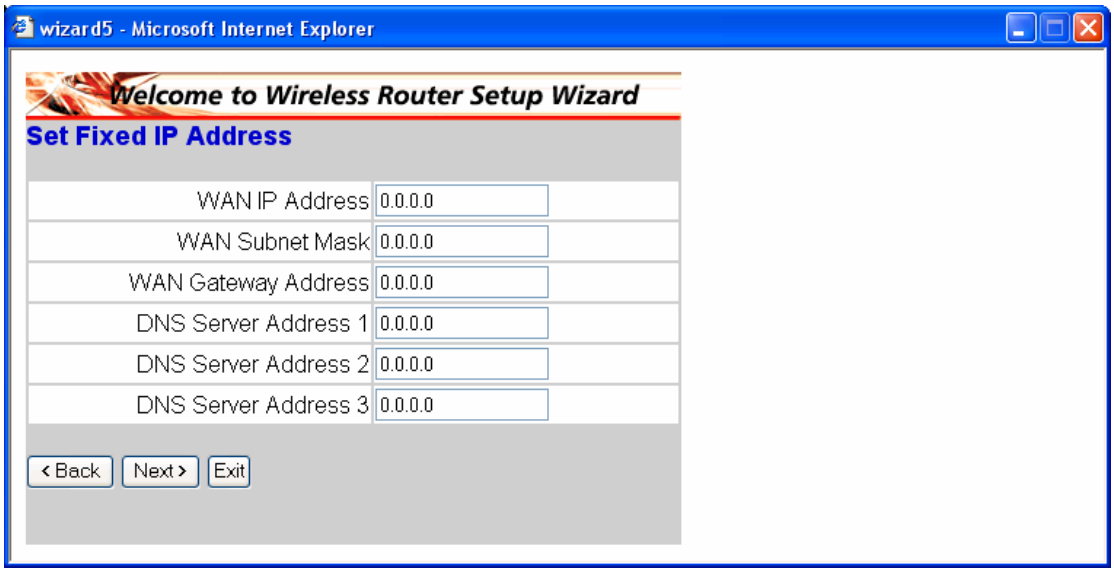


Fixed IP Address:

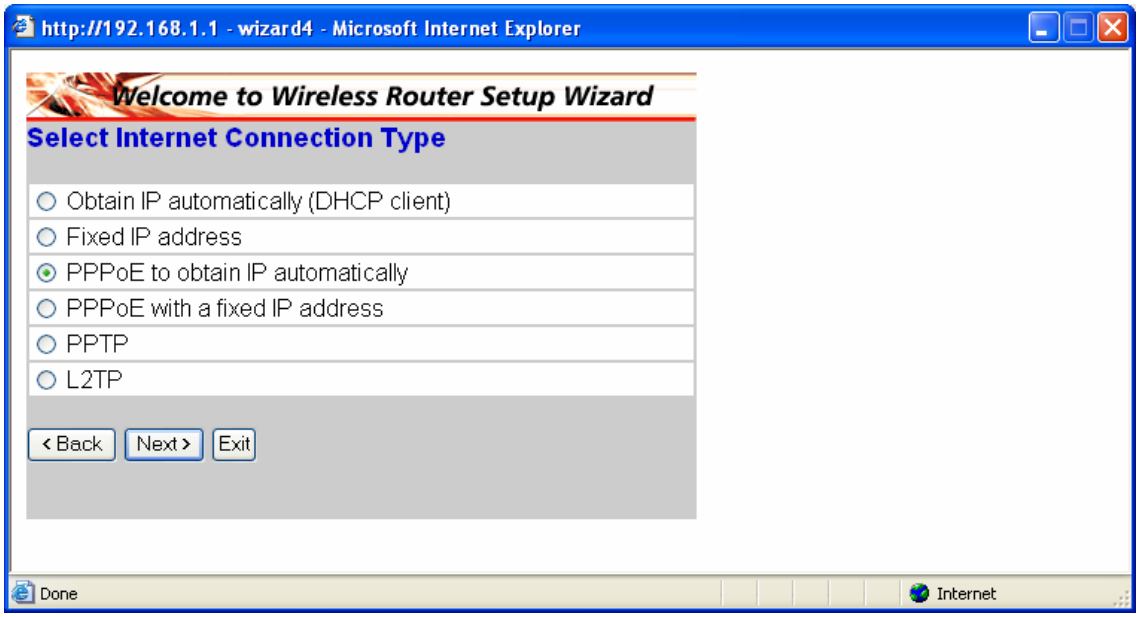


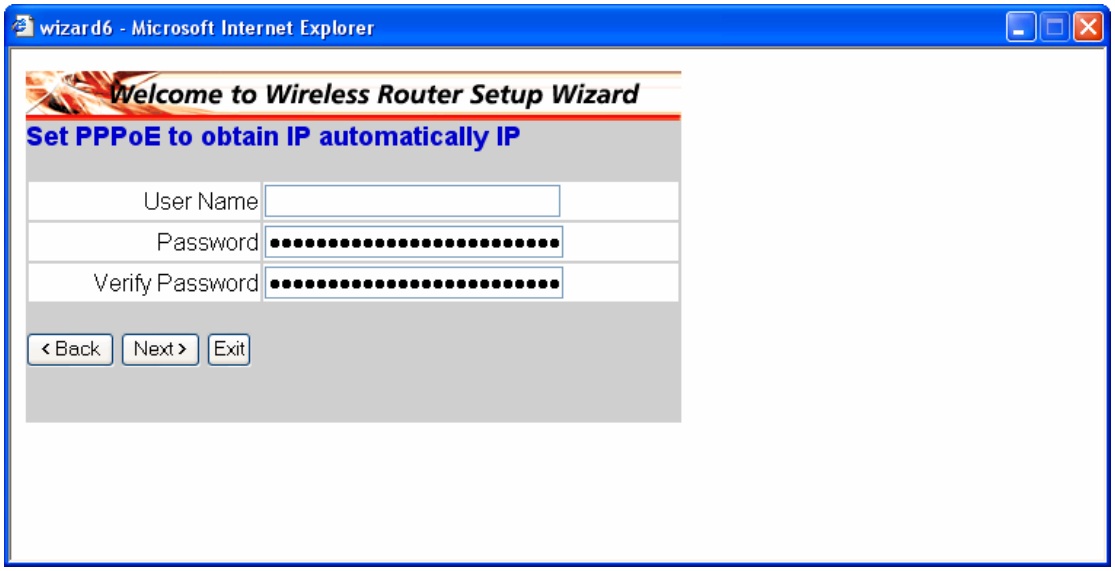
If Fixed IP address is assigned, the below screen will pop up. Please set the WAN

address and DNS server.

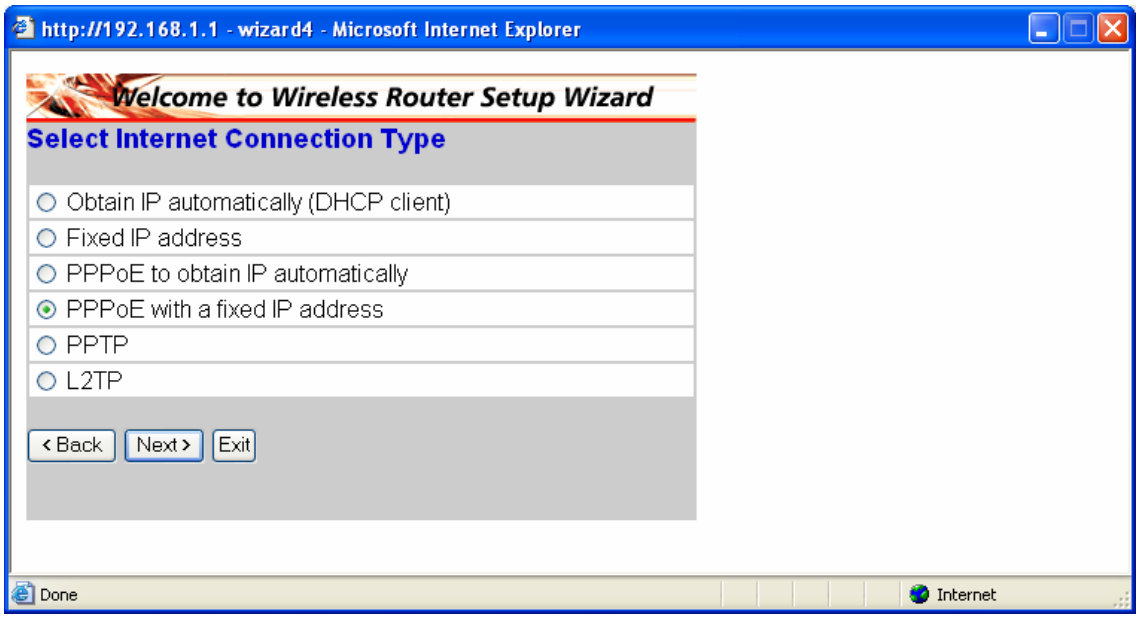


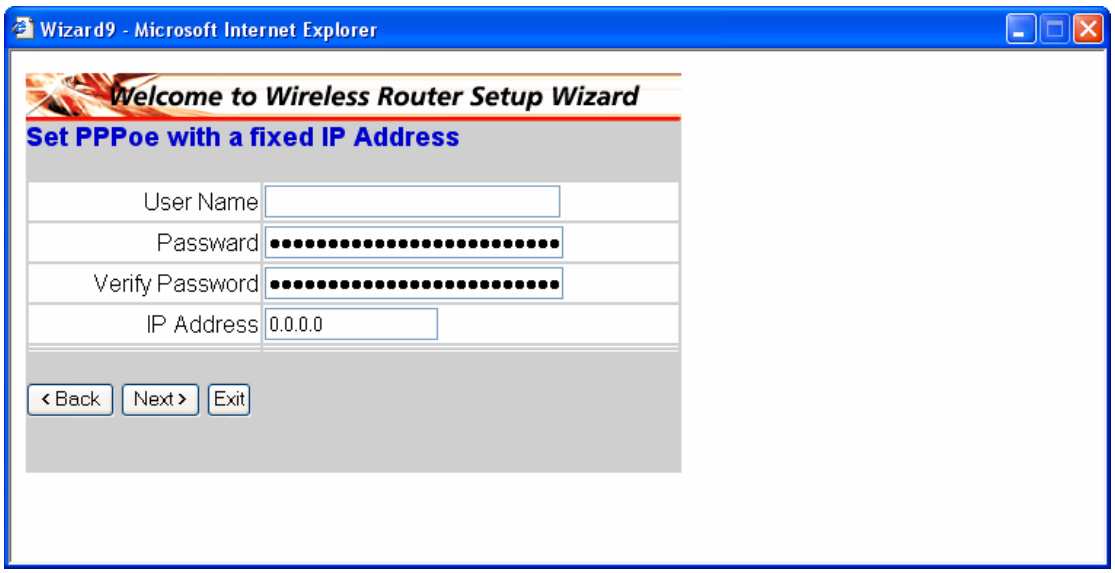
PPPoE to obtain IP automatically:



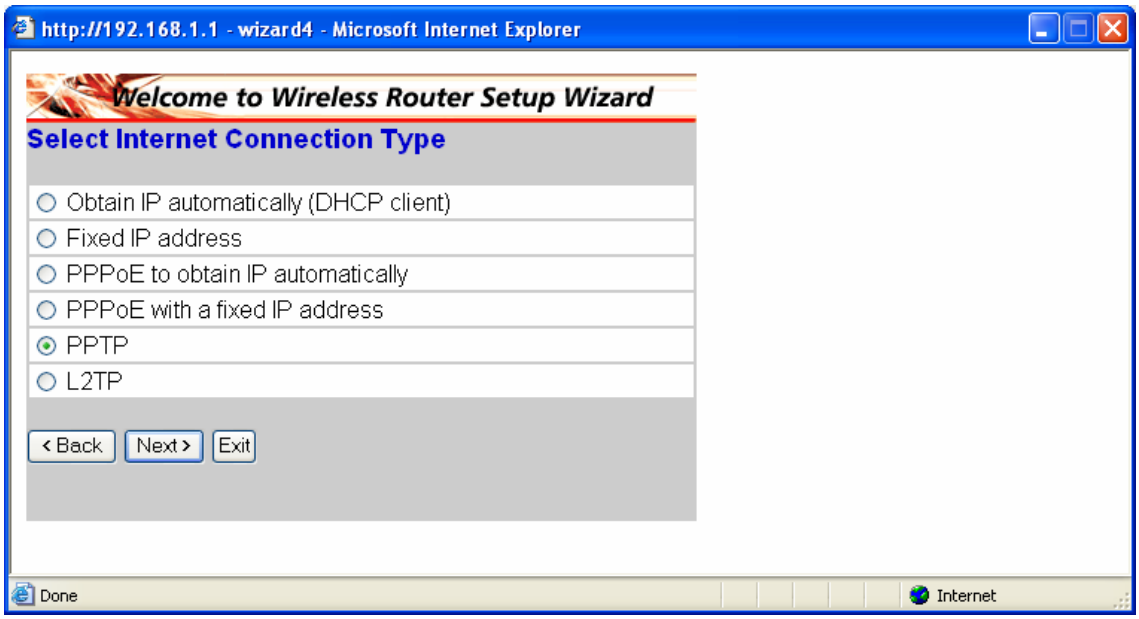


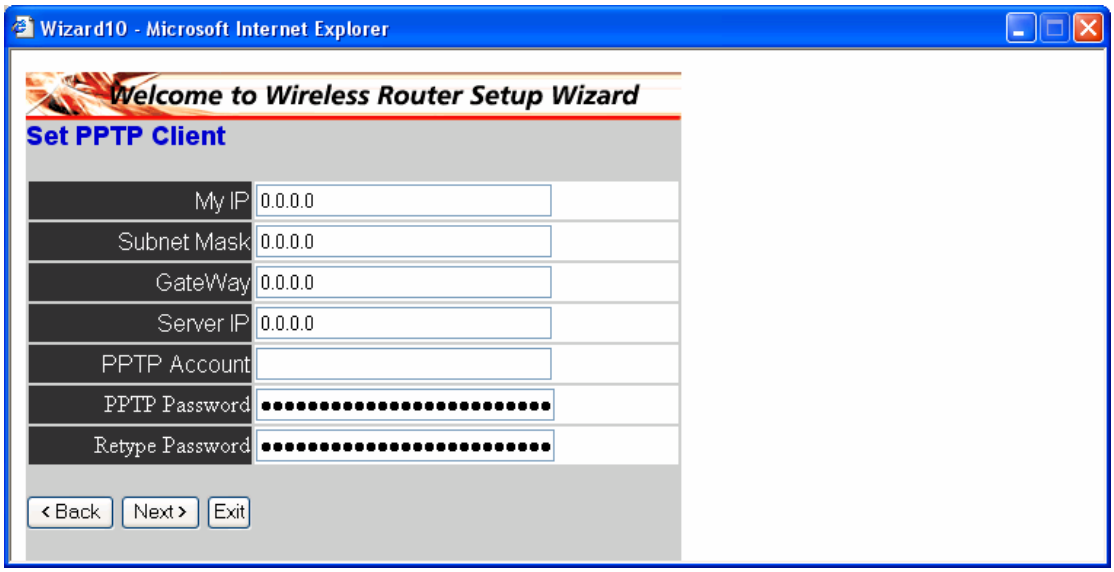
PPPoE with a fixed IP address:



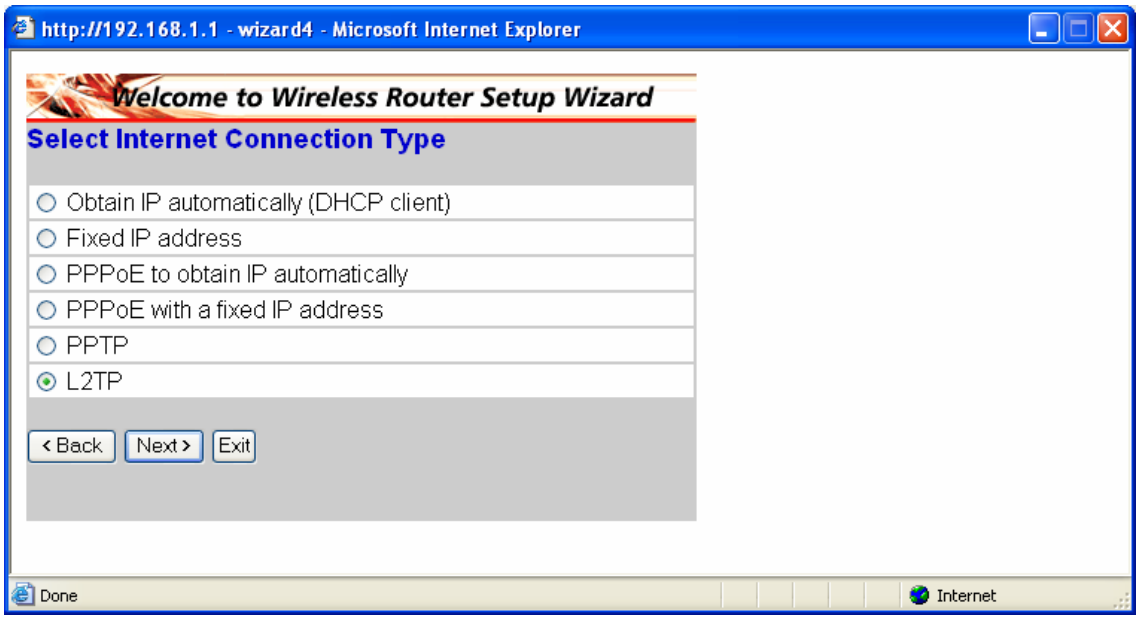


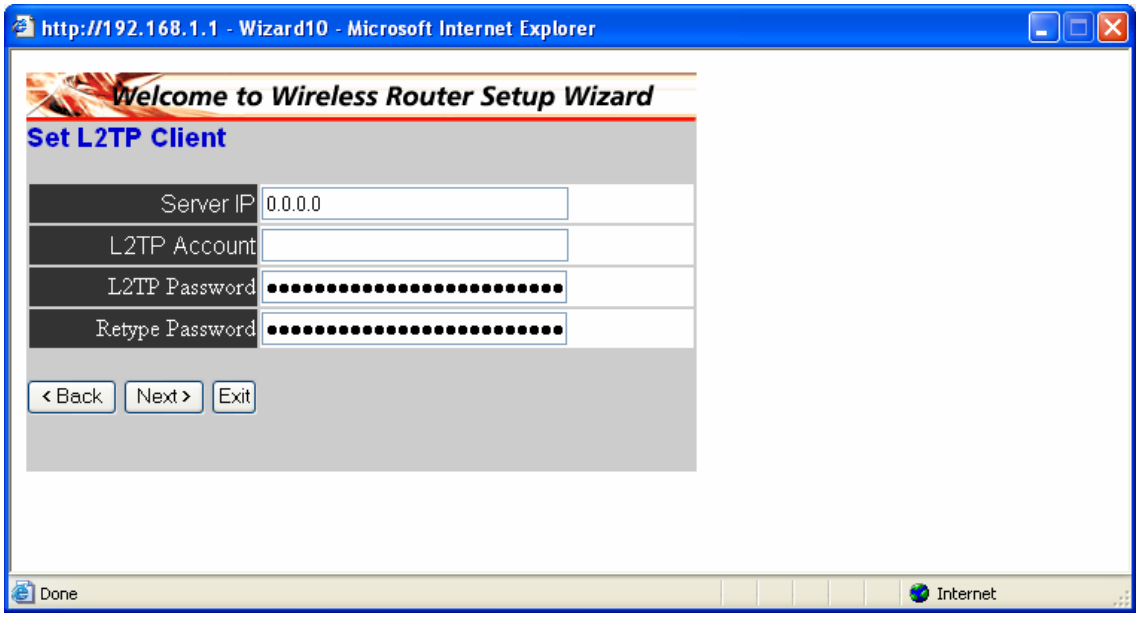
PPTP:


http://192.168.1.1 - wizard4 - Microsoft Internet Explorer
Welcome to Wireless Router Setup Wizard
Select Internet Connection Type
Obtain IP automatically (DHCP client)
Fixed IP address
PPPoE to obtain IP automatically
PPPoE with a fixed IP address
PPTP
L2TP
< Back
Next >
Exit
Done
Internet


Wizard10 - Microsoft Internet Explorer
Welcome to Wireless Router Setup Wizard
Set PPTP Client
My IP
0.0.0.0
Subnet Mask
0.0.0.0
GateWay
0.0.0.0
Server IP
0.0.0.0
PPTP Account
PPTP Password
Retype Password
< Back
Next >
Exit

L2TP:


http://192.168.1.1 - wizard4 - Microsoft Internet Explorer
Welcome to Wireless Router Setup Wizard
Select Internet Connection Type
Obtain IP automatically (DHCP client)
Fixed IP address
PPPoE to obtain IP automatically
PPPoE with a fixed IP address
PPTP
L2TP
< Back
Next >
Exit
Done
Internet

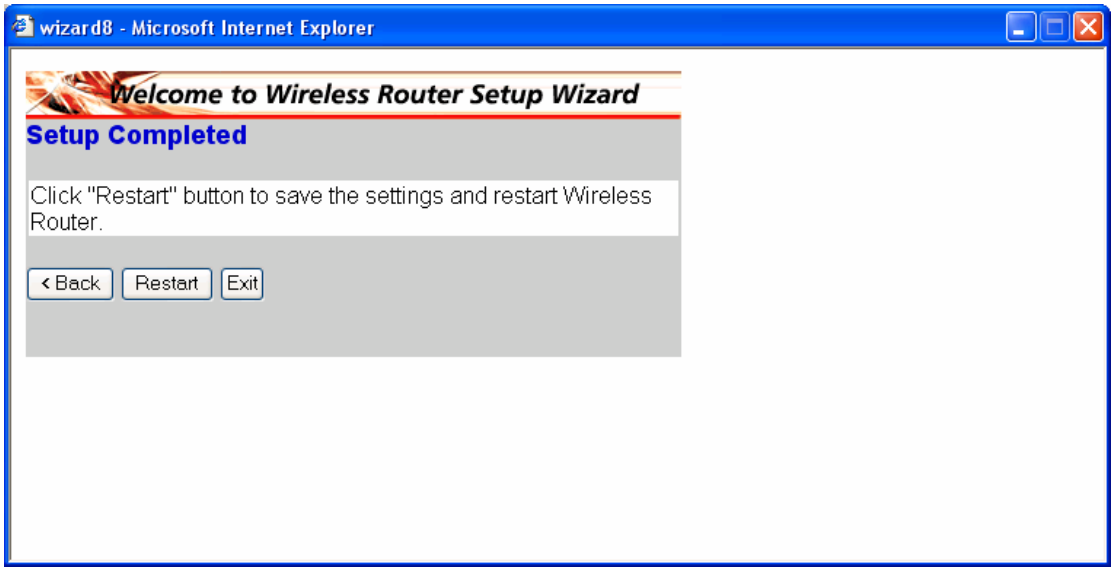

http://192.168.1.1 - Wizard10 - Microsoft Internet Explorer
Welcome to Wireless Router Setup Wizard
Set L2TP Client
Server IP
0.0.0.0
L2TP Account
L2TP Password
Retype Password
< Back
Next >
Exit
Done
Internet

Step 5: Set Wireless LAN connection

Click “enable” to enable wireless LAN. If you enable the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.

Step 6: Restart

The Setup wizard is now completed. The new settings will be effective after the Wireless router restarted. Please click “**Restart**” to reboot the router. If you do not want to make any changes, please click “**exit**” to quit without any changes. You also can go back to modify the setting by clicking “**Back**”.



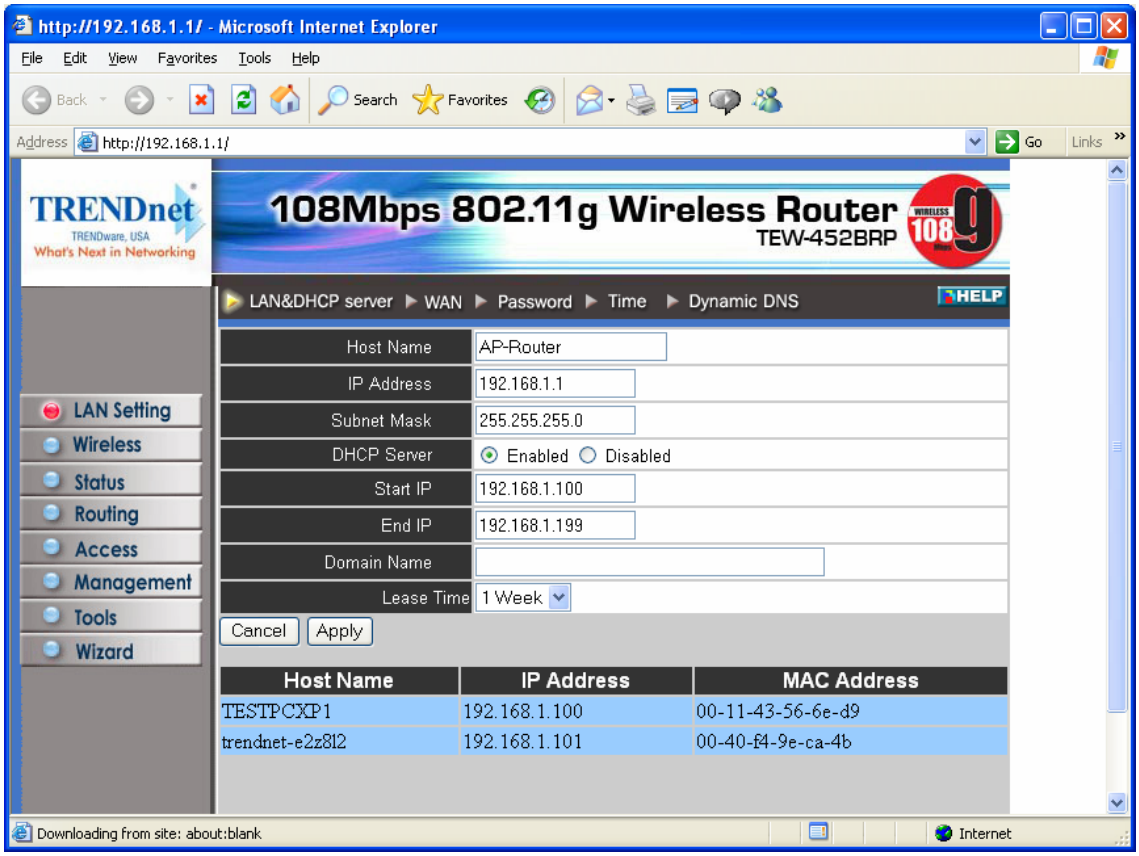
3. Configuration

3.1 LAN Setting

The screen enables you to configure the LAN & DHCP Server, set WAN parameters, create Administrator and User passwords, and set the local time, time zone, and dynamic DNS.

3.1.1 LAN & DHCP Server

This page enables you to set LAN and DHCP properties, such as the host name, IP address, subnet mask, and domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.



Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "AP-Router."

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0.

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

All DHCP client computers are listed in the table at the bottom of the screen, providing

the host name, IP address, and MAC address of the client.

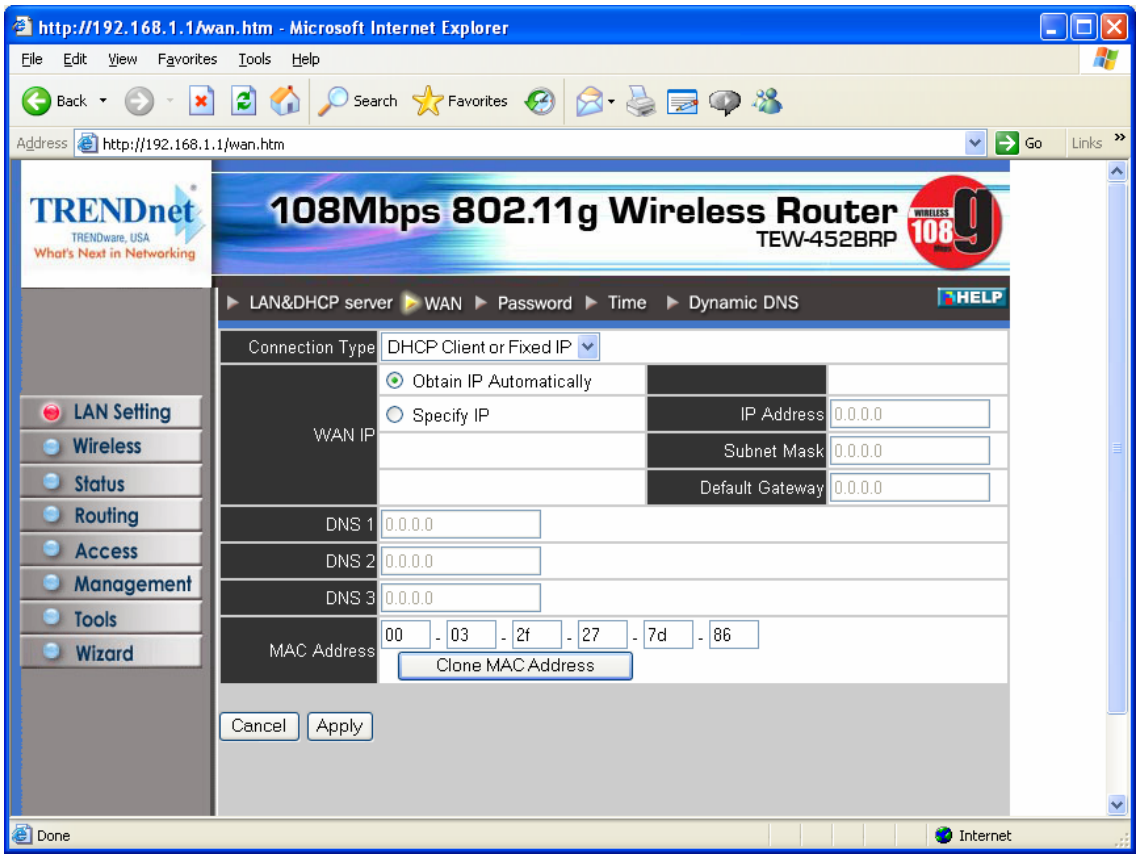
Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Domain Name: Type the local domain name of the network in the text box. This item is optional.

3.1.2 WAN

This screen enables you to set up the router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.



Connection Type: Select the connection type, either DHCP client, Fixed IP or PPPoE from the drop-down list.

WAN IP: Select whether you want to specify an IP address manually, or want DHCP to obtain an IP address automatically. When *Specify IP* is selected, type the IP address, subnet mask, and default gateway in the text boxes. Your ISP will provide you with this information.

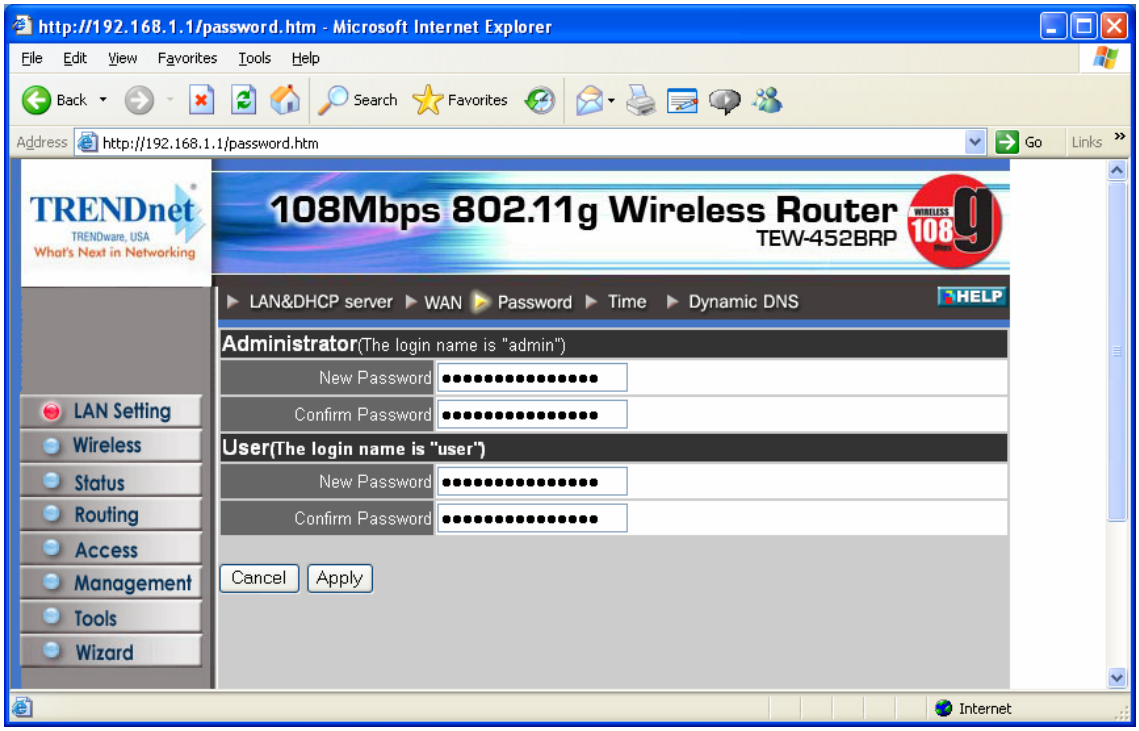
DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

MAC Address: If required by your ISP, type the MAC address of the router WAN interface in this field.

DNS 1/2/3: Type up to three DNS numbers in the text boxes. Your ISP will provide you with this information.

3.1.3 Password

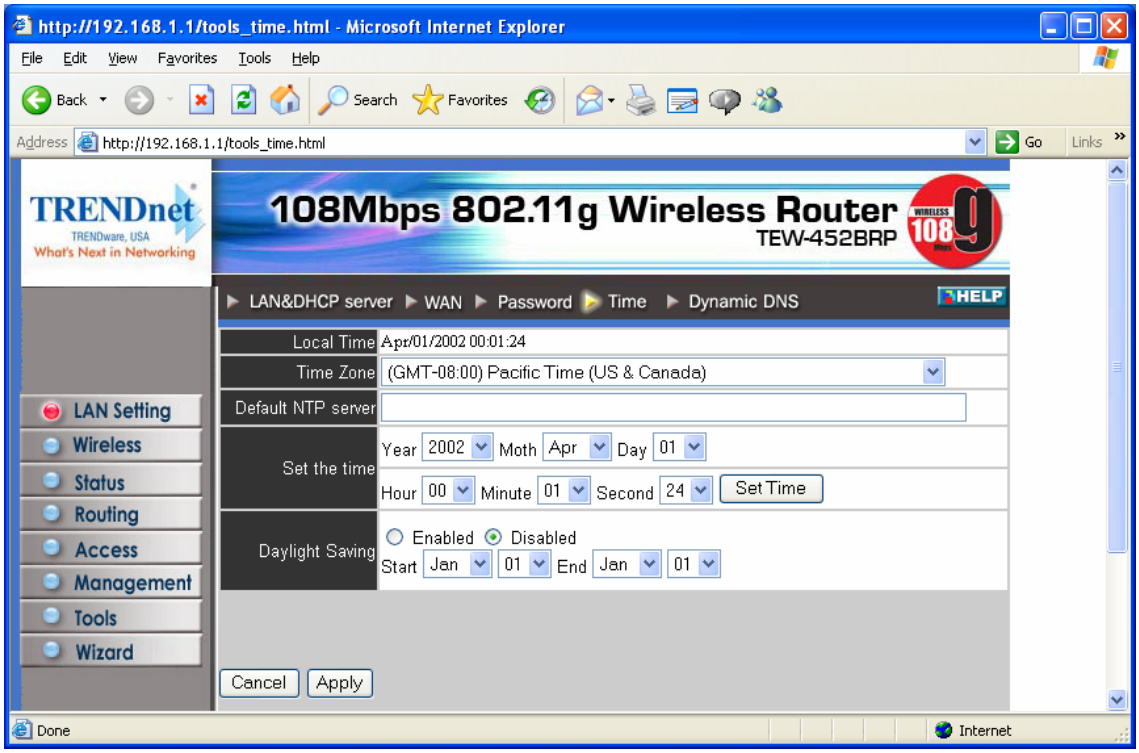
This screen enables you to set administrative and user passwords. These passwords are used to gain access to the router interface.



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

3.1.4 Time

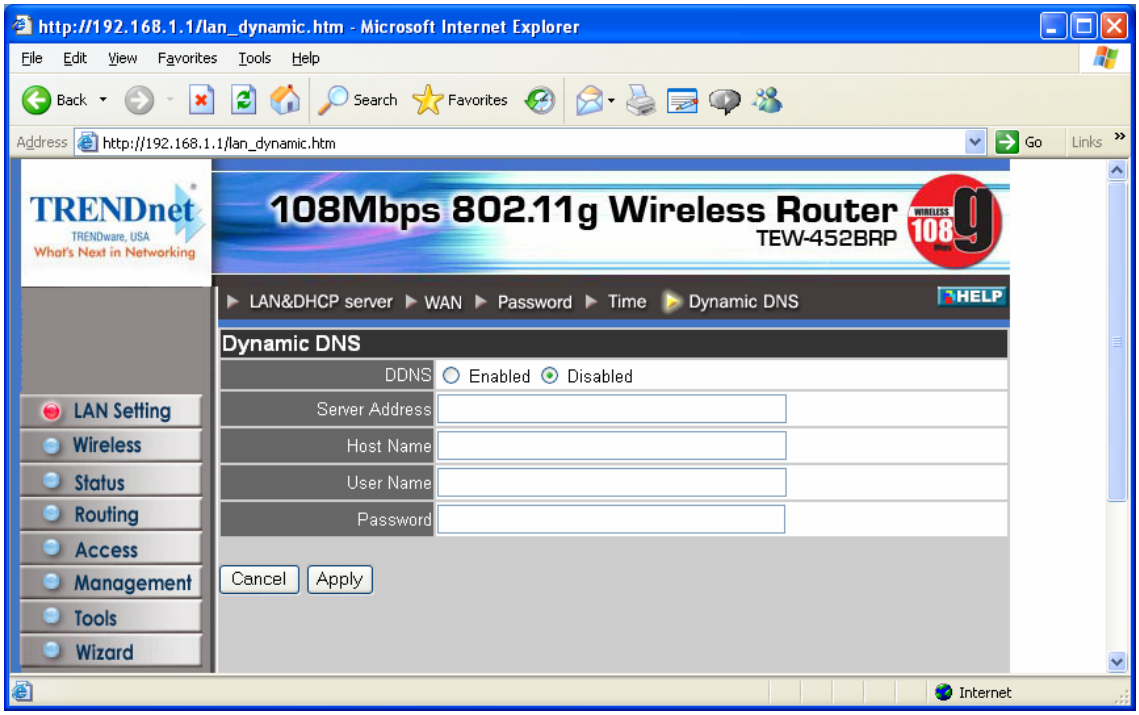
This screen enables you to set the time and date for the router's real-time clock, select your time zone, and enable or disable daylight saving.



Local Time: Displays the local time and date.
Time Zone: Select your time zone from the drop-down list.
Daylight Saving: Enables you to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

3.1.5 Dynamic DNS

This allows the DDNS server what your current IP address is when you are on-line. You firstly need to register your preferred DNS on the DDNS providers. Then, please fill the related information in the below fields: DDNS server address, Host Name, User Name and Password.

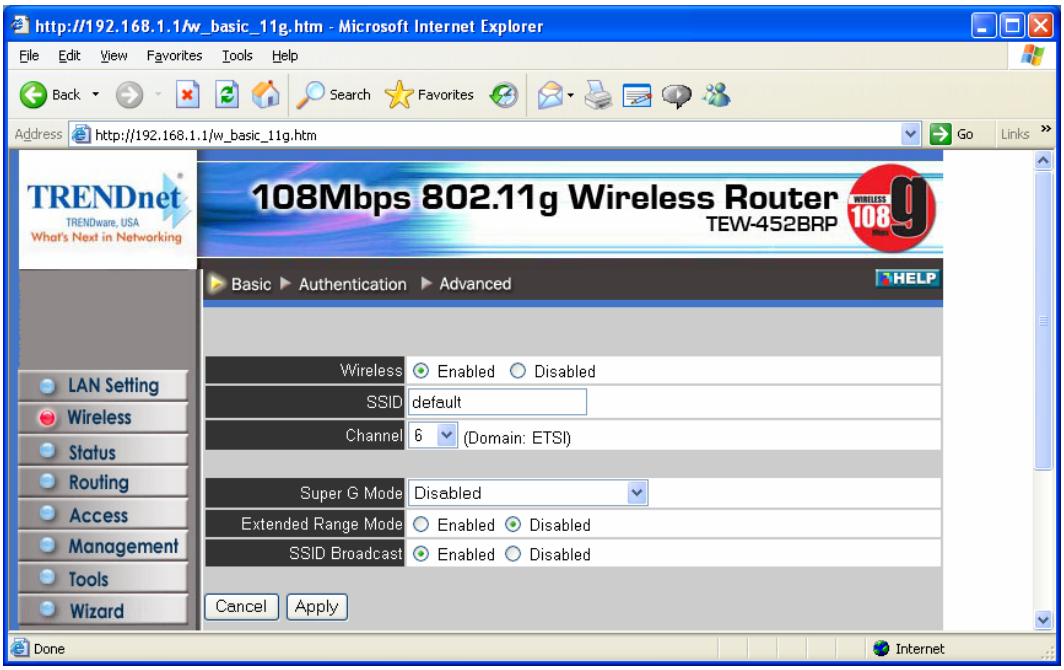


3.2 Wireless

This section enables you to set wireless communications parameters for the router's wireless LAN feature.

3.2.1 Basic

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



Enable/Disable: Enables and disables wireless LAN via the 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 router.

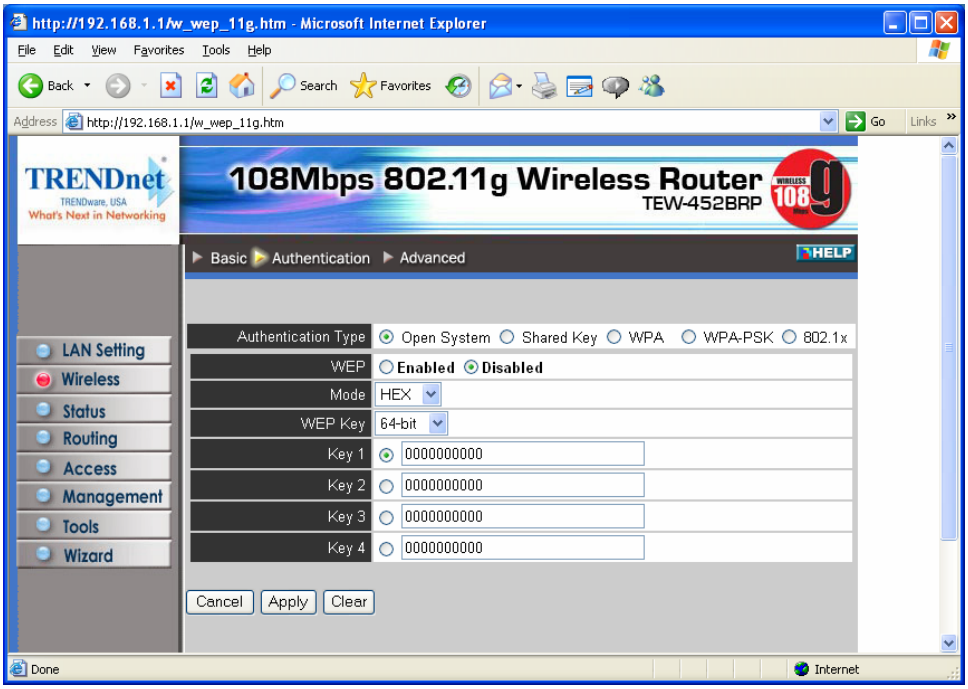
Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

Super G mode: Super G mode is disabled by selecting “Disable” from the drop list. If you like to use Super G to enhance the speed, there are three options on Super G mode: Super G without turbo; Super G with Dynamic turbo and Super G with Static turbo. Turbo mode indicates the combination of two channels to enhance the throughput. Super G without turbo indicates that it is on Super G mode without the channel’s combination. Dynamic turbo is able to automatically detect if any ‘SuperG based’ product is available. If no, the connection is via ‘normal’ G.. Static turbo means it will not go back to ‘normal’ G once it starts.

Extended Range Mode: Enable and disable wireless LAN via router.

3.2.2 Authentication

This screen enables you to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications. Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key. This router also support WPA, WPA-PSK and 802.1X.



Authentication Type: The authentication type default is set to open system. There are five options: Open System; Shared Key; WPA; WPA-PKS and 802.1X.

WEP: Enable or Disabled.
Mode: Select the level of encryption you want from the drop-down list. The router supports, 64- and 128-bit encryption.
WEP Key: Select WEP Key - 64 or 128 bits from the drop-down list.
Key 1 ~ Key 4: Enables you to create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select which key you want to use by clicking the radio button next to the key. Click **Clear** to erase key values.
If **WPA** or **802.1X** is selected, the below screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.
Lifetime: Select the Lifetime of the Encryption Key from 5 Minutes to 1 Day. As soon as the lifetime of the Encryption Key is over, the Encryption Key will be renewed by the Radius server.
Encryption Key: Select the Encryption Key Length Size ranging from 64 to 128 Bits that you would like to use.
RADIUS Server:

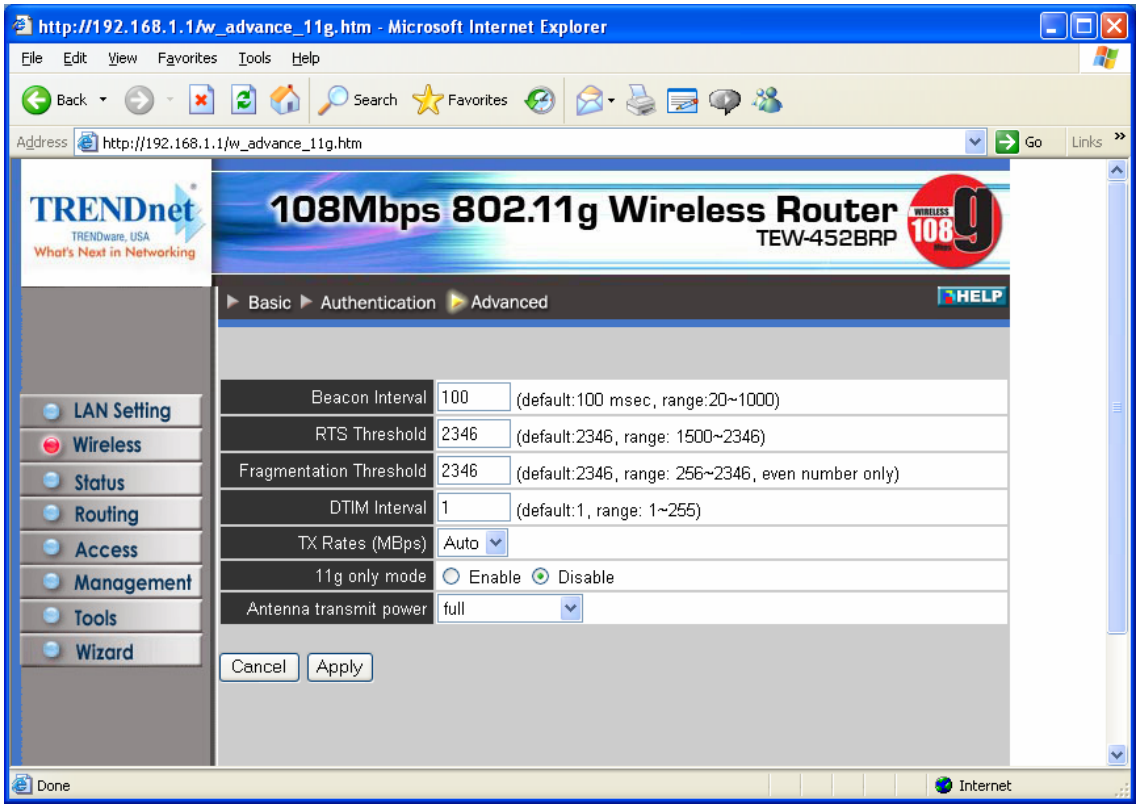
1. Enter the **IP address** of and the **Port** used by the **Primary** Radius Server

   Enter the **Shared Secret**, which is used by the Radius Server.
2. Enter the **IP address** of, **Port** and **Shared Secret** used by the **Secondary** Radius Server.

Note: As soon as 802.1X security is enabled, all the wireless client stations that are connected to the Router currently will be disconnected. The wireless clients must be configured manually to authenticate themselves with the Radius server to be reconnected.
If **WPA-PSK** is selected, please set the PSK key in the passphrase field. The length should be 8 characters at least.

3.2.3 Advanced

This screen enables you to configure advanced wireless functions.



Beacon Interval: Type the beacon interval in the text box. You can specify a value from 1 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 2432 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 256 and 2432 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. You can specify a value between 1 and 65535. The default value is 3.

TX Rates (MBps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

11g only mode: enable or disable.

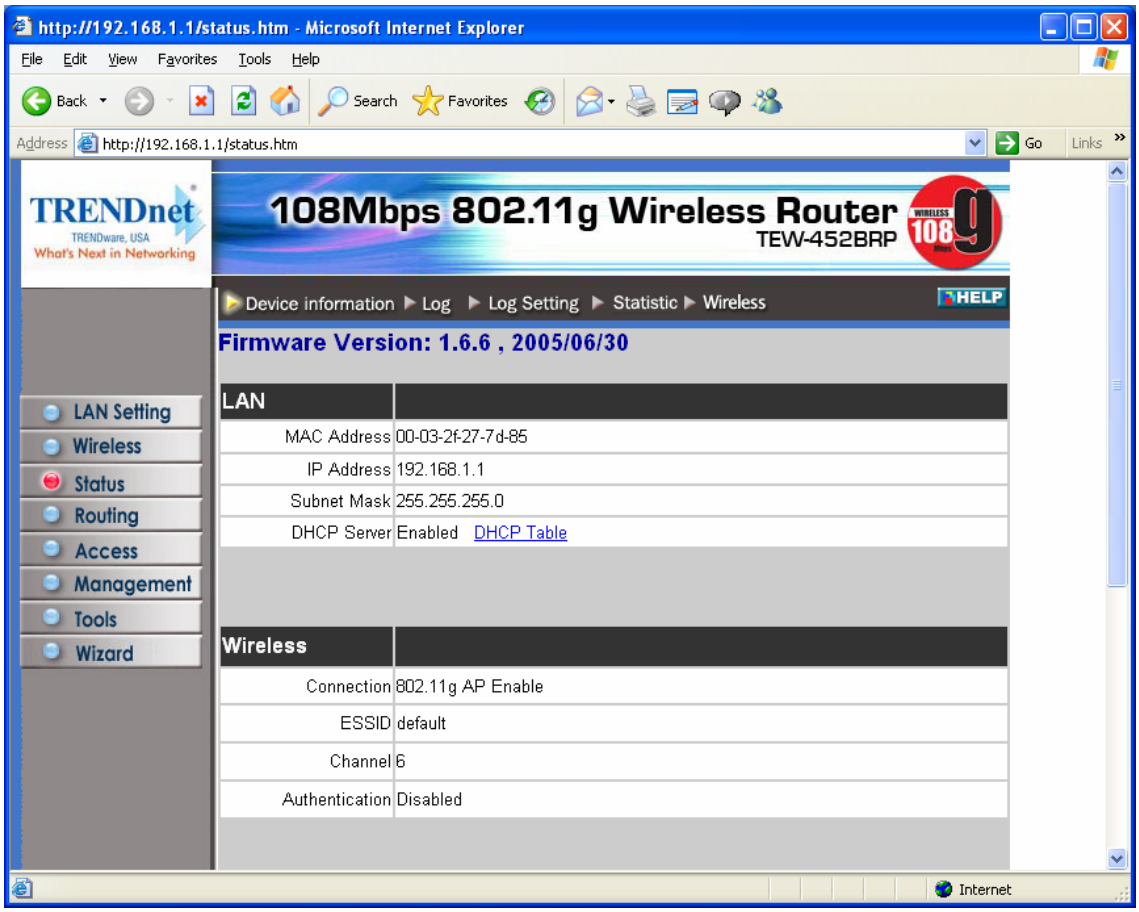
Antenna Transmit Power: Adjust the power of the antenna transmission by selecting from the dropping list.

3.3 Status

This selection enables you to view the status of the router LAN, WAN connections, and view logs and statistics pertaining to connections and packet transfers.

3.3.1 Device Information

This screen enables you to view the router LAN, Wireless and WAN configuration.



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

LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click *DHCP Table* to view a list of client stations currently connected to the router LAN interface.

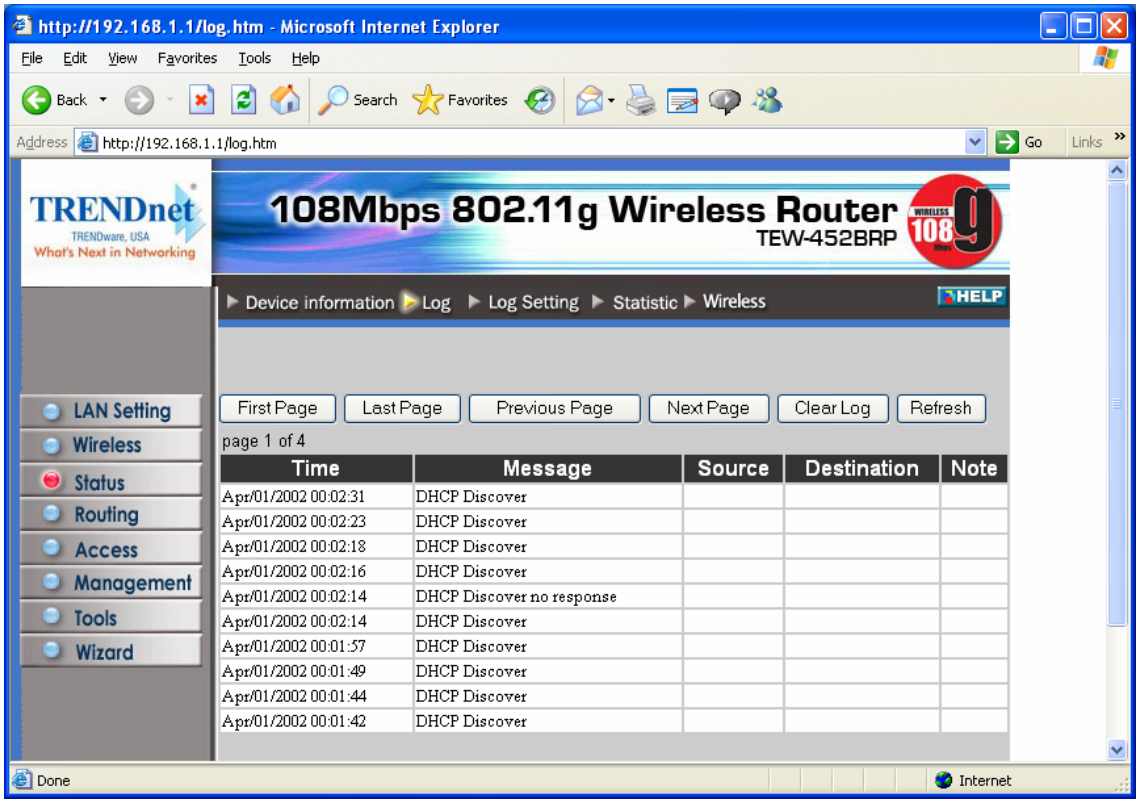
Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether WEP is enabled or not.

WAN: This field displays the router's WAN interface MAC address, DHCP client status,

IP address, subnet mask, default gateway, and DNS.
Click *DHCP Release* to release all IP addresses assigned to client stations connected to the WAN via the router. Click *DHCP Renew* to reassign IP addresses to client stations connected to the WAN.

3.3.2 Log

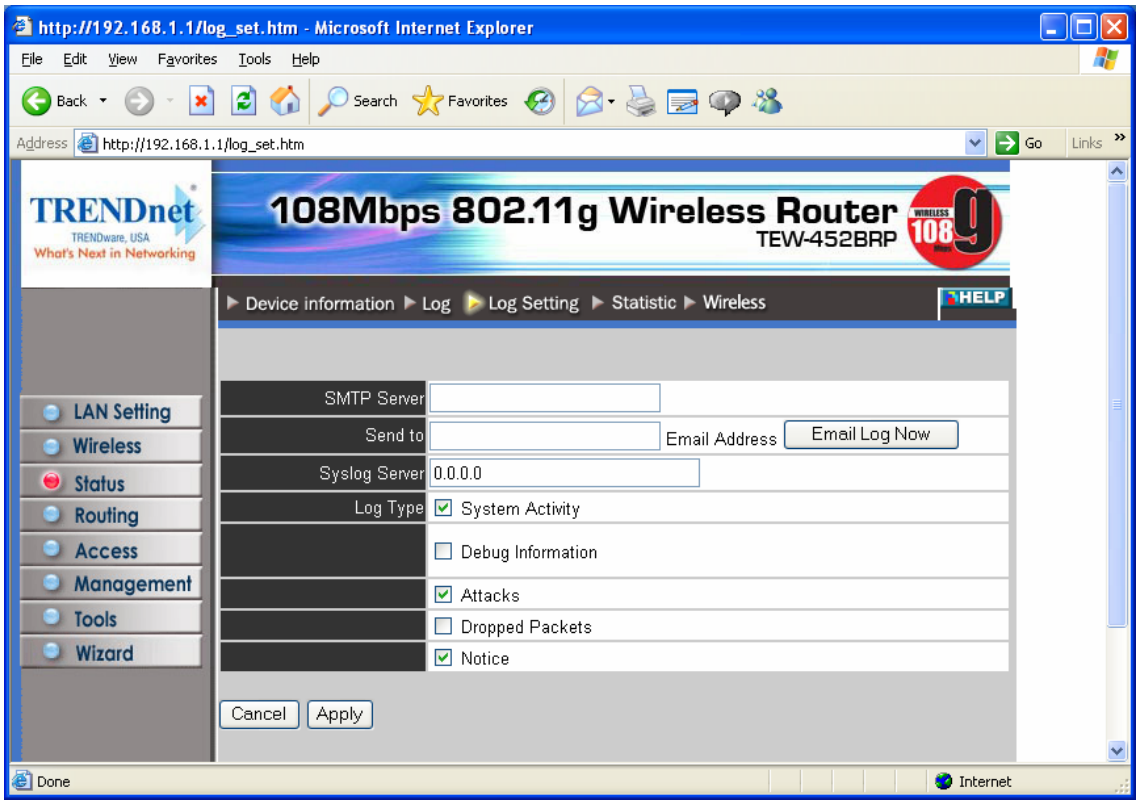
This screen enables you to view a running log of router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:
Click *First Page* to view the first page of the log
Click *Last Page* to view the 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



Time: Displays the time and date that the log entry was created.
Message: Displays summary information about the log entry.
Source: Displays the source of the communication.
Destination: Displays the destination of the communication.
Note: Displays the IP address of the communication

3.3.3 Log Setting

This screen enables you to set router logging parameters.



SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.

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

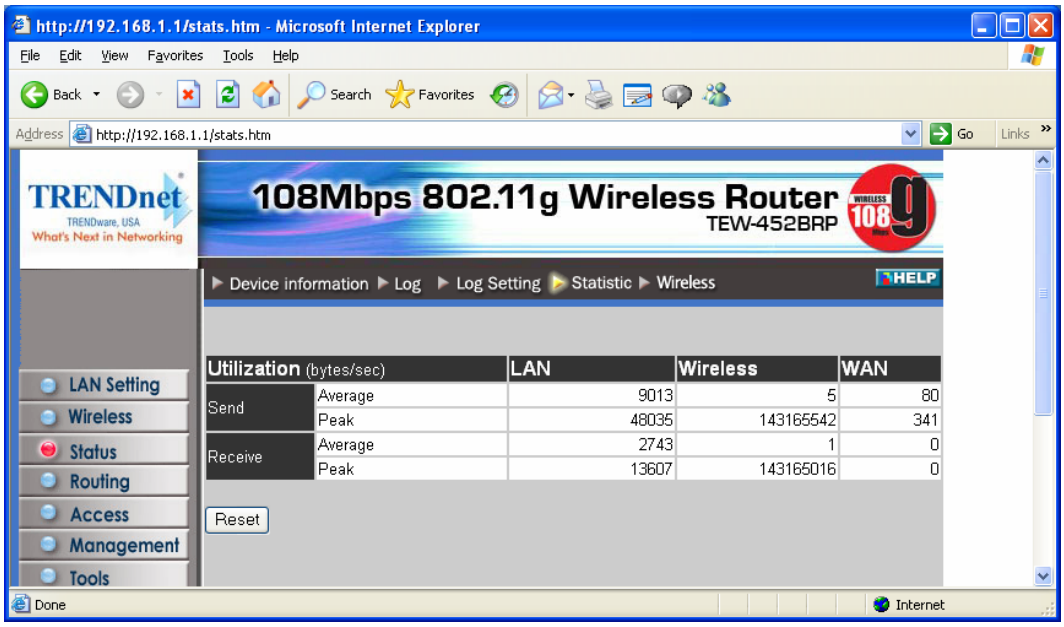
Syslog Server: Type the IP address of the Syslog Server if you want the router to listen and receive incoming Syslog messages.

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

- **System Activity:** Displays information related to router operation.
- **Debug Information:** Displays information related to errors and system malfunction.
- **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.

3.3.4 Statistic

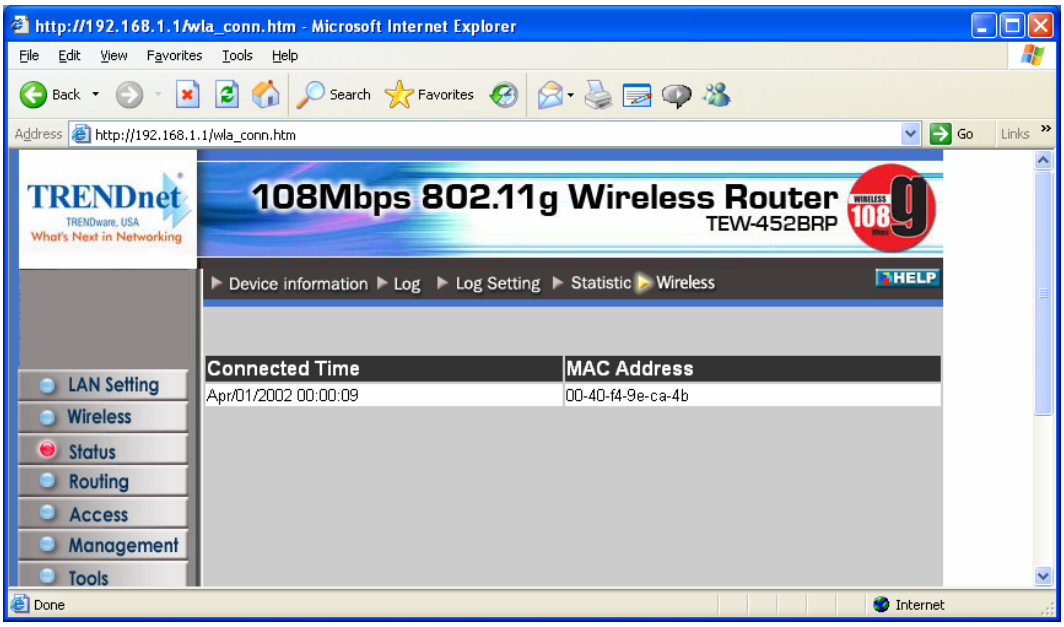
This screen displays a table that shows the rate of packet transmission via the router LAN and WAN ports (in bytes per second).



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

3.3.5 Wireless

This screen enables you to view information about wireless devices that are connected to the wireless router.



Connected Time: Displays how long the wireless device has been connected to the

LAN via the router.

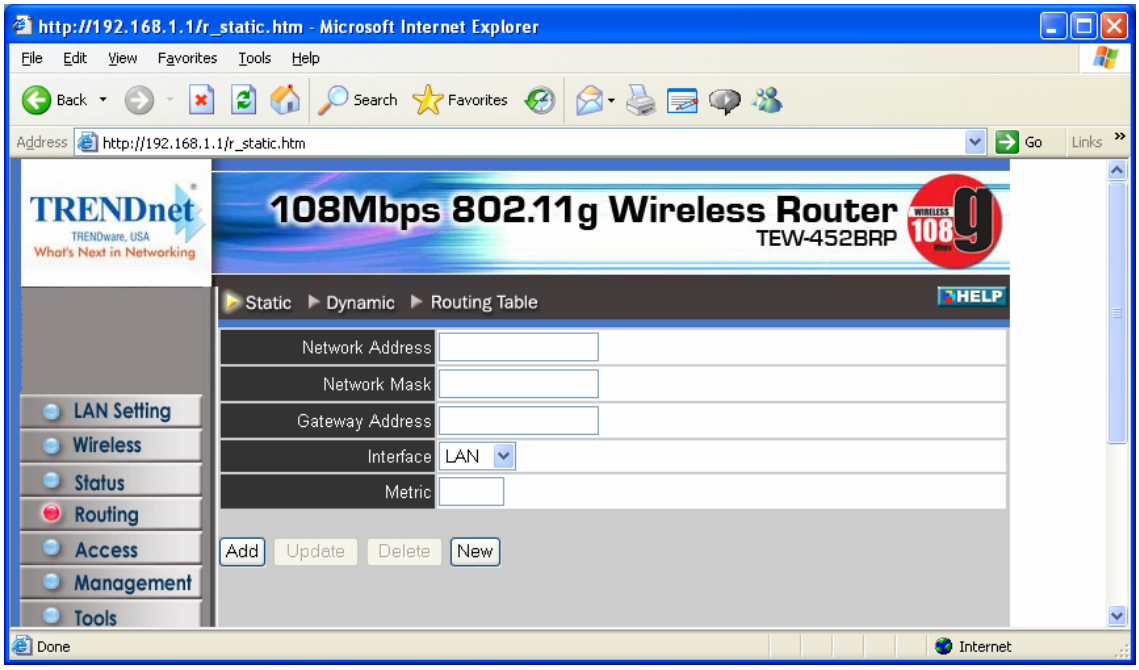
MAC Address: Displays the devices wireless LAN interface MAC address.

3.4 Routing

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

3.4.1 Static

It enables you to set parameters by which the router forwards data to its destination if your network has a static IP address.



Network Address: Type the static IP address your network uses to access the Internet. Your ISP or network administrator provides you with this information.

Network Mask: Type the network (subnet) mask for your network. If you do not type a value here, the network mask defaults to 255.255.255.255. Your ISP or network administrator provides you with this information.

Gateway Address: Type the gateway address for your network. Your ISP or network administrator provides you with this information.

Interface: Select which interface, WAN or LAN, you use to connect to the Internet.

Metric: Select which metric you want to apply to this configuration.

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

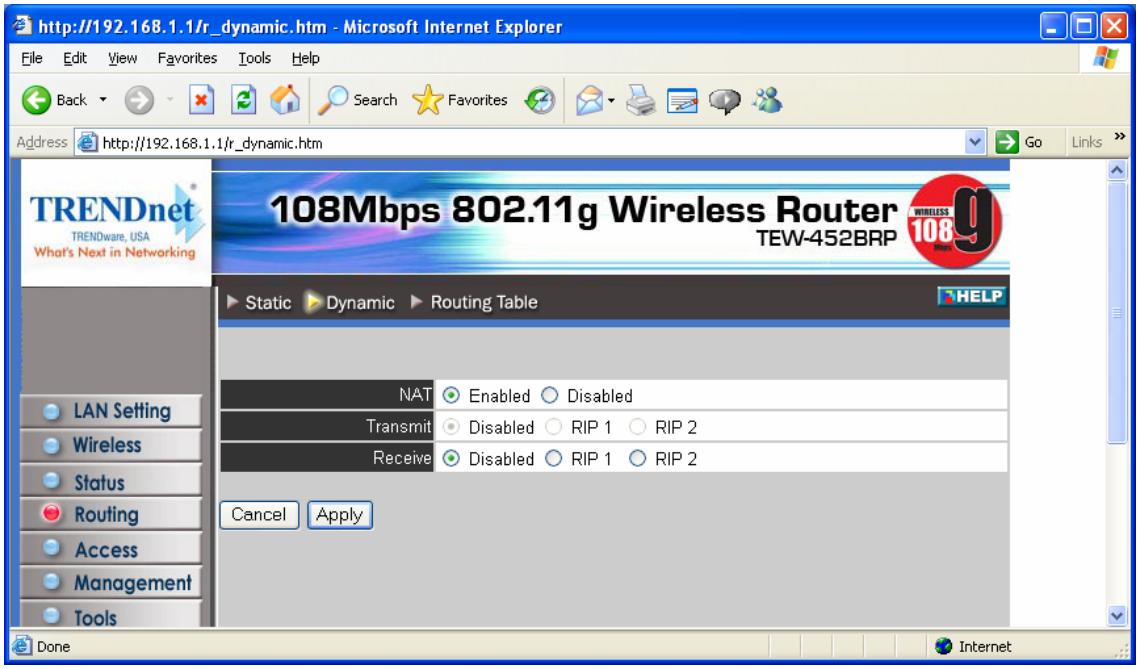
Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click *Update* to confirm the changes.

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.

New: Click *New* to clear the text boxes and add required information to create a new entry.

3.4.2 Dynamic

This screen enables you to set NAT parameters.



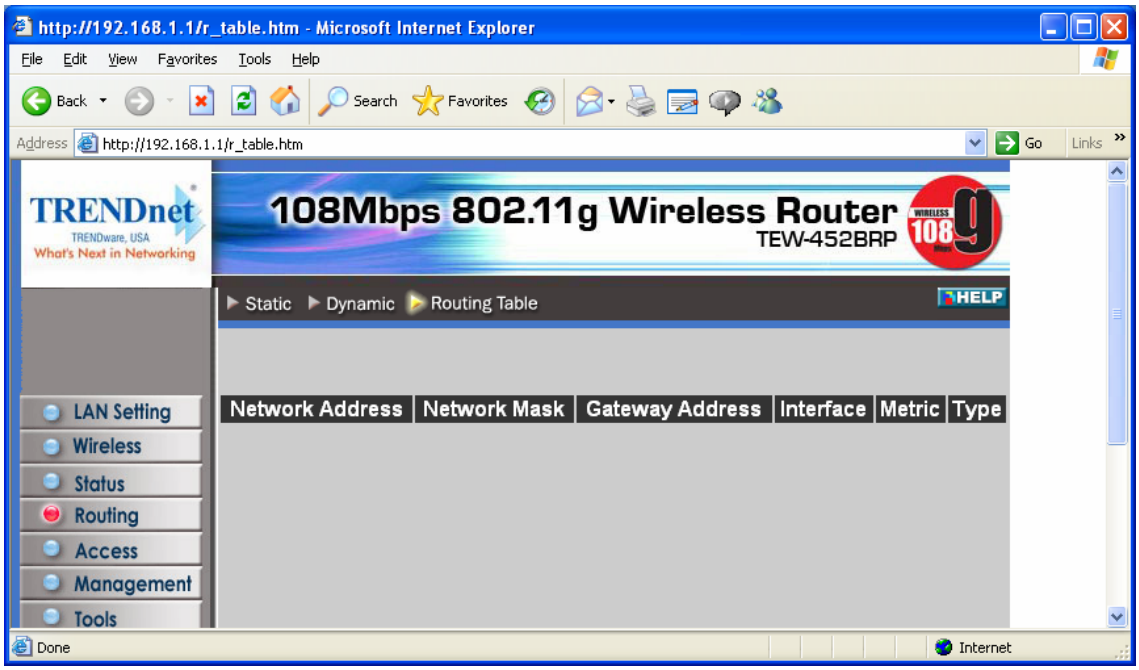
NAT: Click the radio buttons to enable or disable NAT.

Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2

3.4.3 Routing Table

This screen enables you to view the routing table for the router. The routing table is a database created by the 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

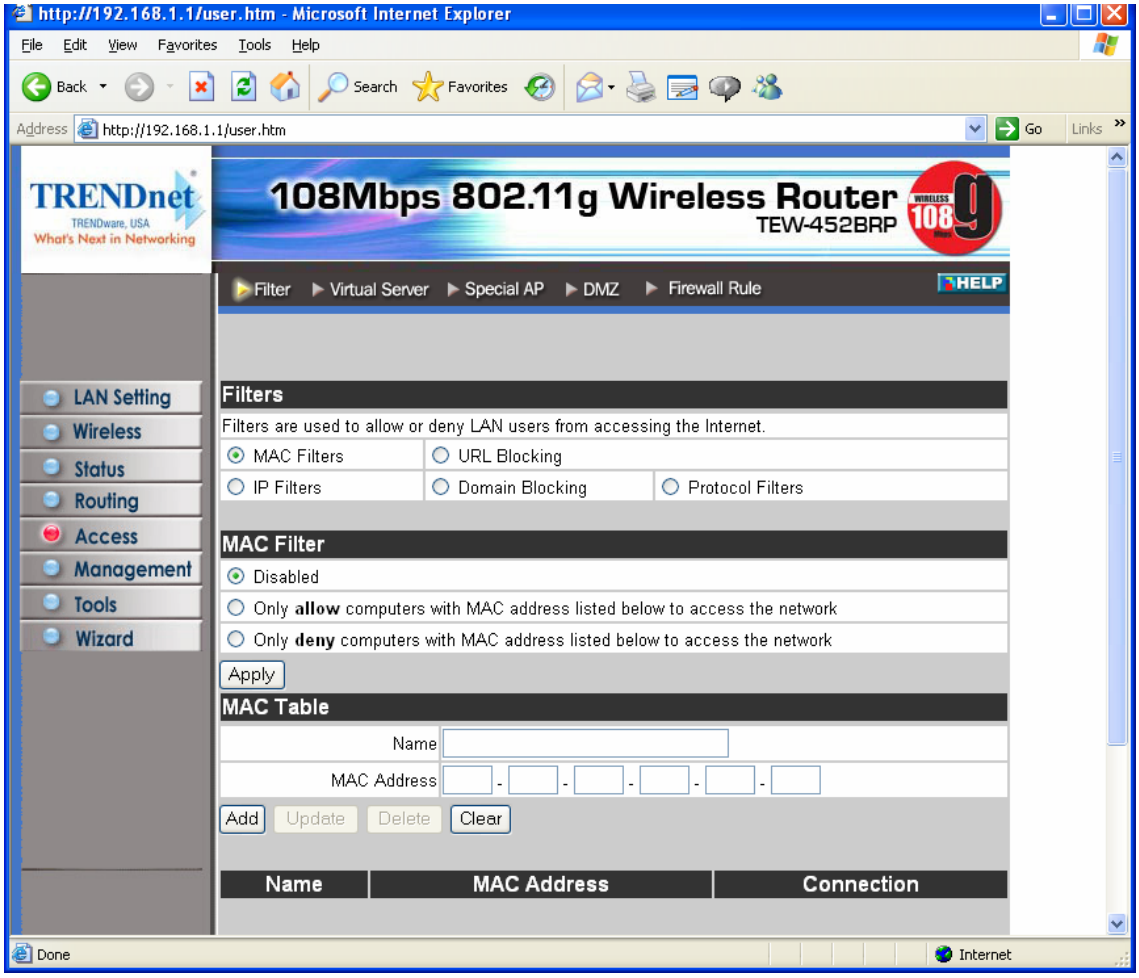
3.5 Access

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.

3.5.1 Filters

Using filters to deny or allow the users to access. Five types of filters to select: MAC, URL blocking, IP, Protocol filter and Domain blocking.

MAC Filters:



MAC Filter: Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to *Disabled* to disable the MAC filter.

Disable: Once the function of MAC filter is disable, those listed in the MAC Table are allowed Internet access.

Enable: All users are allowed Internet access except those user in the MAC Table are deny 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.

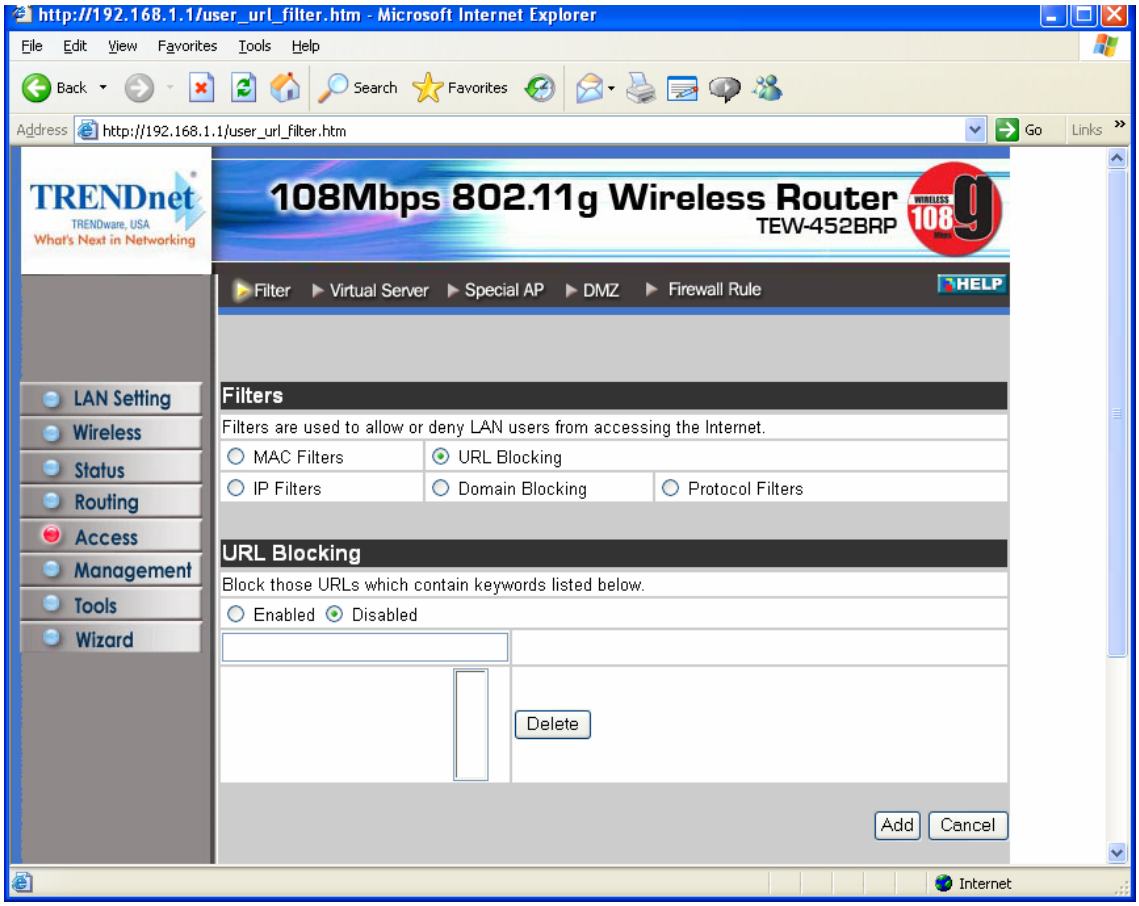
Add: Click to add the user to the list at the bottom of the page.

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.

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

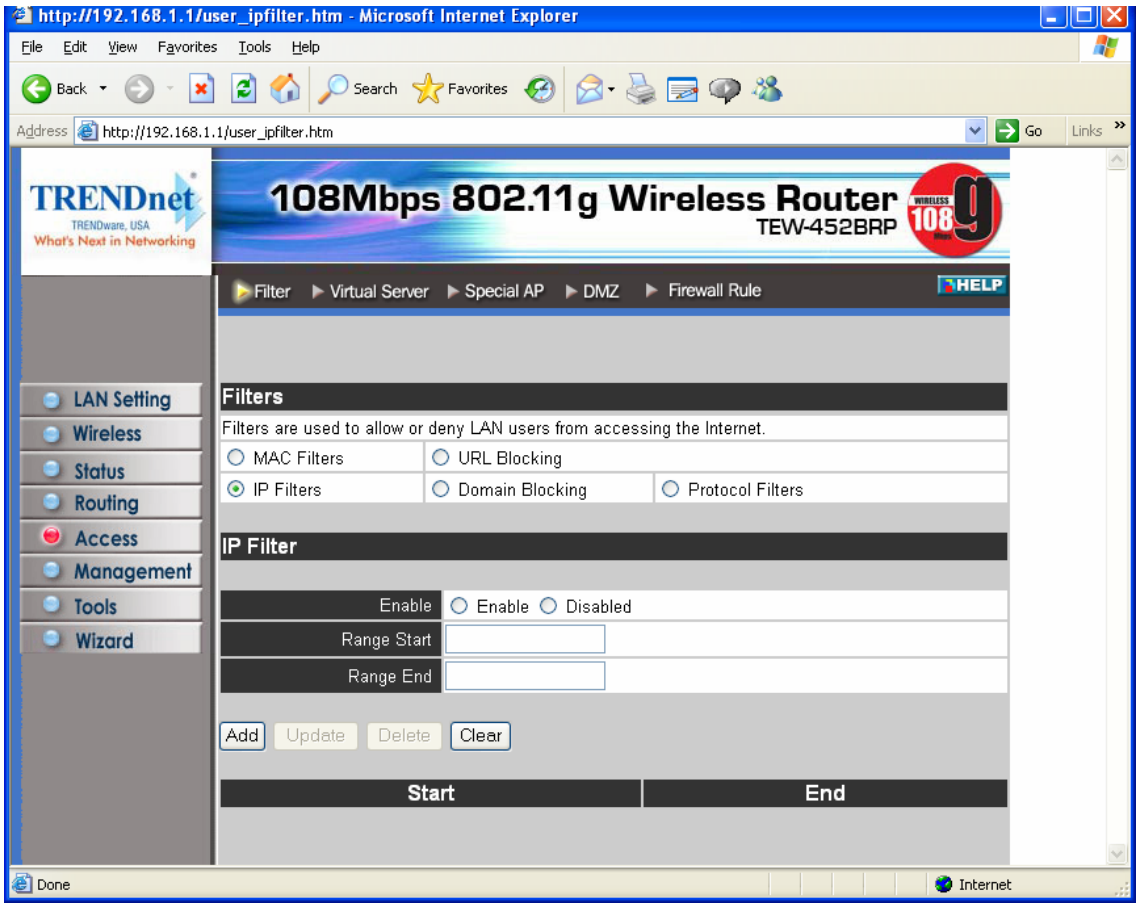
URL Blocking:



You could enable URL blocking to deny the users from accessing the specified URL. Add those specified URL in the text box.

IP Filters:

This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access. 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.)



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

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

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

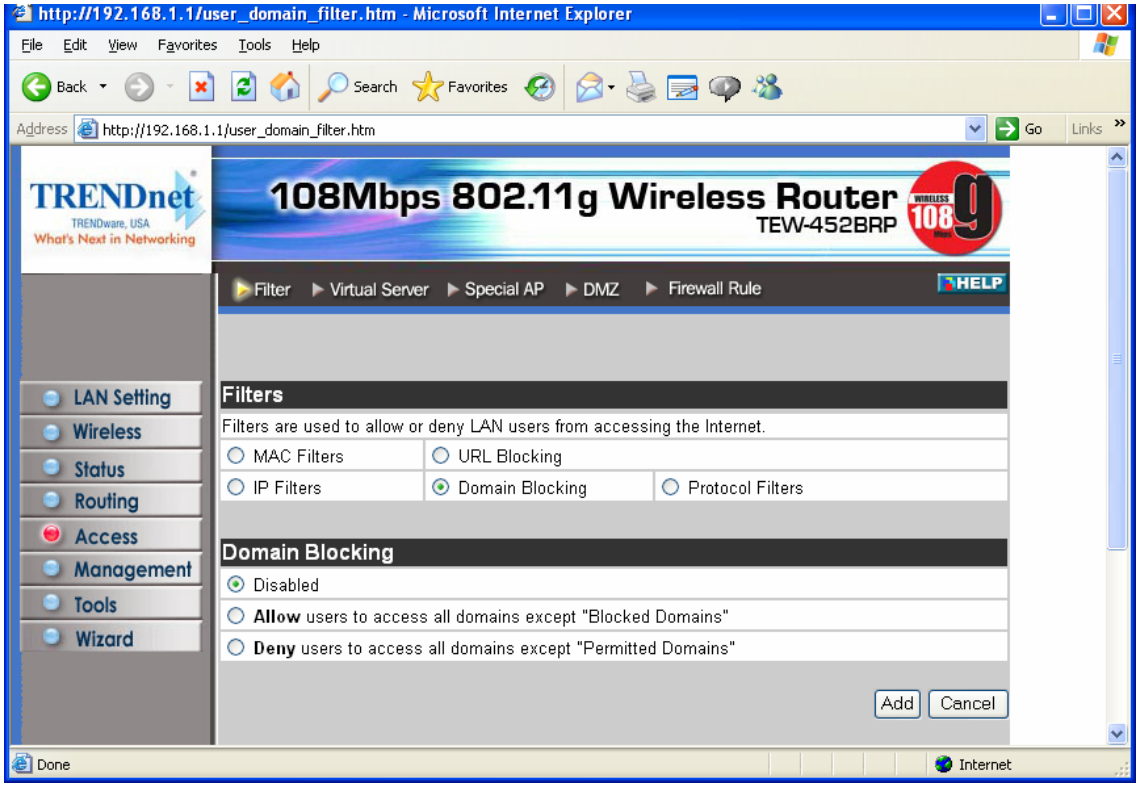
Add: Click to add the IP range to the table at the bottom of the screen.

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.

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

Domain Blocking:

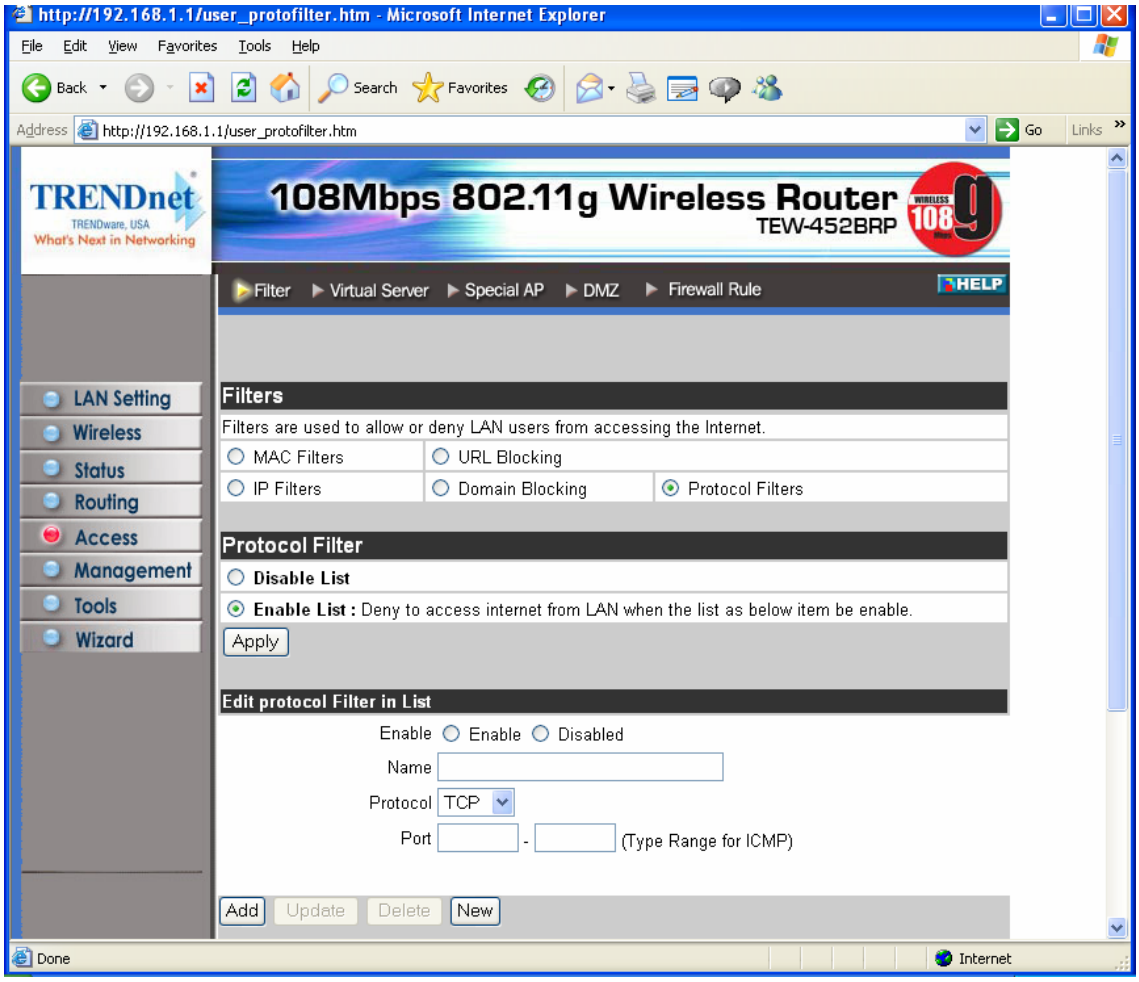


You could specify the domains that allow users to access or deny by clicking one of the two items. Also, add the specified domains in the text box.

Protocol Filters:

This screen enables you to allow and deny access based upon a communications protocol list you create. The protocol filter profiles are listed in the table at the bottom of the page.

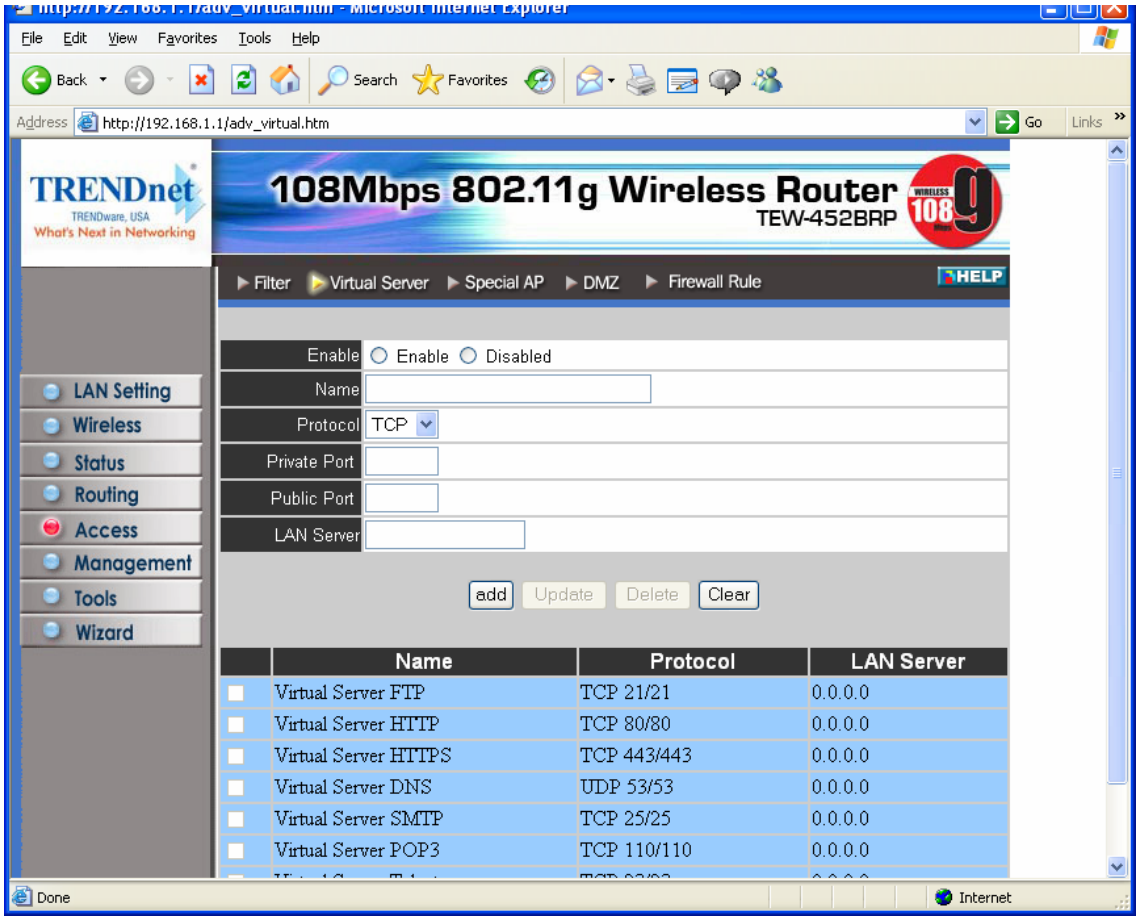
Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit:



3.5.2 Virtual Server

This screen enables you to create a virtual server via the router. If the 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 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 you can edit.



Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select the protocol (TCP or UDP) you want 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.

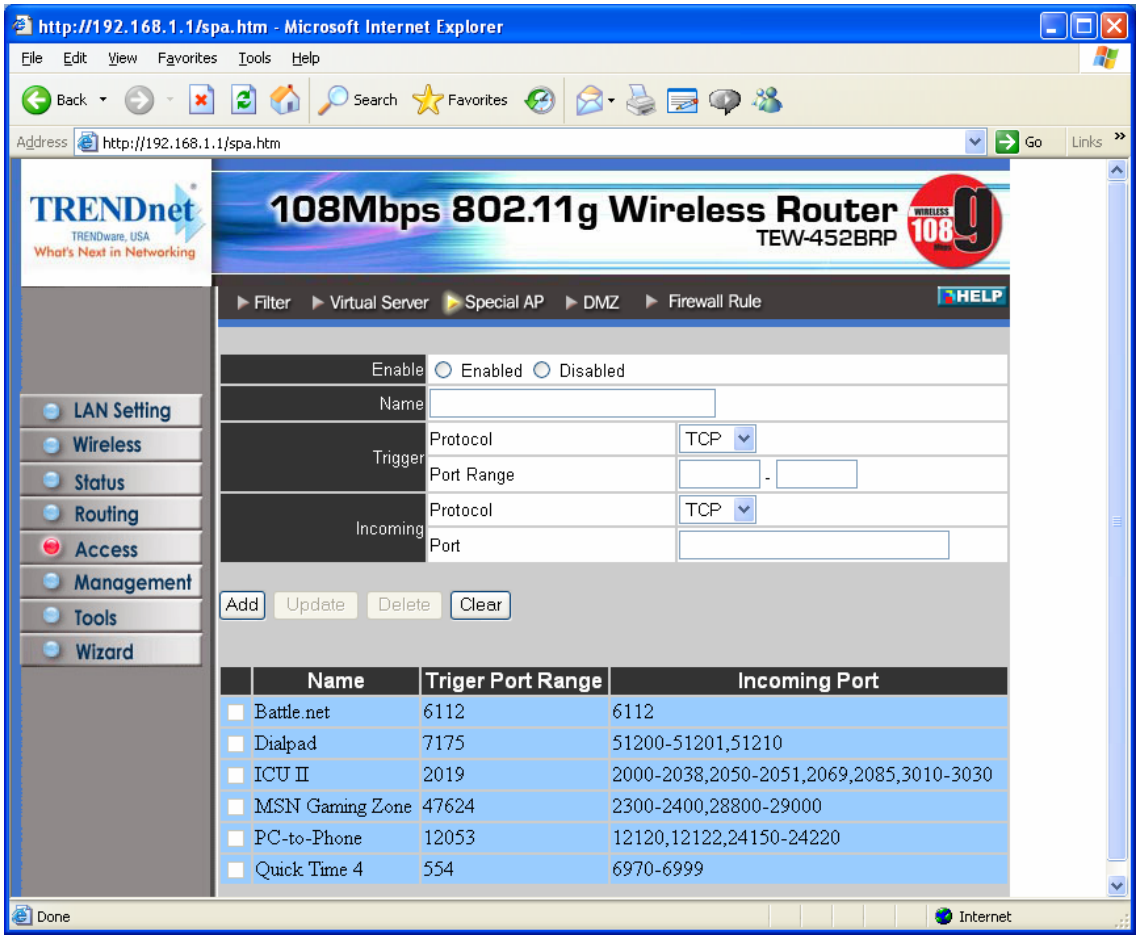
Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

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

3.5.3 Special AP

This screen enables you to specify special applications, such as games, that require multiple connections that are inhibited 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 you can edit.



Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router WAN connection. Click Disabled on a profile to prevent users from accessing the application on the WAN.
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 ICMP) 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.

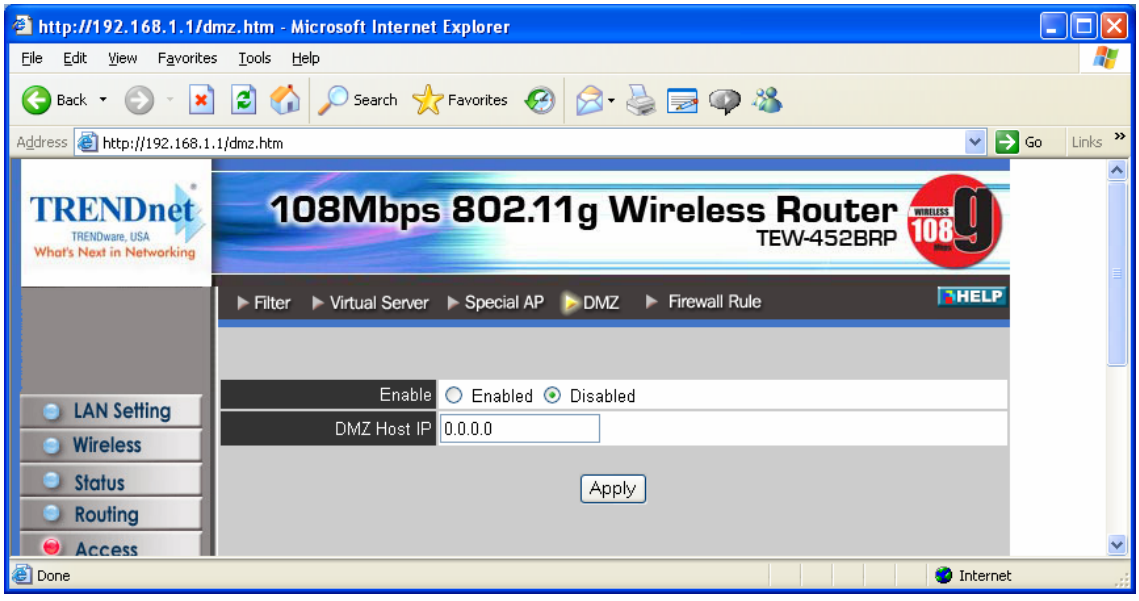
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.

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

3.5.4 DMZ

This screen enables you to create a DMZ for those computers that cannot access Internet applications properly through the router and associated security settings.
Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.



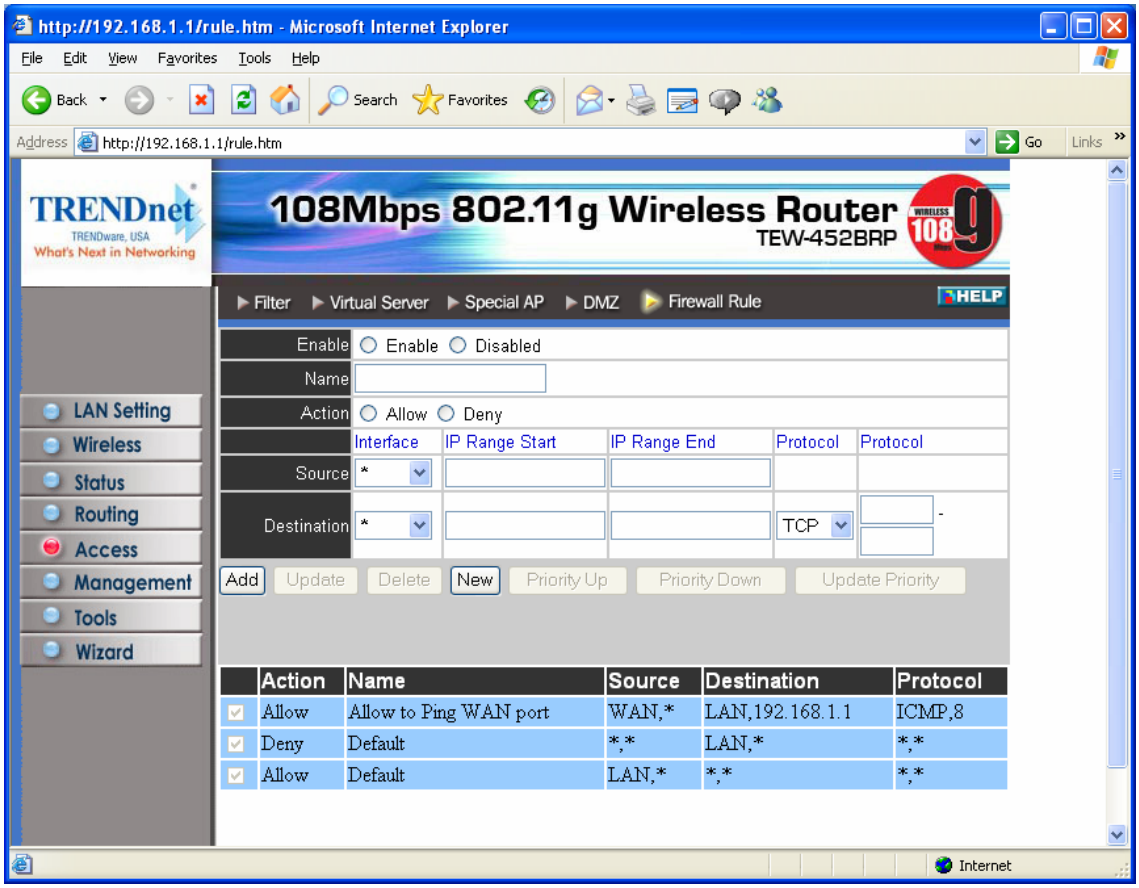
Enable: Click to enable or disable the DMZ.

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.

3.5.5 Firewall Rule

This screen enables you to set up the firewall. The router provides basic firewall functions, by filtering all the packets that enter the router using a set of rules. The rules are in an order sequence list--the lower the rule number, the higher the priority the rule has.



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.

Inactive Timeout: Type the number of seconds of network inactivity that elapses before the router refuses the incoming packet.

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 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.

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.

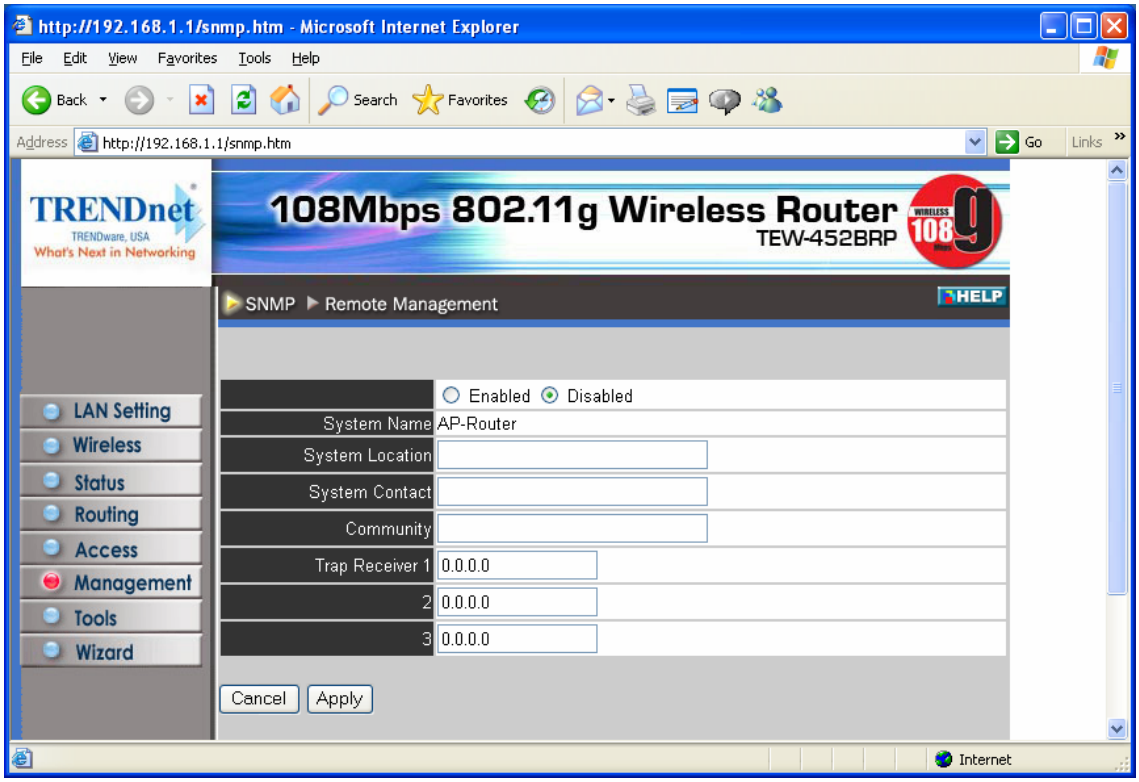
Update Priority: After increasing or decreasing the priority of a rule, click *Update Priority* to save the changes.

3.6 Management

Management enables you to set up SNMP and Remote Management feature.

3.6.1 SNMP

This screen enables you to configure SNMP.



Enabled/Disabled: Click to enable or disable SNMP.

System Name: Displays the name given to the router.

System Location: Displays the location of the router (normally, the DNS name).

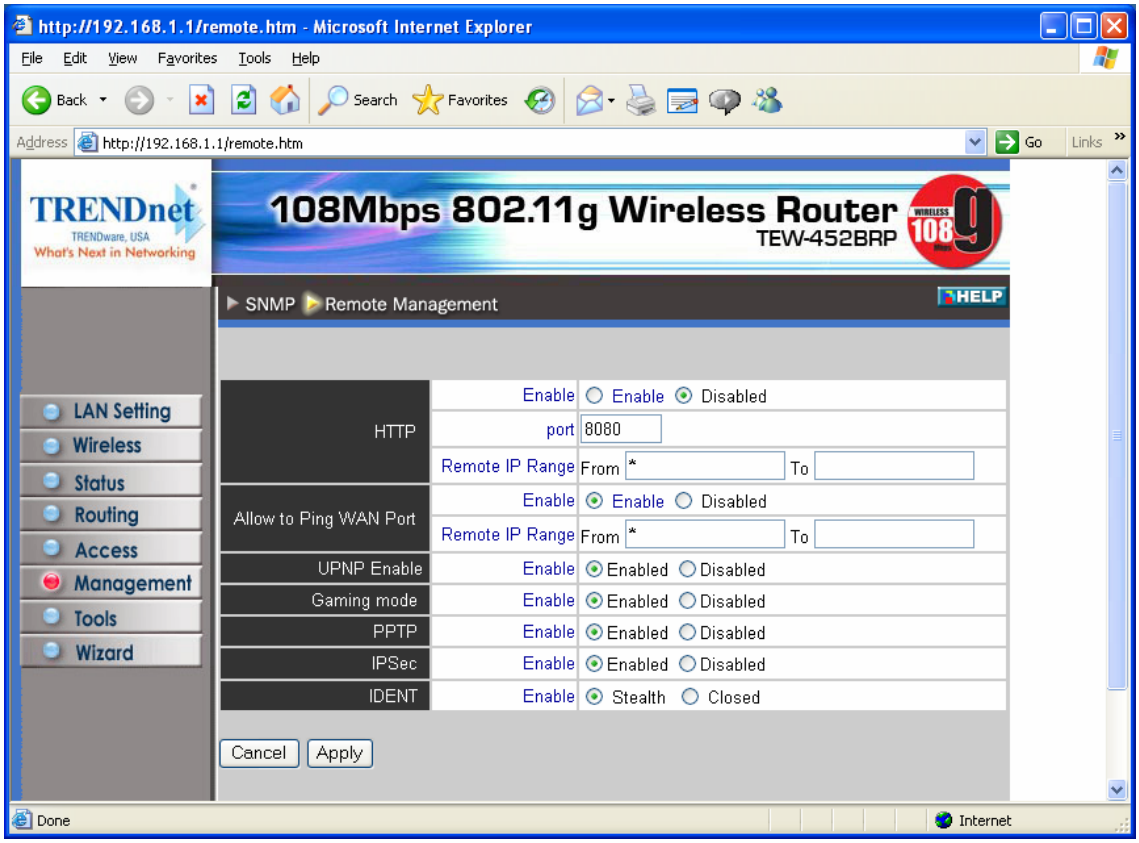
System Contact: Displays the contact information for the person responsible for the router.

Community: SNMP system name for exchanging SNMP community messages. The name can be used to limit SNMP messages passing through the network. The default name is 'public.'

Trap Receiver: Type the name of the destination PC that will receive trap messages.

3.6.2 Remote Management

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



HTTP: Enables you to set up HTTP access for remote management.

- **Enable:** Click to enable or disable HTTP access for remote management.

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

UPNP: UPNP is short for Universal Plug and Play that is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The Router is an UPnP enabled router and will only work with other UPnP devices/softwares. If you do not want to use the UPnP functionality, it can be disabled by selecting "Disabled".

GAMING MODE: If you are experiencing difficulties when playing online games or even certain applications that use voice data, you may need to enable Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode is disabled.

PPTP: Enables you to set up PPTP access for remote management.

IPSec: Enables you to set up IPSec access for remote management.

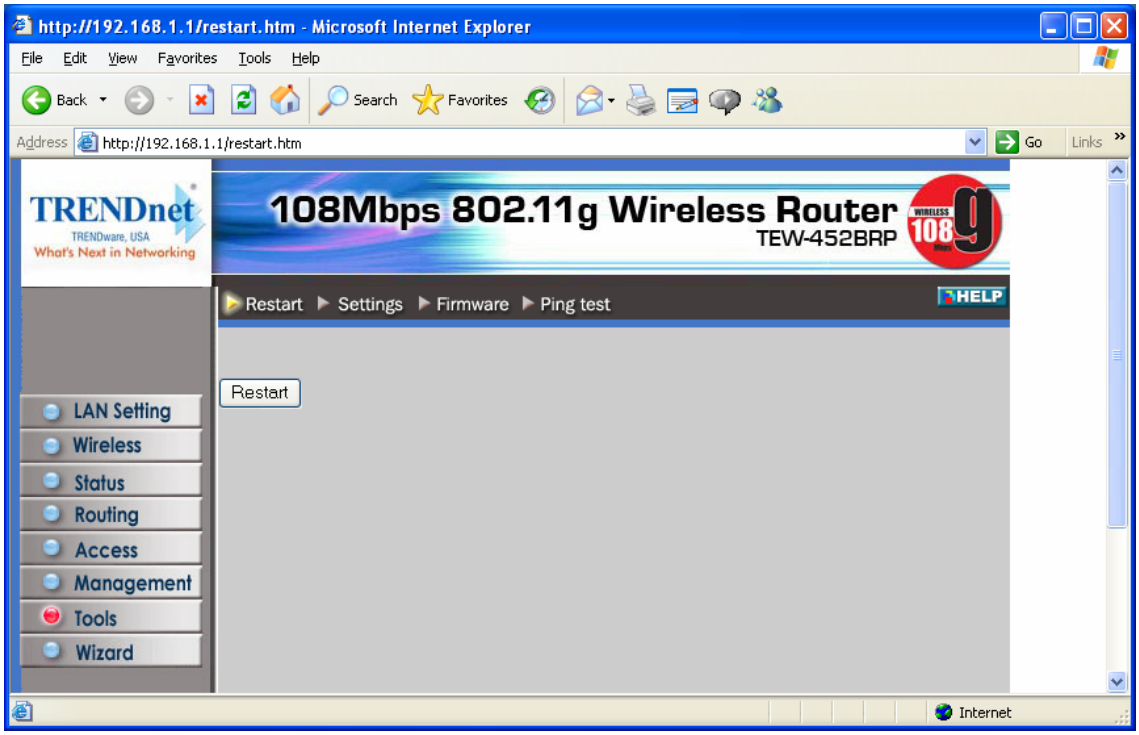
IDENT: Default is stealth. This enables you to set port 113 stealth.

3.7 Tools

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

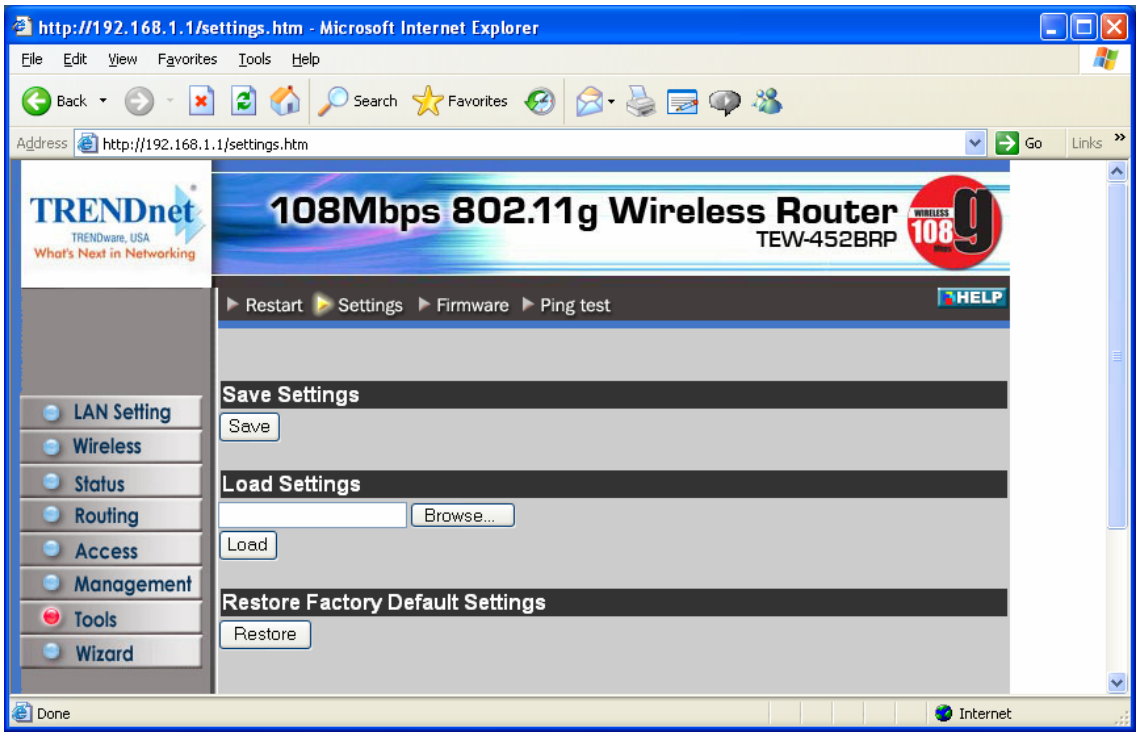
3.7.1 Restart

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



3.7.2 Settings

This screen enables you to save your settings as a profile and load profiles for different circumstances. You can also load the factory default settings, and run a setup wizard to configure the router and router interface.



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

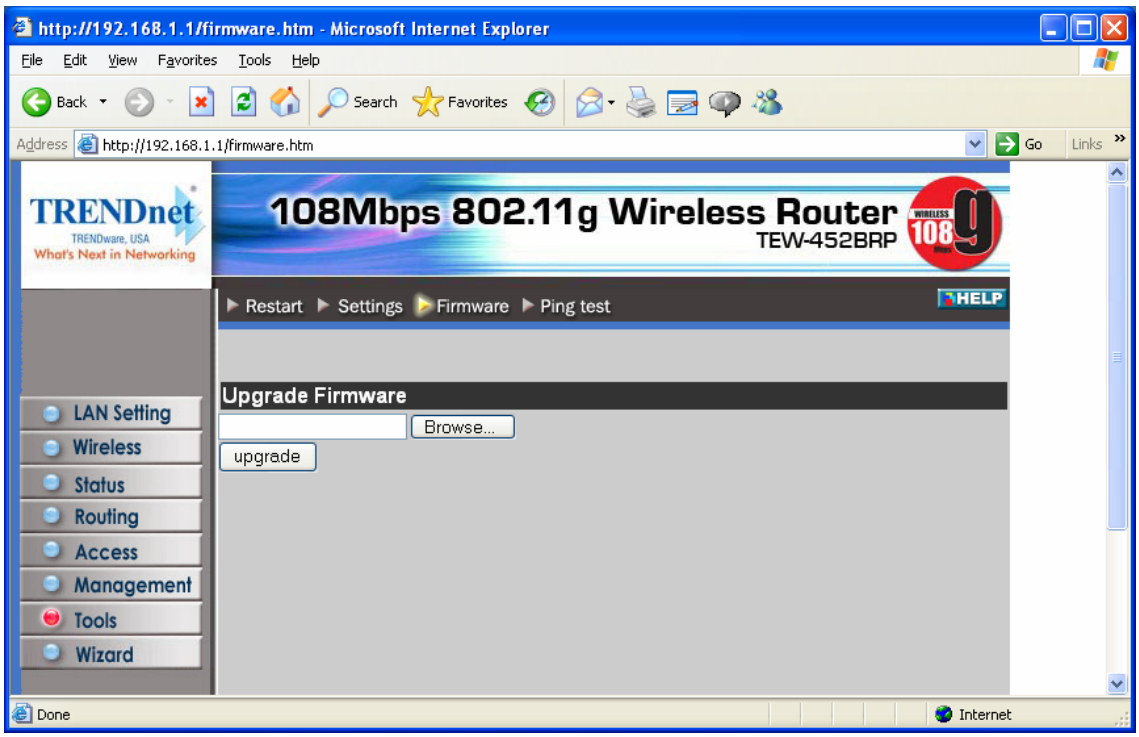
Load Settings: Click *Browse* and go to the location of a stored profile. Click *Load* to load the profile's settings.

Restore Factory Default Settings: Click to restore the default settings. All configuration changes you have made will be lost.

Setup Wizard: click to run a setup wizard that configures the router and interface

3.7.3 Firmware

This screen enables you to keep the router firmware up to date.



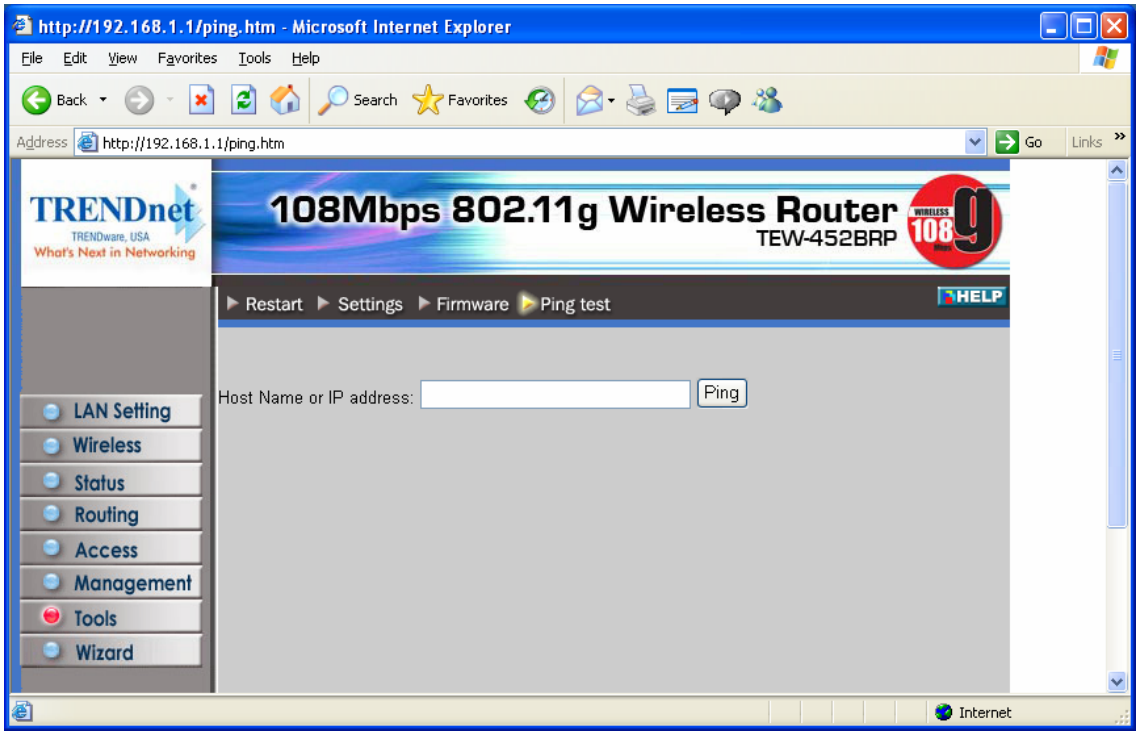
Please follow the below instructions:

1. Download the latest firmware from the manufacturer's Web site, and save it to your disk.
2. 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

3.7.4 Ping Test

The ping test enables you 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.



4. Glossary

Access Point

An interview networking device that seamlessly connects wired and wireless networks

Authentication

Authentication refers to the verification of a transmitted message's integrity.

DMZ

DMZ (DeMilitarized Zone) is a part of a network that is located between a secure LAN and an insecure WAN. DMZs provide a way for some clients to have unrestricted access to the Internet.

DHCP

DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS

DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name

The domain name typically refers to an Internet site address.

DTIM

DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

Filter

Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall

Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware

Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation

Refers to the breaking up of data packets during transmission.

FTP

FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway

Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, *http://www.yahoo.com*).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the realtime clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet INternet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

PPTP

Point-to-Point Tunneling Protocol uses TCP to deal data for tunnel maintenance, and uses PPP for sum up the information carried within the tunnel. The data carried within the tunnel can be compressed or encrypted. The encryption method used is RSA RC4. PPTP can operate when the protocol is supported only on the client and the server located on the other end that the client is corresponds with. No support is essential from any of the routers or servers within the network the two PCs are connecting across.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

Subnet Mask

Subnet Masks (SUBNETwork masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission). The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).

Limited Warranty

TRENDware 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.

Wireless Products – 3 Years Warranty

If a product does not operate as warranted above during the applicable warranty period, TRENDware shall, at its option and expense, repair the defective product or part, deliver to customer an equivalent product or part to replace the defective item, or refund to customer the purchase price paid for the defective product. All products that are replaced will become the property of TRENDware. Replacement products may be new or reconditioned.

TRENDware 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 TRENDware 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 TRENDware office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDware must be pre-authorized by TRENDware with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDWARE PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDWARE'S OPTION, REPAIR OR REPLACEMENT. 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. TRENDWARE NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDWARE'S PRODUCTS.

TRENDWARE 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 TRENDWARE 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 TRENDWARE'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.

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 Year Warranty

TRENDnet®

TRENDware, USA

What's Next in Networking

Product Warranty Registration

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

TRENDnet Technical Support

US/Canada Support Center	European Support Center
Contact **Telephone:** 1(310) 626-6252 **Fax:** 1(310) 626-6267 **Email:** support@trendnet.com **Tech Support Hours** 7:30am - 6:00pm Pacific Standard Time Monday - Friday	**Contact** **Telephone** Deutsch : +49 (0) 6331 / 268-460 Français : +49 (0) 6331 / 268-461 Español : +49 (0) 6331 / 268-462 English : +49 (0) 6331 / 268-463 Italiano : +49 (0) 6331 / 268-464 Dutch : +49 (0) 6331 / 268-465 **Fax**: +49 (0) 6331 / 268-466 **Tech Support Hours** 8:00am - 6:00pm Middle European Time Monday - Friday

TRENDware International, Inc.
3135 Kashiwa Street. Torrance, CA 90505
http://www.TRENDNET.com