User's Guide

TRENDNET ®

4-Port Fast Ethernet Firewall Router
TW100-BRF214

Contents

Product Overview

TW100-BRF214

Package Contents

In addition to your router, the package includes:

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

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

Features

The 4-Port Fast Ethernet Firewall Router, model TW100-BRF214, is easy to setup up and suitable for home office, small office, and medium sized business installations. It comes in a sturdy metal housing, offers four Fast Ethernet Ports, and features advanced QoS, Firewall, and event log functions.

Connection duration and type, firewall status, and system information event logs help with trouble shooting and network maintenance. This router supports dynamic IP, Static IP, PPPoE, PPTP, L2TP, DNS, and dynamic DNS connections. Access controls include URL, IP address, and MAC address filters. Advanced Denial of Service (DoS) capabilities include protection from IP Spoofing, Ping of Death, TCP Flooding and other attacks. Quality of Service (QoS) management functions set port-based bandwidth and DSCP queue priority controls.

- 1 x 10/100Mbps Auto-MDIX port (WAN/Internet)
- 4 x 10/100Mbps Auto-MDIX ports (LAN)
- Supports Cable/DSL Modems with Dynamic IP, Fixed IP, PPPoE, PPTP, and L2TP connection types
- Supports Network Address Port Translation (NAPT)
- Firewall features include NAT and Stateful Packet Inspection (SPI)
- Advanced security features include Denial of Service (DoS) and ARP spoofing prevention
- Website access restriction by URL/Keyword (32 entries)
- MAC Address control to allow or deny access (32 entries)
- Client Filtering by Date/Time using TCP/UDP ports (20 entries)
- Supports Virtual Servers (40 Entries), DMZ (6 Entries), Port Trigger/Port Mapping (10 Entries)
- Multiple VPN pass-through sessions for IPsec, L2TP, and PPTP (100 VPN sessions)
- Supports static routes (20 entries)
- Supports Dynamic DNS service
- Includes port-based bandwidth control and DSCP
- Universal Plug and Play (UPnP) and Application Level Gateway support for Internet applications such as email, FTP, gaming, and more
- Easy Web browser configuration and remote management

Product Hardware Features

Rear View
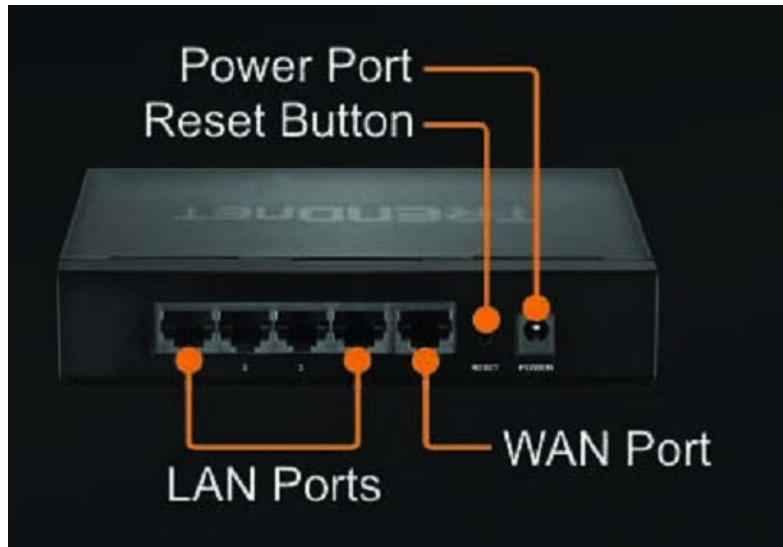
- **Reset Button** –Use an item such as a paperclip to push and hold this button for 15 seconds and release to reset your router to its factory defaults.

- **LAN Ports** – Connect Network cables (also called network cables) from your router LAN ports to your wired network devices.

- **WAN Port**–Connect a Network cable from your router WAN port to your modem.

- **Power Port** – Connect the included power adapter from your router power port and to an available power outlet.
  Note: Use only the adapter that came with your router.

Front View

Diagnostic LEDs

- **Power LED** - This LED indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router.

- **WAN (Link/Activity) LED** – This LED indicator is solid green when your router WAN port is physically connected to the modem Network port (also called network port) successfully with a Network cable. The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router.

- **WLAN (Link/Activity) LED** – This LED indicator is blinking green when the wireless is "On" and functioning properly on your router. This LED indicator will be blinking green rapidly while data is transmitted or received by your wireless clients or wireless network devices connected to your router.

- **LAN 1-4 (Link/Activity) LEDs** – These LED indicators are solid green when the LAN ports are successfully connected to your wired network devices (which are turned on). These LED indicators will blink green while data is transmitted or received through your router's LAN ports.

Application Diagram
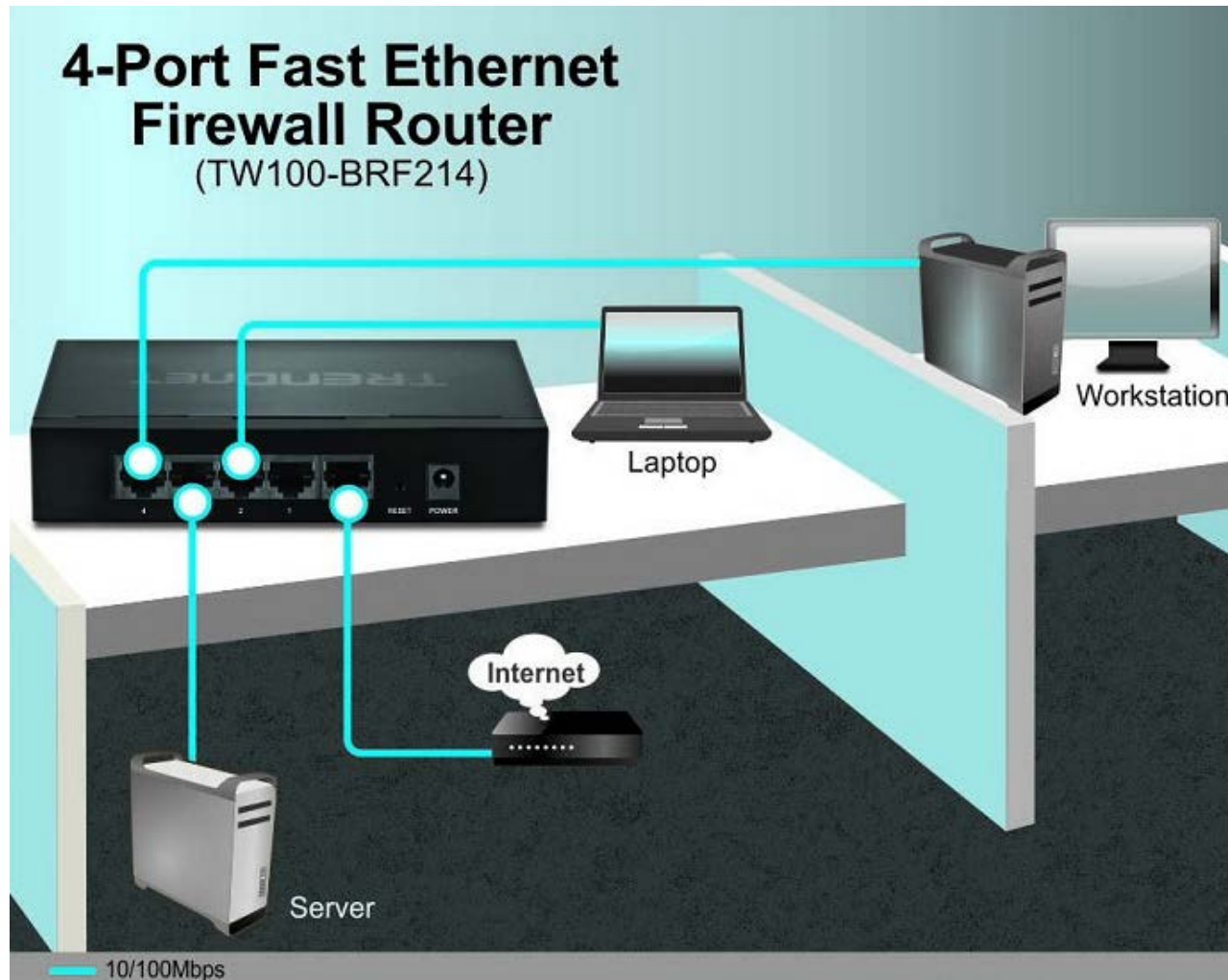
The router is installed in a small office near the modem (supplied by your ISP "Internet Service Provider") and physically connected to the router's WAN port to the modem's network port which connects to the Internet. A network server and computers are connected to the wired Fast Ethernet LAN ports (1-4) located on the back of router thereby providing local connectivity to access network resources and Internet access.

Basic Router Setup

Creating a Home Network

What is a network?

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

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

- **Modem** – Connects a computer or router to the Internet or ISP (Internet Service Provider).

- **Router** – Connects multiple devices to the Internet.

- **Switch** –Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Network ports on your router, you will need an additional switch to add more wired connections.

How to set up a home network

1. For a network that includes Internet access, you'll need:
   - Computers/devices with a Network port or wireless networking capabilities.
   - A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
   - A router to connect multiple devices to the Internet.

2. Make sure that your modem is working properly. Your modem is provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.

3. Set up your router. See "How to setup your router" below.

4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on .

How to setup your router
Refer to the Quick Installation Guide or continue to the next section "Router Installation" on for more detailed installation instructions.

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

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

Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

1. Dynamic IP
Host Name (Optional)
Clone Mac Address (Optional)

2. Static IP
IP address assigned by your ISP: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask: _____. _____._____._____ (e.g. 255.255.255.0)
ISP Gateway Address: _____. _____._____._____(e.g. 215.24.24.1)
Under DNS section
Domain Name Server (DNS) Address: _____. _____._____._____(e.g. 4.2.2.2)
Secondary DNS Address (optional): _____. _____._____._____(e.g. 8.8.8.8)

If you have multiple static IP addresses provided your ISP, under Does ISP provide more IP addresses, check Yes (optional) and enter the additional IP addresses.
Alias IP Address 1: _____. _____._____._____(e.g. 215.24.24.128)
Alias IP Address 2: _____. _____._____._____(e.g. 215.24.24.127)
Alias IP Address 3: _____. _____._____._____(e.g. 215.24.24.126)
Alias IP Address 4: _____. _____._____._____(e.g. 215.24.24.125)
…

3. PPPoE (Dynamic IP or Static IP)
Type (Dynamic IP)
User Name: _____
Password: _____
Retype Password: _____
Service Name (optional): _____

Type (Static IP)
User Name: _____
Password: _____
Retype Password: _____
Service Name (optional): _____
IP Address: : _____. _____._____._____(e.g. 215.24.24.129)
Primary DNS Address: _____. _____._____._____(e.g. 215.24.24.50)
Secondary DNS Address: _____. _____._____._____(e.g. 215.24.24.51)

4. PPTP
Type (Dynamic IP or Static IP)
PPTP Account: _____
PPTP Password: _____
Retype Password: _____
Service IP: _____. _____._____._____(e.g. 215.24.24.130)
My IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____(e.g. 255.255.255.0)
Gateway:_____. _____._____._____(e.g. 215.24.24.1)

5. L2TP
Type (Dynamic IP or Static IP)
PPTP Account: _____
PPTP Password: _____
Retype Password: _____
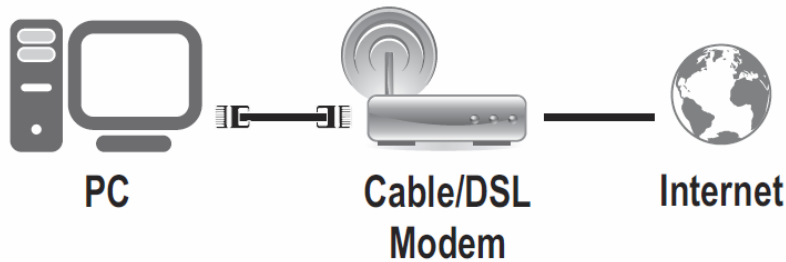Service IP: _____. _____._____._____(e.g. 215.24.24.130)
My IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____(e.g. 255.255.255.0)
Gateway:_____. _____._____._____(e.g. 215.24.24.1)

Hardware Installation

1. Verify that you have an Internet connection when connecting your computer directly to your modem.

2. Turn off your modem.

3. Disconnect the Network cable from your computer to your modem.

4. Using a Network cable, connect the WAN port on the router to your modem.

5. Using another Network cable, connect your computer to one of the four LAN ports on the router.

6. Connect the power adapter to your router and then to a power outlet.

7. Turn on your modem.

8. Verify that the following front panel LED indicators on your router: Power (Solid Green), LAN 1, 2, 3, or 4 (Solid/Blinking Green for ports for which devices are connected), WAN (Solid/Blinking Green).
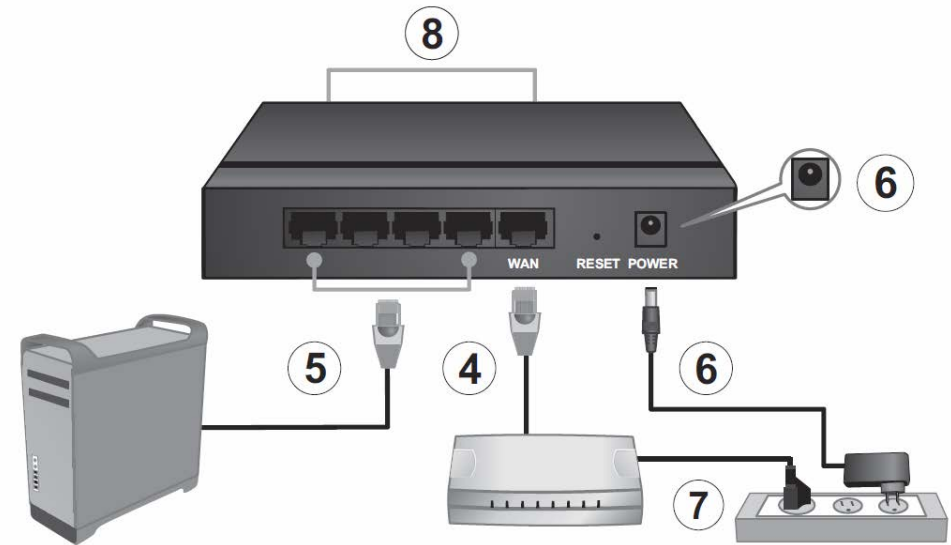
Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1. Your router will prompt you for a user name and password.
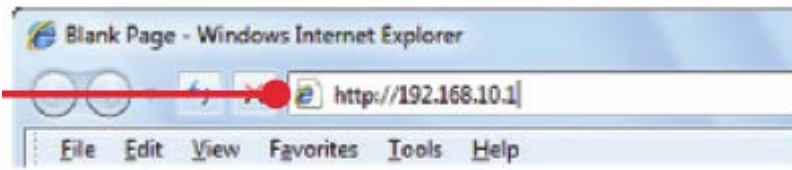
2. Next to Language, click the drop-down list to select your preferred language. Enter the default user name and password and then click Login.

Default User Name: **admin**

Default Password: **admin**
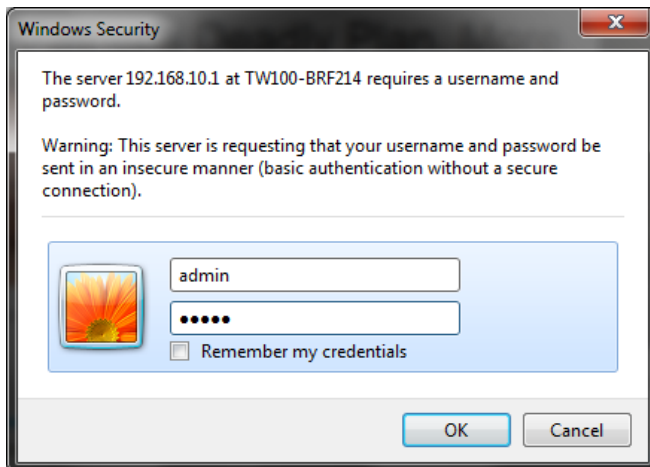
3. Click **Quick Setup** to start the Setup Wizard.
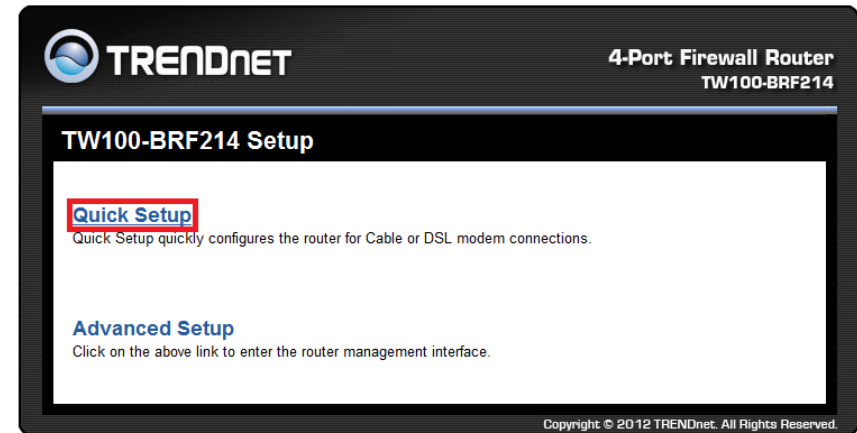
4. Select your Time Zone from the drop-down list and set the Daylight Savings Time if applicable. Click Next.
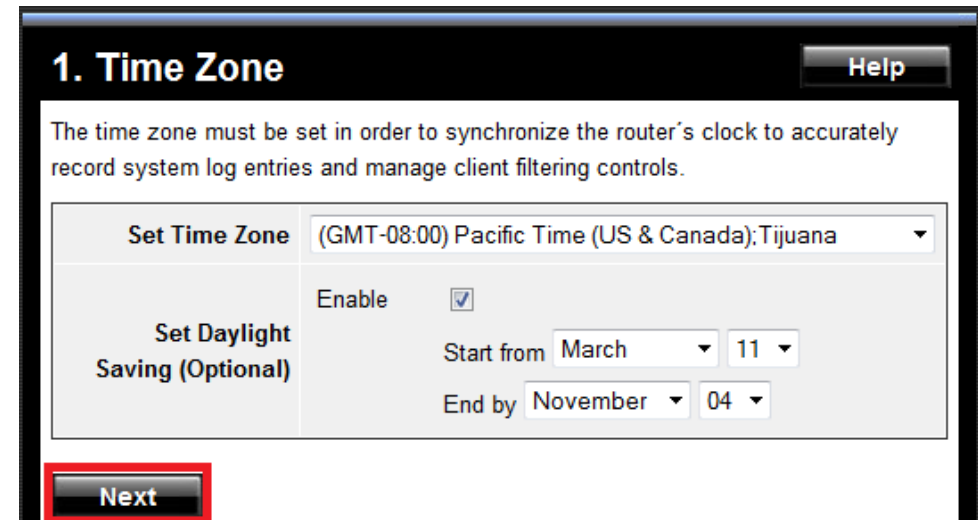
5. This section determines what method the router will use to interface with your ISP service. Dynamic IP is typical for most ISP services.

6. Select Dynamic IP configuration (Dynamic IP is typical for most ISP services. Verify with your ISP).

Note: If you know that your ISP requires a configuration other than Obtain IP Automatically (Dynamic IP) or if you are having difficulty completing the router installation, please contact your ISP to verify all required settings for one of the options listed on page 6. The options listed on page 6 match the settings options available to choose from.

7. Click Next to bypass the cloning of your computer's MAC address (Cloning is required for instances when your router would need to be identified as the same address as your computer).
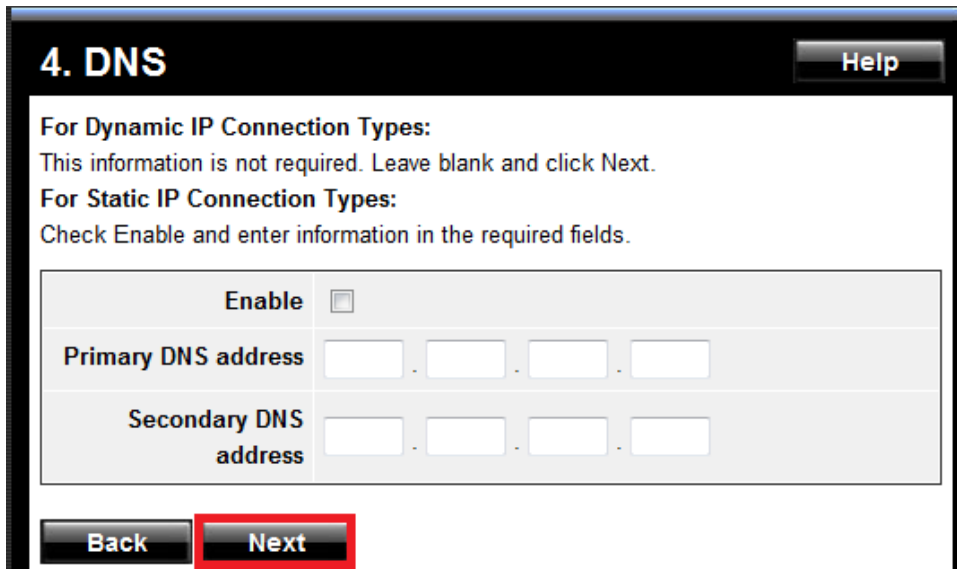
8. Click Next to use your ISP DNS service.

Note: Otherwise, if you would like to specify your own DNS servers to use, check the Enable box and under Primary and Secondary DNS address fields enter in the IP addresses of DNS servers you would like to use.
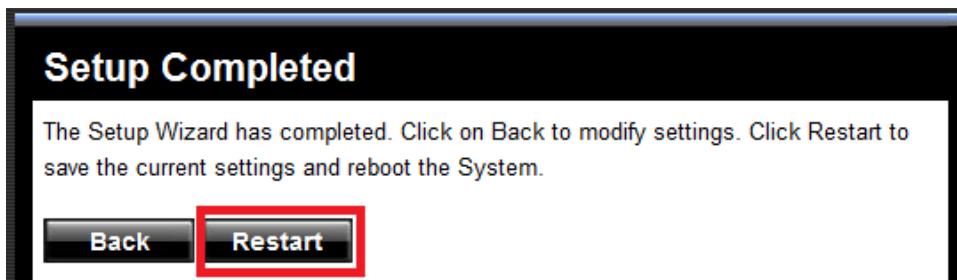
9. Click **Restart**.

10. Wait for your router to reboot.
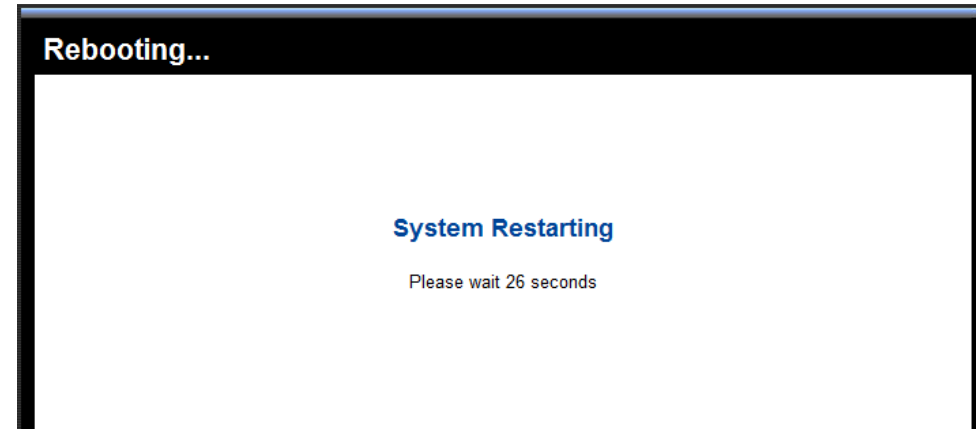
11. Verify you have an Internet connection by opening a Web browser on your computer.

Note: If you cannot access the Internet, power down your modem and router again. Occasionally certain modems need to be power cycled to adopt new router settings.

Connect additional wired devices to your network

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

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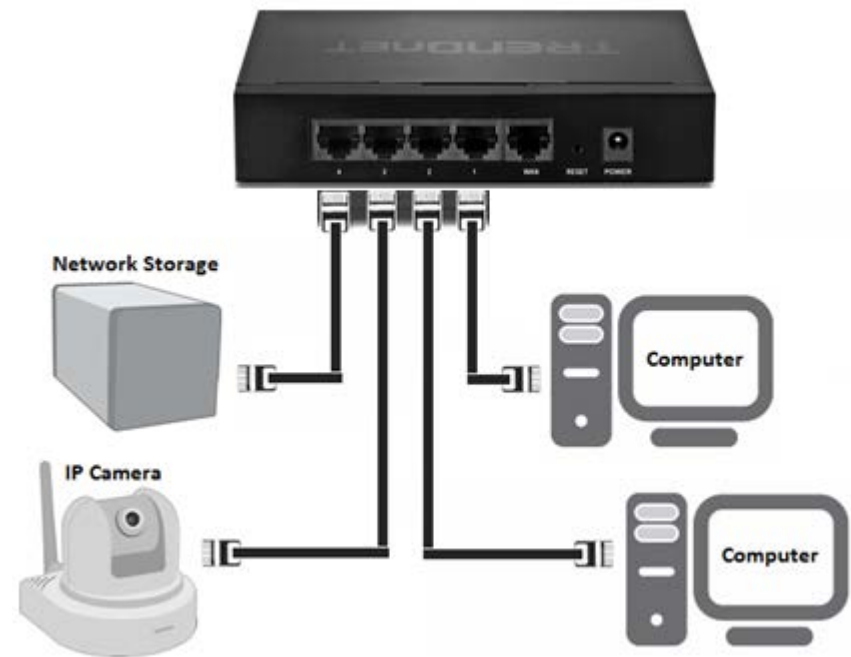
Access Control Filters

Access control basics

Advanced Setup > Firewall

Client Filtering

Advanced Setup > Firewall > Client Filtering

You may want apply client filtering (outbound packet filter) to deny access to specific types of traffic from computers or devices on your local network to the Internet. You can also apply a specified schedule when you would like the filters activated or deactivated.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **Firewall**, then click on **Client Filtering**.

3. In the entry list, choose an entry to modify and enter the required information.

	IP	Port	Type
1.	192.168.10.___ ~ ___	___ ~ ___	◉ TCP ◯ UDP

- **IP** – Enter the IP address range (use last IP address number only such as 192.168.10.101-192.168.10.110) to apply the filter. IP addresses not included in the range will not be blocked from accessing the traffic specified in the filter.
- **Port** – Enter the range of port numbers to block or deny access. To specify all port numbers, enter the range 1 ~ 65535 to block all access. For a range of specific port numbers, enter a port range within the range of 1-65535 (*e.g. 21 ~ 30)* and for a single port, enter the same number in both range fields (*e.g. 21 ~ 21).*

- **Type** – Select the protocol type of traffic to block or deny access. **TCP** or **UDP**.

Examples: To block web browsing access, under **Port** enter the port range 80 ~ 80 and under **Type**, select **TCP**.

To block FTP file transfer access, under **Port** enter the port range 20 ~ 21 and under **Type**, select **TCP**.

4. The remaining fields allow you to specify a set schedule when the filter is activated.

Note: Please ensure that the router System Time is configured correctly under System > System Time to ensure the filter applies accordingly to the schedule defined. To configure the System Time, see page 17.

Block Time	Day	Time	Enable
◉ Always ◯ Block	___ ▾ ~ ___ ▾	___ ▾ ~ ___ ▾	☐

- **Block Time** – Select **Block** to specify a set schedule when the filter should be activated or deactivated, otherwise, select **Always** to keep the filter activated at all times.
- **Day** – If the **Block** option under **Block Time** is selected and you are defining a schedule, click the drop-down list and select the days.
- **Enable** – Check this option to enable the access filter. The access filter will not in affect/activated if the option is unchecked.

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: If you would like to discard the changes, click Cancel before you click Apply.

[**Apply**] [**Cancel**]

MAC address filters
Advanced Setup > Firewall > MAC Control

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this router's wired or wireless network.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **Firewall**, then click on **MAC Control**.

3. Add the MAC addresses to the MAC Address Control List first before applying the MAC filter function.

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

To add MAC addresses to the MAC Address Control List, you can choose to add MAC addresses by manually typing the address in manually or selecting a MAC address from your router's DHCP client list.

- **Add MAC Address -** Enter the 12-digit MAC address in the fields provided . (e.g. *00-11-22-AA-BB-CC)*

OR

- **DHCP Client -** Click the **DHCP Client** drop-down list and select the MAC address you would like to add. After you select the MAC address, click **Clone** to copy the MAC address to the **Add MAC Address** fields.

  Note: You can also check the router DHCP List for the MAC addresses of the devices on your network, see "Setup the DHCP server on your router" on page 19 or refer to your computer or device documentation to find the MAC address.

4. Click **Apply** at the bottom of the page to add the address to the MAC Address Control List. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

To verify that the MAC address is added, the MAC address entry should appear in the **MAC Address Control List**.

*Note: To delete a MAC address from the MAC Address Control list, click **Delete** next to the entry. Then click **Apply** at the bottom of the page to apply the changes and after the changes have been applied, click **Continue** on the following page.*

4. Once you have added all of the MAC addresses to the MAC Address Control List, review the MAC Address Control options and select the option to apply.

*Note: Do not configure this setting until you have added the MAC addresses to the MAC Address Control List first. The recommended option is to only **Deny all to pass except the following MACs** which will only allow the MAC addresses listed in the MAC Address Control List and deny all others devices that are unlisted.*

- **MAC Address Control**
    - o **Enable** - Check the option to enable the MAC address control feature. If this option is unchecked MAC address control will be disabled.
    - o **Allow all to pass except the following MACs** – Selecting this option will allow all other devices access to your network and only deny the device MAC addresses listed in the MAC Address Control List.
    - o **Deny all to pass except the following MACs** – Select this option will deny all other devices access to your network and only allow the device MAC addresses listed in the MAC Address Control List.

MAC Address Control
☐ Enable
◉ Allow all to pass except the following MACs.
○ Deny all to pass except the following MACs.

5. Click **Apply** at the bottom of the page to apply the changes**.** After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Apply   Cancel

Domain/URL Filters
Advanced Setup > Firewall > URL Filter

You may want to block computers or devices on your network access to specific websites (e.g. *www.trendnet.com, etc.)*, also called domains or URLs (Uniform Resource Locators). You may also enter a keyword (e.g. instead of complete URL to generally block computers or devices access to websites that may contain the keyword in the URL or on the web page.

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and **Firewall**, then click on **URL Filter**.

3. Review the Domain/URL blocking settings.

- **URL filter function** – Select **Enabled** to enable URL filtering on your router. Selecting disabled will disable the URL filtering function on your router.

URL filter function   ◉ Enabled ○ Disabled

- **Add URL -** Enter the Website/URL/domain (e.g.*www.trendnet.com)* or keyword (e.g. *trendnet*) to block access.

Add URL   www.trendnet.com

For each website/URL/domain you enter, click **Apply** at the bottom of the page to add the website/URL/domain to the list. After the settings have been applied, click **Continue** on the following page**.**

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

To verify that the entries were successfully added, check if the entries appear in the list.

To delete a website/URL/domain entry, click on the entry in the list, then click **Delete**.

Once the entry is removed from the list, click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

To verify that the entries were successfully removed, check if the entries are no longer listed.
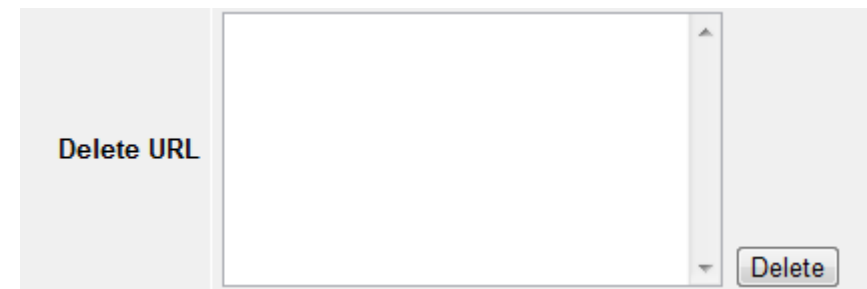
Advanced Router Setup

Access your router management page

Note: Your router management page http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1. Your router will prompt you for a user name and password.
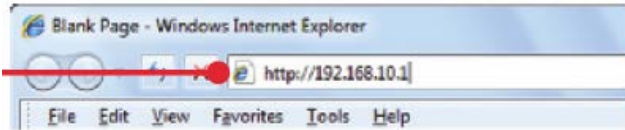
2. Enter the default user name and password and then click **OK**.

*Note: Other web browsers may display a **Log In** or **Submit** button instead of **OK**.*

Default User Name: **admin**   Default Password: **admin**
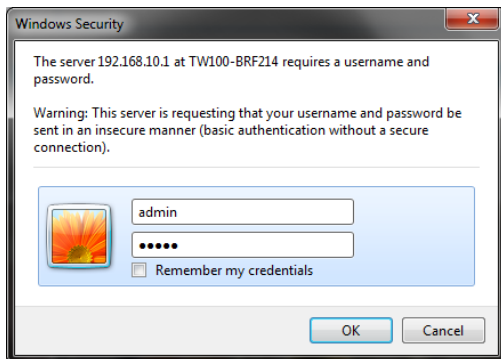
3. At the main Login page, click on **Advanced Setup**.

Change your router login password

Advanced Setup > System > Administrator Settings

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **System**, then click on **Administrator Settings**.

3. Under the **Password** section, in the **Current Password** field, type in your current password assigned to the router (Default Password: **admin**). In the **Password** field, enter the new password, and in the **Re-type password** field, retype the new password again to confirm.

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

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

Set your router date and time

Advanced Setup > System > System Time

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **System Time**.

3. Next to **Set Time Zone**, click the drop-down list to select your **Time Zone**.

4. You can choose one of the following options to set your router date and time:

- **Set the Time** – Set your router date and time manually in the **Set the Time** section. Click **Apply** at the bottom of the page to apply the changes then click **Continue** on the following page.
  Note: Time is specified in 24-hour format.

  OR

- **Default SNTP Server (Optional)** – Set your router date and time to synchronize with an SNTP (Simple Network Time Protocol) server address (e.g. pool.ntp.org). Check the **Enable** option and enter the SNTP server address in the **Server IP** field, (e.g. pool.ntp.org).

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

5. Additionally, you can configure the Daylight Savings Time settings if it applied in your Time Zone.

Next to **Set Daylight Saving (Optional)**, check the **Enable** option and click the drop-down lists to set the annual range when daylight savings time is in effect.

6. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
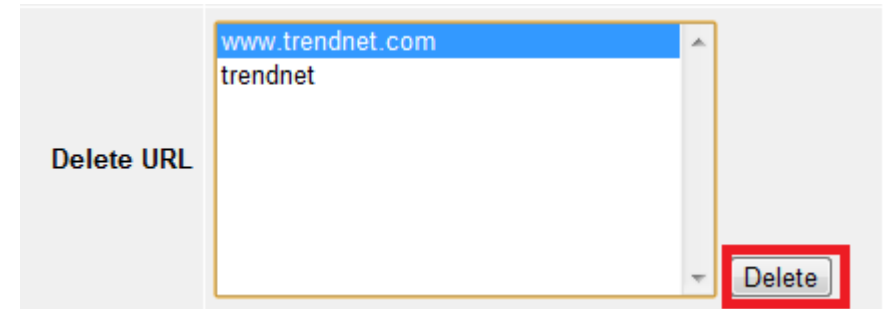*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

You can verify the time/date settings next to **Local Time** at the top of the page. **Local Time** displays the current date and time set on your router.

Manually configure your Internet connection

Advanced Setup > WAN

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **WAN**.

3. Select the type of Internet connection provided by your Internet Service Provider (ISP).

Note: *If you select the Internet connection type radio button option in the center of the page,* click **Next** *at the bottom of the page to continue, otherwise if you select your Internet connection type from the left-hand panel, continue to the next step.*

4. Complete the fields required by your ISP.

Note: *Complete the optional settings only if required by your ISP.*

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click* **Cancel** *before you click* **Apply.**

(For Static IP connection types) Additionally, if you are using a connection type that requires a static IP address, you may need to specify the DNS server IP addresses under the **DNS** section located in the left-hand panel. Click **Apply** at the bottom of the page.
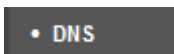
Note: *If you are unsure which Internet connection type you are using, please contact your ISP.* **Note:** *If your ISP requires a host name to be specified, you can specify it under Advanced Setup > WAN > Dynamic IP, in the* **Host Name** *field. To save changes, click* **Apply** *at bottom of the page.*

Clone a MAC address

Advanced Setup > WAN > Dynamic IP

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

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **WAN**, then click on **Dynamic IP.**

3. Find the **MAC Address** section shown below.

4. Click either **Clone MAC Address** to clone the MAC address of the computer you are currently using or manually enter the 12-digit MAC address of your old router.

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click* **Cancel** *before you click* **Apply.**

Change your router IP address

Advanced Setup > LAN > LAN Settings

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

Note: *If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.*

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **LAN**, then click on **LAN Settings**.

3. Enter the router IP address settings.

| IP Address | 192 | . | 168 | . | 10 | . | 1 |
| Subnet Mask | 255 | . | 255 | . | 255 | . | 0 |

- **IP Address** – Enter the new router IP address. (e.g. *192.168.200.1*)
- **Subnet Mask** – Enter the new router subnet mask. (e.g. *255.255.255.0*)

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

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click **Cancel** before you click **Apply.***

Apply   Cancel

Note: *You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default http://192.168.10.1 using your new router IP address will use the following format using your new router IP address http://(new.router.ipaddress.here) to access your router management page.*

Set up the DHCP server on your router

Advanced Setup > LAN > LAN Settings

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

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **LAN**, then click on **LAN Settings**.

3. Review the DHCP Server settings.

- **This Gateway acts as a DHCP Server** – Enables or Disables the DHCP server.
- **IP Pool Starting Address** – Changes the starting address for the DHCP server range. (use last IP address number only such as *192.168.10.20*)
- **End IP** – Changes the last address for the DHCP server range. (use last IP address number such as *192.168.10.30*)

Note: *The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*

- **Lease Time** – Click the drop-down list to select the lease time.
  Note: The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.

- **Local Domain Name (optional)** – Specifies a domain name to assign to computers or devices. (e.g. *trendnet.com*)

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

You can view the list of active lease entries for computers or devices that have been assigned IP addresses automatically from the DHCP server on your router by clicking **DHCP Client List** in the left-hand panel. You can click **Refresh** to refresh the list.

Host Name	IP Address	MAC Address	Remaining Time	Static
	192.168.10.101	00:14:D1:26:E4:76	21:11:01	☐

Set up DHCP reservation

Advanced Setup > LAN > DHCP Client List

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding or port mapping, see "Virtual Server" on page 27 or "Port Mapping" on page) or special applications (also called port triggering, see "Special Applications" on page 28).

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **LAN**, then click on **DHCP Client List**.

3. You can choose one of the following options to assign a DHCP reservation

You can select from the list of active lease entries for computer or devices that have been assigned IP addresses automatically from the DHCP server on your router. To set the IP address currently used to a static DHCP reservation, check the **Static** option next to the entry.

Host Name	IP Address	MAC Address	Remaining Time	Static
	192.168.10.101	00:14:D1:26:E4:76	21:11:01	☐

- **Host Name** – Name of the computer or network device.
- **IP Address** – The IP address currently assigned to the computer or network device.
- **MAC Address** – The MAC (Media Access Control) address of the computer or network device.
- **Remaining Time** – The remaining lease time of the IP address assigned.
- **Static** – If checked, assigns the current IP address to the computer or network device as a DHCP Reservation.

Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **OK**.*

OR

You can manually add a DHCP Reservation by manually entering in the information under **Static Client Configuration** if the entry does appear in the list.

- **Host Name** – Enter the host name of the computer or network device to assign the reservation.
- **IP Address** – Enter the IP address to assign to the reservation. (use last IP address number such as *192.168.10.102)*
  Note: You cannot assign IP addresses outside of the DHCP range. The IP address is required to be within the DHCP IP address range (IP Pool Starting & Ending IP).
- **MAC Address** – Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC)*

Click **Add** to add the DHCP Reservation to the list of active lease entries.

Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **OK**.*

To remove an existing reservation, uncheck the **Static** option next to the entry in the list and click **OK** to apply the setting.

Enable/disable UPnP on your router

Advanced Setup > System > Administrator Settings

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

1. Log into your router management page (see "Access your router management page" on <u>page 16</u>).

2. Click on **Advanced Setup** and click on **System**, then click on **Administrator Settings**.

3. Under **UPnP**, check **Enable** or uncheck to disable UPnP on your router.

- **Enable** - Check the box to enable UPnP (Universal Plug and Play) functionality.
- **Advertise Time** - This is the interval the router will send out UPnP advertisements. By default, the router is configured to send out an advertisement every 1800 seconds.

Note: It is recommended to leave the UPnP setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Allow VPN connections through your router

Advanced Setup > NAT > Passthrough

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling.

If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Passthrough**.

3. Next to **PPTP passthrough, IPsec passthrough, or L2TP passthrough** (depending the VPN protocol your corporation requires) check to Enable or uncheck to Disable the VPN passthrough feature on your router.

Note: It is recommended to leave these settings enabled.

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Allow FTP connections using an FTP Non-standard port

Advanced Setup > NAT > Passthrough

The FTP (File Transfer Protocol) non-standard port setting applies only if you are hosting an FTP server on your local network which is accessible from computers or network devices located on the Internet and using a different port setting other than the standard TCP port 21 for server connections. If you encounter connection issues using a different port for FTP server connections other than TCP port 21, use the FTP non-standard port setting to specify a different port used for FTP communication.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Passthrough**.

3. Under **FTP**, in the field labeled **Non-standard FTP port**, enter the FTP port (other than the standard port 21) that you would like to use for FTP server connections.

Note: Select a port number from the port range of 0-65535. The port setting must match the port number assigned on your FTP server.

4. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **OK.***

Allow NetMeeting H.323 connections through your router

Advanced Setup > NAT > Passthrough

The NetMeeting H.323 passthrough applies only to you if you are using the NetMeeting application on your network. NetMeeting is a Windows-based application used for VoIP (Voice over IP) and video conferencing communications over the Internet. The NetMeeting application requires the use of the H.323 protocol for video/audio conferencing. If you use the NetMeeting application in your network for video conferencing, please ensure the NetMeeting H.323 passthrough option is checked (Enabled).

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Passthrough**.

3. Under **NetMeeting**, check the **H323/Netmeeting passthrough** option to enable the protocol required for the NetMeeting application to communicate through your router. Unchecking this option will disable the feature.

Note: It is recommended to leave these settings enabled.

4. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **OK.***

Allow/deny ping requests to your router from the Internet

Advanced Setup > Firewall > Block WAN Ping

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **Firewall**, then click on **Block WAN Ping**.

3. Check the **Block PING from WAN side** option to deny ping requests from the Internet to your router. Uncheck the option to allow ping requests from the Internet to your router.

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Identify your network on the Internet

Advanced Setup > WAN > Dynamic DNS

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

Note: First, you will need to sign up for one of the DDNS service providers listed in the Server Address drop-down list.

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *dyndns.com, no-ip.com*, etc.)

2. Log into your router management page (see "Access your router management page" on page 16).

3. Click on **Advanced Setup** and click on **WAN**, then click on **Dynamic DNS**.

4. Check the **Use Dynamic DNS Service** option to Dynamic DNS.

5. In the **Server Provider** drop-down list, select the provider you selected, and enter your information in the fields.

- Host Name: Personal URL provided to you by your Dynamic DNS service provider (e.g. trendnet.dyndns.biz)
- User Name: The user name needed to log in to your Dynamic DNS service account
- Password: This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.

6. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: If you would like to discard the changes, click Cancel before you click Apply.

Allow remote access to your router management page

Advanced Setup > System > Administrator Settings

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Administrator Settings**.

3. Under the **Remote Management** section, check the **Enable** option.

Note: Unchecking the Enable option will disable Remote Management.

Remote Management

Enable	☐			
IP Address	0	. 0	. 0	. 0
	(0.0.0.0: means all legal ip address can access the device.)			
Port	8080			

- **IP Address** – It is recommended to leave this setting as 0.0.0.0, to allow remote access from anywhere on the Internet.
  Note: You can enter an Internet IP address that is allowed to access your router management page and all others will be denied.

- **Port**– It is recommended to leave this setting as 8080.
  Note: *If you have configured port 8080 for another configuration section such as virtual server, port mapping or port trigger, please change the port to use. (Recommended port range 1024-65534)*

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

[**Apply**] [**Cancel**]

Open a device on your network to the Internet

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

DMZ

Advanced Setup > Firewall > DMZ

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

It is strongly recommended to use **Virtual Server** (also called port forwarding, see "Virtual Server" on page 27) or **Port Mapping** (see on page 28) to allow access to your computers or network devices from the Internet.

1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address (or you can use the DHCP reservation feature to ensure the device has a fixed IP address) (see "Set up DHCP reservation" on page 20).

      A. Signing up for a Dynamic DNS service (outlined in the DDNS section page 24) will provide identification of the router's network from the Internet.

2. Log into your router management page (see "Access your router management page" on page 16).

3. Click on **Advanced Setup** and click on **Firewall**, then and click on **DMZ**.

4. Next to **DMZ function**, click **Enabled**.

DMZ function	◉ Enabled ○ Disabled

5. In the **DMZ Host** field, enter the IP address you assigned to the computer or network device to expose to the Internet. (use last IP address number such as *192.168.10.101*) The entry will appear in the list when it has successfully been added.

6. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

Public IP drop-down list

If you have a dynamic IP WAN/Internet connection, then the **Public IP** drop-down list will only list the single IP address assigned to you by your ISP and you will only have one IP address available at any given time for these Internet connection.

Note: You will only be able to specify assign multiple DMZ public IP entries when using the Static IP WAN Internet connection type.

If you have a static IP WAN/Internet IP connection type, the **Public IP** drop-down list will have your static IP address listed.

Contact your ISP for details if you have more than one static public IP address available.

If your ISP has assigned you with multiple static IP addresses and you would like to add multiple static WAN public IP addresses:

a. Log into your router management page (see "Access your router management page" on page 16).

b. Click on **Advanced Setup** and click on **WAN**, then click on **Static IP**.

c. Next to **Does ISP provide more IP addresses** option, check **Yes**.

d. Under **Alias IP Address**, enter each additional static public IP address, then click **Add** for each IP address additional IP address will also be listed and available to select from.

e. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

If you have multiple static WAN/Internet IP addresses assigned by your ISP (Internet Service Provider), you can map these WAN/Internet IP addresses to a local computer or device on your network and expose these computers or devices on your network to the Internet to allow anyone to access them. Your router includes the capability of forwarding all the ports and services available on the WAN/Internet IP side IP address and forwarding them to specified IP address (computers or network devices) on your network.

Virtual Server

Advanced Setup > NAT > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see DMZ on page 25) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (See DynDNS section).

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Virtual Server**.

3. Review the virtual server settings.

Enabled	☐
Private IP	192.168.10. [ ]
Private Port	[ ]
Public Port	Type [TCP ▼] [ ]
Comment	[ ]

- **Enabled** – Checking the **Enabled** option turns on the virtual server and unchecking the option turns off the virtual server.
- **Private IP** – Enter the IP address of the device to forward the port (use last IP address number such as *192.168.10.101*)
  Note: You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Private Port** – Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Public Port** –
  - **Type** – Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).
    Note: Please refer to the device documentation to determine which ports and protocols are required.
  - In the empty field, enter the port number used to access the device from the Internet.

*Note: The **Public Port** can be assigned a different port number than the **Private Port** (also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required.*

- **Comment** – You can enter a comment for the virtual server to make it more easily identifiable.

4. Click **Add** to add the virtual server entry to the list. [Add]

Rules Listing				0/40(using/max)
Comment	Private IP	Private Port	Public Port	Action

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

[Apply] [Cancel]

To modify an entry, next to the entry under **Action** in the list, click the notepad icon and the virtual server fields will populate with the settings of the entry. Modify the settings and click **Modify** [Modify]. Then click **Apply** at the bottom of the page.

To delete an entry, next to the entry under **Action** in the list, click the trash icon and click **Apply** at the bottom of the page.

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (See DynDNS section).

2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)

3. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 20).
Note: You may need to reference your camera documentation on configuring a static IP address.

4. Log into your router management page (see "Access your router management page" on page 16).

5. Click on **Advanced Setup** and click on **NAT**, then click on **Virtual Server**.

6. Click **Enabled** to turn on the virtual server.

7. Next to **Private IP**, enter the IP address assigned to the camera. (use the last IP address number such as *192.168.10.101*)

8. For the **Private Port,** enter the port number **80**

9. For **Public Port**, select the **Type** as **TCP** and enter the port number **80**.

10 Next to **Comment**, you can enter a comment for the virtual server to make it more easily identifiable. (*e.g. TRENDnet Camera*)

Enabled	☑
Private IP	192.168.10. 101
Private Port	80
Public Port	Type TCP ▼ 80
Comment	TRENDnet Camera

10. Click **Add** to add the virtual server to the list.

Rules Listing				1/40(using/max)	
	Comment	**Private IP**	**Private Port**	**Public Port**	**Action**
☑	TRENDnet Camera	192.168.10.101	80	tcp / 80	✎ 🗑

11. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **Apply**.*

Apply **Cancel**

Port Mapping
Advanced Setup > NAT > Port Mapping

The Port Mapping function is similar to the virtual server function except you cannot specify a different public port and private port (also known as port redirection). The ports you specify in Port Mapping are set to be the same for both public and private ports. Also, in the port mapping section, would will be able to specify multiple ports per entry instead of one port per entry.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Port Mapping**.

3. Review the port mapping settings.

Enabled	☐
Comment	
Server IP	192.168.10.
Mapping Ports (port1, port2, port3-port4...)	Type TCP ▼

- **Enabled** – Checking the **Enabled** option turns on the port mapping and unchecking the option turns off the port mapping.
- **Comment** – You can enter a comment for the virtual server to make it more easily identifiable.
- **Server IP** – Enter the IP address of the device to forward the port (use last IP address number such as *192.168.10.101)*

  Note: You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Mapping Ports (port1,port2,port3,port4…)** –
  - **Type** – Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).

    Note: Please refer to the device documentation to determine which ports and protocols are required.
  - In the empty field, enter the port or ports used to access the device from the Internet. (*e.g. 20,21,22,23,24, etc.)*

Note: Please refer to the device documentation to determine which ports and protocols are required.

4. Click **Add** to add the port mapping entry to the list. [Add]

Rules Listing			0/10(using/max)
Comment	Server IP	Mapping Ports	Action

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

[Apply] [Cancel]

To modify an entry, next to the entry under **Action** in the list, click the notepad icon and the port mapping fields will populate with the settings of the entry. Modify the settings and click **Modify** [Modify]. Then click **Apply** at the bottom of the page.

To delete an entry, next to the entry under **Action** in the list, click the trash icon and click **Apply** at the bottom of the page.

Port Trigger

Advanced Setup > NAT > Port Trigger

Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on page 21.

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **NAT**, then click on **Port Trigger**.

3. Review the port trigger settings.

Enabled	☐
Trigger Port	___ ~ ___
Trigger Type	TCP ▾
Public Port	___ ~ ___
Type	TCP ▾
Comment	___

- **Enabled** – Checking the **Enabled** option turns on the virtual server and unchecking the option turns off the virtual server.
- **Trigger Port** – Enter the ports or port range requested by the device. (e.g. *554-554 or 6112-6112).*

- **Trigger Type** – Select the protocol requested by the device. **TCP, UDP**, or you can select **Both** to choose both TCP and **UDP.**

  Note: Please refer to the device documentation to determine which ports and protocols are required.

- **Public Port** – Enter the ports or port range to open on your router to forward to the device. (e.g. 2000-2000 or *2000-2038).*

- **Type** – Select the protocol for the public ports to open on your router to forward to the device. **TCP, UDP**, or you can select **Both** to choose both TCP and **UDP.**

- *Note: Please refer to the device documentation to determine which ports and protocols are required.*

- **Comment** – You can enter a comment for the virtual server to make it more easily identifiable**.**

4. Click **Add** to add the port trigger entry to the list. [Add]

Rules Listing			0/10(using/max)
Comment	Trigger Port	Public Port	Action

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

[Apply] [Cancel]

To modify an entry, next to the entry under **Action** in the list, click the notepad icon and the port trigger fields will populate with the settings of the entry. Modify the settings and click **Modify** [Modify] . Then click **Apply** at the bottom of the page.

To delete an entry, next to the entry under **Action** in the list, click the trash icon and click **Apply** at the bottom of the page.

Set up Quality of Service (QoS) on your router

Advanced Setup > QoS

The QoS section allows you to configure quality of service features such as port based rate limiting or DSCP (Differentiated Services Code Point or Diffserv) in order to prioritize specific types of traffic through your router.

Port Based

Advanced Setup > QoS > Port Based

The port based rate limiting feature allows you to set and control the amount of bandwidth (kbps) allowed per port.

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **QoS**, then click on **Port Based**.

3. Under **Settings,** check the **Enable Rate Control** option to enable port based rate limiting.

Settings	
Enable Rate Control	☑

4. Next to each port, enter the amount of bandwidth in kbps to allocate per port.

LAN-1	LAN-1	0	kbps
LAN-2	LAN-2	0	kbps
LAN-3	LAN-3	0	kbps
LAN-4	LAN-4	0	kbps
WAN	WAN	0	kbps

5. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **OK.***

DSCP Based

Advanced Setup > QoS > Port Based

The DSCP based QoS feature allows you to configure DSCP (Diffserv) QoS parameters for the purpose of end-to-end QoS prioritization working together with other devices on your network that support DSCP. Configuration of this feature requires that the user have more advanced knowledge of DSCP (Differv) QoS prioritization.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **QoS**, then click on **DSCP Based**.

3. Under **Settings,** check the **Enable DSCP** option to enable DSCP based QoS.

3. Review the DSCP based QoS settings and apply the settings accordingly.

- **Queue weight (High, Medium, Low)** – For each weight, enter the weights according to the overall DSCP QoS configuration of your network devices.
- **Enable Rule** – Check the option to enable the DSCP based QoS rule to apply traffic prioritization.
- **DSCP Value** – Enter the DSCP value for the rule.
- **Queue Map** – Select a priority queue weight from the drop-down list to apply to the rule.
- **Description** – Enter a brief description to make the rule more easily identifiable to it's purpose. Click Add and it will appear in the Rules Listing table. Click OK to save the changes.
- **Rules Listing Table** – After DSCP rules are added they will appear in this table. To modify an entry, under Action, click the notepad icon next to the entry and the information will populate the fields provided. After modifying the entry, click Modify. To delete an entry, under Action, click the trash icon. Click OK to save the changes.

4. Click **Add** to add the DSCP entry to the list.

5. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **OK.***

To modify an entry, next to the entry under **Action** in the list, click the notepad icon and the DSCP fields will populate with the settings of the entry. Modify the settings and click **Modify** . Then click **Apply** at the bottom of the page.

To delete an entry, next to the entry under **Action** in the list, click the trash icon and click **Apply** at the bottom of the page.

Prevent ARP spoofing attacks on your network

Advanced Setup > Routing > ARP Binding Table

The ARP binding feature provides an additional security feature and allows you to map specific MAC addresses to specific IP addresses which can prevent spoofing attacks (computers or devices pretend to be an IP address or MAC address that they are actually not). Since there is an entry in the ARP binding table, communication requests from computers or devices that do not match the entry in both IP address and MAC address will be denied.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **Routing**, then click on **ARP Binding Table**.

3. Check the **ARP spoofing prevention** option to enable the feature.

ARP spoofing prevention	☑

4. Review the ARP binding settings.

Bind	☐
Host Name	
IP Address	
MAC Address (XX:XX:XX:XX:XX:XX)	

- **Bind** - Check the option to enable the ARP binding entry.
- **Host Name** - Enter the host/computer/device name for the binding entry.
- **IP Address** - Enter the IP address of the computer or device for the binding entry.
- **MAC Address** - Enter the 12-digit MAC address of the computer or device for the binding entry, then click Add and click OK to save the changes.
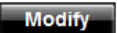
  (ex. AA:BB:CC:11:22:33)

4. Click **Add** to add the ARP binding entry to the list. [Add]

5. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.
*Note: If you would like to discard the changes, click **Cancel** before you click **OK**.*
[OK] [Cancel]

To modify an entry, next to the entry under **Action** in the list, click the notepad icon and the ARP binding fields will populate with the settings of the entry. Modify the settings and click **Modify** [Modify]. Then click **Apply** at the bottom of the page.

To delete an entry, next to the entry under **Action** in the list, click the trash icon and click **Apply** at the bottom of the page.

Prevent DoS (Denial of Service) attacks on your network

Advanced Setup > Firewall > DoS

The DoS (Denial of Service) feature allows you to enable advanced firewall protection for the most common denial of service attacks from the Internet. Denial of service are typically initiated by hackers or malicious users that are attempting to steal confidential information or purposely sending repeating false communication requests in order to stop a system (router, network device, computer) from working or functioning or significantly reducing a system's performance. Your router supports both DoS detection and prevention.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **Firewall**, then click on **DoS**.

3. Under **Settings**, check the **Enabled** option to enable the feature.

4. Under **Options**, check the DoS attacks you would you're your router to detect and prevent. For some types of attacks, you can set the threshold value before your router is triggered to prevent/deny the specified protocol/traffic.

5. Click **OK** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **OK.***

Enable/Disable NAT on your router

Advanced Setup > WAN > NAPT

Checking this option enables NAPT (Network Address and Port Translation) or also known as NAT (Network Address Translation) on your router which allows multiple private IP addresses on your LAN through a single IP Internet public IP address assigned by your ISP. NAPT enabled is the default setting and is recommended setting. Unchecking this option will disabled NAPT or NAT and allow your router to work in Route mode only which can be configured under the Routing section. Disabling NAT will not put your router in bridge mode. ***Note:*** *Disabling this feature assumes that you have some general networking knowledge.*

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **WAN**, then click on **NAPT**.

3. Under **Operating Mode,** check the **NAPT** option to enable NAT or uncheck to disable NAT.

Note: *It is recommended to leave this setting enabled.*

Operating Mode	
NAPT	☑

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click ***Cancel*** before you click ***Apply.***

Enable/Disable IGMP Snooping on your router

Advanced Setup > LAN > IGMP Snooping

If you run multicast traffic on your network, the IGMP (Internet Group Management Protocol) snooping feature will enable multicast traffic filtering on the LAN ports of your router. IGMP snooping will listen and detect multicast traffic on your router LAN ports and ensure that only the ports that require multicast communication will send and receive multicast traffic instead of sending and receiving multicast traffic on all LAN ports. Multicast traffic can sometimes cause unnecessary and high traffic load on your switch or router device which results in slow connectivity between devices on your network and to the Internet. It is strongly recommended to enable IGMP snooping if you use multicast communication on your network in order to prevent slow connectivity and high traffic loads on your router.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **LAN**, then click on **IGMP Snooping**.

3. Next to **IGMP Snooping**, check the **Enabled** option to enable IGMP snooping on your router.

IGMP Snooping	☑ Enabled

4. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click ***Cancel*** before you click ***Apply.***

Add static routes to your router

Advanced Setup > Routing > Static Routing

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

Note: *Configuring this feature assumes that you have some general networking knowledge.*
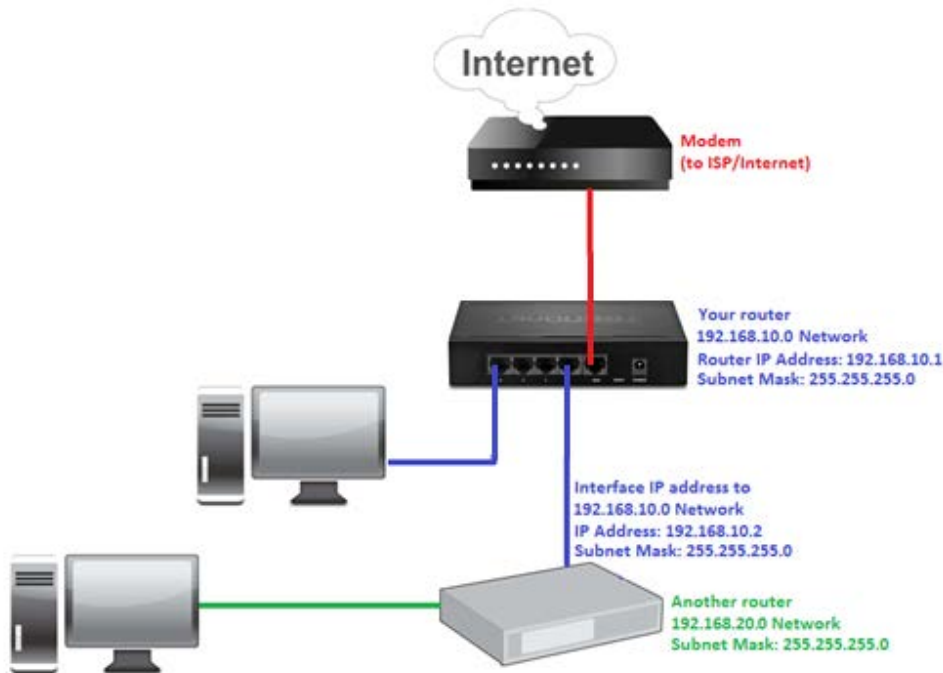
1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and **Routing,** then click on **Static Routing**.

3. Review the static routing settings.

- **Destination LAN IP** – Enter the IP network address of the destination network for the route.
  (e.g. *192.168.20.0*)
- **Subnet Mask** – Enter the subnet mask of the destination network for the route.
  (e.g. *255.255.255.0*)
- **Gateway** – Enter the gateway to the destination network for the route.
  (e.g. *192.168.10.2*)

4. Click **Add** to save the static route then click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

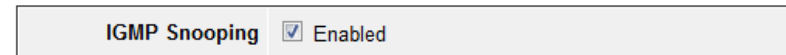**Note:** *If you would like to discard the changes, click Cancel before you click Apply.*

To delete an entry, next to the entry in the list, click Delete and click **Apply** at the bottom of the page.

Enable dynamic routing on your router

Advanced Setup > Routing > Dynamic Routing

You may want to setup your router to route computers or devices on your network to other local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other routers to exchange information about the network.

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and **Routing,** then click on **Dynamic Routing**.

3. Review the dynamic routing settings.

Enable Dynamic Routing	☑
Working Mode	Router
Listen Mode	Disabled
Supply Mode	Disabled

- **Enable Dynamic Routing** – Check the option to enable dynamic routing or uncheck to disable dynamic routing.
- **Working Mode** – Select the operation mode for your router when using dynamic routing.
  - o **Router** – Use this mode when using your router to route traffic locally only and not being used for a NAT default gateway to the Internet.
  - o **Default Gateway** - Use this mode when using your router to route traffic locally and simultaneously used as a NAT default gateway to the Internet.

- **Listen Mode** – Click the drop-down list to select which dynamic routing protocols your router will receive from other router so your router can build routes to other networks.
  - o **Disabled** – Disable receiving routing information from other routers to your router.
  - o **RIP 1** - Receive routing information from other routers using the RIP version 1 protocol.
  - o **Both (RIP1+RIP2) –** Receive routing information from other routers using both RIP version 1 & 2 protcols.
  - o **RIP 2** – Receive routing information from other routers using the RIP version 2 protocol.
- **Supply Mode** – Click the drop-down list to select which dynamic routing protocols your router will send out to other routers so other routers can dynamically build routes to your network.
  - o **Disabled** – Disable sending routing information from your router to other routers.
  - o **RIP 1** - Sends out routing information to other routers using the RIP version 1 protocol.
  - o **RIP 2 Broadcast** – Broadcasts routing information to other routers using the RIP version 2 protocol
  - o **RIP 2 Multicast** – Sends out routing information via multicast to other routers using the RIP version 2 protocol.

4. Click **Add** to save the static route then click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Apply	Cancel

You can view the routes defined in your router in the Routing Table section (Advanced Setup > Routing > Routing Table). You can click **Refresh** Refresh to refresh the table.

Destination Network IP	Subnet Mask	Gateway IP
0.0.0.0	0.0.0.0	10.10.10.254
10.10.10.0	255.255.255.0	10.10.10.0
192.168.10.0	255.255.255.0	192.168.10.0

.

Router Maintenance & Monitoring

Reset your router to factory defaults

Advanced Setup > System > Configuration Tools

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on page 38.

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

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

  OR

- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Configuration Tools.**

3. Under **Restore to Factory Default**, click **Reset**. When prompted to confirm this action, click **OK**. Wait for your router to reboot. Your router will be reset to default settings after reboot.

Reset to Factory Default

To reset the factory default settings of the Firewall Router, click on the "Reset" button. You will be asked to confirm your decision.

[Reset]
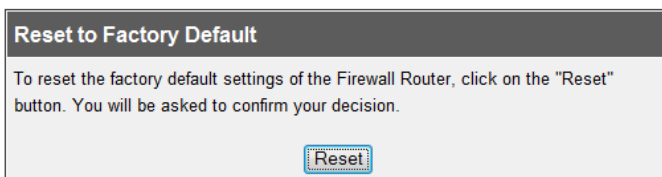
Router Default Settings

Administrator User Name	admin
Administrator Password	admin
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199

Backup and restore your router configuration settings

Advanced Setup > System > Configuration Tools

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

To backup your router configuration:

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **System**, then click on **Configuration Tools**.

3. Under **Backup Settings**, click **Backup Settings**.

Backup Settings

Please press the "Backup Settings" button to save the configuration data to your PC

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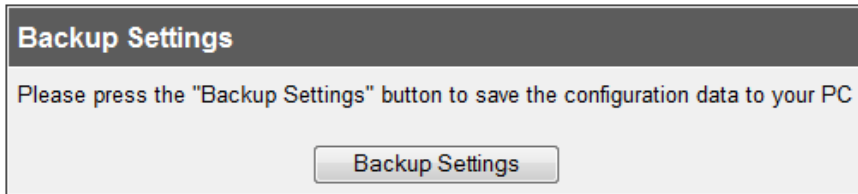
4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: yearmmdd-*cfg.bin)*

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on).

2. Click on **Advanced Setup** and click on **System**, then click on **Configuration Tools**.

3. Under **Restore Configuration Settings**, next to **Load Settings**, depending on your web browser, click on **Browse** or **Choose File**.

Restore Settings

Enter the path and name of the backup file then press the "Restore Settings" button below. You will be prompted to confirm the backup restoration.

[Browse...] [Restore Settings]

Restore Settings

Enter the path and name of the backup file then press the "Restore Settings" button below. You will be prompted to confirm the backup restoration.

[Choose File] No file chosen   [Restore Settings]

A separate file navigation window should open.

4. Select the router configuration file to restore and click **Restore Settings**.

(Default Filename: yearmmdd-*cfg.bin*). If prompted to confirm the action, click **Yes** or **OK**.

5. Wait for the router to restore settings and reboot.

Upgrade your router firmware

Advanced Setup > System > Firmware Upgrade

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

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

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

2. Unzip the file to a folder on your computer.

Please note the following:

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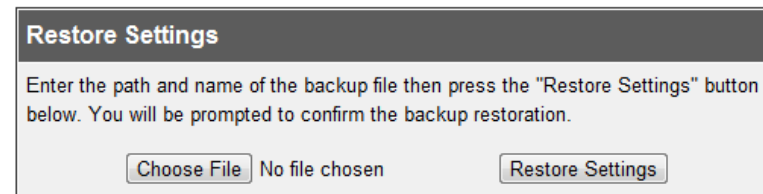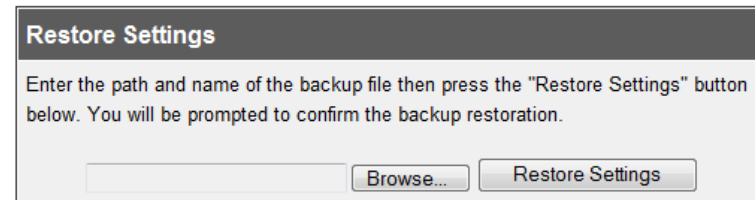- Any interruptions during the firmware upgrade process may permanently damage your router.

3. Log into your router management page (see "Access your router management page" on).

4. Click on **Advanced Setup** and click on **System**, then click on **Firmware Upgrade**.

Your router's current firmware version information will be listed as "**Current Firmware Version:**" and "**Firmware Date:**" .

5. Depending on your web browser, next to **Upgrade Firmware**, click **Browse** or **Choose File**.

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

7. Click **Apply** at the bottom of the page to start the firmware upgrade. If prompted to confirm the action, click **yes** or **OK**. Wait for your router to complete the firmware upgrade process and reboot.

Restart your router

Advanced Setup > System > Reboot

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.
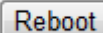
There are two methods that can be used to restart your router.

- **Turn the router off** for 10 seconds by disconnecting the power adapter connector from the power port located on the rear panel of your router, see "Product Hardware Features" on page 2. Then plug the power adapter connector back into the power port.
  Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.

  OR

- **Router Management Page** – This is also known as a soft reboot or restart.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Reboot**. Click the **Reboot** button. If prompted to confirm the action, click **yes** or **OK**.

Reboot

Check connectivity using the router management page

Advanced Setup > System > Network Diagnostics

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) and DNS Lookup test tools on your router management page.

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Network Diagnostics.**

3. To run a network connectivity test:

- Using the ping tool, under the Ping section next to Ping this IP Address, enter in the IP address *(e.g. 192.168.10.101)* to test and click Ping. You will see the ping test results in the Ping Results window.

- Using the DNS Lookup tool, under the **DNS Lookup** section next to **Domain name / URL**, enter in the domain or name/URL/web address (*e.g.www.trendnet.com*) to test and click **Lookup**. You will see the DNS Lookup results in the **DNS Lookup Results** window.

4. You will receive a *success* or *fail* result message of the IP address, host or domain name/URL/web address you entered providing a basic indication of the router's connectivity to the Internet or devices that are connected to your network.

Success Message: Testing ...   Successfully updated

Fail Message: Testing ...   Failed to update

Check the router system information

Advanced Setup > System > Status

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**. Then click on **Status**.

3. Review the device information.

WAN (Internet) Information

WAN	
Connection Type	Dynamic IP
WAN IP	
Subnet Mask	
Gateway	
DNS	
Secondary DNS	
Cable/DSL	Connected

- **Connection Type –** Displays the WAN (Internet) connection type.
- **WAN IP –** The current IP address assigned to your router WAN port or interface configuration.
- **Subnet Mask -** The current subnet mask assigned to your router WAN port or interface configuration.
- **Gateway –** The current gateway assigned to your router WAN port or interface configuration.

- **DNS (Domain Name System)** – The primary DNS address assigned to your router port or interface configuration.
- **Secondary DNS** – The secondary DNS address assigned to your router port or interface configuration.
- **Cable/DSL** – Displays the current WAN (Internet) connection status. When using DHCP Client (or Dynamic IP address) Internet connection type, you will provide the option to Release and Renew your IP address settings.

Release   Renew

Other Internet connection types such as PPPoE will provide the option to Connect and Disconnect.

Disconnect   Connect

Wired LAN Information

LAN	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

- **IP Address -** Displays your router's current IP address.
- **Subnet Mask –** Displays your router's current subnet mask.
- **DHCP Server -** Display your router's DHCP server status, enabled or disabled, and provides a link to the DHCP client listing.

System Information

- **System Time** – Display the router's current time and date settings.
- **System Boot Up Time** – The duration your router has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Connected Clients** – Displays the number of devices that are currently connected to the router.
- **Runtime Code Version –** The current firmware version your router is running.
- **LAN MAC Address** – The current MAC address of your router's wired LAN or interface configuration.
- **WAN MAC Address** – The current MAC address used by your router's WAN port or interface configuration.
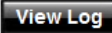
View your router log

Advanced Setup > System > Log Setting

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

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Log Setting**.

3. You can select from the following log types under the **Logs** section:

- **Outgoing (Internet) connections** – Click [View Log] to display log information related to outgoing Internet connections such as connections to your ISP.
- **System** - Click [View Log] to display log information related to router system functions such as device debug log information.
- **Firewall** – Click [View Log] to display log information related to security function on your router such as DoS, dropped packets, etc.

4. Review the device log information.

- **Time** – Displays the time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly. (See "Set your router date and time" on page 17)
- **Packet Information** – Displays a notification regarding the protocol and log message.

For Router Log Navigation, scroll the page down or up to navigate the log file.

Next to the **Download Log** option, you can also download the log file (.txt format) to a location on your computer by clicking **Download**. Then select a location on your local computer to save the log file.
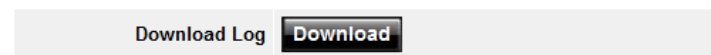
Configure your router log

Advanced Setup > System > Log Setting

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

Send router logs to your e-mail address

1. Log into your router management page (see "Access your router management page" on page 16).

2. Click on **Advanced Setup** and click on **System**, then click on **Log Setting**.

3. Under the **Settings** section, click the **Email Log** option.

Email Log	☑

4. Review the e-mail log settings.

Send Email	send
Sender Email Address	
Receiver Email Address	
SMTP Server	0.0.0.0
Enable Authentication	☐
Account Name	
Password	
Re-type Password	

- **Send Email** – Click **send** to send a test e-mail with the current router log using your email settings.
- **Sender Email Address** – Enter a sender e-mail address. (e.g. *router@trendnet.com*)

  Note: *This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.*
- **Receiver Email Address** – Enter your e-mail address or the email address you would like to send the log file.
- **SMTP Server** – Enter the IP address (e.g. *10.10.10.10*) or domain name (e.g. *mail.trendnet.com*) of your e-mail server.
- **Enable Authentication** – Check this option if your e-mail service requires authentication. Otherwise, if your e-mail service does not require authentication, leave this option unchecked.

  Note: *If you are unsure of this setting check with your e-mail service provider if authentication is required.*
- **Account Name** – For authentication, enter your account user name for your e-mail service.
- **Password** – For authentication, enter your password for your e-mail service.
- **Re-type Password** – For password confirmation, re-enter your password for your e-mail service.

  Note: *The port used for SMTP is the default TCP/UDP port 25.*

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

Note: *If you would like to discard the changes, click **Cancel** before you click **Apply.***

Apply	Cancel

Send router logs to an external log server

1. Log into your router management page (see "Access your router management page" on <ins>page 16</ins>).

2. Click on **Advanced Setup** and click on **System**, then click on **Log Setting**.

3. Under the **Settings** section, click the **Remote Log** option.

Settings	
Remote Log	☑

4. **Log Server**, enter the IP address of the external log server to send router logging.

Log Server	0.0.0.0

5. Click **Apply** at the bottom of the page to apply the changes. After the settings have been applied, click **Continue** on the following page.

*Note: If you would like to discard the changes, click **Cancel** before you click **Apply.***

Apply   Cancel

Router Management Page Structure

Quick Setup

- Setup Wizard

Advanced Setup

System

- System Time
- Administrator Settings
  - o Password Settings
  - o Remote Management
  - o UPnP
- Network Diagnostics
  - o Ping Test
  - o DNS Lookup
- Firmware Upgrade
- Configuration Tools
  - o Reset to Factory Default
  - o Backup Settings
  - o Restore Settings
- Status
  - o WAN Information
  - o LAN Information
  - o System Information
- Log Setting
  - o View/Download Logs
  - o Remote Log (Syslog)
  - o E-mail Log
- Reboot

WAN

- Dynamic IP
- Static IP
- PPPoE
- PPTP
- L2TP
- DNS
- Dynamic DNS
- NAPT

LAN

- LAN Settings
- IP Address Settings
- DHCP Server
- IGMP Snooping
- DHCP Client List
- Static DHCP Client / DHCP Reservation

NAT

- Virtual Server
- Port Trigger
- Port Mapping
- Passthrough
  - o VPN
  - o Non-standard FTP
  - o NetMeeting

Firewall

- Block WAN Ping
- Client Filtering
- MAC Control
- DMZ
  - o Multiple DMZ (One-to-one NAT)
- URL Filter
- DoS (Denial of Service)

Routing

- Routing Table
- Static Routing
- Dynamic Routing
- ARP Binding

QoS (Quality of Service)

- Port Based
- DSCP Based (Diffserv)

Home

- Quick Setup
- Advanced Setup

Logout

- Log out of router management page

Technical Specifications

Hardware	
Standards	IEEE 802.3 10BASE-T Ethernet; IEEE 802.3u 100BASE-TX Fast Ethernet
WAN	1 x 10/100Mbps Auto-MDIX port (Internet)
LAN	4 x 10/100Mbps Auto-MDIX ports
Cabling	Ethernet: Cat. 5 up to 100 m Fast Ethernet: Cat. 5, 5e, 6 up to 100 m
Data Transfer Rate	Ethernet : 10Mbps/20Mbps (Half-Duplex/Full-Duplex) Fast Ethernet: 100Mbps/200Mbps (Half-Duplex/Full-Duplex)
LED Indicators	Power, WAN, Link/Act, LAN ports 1-4
Dimension	148 x 105 x 29 mm (5.8 x 4.1 x 1.1 in)
Weight	437 g (15.4 oz.)
Temperature	Operating: 0°C ~ 40°C (32°F ~ 104°F) Storage: -10° C ~ 70° C (14° F ~ 158° F)
Humidity	Max. 90% (non-condensing)
Power	Input: 100~240V AC, 50~60Hz Output: 5V DC, 1A
Power Consumption	4.1 W (max)
Certifications	CE, FCC
Router	
Connection Type	Dynamic IP, Static (Fixed) IP, PPPoE, PPTP, L2TP
Network Protocols	TCP/IP, NAT/SPI, UDP, ICMP, PPPoE, UPnP, HTTP, DHCP,

	PAP, CHAP, DNS, DDNS, ARP, IGMP Snooping, NAPT, Multi-DMZ, DSCP
Firewall	NAT/SPI DoS (Denial of Service) Prevention Options ARP Binding & ARP Spoofing Prevention MAC Address Filter (32 entries) URL/Keyword Filter (32 entries) Client Filtering w/Scheduling (20 entries) Port Trigger/Special Applications (10 entries) Virtual Servers (40 entries) Port Mapping (10 entries) DMZ (6 entries)
Application Layer Gateway (ALG)	Non-Standard FTP Port Netmeeting/H.323 IPSec, L2TP, PPTP pass-through (Up to 100 VPN sessions)
QoS	Port-based bandwidth control (Kbps) and DSCP
Routing	Static Routes (20 entries) & Dynamic RIPv1/2
Management	Web browser configuration, Firmware upgrade through web browser, Save/Restore configuration, Ping tool, Internal Log, DNS Lookup

Troubleshooting

Q: I typed http://192.168.10.1 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?
Answer:
1. Check your hardware settings again. See "Router Installation" on page 2.
2. Make sure the LAN and WAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Obtain an IP address automatically* or *DHCP* (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.

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

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

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

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

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?
Answer:
Contact your Internet Service Provider (ISP) for the correct information.

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

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?
Answer:
1. Verify that you can get onto the Internet with a direct connection into your modem (meaning, plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7

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

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

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

MAC OS X

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

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

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

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

Graphical Method

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

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

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

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

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

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

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

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

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

MAC OS 10.4/10.5/10.6
    a. From the **Apple**, drop-down list, select **System Preferences**.
    b. Click the **Network** icon.
    c. From the **Location** drop-down list, select **Automatic**.
    d. Select and view your Network connection.
        In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Network** and select the **TCP/IP** tab.
        In MAC OS 10.5/10.6, in the left column, select **Network**.
    e. Configure TCP/IP to use DHCP.

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

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

How to find your MAC address?

In Windows 2000/XP/Vista/7,

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

In MAC OS 10.4,

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

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

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

In MAC OS 10.5/10.6,

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

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

3. Click the **Advanced** button.

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

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of Directive 2004/108/EC of the Council (European Parliament) on the EMC directive and Energy-related products Directive 2009/125/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of Directive 2004/108/EC on the EMC directive and Energy-related products Directive 2009/125/EC:

- **EN 55022 : 2006 + A1 : 2007 Class B**
- **EN 61000-3-2 : 2009**
- **EN 61000-3-3 : 2008**
- **EN 55024 : 1998 + A1 : 2001 + A2 : 2003**

[cs] Česky [Czech]	TRENDnet tímto prohlašuje, že tento TW100-BRF214 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2004/108/ES.
[da] Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TW100-BRF214 overholder de væsentlige krav og øvrige relevante krav i direktiv 2004/108/EF.
[de] Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TW100-BRF214 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2004/108/EG befindet.
[et] Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TW100-BRF214 vastavust direktiivi 2004/108/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
[en] English	Hereby, TRENDnet, declares that this TW100-BRF214 is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.
[es] Español [Spanish]	Por medio de la presente TRENDnet declara que el TW100-BRF214 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2004/108/CE.
[el] Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΩΝΕΙ ΟΤΙ TW100-BRF214 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2004/108/ΕΚ.
[fr] Français [French]	Par la présente TRENDnet déclare que l'appareil TW100-BRF214 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2004/108/CE.
[it] Italiano [Italian]	Con la presente TRENDnet dichiara che questo TW100-BRF214 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2004/108/CE.
[lv] Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TW100-BRF214 atbilst Direktīvas 2004/108/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

[lt] Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TW100-BRF214 atitinka esminius reikalavimus ir kitas 2004/108/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TW100-BRF214 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2004/108/EG.
[mt] Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TW100-BRF214 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2004/108/EC.
[hu] Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TW100-BRF214 megfelel a vonatkozó alapvetõ követelményeknek és az 2004/108/EC irányelv egyéb elõírásainak.
[pl] Polski [Polish]	Niniejszym TRENDnet oświadcza, że TW100-BRF214 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2004/108/EC.
[pt] Português [Portuguese]	TRENDnet declara que este TW100-BRF214 está conforme com os requisitos essenciais e outras disposições da Directiva 2004/108/CE.
[sl] Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TW100-BRF214 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2004/108/ES.
[sk] Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TW100-BRF214 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2004/108/ES.
[fi] Suomi [Finnish]	TRENDnet vakuuttaa täten että TW100-BRF214 tyyppinen laite on direktiivin 2004/108/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar TRENDnet att denna TW100-BRF214 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2004/108/EG.

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.

TW100-BRF214 – 3 Years Warranty

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

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

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

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

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

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

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

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

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

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

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

PWP05202009v2   2012/4/20

TRENDNET ®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA