

User's Guide



4 - Port VPN Router

TW100-BRV214

Contents

Product Overview	1
Package Contents	1
Features	1
Product Hardware Features.....	2
Application Diagram	4
Basic Router Setup	5
Creating a Home Network	5
Router Installation	6
Virtual Private Networking (VPN)	12
Creating a Virtual Private Network.....	12
IPsec (Internet Protocol Security).....	13
Site-to-Site VPN.....	13
Client-Server VPN (Server Mode).....	17
PPTP (Point-to-Point Tunneling Protocol)	19
Client-Server VPN (Server Mode).....	19
Client-Server VPN (Client Mode).....	21
L2TP (Layer 2 Tunneling Protocol)	24
Client-Server VPN (Server Mode).....	24
Client-Server VPN (Client Mode).....	25
Access Control Filters	29
Access control basics	29
MAC Control.....	29
URL Filters	30
Keyword Blocking.....	31
Packet Outbound/Inbound Filters.....	31

Advanced Router Setup	34
Access your router management page.....	34
Set your router date and time	35
Clone a MAC address.....	36
Change your router IP address	37
Set up the DHCP server on your router	37
Set up DHCP reservation	39
Enable/disable UPnP on your router	40
Allow/deny VPN connections through your router.....	41
Allow/deny multicast streaming through your router	41
Enable/disable DoS (Denial of Service) Prevention	42
Allow/deny ping requests to your router from the Internet.....	42
Identify your network on the Internet	43
Allow remote access to your router management page.....	44
Open a device on your network to the Internet.....	45
DMZ.....	45
Virtual Computers	45
Virtual Server	46
Special Applications	47
Prioritize traffic using QoS (Quality of Service)	48
Create schedules	49
Add static routes to your router.....	50
Enable dynamic routing on your router	51
Enable route mode on your router.....	52
Using WoL (Wake on LAN) on your router	52
Router Maintenance & Monitoring	53
Reset your router to factory defaults.....	53

Router Default Settings 53

Backup and restore your router configuration settings 54

Upgrade your router firmware 55

Restart your router 56

Check connectivity using the router management page 56

Check the router status information 57

View your router log 59

Configure your router log 60

Enable SNMP on your router 61

Router Management Page Structure 63

Technical Specifications..... 64

Troubleshooting..... 65

Appendix 66

Product Overview



TW100-BRV214

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 (12V DC, 1A)

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

Features

The 4-Port VPN Router, model TW100-BRV214, manages up to 80 Virtual Private Network (VPN) tunnels. IPSec, L2TP, and PPTP VPN pass-through sessions are supported and a configurable firewall ensures the highest level of security.

Four Fast Ethernet ports on the back of the router help extend a wired network. Advanced Stateful Packet Inspection (SPI) and Network Address Translation (NAT) encryption protects your digital network. Advanced features include advanced Quality of Service (QoS) controls, Domain filtering, and packet filtering.

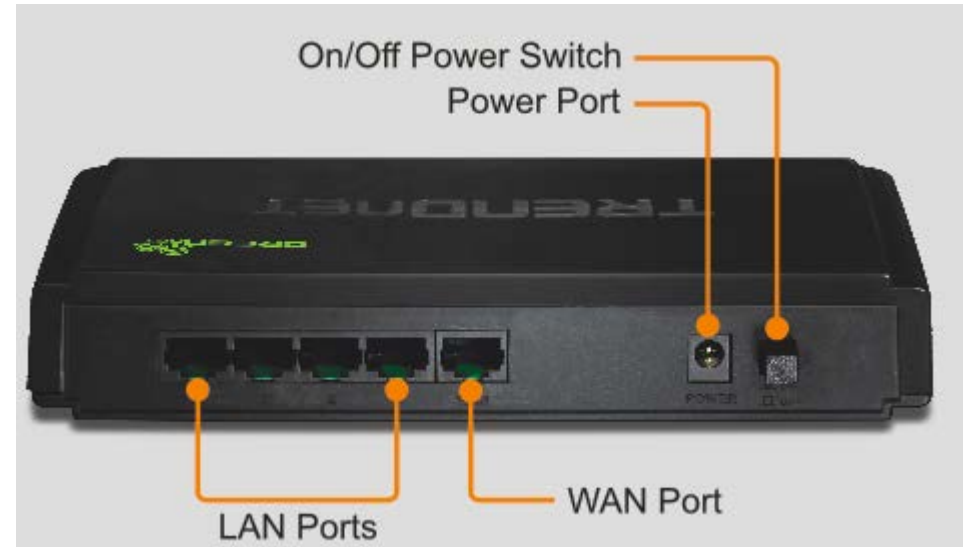
- 4 x 10/100 Mbps Auto-MDIX LAN ports
- 1 x 10/100 Mbps WAN port (Internet)
- On/off button
- Compatible with most popular cable/DSL Internet service providers using Dynamic/Static IP, PPPoE, PPTP and L2TP protocols
- Firewall protection with Network Address Translation (NAT), Stateful Packet Inspection (SPI), and Denial of Service (DoS) prevention
- Supports up to 80* PPTP/L2TP/IPsec tunnels
- Supports up to 100 PPTP/L2TP/IPsec VPN pass through sessions
- Access Control: Virtual Servers, MAC/IP Packet Filters, URL/Keyword Filters, Demilitarized Zone (DMZ) host, and Multi-DMZ
- Set device time using Network Time Protocol (NTP) and define schedules for Virtual Server, Packet Filters, and Quality of Service (QoS)
- Quality of Service (QoS) traffic prioritization via IP/(TCP/UDP) ports with 3 priority queues
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications
- Supports Internet Group Multicast Protocol IGMPv1/2 pass through for multicast applications
- Supports static and dynamic RIP v1/2 routing
- Dynamic DNS Client for dynamic Internet IP resolution
- Device monitoring using the Internal System Log, External Syslog, E-mail Alert, and SNMPv1/2c

- Local/Remote management via Web browser, upgrade firmware, and backup/restore configuration

*The number of supported concurrent VPN tunnels is dependent upon available bandwidth.

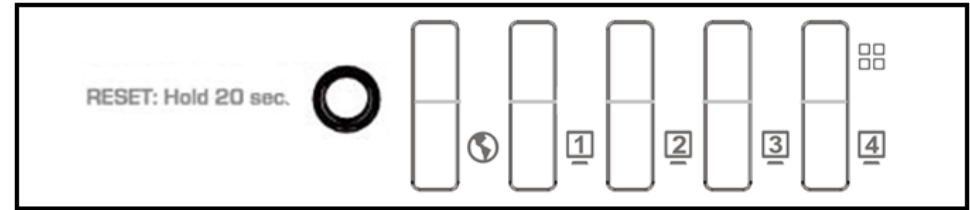
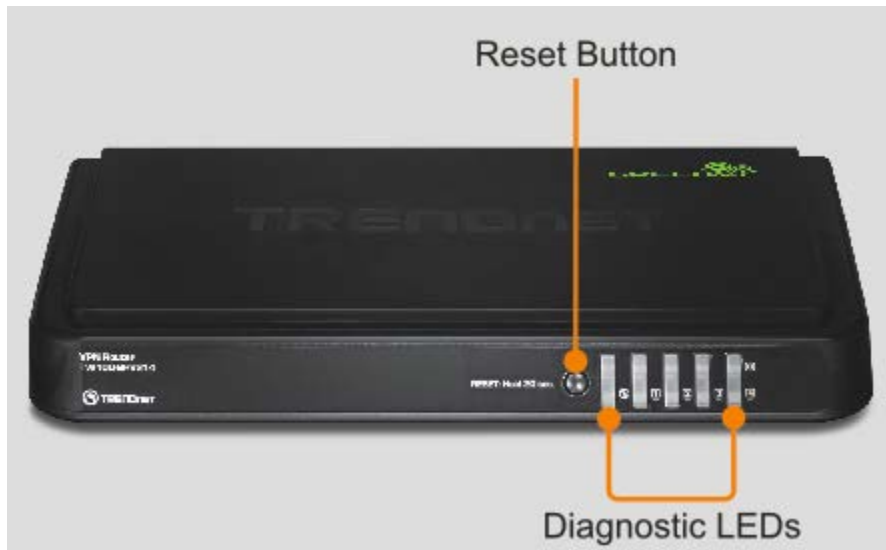
Product Hardware Features

Rear Panel View







- **LAN Ports** – Connect Ethernet cables (also called network cables) from your router LAN ports and to your wired network devices.
- **WAN Port** - Connect an Ethernet cable (also called network cable) from your router WAN port and to your xDSL/Cable 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.
- **On/Off Power Switch** – Push your router On/Off push button power switch to turn your router “On” (Inner position) or “Off” (Outer position).

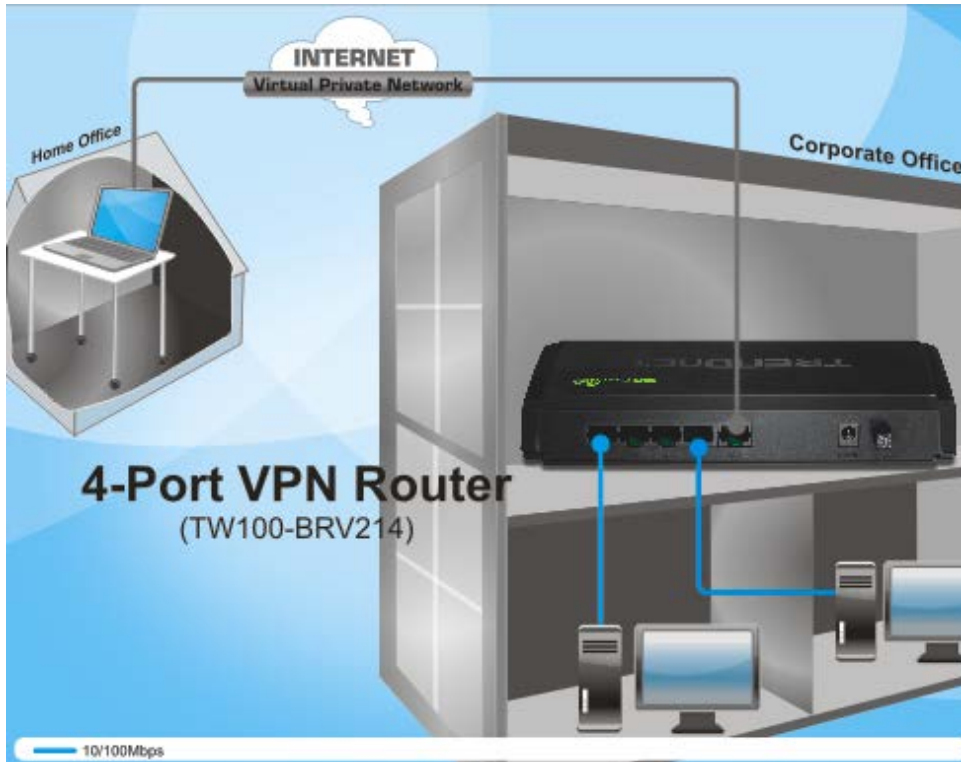
Front Panel View



Front Panel Button and LEDs

-  **Reset Button** – Push and hold this button for 20 seconds and release to reset your router to its factory defaults. The LEDs will blink rapidly when the reset process is activated.
-  **WAN (Link/Activity)** – This LED indicator is solid green when your router WAN port is physically connected to the xDSL/Cable modem Ethernet port (also called network port) successfully with an Ethernet cable (also called network cable). The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router.
-  **LAN 1-4 (Link/Activity)** – These LED indicators are solid green when the LAN ports are physically connected to your wired network devices successfully with an Ethernet cable (also called network cable). These LED indicators will be blinking green while data is transmitted or received through your router LAN ports.
-  **Status** - This LED indicator is blinking green when your router is ready and working successfully. If this LED indicator is solid green on or off, your router is not receiving power or not working properly.

Application Diagram



The router is installed in a main office location which is connected to the Internet. Desktop computers are connected to the four LAN ports of the router using Ethernet cables (also called network cables) allowing these computers to access the Internet. The router is also configured as a Virtual Private Network (VPN) server to allow secure remote access (over the Internet) to work related files and media located at the main office to an employee working from an outside home office location.

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 web cameras.

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

How to set up a home network

1. For a network that includes Internet access, you'll need:

- Computers/devices with an Ethernet port (also called network port)
- A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP)
- A router to connect your computers and devices and also connects to the modem.

2. Make sure that your modem is working. Your ISP can help you set up your modem and verify that it's working correctly.

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 page 11.

How to setup your router

The easiest way and fastest way to follow the included Quick Installation Guide or continue to the next section "Router Installation" on page 6, and complete the remaining sections of "Router Installation".

Where to find more help

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

- <http://www.trendnet.com/support>
(documentation, downloads, FAQs, how to contact technical support)
- Internet service to your home, provided by an ISP (Internet Service Provider)
- Autorun CD (Quick Installation Guide)

Router Installation

Before you Install

It is recommended, that you verify your Internet connection type with your ISP (Internet Service Provider) and ensure you have all the information for one of the following connection types below before proceeding with the router installation.

1. Obtain IP Address Automatically (DHCP)

Host Name (Optional)

Clone Mac Address (Optional)

2. Fixed IP address

WAN IP Address: _____

(e.g. 215.24.24.129)

WAN Subnet Mask: _____

WAN Gateway IP Address: _____

DNS Server Address 1: _____

DNS Server Address 2: _____

3. PPPoE to obtain IP automatically

User Name: _____

Password: _____

4. PPPoE with a fixed IP address

User Name: _____

Password: _____

IP Address: _____ (e.g. 215.24.24.129)

5. PPTP

Type (Dynamic IP or Static IP)

My IP Address: _____

(e.g. 215.24.24.129)

Subnet Mask: _____

Gateway: _____

Server IP: _____

PPTP Account: _____

PPTP Password: _____

6. L2TP

Type (Dynamic IP or Static IP)

My IP Address: _____

(e.g. 215.24.24.129)

Subnet Mask: _____

Gateway: _____

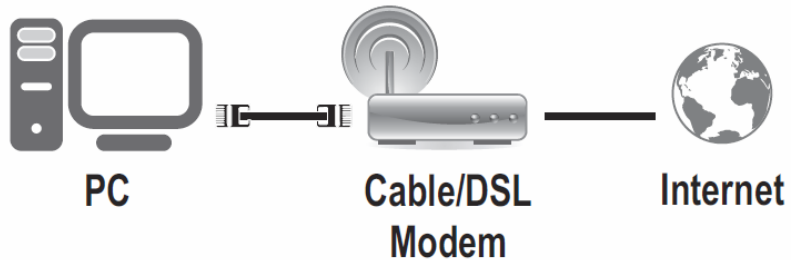
Server IP: _____

L2TP Account: _____

L2TP Password: _____

Hardware Installation

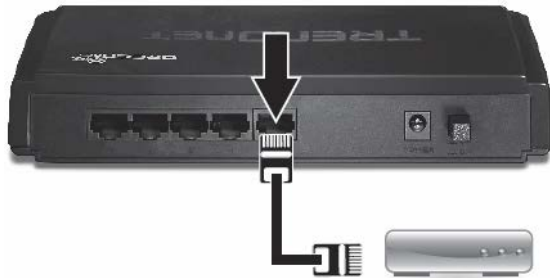
1. Verify that you have an Internet connection when connecting your computer directly to the modem. Open your browser (e.g. Internet Explorer, Firefox, Chrome, Safari, or Opera) and type in a URL (e.g. <http://trendnet.com>) in the address bar.



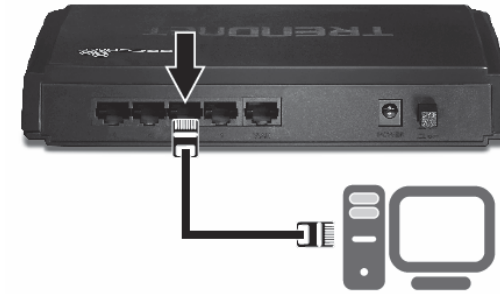
2. Turn off your modem.

3. Disconnect the Ethernet cable (also called network cable) from your modem and your computer.

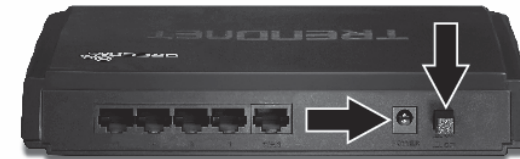
4. Connect one end of a network cable to your router WAN port. Connect the other end of the network cable to your Cable modem network port.




5. Connect one end of a network cable to one of your router LAN ports (1-4). Connect the other end of the network cable to the computer Ethernet port (also called network port).



6. Connect the included power adapter to your router Power Port and then to an available power outlet. Push the On/Off Power Switch on your router to the "On" (inner) position.

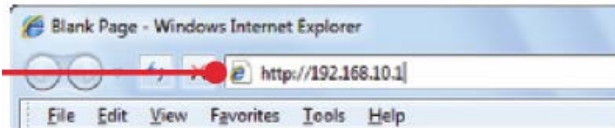


7. Turn on your modem.

8. Verify that the following front panel LED indicators on your router (**Status**  and **WAN** is solid green, and the **LAN** port for which your computer is connected is solid 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 password.



2. Enter the System Password and click **Login**.

Default System Password: **admin**

System Password :

3. Make sure the **Wizard** option is selected and then click **Enter**.

Note: If the Setup Wizard does not automatically appear, click **Wizard** at the top of the page.

4. Click **Next**.

5. Enter the Old Password (Default: **admin**), enter a New Password and enter the password again next to Reconfirm to verify the New Password.

Note:

1. Setting a password prevents other users from accessing the router management page.
2. It is recommended that you enter a new password. If you decide to change the default password, please write down the new password.
3. Password is limited up to 9 characters.

6. Click the drop-down list and select your **Time Zone**. Click **Next**.

Setup Wizard - Setup Time Zone [EXIT]

(GMT-08:00) Pacific Time (US & Canada)

Detect Again

< Back [Start > Password > Time > LAN/WAN > Summary > Finish!] Next >

7. Select **Auto Detecting WAN Type** and the click **Next**.

Setup Wizard - Select WAN Type [EXIT]

Auto Detecting WAN Type

Setup WAN Type Manually

< Back [Start > Password > Time > LAN/WAN > Summary > Finish!] Next >

8. Configure the settings based on information provided by your Internet Service Provider (ISP). Follow the wizard instructions to complete your configuration.

Note: Each Internet connection type may have different options.

Setup Wizard - Select WAN Type [EXIT]

ISP assigns you a static IP address. (Static IP Address)

Obtain an IP address from ISP automatically. (Dynamic IP Address)

Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

Some ISPs require the use of PPTP to connect to their services. (PPTP)

Some ISPs require the use of L2TP to connect to their services. (L2TP)

< Back [Start > Password > Time > LAN/WAN > Summary > Finish!] Next >

Note: When configuring your Internet connection settings. It is optional to change your LAN IP network settings. It is recommended to leave this setting at default.

▶ LAN IP Address 192.168.10.1

11. Click **Apply Settings**.

Note: You can check the network testing option to run an Internet connection test before applying the settings.

Setup Wizard - Summary [EXIT]

Please confirm the information below

Enable

[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	
WAN's MAC Address	00:50:18:21:D6:32

Do you want to proceed the network testing?

< Back [Start > Password > Time > LAN/WAN > **Summary** > Finish!] Apply Settings

12. Please wait until the router applies the changes and reboots.

Note: If you checked the option to run network testing (Internet connection test), you will see the status message below.

Setup Wizard - WAN Connection Test [EXIT]

Try to connect to Internet...

Please wait 15 seconds...

< Back [Start > Password > Time > LAN/WAN > Summary > **Finish!**] Next >

13. Click **Finish**.

Setup Wizard - Finish [EXIT]

Configuration is Completed.

Please click "Finish" to restart the device.
Or you can click "Configure Again" to setup the wizard again.

Configure Again [Start > Password > Time > LAN/WAN > Summary > **Finish!**] Finish

Note: If you checked the option to run network testing (Internet connection test) and the test is success, you will receive the message below along with your Internet connection settings.

Setup Wizard - Finish [EXIT]

Congratulations!!

The Internet connection is established.
Connection information is

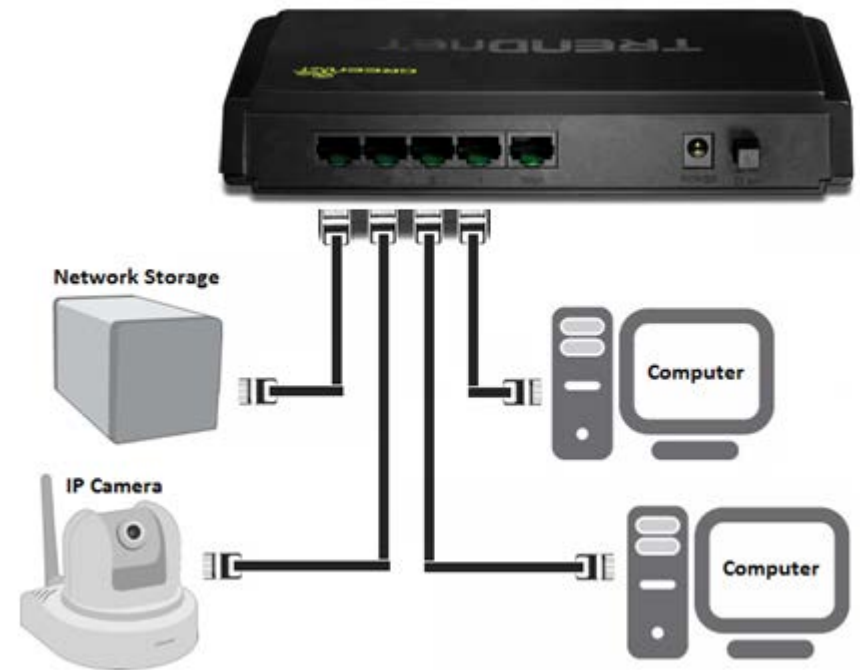
WAN Type	Dynamic IP Address
IP Address	10.10.10.106
Subnet Mask	255.255.255.0
Gateway	10.10.10.254
DNS	10.10.10.254,0.0.0.0

< Back [Start > Password > Time > LAN/WAN > Summary > **Finish!**] Finish

Connect additional wired devices to your network

You can connect an additional computer or device to your network by connecting one end of an Ethernet cable (also called network cable) from your computer or device Ethernet port (also called network port) 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.



Virtual Private Networking (VPN)

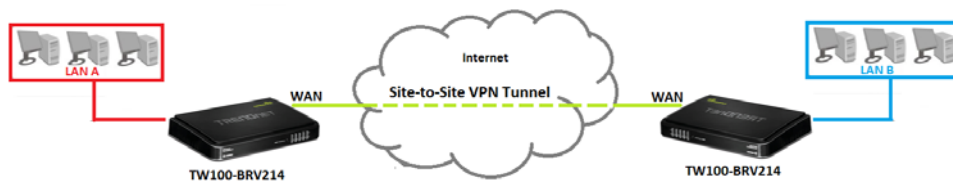
Creating a Virtual Private Network

What is a VPN?

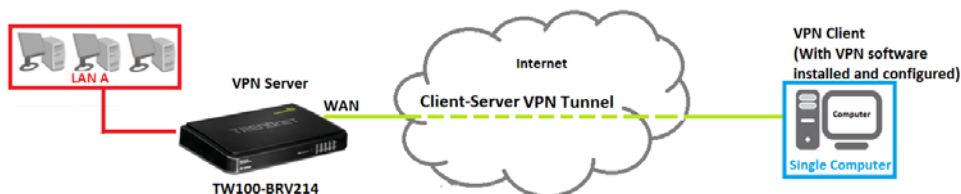
A VPN provides secure communications typically over the Internet by creating a secure tunnel between two or more VPN routers (gateways) also known as a site-to-site VPN or between a single client computer and a VPN router (gateway) also known as a client-server VPN.

On your VPN router, the following types of tunnels can be created:

- **Site-to-Site VPN** – Connects two or more VPN routers (gateways) allowing the LAN network from each router to securely communicate to each other over the Internet.



- **Client-Server VPN** – A single client computer or device with VPN client software installed connects to a VPN router (gateway) allow the single client computer or device to securely communicate to the LAN network of the VPN router over the Internet.



Tunneling methods supported by your router:

- **IPsec (Internet Protocol Security) VPN** – This type of VPN can be used for either Site-to-Site VPN or Client-Server VPN however, the most common application for this type is a Site-to-Site VPN. This type of VPN can provide highest degree of security. For a Client-Server VPN, typically, a third party VPN client software is required to be installed and configured and can be difficult when installing and configuring on VPN client computers. This VPN type can provide the highest degree of security.
- **PPTP (Point-to-Point Tunneling Protocol) VPN** – This type of VPN can be used for Client-Server VPN only however both server mode and client mode are supported on your router. Most computer operating systems already include a pre-installed PPTP VPN client software that can be easily configured which eliminates the need for an additional third party VPN client software to be purchased and installed. Since it provides less security overall than IPsec VPN, it is not recommended for a Site-to-Site VPN.
- **L2TP (Layer 2 Tunneling Protocol) VPN** – This type of VPN is very similar to PPTP VPN as it is most commonly used for a Client-Server VPN, pre-installed on most computer operating systems and easy to configure, and provides less overall security than IPsec VPN. Most of the current operating systems with L2TP VPN client software pre-installed use L2TP VPN in conjunction with IPsec VPN to improve the overall security provided. This router does not support the L2TP over IPsec VPN method.
- **GRE (Generic Routing Encapsulation) Tunneling** – This is strictly a tunneling protocol as it does not provide any security mechanisms and it can only be used for Site-to-Site tunneling to another router with GRE tunneling support but in most current implementations can be used in conjunction with IPsec or PPTP/L2TP to add security mechanisms. Because of the nature of how GRE works, the benefits include allow multicast traffic and allowing dynamic routing protocols to pass through the tunnel compared to IPsec VPN. This router does not support GRE over IPsec VPN or GRE over PPTP/L2TPVPN methods.

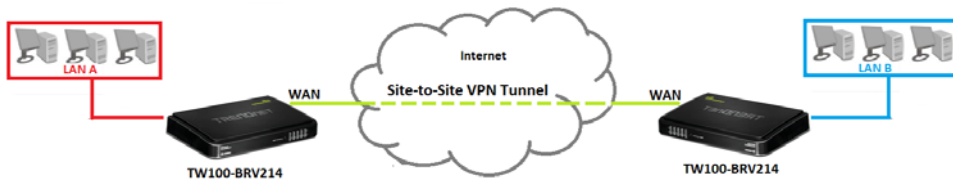
Important Note: For any tunneling or VPN method used, to avoid IP address conflict and to ensure connectivity, it is required that each end (LAN IP network or single client) of the VPN tunnel is configured with a different IP network or subnet.

IPsec (Internet Protocol Security)

Site-to-Site VPN

Configuration > Security Setting > VPN-IPsec

To configure an IPsec Site-to-Site VPN tunnel between two VPN routers:



- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

VPN Router B WAN (Internet) IP Address: 10.10.10.20

- Make sure the LAN IP network on each VPN router is different.

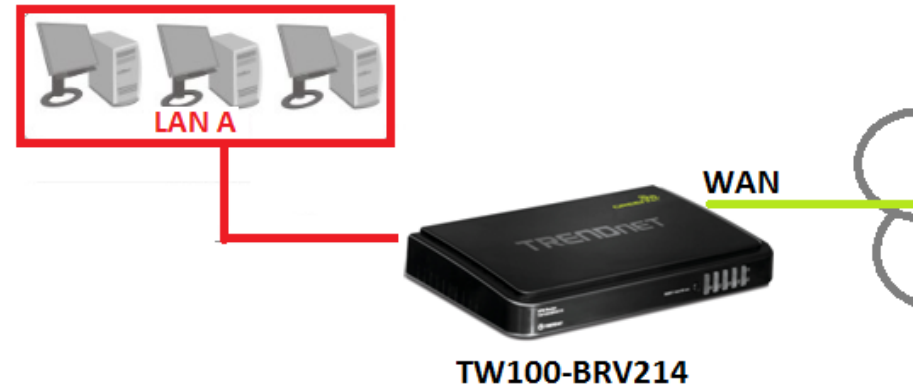
Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.255.0

VPN Router A Configuration



1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-IPsec**.

3. Next to **VPN-IPsec**, check the **Enable** option to enable IPsec.

Note: If **Enable** is not checked, then this will disable all IPsec functionality on your router.

▶ VPN-IPsec	<input checked="" type="checkbox"/> Enable
-------------	--

4. For **ID 1**, check the **Enable** option and then click **Edit**.

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1					Edit	<input checked="" type="checkbox"/>

5. Next to **Tunnel Name**, enter the tunnel name in the field. (e.g. *Tunnel 1*)

▶ Tunnel Name	<input type="text" value="Tunnel 1"/>
---------------	---------------------------------------

6. Enter the network settings for the IPsec Site-to-Site VPN tunnel.

▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Remote Netmask	<input type="text"/>
▶ Remote Gateway	<input type="text"/>

Note: Generally speaking if the LAN IP address setting of the router is 192.168.X.1 / 255.255.255.0, then the IP network will be identified as 192.168.X.0, X being any number from 0-254.

- **Local Subnet** – The local LAN IP subnet or network of your local VPN router. (e.g. 192.168.10.0)
- **Local Netmask** – The local LAN subnet mask of your local VPN router. (e.g. 255.255.255.0)
- **Remote Subnet** – The remote LAN IP subnet or network of your remote VPN router. (e.g. 192.168.100.0)
- **Remote Netmask** – The remote LAN subnet mask of your remote VPN router. (e.g. 255.255.255.0)
- **Remote Gateway** – The remote WAN (Internet) IP address of your remote VPN router. (e.g. 10.10.10.20) **Note:** If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.

Based on the example, the network settings will be the following:

▶ Local Subnet	<input type="text" value="192.168.10.0"/>	Router A LAN IP Network
▶ Local Netmask	<input type="text" value="255.255.255.0"/>	Router A LAN Subnet Mask
▶ Remote Subnet	<input type="text" value="192.168.100.0"/>	Router B LAN IP Network
▶ Remote Netmask	<input type="text" value="255.255.255.0"/>	Router B LAN Subnet Mask
▶ Remote Gateway	<input type="text" value="10.10.10.20"/>	Router B WAN IP Address

7. Next to **Preshare Key**, enter the preshared key for your IPsec tunnel.

Note: The value 1234567890 is shown as an example. It is strongly recommended to enter your own preshared key for the IPsec VPN tunnel. Write down the preshared key you enter as it will also need to be entered when configuring VPN Router B.

▶ Preshare Key	<input type="text" value="1234567890"/>
----------------	---

Note: The preshared key can consist of alphanumeric characters (a,b,c,?,*,/,1,2, etc.)

8. Click the **PFS Group** drop-down list, and select **Same as Phase 1**.

▶ PFS Group	<input type="text" value="Same as Phase1"/>
-------------	---

9. Next to **Dead Peer Detection (DPD)**, check the **Enable** option.

▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable ▶ Timeout: <input type="text" value="180"/> Second(s) ▶ Delay: <input type="text" value="30"/> Second(s)
-----------------------------	---

10. Next to **IKE Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128** and click the **DH Group** drop-down list and select **Group 2**. Check the **Enable** option.

Note: The IKE proposal settings must match the setting configured in VPN Router A.

▶ Set IKE Proposal		<input checked="" type="checkbox"/> Enable		
ID	Encryption	Authentication	DH Group	Enable
1	<input type="text" value="AES-128"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group2"/>	<input checked="" type="checkbox"/>

11. Next to **IPsec Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128**. Check the **Enable** option.

Note: The IPsec proposal settings must match the setting configured in VPN Router A.

▶ Set IPsec Proposal		<input checked="" type="checkbox"/> Enable
ID	Encryption	Authentication
1	AES-128 ▼	SHA1 ▼
		<input checked="" type="checkbox"/> Enable

12. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

To view the status of the IPsec Site-to-Site VPN tunnel, click **Back** at the bottom of the page to go back to the main IPsec VPN configuration page.

VPN Router A Tunnel Status

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1	Tunnel 1	192.168.100.0/ 255.255.255.0	10.10.10.20	Wait for Traffic...	<input type="button" value="Edit"/> <input type="button" value="Connect"/>	<input checked="" type="checkbox"/>

VPN Router B Configuration



1. Log into your router management page (see "Access your router management page" on [page 34](#)).

Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.1.

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-IPsec**.

3. Next to **VPN-IPsec**, check the **Enable** option to enable IPsec.

Note: If **Enable** is not checked, then this will disable all IPsec functionality on your router.

▶ VPN-IPsec Enable

4. For **ID 1**, check the **Enable** option and then click **Edit**.

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1					<input checked="" type="button" value="Edit"/>	<input checked="" type="checkbox"/>

5. Next to **Tunnel Name**, enter the tunnel name in the field. (e.g. *Tunnel 1*)

▶ Tunnel Name

6. Enter the network settings for the IPsec Site-to-Site VPN tunnel.

▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Remote Netmask	<input type="text"/>
▶ Remote Gateway	<input type="text"/>

Note: Generally speaking if the LAN IP address setting of the router is 192.168.X.1 / 255.255.255.0, then the IP network will be identified as 192.168.X.0, X being any number from 0-254.

- **Local Subnet** – The local LAN IP subnet or network of your local VPN router. (e.g. 192.168.100.0)
- **Local Netmask** – The local LAN subnet mask of your local VPN router. (e.g. 255.255.255.0)
- **Remote Subnet** – The remote LAN IP subnet or network of your remote VPN router. (e.g. 192.168.10.0)
- **Remote Netmask** – The remote LAN subnet mask of your remote VPN router. (e.g. 255.255.255.0)
- **Remote Gateway** – The remote WAN (Internet) IP address of your remote VPN router. (e.g. 10.10.10.10) **Note:** If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.

Based on the example, the network settings will be the following:

▶ Local Subnet	192.168.100.0	Router B LAN IP Network
▶ Local Netmask	255.255.255.0	Router B LAN Subnet Mask
▶ Remote Subnet	192.168.10.0	Router A LAN IP Network
▶ Remote Netmask	255.255.255.0	Router A LAN Subnet Mask
▶ Remote Gateway	10.10.10.10	Router A WAN IP Address

7. Next to **Preshare Key**, enter the preshared key for your IPsec tunnel.

Note: The preshared key entered must be the same as the preshared key configured in VPN Router A.

▶ Preshare Key	1234567890
----------------	------------

Note: The preshared key can consist of alphanumeric characters (a,b,c,?,*,/,1,2, etc.)

8. Click the **PFS Group** drop-down list, and select **Same as Phase 1**.

▶ PFS Group	Same as Phase1
-------------	----------------

9. Next to **Dead Peer Detection (DPD)**, check the **Enable** option.

▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable
	▶ Timeout: 180 Second(s)
	▶ Delay: 30 Second(s)

10. Next to **IKE Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128** and click the **DH Group** drop-down list and select **Group 2**. Check the **Enable** option.

Note: The IKE proposal settings must match the setting configured in VPN Router A.

▶ Set IKE Proposal		<input checked="" type="checkbox"/> Enable		
ID	Encryption	Authentication	DH Group	Enable
1	AES-128	SHA1	Group2	<input checked="" type="checkbox"/>

11. Next to **IPsec Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128**. Check the **Enable** option.

Note: The IPsec proposal settings must match the setting configured in VPN Router A.

▶ Set IPsec Proposal		<input checked="" type="checkbox"/> Enable	
ID	Encryption	Authentication	Enable
1	AES-128	SHA1	<input checked="" type="checkbox"/>

12. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>
--

To view the status of the IPsec Site-to-Site VPN tunnel, click **Back** at the bottom of the page to go back to the main IPsec VPN configuration page. Under **Action**, click **Connect** to establish the VPN tunnel.

VPN Router B Tunnel Status

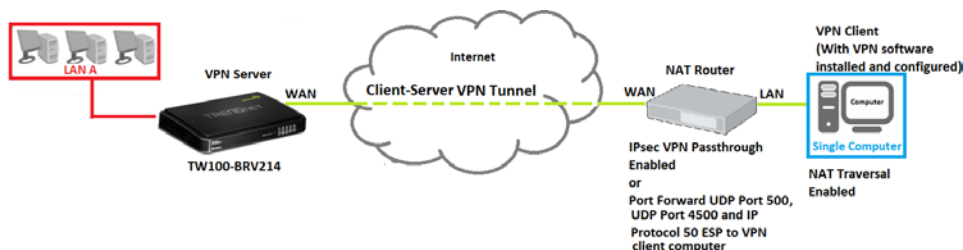
ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1	Tunnel 1	192.168.10.0/ 255.255.255.0	10.10.10.10	Connected	<input type="button" value="Edit"/> <input type="button" value="Disconnect"/>	<input checked="" type="checkbox"/>

For details on configuring additional IPsec VPN options, see the Appendix.

Client-Server VPN (Server Mode)

Configuration > Security Setting > VPN-IPsec

To configure your router to allow IPsec VPN connections from remote VPN client computers or devices:



- Typically, the single client computer is connecting to the Internet through a router with NAT enabled. To establish an IPsec VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, enable NAT-T (NAT Traversal) to establish VPN connections through devices with NAT enabled. If the router with NAT enabled does not support IPsec VPN pass through, ports

(UDP 500, UDP 4500, IP Protocol 50: ESP) may need to be forwarded to your VPN client computer.

- If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router.

Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

Router with NAT enabled LAN IP Settings: 192.168.100.1 / 255.255.255.0

- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

1. Log into your router management page (see “Access your router management page” on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-IPsec**.

3. Next to **VPN-IPsec**, check the **Enable** option to enable IPsec.

Note: If **Enable** is not checked, then this will disable all IPsec functionality on your router.

▶ VPN-IPsec	<input checked="" type="checkbox"/> Enable
-------------	--

4. Next to **NAT Traversal**, check the **Enable** option.

▶ NAT Traversal	<input checked="" type="checkbox"/> Enable
-----------------	--

5. Next to **Dynamic VPN**, check the **Enable** option and click **Edit**.

Item	Status	Action	Enable
Dynamic IP VPN		Edit	<input checked="" type="checkbox"/>

6. Next to **Tunnel Name**, enter the tunnel name in the field. (e.g. *Tunnel 1*)

▶ Tunnel Name	<input type="text" value="Tunnel 1"/>
---------------	---------------------------------------

7. Enter the network settings for the IPsec VPN Server.

▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>

- **Local Subnet** – The local LAN IP subnet or network of your local VPN router.
(e.g. *192.168.10.0*)
- **Local Netmask** – The local LAN subnet mask of your local VPN router.
(e.g. *255.255.255.0*)

8. Next to **Preshare Key**, enter the preshared key for your IPsec tunnel.

Note: The preshared key entered must be the same as the preshared key configured in VPN Router A.

▶ Preshare Key	<input type="text" value="1234567890"/>
----------------	---

Note: The preshared key can consist of alphanumeric characters (a,b,c,?,*,/,1,2, etc.)

9. Click the **PFS Group** drop-down list, and select **Same as Phase 1**.

▶ PFS Group	<input type="text" value="Same as Phase1"/>
-------------	---

10. Next to **Dead Peer Detection (DPD)**, check the **Enable** option.

▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable ▶ Timeout: <input type="text" value="180"/> Second(s) ▶ Delay: <input type="text" value="30"/> Second(s)
-----------------------------	---

11. Next to **IKE Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128** and click the **DH Group** drop-down list and select **Group 2**. Check the **Enable** option.

▶ Set IKE Proposal		<input checked="" type="checkbox"/> Enable		
ID	Encryption	Authentication	DH Group	Enable
1	<input type="text" value="AES-128"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group2"/>	<input checked="" type="checkbox"/>

12. Next to **IPsec Proposal**, check the **Enable** option. Next to **ID 1**, click the **Encryption** drop-down list and select **AES-128**. Check the **Enable** option.

▶ Set IPsec Proposal		<input checked="" type="checkbox"/> Enable		
ID	Encryption	Authentication		Enable
1	<input type="text" value="AES-128"/>	<input type="text" value="SHA1"/>		<input checked="" type="checkbox"/>

13. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>
--

Note: For the VPN client computer, you will require a third party IPsec VPN software to be installed configured matching the IPsec VPN settings on your router. Please refer to the your VPN software User's Guide/Manual for configuring the VPN settings.

Below is your router VPN configuration based on the IPsec Client-Server VPN (Server Mode) procedure.

- **LAN IP Network:** 192.168.10.0 / 255.255.255.0
- **NAT-T (NAT Traversal):** Enabled
- **IPsec Mode:** Main
- **Tunnel Method:** IKE
- **Encapsulation:** ESP
- **Preshared Key:** <preshared key you entered in VPN configuration>
- **IKE Proposal:** AES-128 / SHA1 / DH Group 2
- **IPsec Proposal:** AES-128 / SHA1
- **PFS (Perfect Forward Secrecy):** Enabled DH Group 2

To view the status of the IPsec Site-to-Site VPN tunnel, click **Back** at the bottom of the page to go back to the main IPsec VPN configuration page. When the client is connected, the **Status** will change from Wait for Traffic... to Connected.

Item	Status	Action	Enable
Dynamic IP VPN	Wait for Traffic...	<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

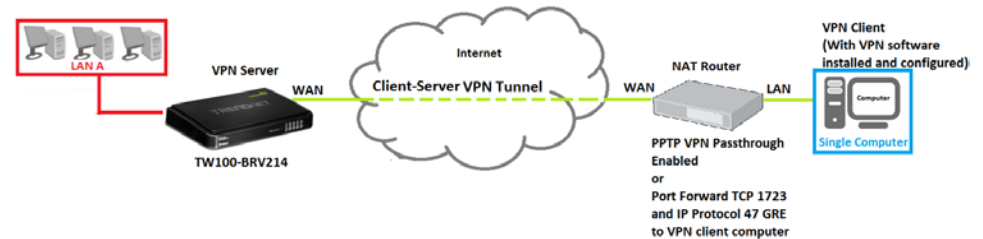
For details on configuring additional IPsec VPN options, see the Appendix.

PPTP (Point-to-Point Tunneling Protocol)

Client-Server VPN (Server Mode)

Configuration > Security Setting > VPN-PPTP Server

To configure your router to allow PPTP VPN connections from remote VPN client computers or devices:



- Typically, the single client computer is connecting to the Internet through a router with NAT enabled. To establish a PPTP VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, PPTP VPN passthrough must be enabled on the router with NAT enabled. If the router with NAT enabled does not support PPTP VPN pass through, ports (TCP 1723, IP Protocol 47: GRE) may need to be forwarded to your VPN client computer.
- If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router.

Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

Router with NAT enabled LAN IP Settings: 192.168.100.1 / 255.255.255.0

- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-PPTP Server**.

3. Next to **VPN-PPTP Server**, check the **Enable** option to enable the PPTP server.

▶ VPN-PPTP Server	<input checked="" type="checkbox"/> Enable
-------------------	--

4. Next to **Server virtual IP**, enter the LAN IP address of your router.

Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged.

▶ Server virtual IP	<input type="text" value="192.168.10.1"/>
---------------------	---

5. Enter the IP address range to assign to PPTP VPN clients.

Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave these settings at default. Router default DHCP server range: 192.168.10.101-192.168.10.199

▶ IP Pool Start Address	<input type="text" value="10"/>
▶ IP Pool End Address	<input type="text" value="100"/>

- **IP Pool Start Address** – Changes the starting address for the PPTP VPN server range. (e.g. 192.168.10.10)
- **IP Pool End Address** – Changes the last address for the PPTP VPN server range. (e.g. 192.168.10.100)

6. Next to **Authentication Protocol**, check **MS_CHAP** and **MS_CHAPv2**.

▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS_CHAP <input checked="" type="checkbox"/> MS_CHAPv2
---------------------------	--

7. Next to **MPPE Encryption Mode**, check the **Enable** option.

▶ MPPE Encryption Mode	<input checked="" type="checkbox"/> Enable
------------------------	--

8. Next to **Encryption Length**, to ensure highest compatibility, check **40 bits**, **56 bits**, and **128 bits**.

▶ Encryption Length	<input checked="" type="checkbox"/> 40 bits <input checked="" type="checkbox"/> 56 bits <input checked="" type="checkbox"/> 128 bits
---------------------	--

9. Under **User Accounts** next to **ID 1**, enter the **User Name** and **Password** used by PPTP VPN clients to authenticate.

Note: The same account can be used by multiple PPTP VPN clients.

ID	User Name	Password
1	<input type="text" value="trendnet1"/>	<input type="text" value="trendnet1"/>

10. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page. Clicking **PPTP Client** will bring you to the **PPTP Client** mode configuration page.

<input type="button" value="PPTP Client"/> <input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>
--

Note: For the VPN client computer, you will require a third party PPTP VPN software to be installed configured matching the PPTP VPN settings on your router. Typically, PPTP VPN software is pre-installed with most operating systems. Please refer to the your operating system User's Guide/Manual for configuring the VPN settings. See Appendix.

To view the status of connected PPTP VPN clients, check the **Connection Status** section. When a PPTP VPN client is connected, they will be listed under **Connection Status**. You can click **Disconnect** to disconnect the PPTP VPN client.

Connection Status				
User Name	Peer IP	Virtual IP	Peer Call ID	Operation
trendnet1	10.10.10.20	192.168.10.10	353074	<input type="button" value="Disconnect"/>

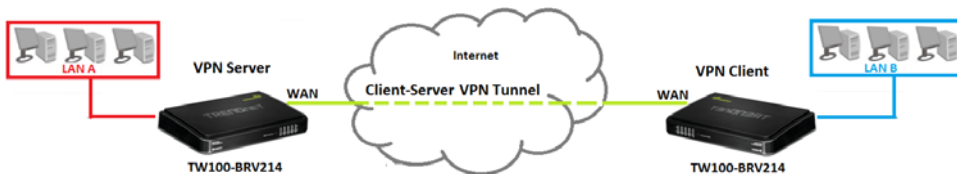
Client-Server VPN (Client Mode)

Configuration > Security Setting > VPN-PPTP Client

Your router can be configured as a PPTP VPN client to connect to a PPTP VPN server allowing your LAN IP network access to through the VPN tunnel. This method should only be used when experiencing compatibility or connectivity issues with establishing an IPsec Site-to-Site VPN.

Note: For connecting LAN network through a VPN over the Internet, it is strongly recommended to use an IPsec Site-to-Site VPN.

To configure a PPTP Client-Server VPN tunnel between two VPN routers:



- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

VPN Router B WAN (Internet) IP Address: 10.10.10.20

- Make sure the LAN IP network on each VPN router is different.

Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

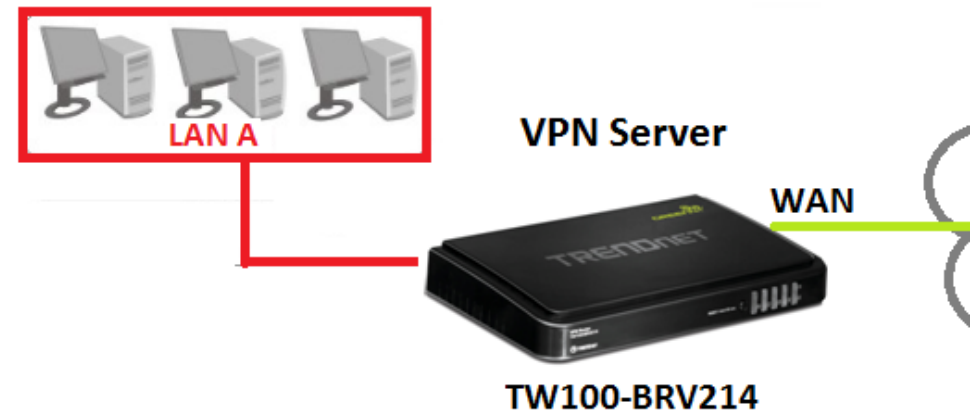
Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.255.0

VPN Router A Configuration (Server Mode)

Configuration > Security Setting > VPN-PPTP Server



- Log into your router management page (see "Access your router management page" on [page 34](#)).
- Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-PPTP Server**.
- Next to **VPN-PPTP Server**, check the **Enable** option to enable the PPTP server.

▶ VPN-PPTP Server	<input checked="" type="checkbox"/> Enable
-------------------	--

- Next to **Server virtual IP**, enter the LAN IP address of your router.

Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged.

▶ Server virtual IP	192.168.10.1
---------------------	--------------

5. Enter the IP address range to assign to PPTP VPN clients.

Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave these settings at default. Router default DHCP server range: 192.168.10.101-192.168.10.199

▶ IP Pool Start Address	<input type="text" value="10"/>
▶ IP Pool End Address	<input type="text" value="100"/>

- **IP Pool Start Address** – Changes the starting address for the PPTP VPN server range. (e.g. 192.168.10.10)
- **IP Pool End Address** – Changes the last address for the PPTP VPN server range. (e.g. 192.168.10.100)

6. Next to **Authentication Protocol**, check **MS_CHAP** and **MS_CHAPv2**.

▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS_CHAP <input checked="" type="checkbox"/> MS_CHAPv2
---------------------------	--

7. Next to **MPPE Encryption Mode**, check the **Enable** option.

▶ MPPE Encryption Mode	<input checked="" type="checkbox"/> Enable
------------------------	--

8. Next to **Encryption Length**, to ensure highest compatibility, check **40 bits**, **56 bits**, and **128 bits**.

▶ Encryption Length	<input checked="" type="checkbox"/> 40 bits <input checked="" type="checkbox"/> 56 bits <input checked="" type="checkbox"/> 128 bits
---------------------	--

9. Under **User Accounts** next to **ID 1**, enter the **User Name** and **Password** used by PPTP VPN clients to authenticate.

Note: The same account can be used by multiple PPTP VPN clients.

ID	User Name	Password
1	<input type="text" value="trendnet1"/>	<input type="text" value="trendnet1"/>

10. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page. Clicking **PPTP Client** will bring you to the **PPTP Client** mode configuration page.

<input type="button" value="PPTP Client"/> <input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>
--

Note: For the VPN client computer, you will require a third party PPTP VPN software to be installed configured matching the PPTP VPN settings on your router. Typically, PPTP VPN software is pre-installed with most operating systems. Please refer to the your operating system User's Guide/Manual for configuring the VPN settings. See Appendix.

To view the status of connected PPTP VPN clients, check the **Connection Status** section. When a PPTP VPN client is connected, they will be listed under **Connection Status**. You can click **Disconnect** to disconnect the PPTP VPN client.

Connection Status				
User Name	Peer IP	Virtual IP	Peer Call ID	Operation
trendnet1	10.10.10.20	192.168.10.10	353074	<input type="button" value="Disconnect"/>

VPN Router B Configuration (Client Mode)

Configuration > Security Setting > VPN-PPTP Client



1. Log into your router management page (see "Access your router management page" on [page 34](#)).

Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.1.

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-PPTP Client**.

3. Next to **VPN-PPTP Client**, check the **Enable** option to enable the PPTP client.

▶ VPN-PPTP Client	<input checked="" type="checkbox"/> Enable
-------------------	--

4. Review the settings below.

ID	Name	Peer IP/Domain	User Name	Password	Peer Subnet	Connect	Option	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand Maximum Idle Time <input type="text" value="600"/> seconds <input type="radio"/> Auto <input type="radio"/> Manual <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

- **Name** – Enter a name for the tunnel. (e.g. *Tunnel 1*)
- **Peer IP/Domain** – The remote WAN (Internet) IP address of your remote VPN router. (e.g. *10.10.10.10*) **Note:** If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.
- **Username** – Enter the user name account info required by the remote VPN router. (e.g. *trendnet1*)
- **Password** – Enter the password account info required by the remote VPN router (e.g. *trendnet1*)
- **Peer Subnet** – The remote LAN IP subnet/netmask in CIDR (Classless Inter-Domain Routing) notation or network of your remote router. (e.g. *192.168.10.0/24* where the */24* represents *255.255.255.0* subnet mask)
- **Connect** – The mode which the VPN tunnel should be connected.
 - **On demand** – (Recommended) This mode will connect only when the traffic is sent through VPN tunnel and disconnect automatically after the **Maximum Idle Time** specified is reached.
 - **Auto** – This mode will keep the tunnel always established.

- **Manual** – This mode will allow you to manually control if the VPN connection is established or disconnected by clicking **Connect** or **Disconnect** buttons.
- **Option**
 - **MPPE (Microsoft Point-to-Point Encryption)** – This will enable MPPE if required by the PPTP server.
 - **NAT (Network Address Translation)** – This will enable NAT over the VPN tunnel in order to access the Internet.
 - If the LAN IP network of both VPN routers is the same (e.g. 192.168.10.1 / 255.255.255.0), then leave the NAT option disabled. **Note:** It is strongly recommended that the LAN IP networks on both VPN routers are different.
 - If the LAN IP network of both VPN routers is different, then enable the NAT option.

Based on the example, the client settings will be the following:

ID	Name	Peer IP/Domain	User Name	Password	Peer Subnet	Connect	Option	Enable
1	Tunnel 1	10.10.10.10	trendnet1	*****	192.168.10.0/24	<input checked="" type="radio"/> On demand Maximum Idle Time <input type="text" value="600"/> seconds <input type="radio"/> Auto <input type="radio"/> Manual <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	<input checked="" type="checkbox"/> MPPE <input checked="" type="checkbox"/> NAT	<input checked="" type="checkbox"/>

10. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page.

<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>
--

Under **Connection Status**, click **Connect** to connect the PPTP VPN client. You can also click **Disconnect** to disconnect the PPTP VPN client.

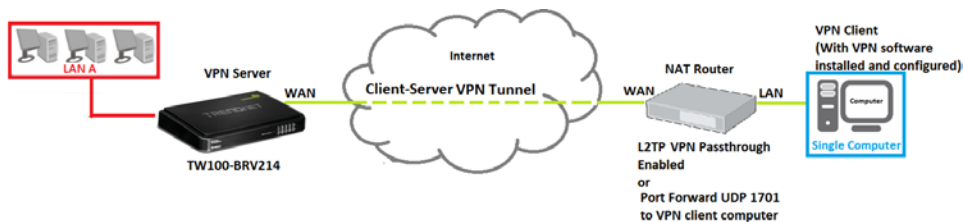
Connection Status				
ID	Tunnel Name	Virtual IP	Remote IP	Status
1	Tunnel 1	0.0.0.0	0.0.0.0	Wait for traffic... <input type="button" value="Connect"/>

L2TP (Layer 2 Tunneling Protocol)

Client-Server VPN (Server Mode)

Configuration > Security Setting > VPN-L2TP Server

To configure your router to allow L2TP VPN connections from remote VPN client computers or devices:



- Typically, the single client computer is connecting to the Internet through a router with NAT enabled. To establish a L2TP VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, L2TP VPN passthrough must be enabled on the router with NAT enabled. If the router with NAT enabled does not support L2TP VPN pass through, ports (UDP 1701, IP Protocol 47: GRE) may need to be forwarded to your VPN client computer.
- If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router.

Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

Router with NAT enabled LAN IP Settings: 192.168.100.1 / 255.255.255.0

- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-L2TP Server**.

3. Next to **VPN-L2TP Server**, check the **Enable** option to enable the L2TP server.

▶ VPN-L2TP Server	<input checked="" type="checkbox"/> Enable
-------------------	--

4. Next to **Server virtual IP**, enter the LAN IP address of your router.

Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged.

▶ Server virtual IP	192.168.10.1
---------------------	--------------

5. Enter the IP address range to assign to L2TP VPN clients.

Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave these settings at default. Router default DHCP server range: 192.168.10.101-192.168.10.199

▶ IP Pool Start Address	10
▶ IP Pool End Address	100

- IP Pool Start Address** – Changes the starting address for the L2TP VPN server range. (e.g. 192.168.10.10)
- IP Pool End Address** – Changes the last address for the L2TP VPN server range. (e.g. 192.168.10.100)

6. Next to **Authentication Protocol**, check **MS_CHAP** and **MS_CHAPv2**.

▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS_CHAP <input checked="" type="checkbox"/> MS_CHAPv2
---------------------------	--

7. Next to **MPPE Encryption Mode**, check the **Enable** option.

▶ MPPE Encryption Mode	<input checked="" type="checkbox"/> Enable
------------------------	--

8. Next to **Encryption Length**, to ensure highest compatibility, check **40 bits**, **56 bits**, and **128 bits**.

▶ Encryption Length	<input checked="" type="checkbox"/> 40 bits <input checked="" type="checkbox"/> 56 bits <input checked="" type="checkbox"/> 128 bits
---------------------	--

9. Under **User Accounts** next to **ID 1**, enter the **User Name** and **Password** used by L2TP VPN clients to authenticate.

Note: The same account can be used by multiple L2TP VPN clients.

ID	User Name	Password
1	<input type="text" value="trendnet1"/>	<input type="text" value="trendnet1"/>

10. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page. Clicking **L2TP Client** will bring you to the **L2TP Client** mode configuration page.

<input type="button" value="L2TP Client"/> <input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Refresh"/>
--

Note: For the VPN client computer, you will require a third party L2TP VPN software to be installed configured matching the L2TP VPN settings on your router. Typically, L2TP VPN over IPsec is pre-installed with most operating systems which your router does not support. See Appendix.

To view the status of connected L2TP VPN clients, check the **Connection Status** section. When a L2TP VPN client is connected, they will be listed under **Connection Status**. You can click **Disconnect** to disconnect the L2TP VPN client.

Connection Status				
User Name	Peer IP	Virtual IP	Peer Call ID	Operation
trendnet1	10.10.10.20	192.168.10.10	353074	<input type="button" value="Disconnect"/>

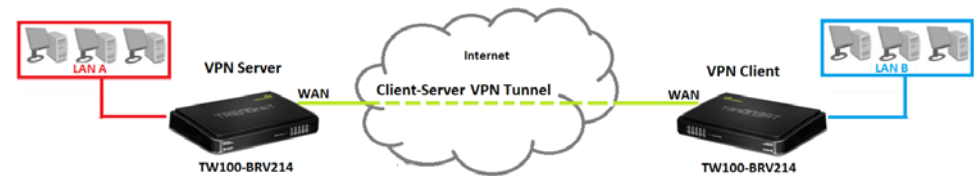
Client-Server VPN (Client Mode)

Configuration > Security Setting > VPN-L2TP Client

Your router can be configured as a L2TP VPN client to connect to a L2TP VPN server allowing your LAN IP network access to through the VPN tunnel. This method should only be used when experiencing compatibility or connectivity issues with establishing an IPsec Site-to-Site VPN.

Note: For connecting LAN network through a VPN over the Internet, it is strongly recommended to use an IPsec Site-to-Site VPN.

To configure a L2TP Client-Server VPN tunnel between two VPN routers:



- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the **Status** page. See page 57 for checking the status page.

Example:

VPN Router A WAN (Internet) IP Address: 10.10.10.10

VPN Router B WAN (Internet) IP Address: 10.10.10.20

- Make sure the LAN IP network on each VPN router is different.

Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 37 for changing the LAN IP address.

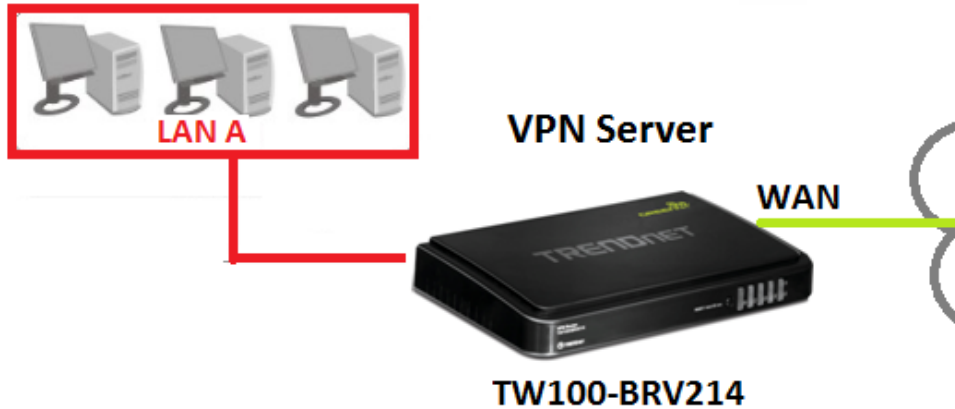
Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.255.0

VPN Router A Configuration (Server Mode)

Configuration > Security Setting > VPN-L2TP Server



1. Log into your router management page (see “Access your router management page” on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-L2TP Server**.

3. Next to **VPN-L2TP Server**, check the **Enable** option to enable the L2TP server.

▶ VPN-L2TP Server	<input checked="" type="checkbox"/> Enable
-------------------	--

4. Next to **Server virtual IP**, enter the LAN IP address of your router.

Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged.

▶ Server virtual IP	192.168.10.1
---------------------	--------------

5. Enter the IP address range to assign to L2TP VPN clients.

Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave these settings at default. Router default DHCP server range: 192.168.10.101-192.168.10.199

▶ IP Pool Start Address	10
▶ IP Pool End Address	100

- **IP Pool Start Address** – Changes the starting address for the L2TP VPN server range. (e.g. 192.168.10.10)
- **IP Pool End Address** – Changes the last address for the L2TP VPN server range. (e.g. 192.168.10.100)

6. Next to **Authentication Protocol**, check **MS_CHAP** and **MS_CHAPv2**.

▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS_CHAP <input checked="" type="checkbox"/> MS_CHAPv2
---------------------------	--

7. Next to **MPPE Encryption Mode**, check the **Enable** option.

▶ MPPE Encryption Mode	<input checked="" type="checkbox"/> Enable
------------------------	--

8. Next to **Encryption Length**, to ensure highest compatibility, check **40 bits**, **56 bits**, and **128 bits**.

▶ Encryption Length	<input checked="" type="checkbox"/> 40 bits <input checked="" type="checkbox"/> 56 bits <input checked="" type="checkbox"/> 128 bits
---------------------	--

9. Under **User Accounts** next to **ID 1**, enter the **User Name** and **Password** used by L2TP VPN clients to authenticate.

Note: The same account can be used by multiple L2TP VPN clients.

ID	User Name	Password
1	trendnet1	trendnet1

10. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page. Clicking **L2TP Client** will bring you to the **L2TP Client** mode configuration page.

L2TP Client **Save** Undo Refresh

Note: For the VPN client computer, you will require a third party L2TP VPN software to be installed configured matching the L2TP VPN settings on your router. Typically, L2TP VPN over IPsec is pre-installed with most operating systems which your router does not support. See Appendix.

To view the status of connected L2TP VPN clients, check the **Connection Status** section. When a L2TP VPN client is connected, they will be listed under **Connection Status**. You can click **Disconnect** to disconnect the L2TP VPN client.

Connection Status				
User Name	Peer IP	Virtual IP	Peer Call ID	Operation
trendnet1	10.10.10.20	192.168.10.10	353074	Disconnect

VPN Router B Configuration (Client Mode)

Configuration > Security Setting > VPN-L2TP Client



1. Log into your router management page (see "Access your router management page" on [page 34](#)).

Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.1.

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **VPN-L2TP Client**.

3. Next to **VPN-L2TP Client**, check the **Enable** option to enable the L2TP client.

▶ VPN-L2TP Client Enable

4. Review the settings below.

ID	Name	Peer IP/Domain	User Name	Password	Peer Subnet	Connect	Option	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand Maximum Idle Time <input type="text" value="600"/> seconds <input type="radio"/> Auto <input type="radio"/> Manual <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

- **Name** – Enter a name for the tunnel. (e.g. Tunnel 1)
- **Peer IP/Domain** – The remote WAN (Internet) IP address of your remote VPN router. (e.g. 10.10.10.10) **Note:** If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.
- **Username** – Enter the user name account info required by the remote VPN router. (e.g. trendnet1)
- **Password** – Enter the password account info required by the remote VPN router (e.g. trendnet1)
- **Peer Subnet** – The remote LAN IP subnet/netmask in CIDR (Classless Inter-Domain Routing) notation or network of your remote router. (e.g. 192.168.10.0/24 where the /24 represents 255.255.255.0 subnet mask)
- **Connect** – The mode which the VPN tunnel should be connected.
 - **On demand** – (Recommended) This mode will connect only when the traffic is sent through VPN tunnel and disconnect automatically after the **Maximum Idle Time** specified is reached.
 - **Auto** – This mode will keep the tunnel always established.
 - **Manual** – This mode will allow you to manually control if the VPN connection is established or disconnected by clicking **Connect** or **Disconnect** buttons.
- **Option**
 - **MPPE (Microsoft Point-to-Point Encryption)** – This will enable MPPE if required by the PPTP server.

- **NAT (Network Address Translation)** – This will enable NAT over the VPN tunnel in order to access the Internet.
 - If the LAN IP network of both VPN routers is the same (e.g. 192.168.10.1 / 255.255.255.0), then leave the NAT option disabled. **Note:** *It is strongly recommended that the LAN IP networks on both VPN routers are different.*
 - If the LAN IP network of both VPN routers is different, then enable the NAT option.

Based on the example, the client settings will be the following:

ID	Name	Peer IP/Domain	User Name	Password	Peer Subnet	Connect	Option	Enable
1	Tunnel 1	10.10.10.10	trendnet1	*****	192.168.10.1	<input checked="" type="radio"/> On demand Maximum Idle Time <input type="text" value="600"/> seconds <input type="radio"/> Auto <input type="radio"/> Manual <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	<input checked="" type="checkbox"/> MPPE <input checked="" type="checkbox"/> NAT	<input checked="" type="checkbox"/>

10. Click **Save** at the bottom of the page to save the changes.

Note: *If you would like to discard the changes, click **Undo** before you click **Save**. Clicking **Refresh** will reload the page.*

Under **Connection Status**, click **Connect** to connect the L2TP VPN client.

Connection Status				
ID	Tunnel Name	Virtual IP	Remote IP	Status
1	Tunnel 1	0.0.0.0	0.0.0.0	Wait for traffic... <input type="button" value="Connect"/>

You can also click **Disconnect** to disconnect the L2TP VPN client.

Connection Status				
ID	Tunnel Name	Virtual IP	Remote IP	Status
1	Tunnel 1	192.168.10.10	192.168.10.1	Connected <input type="button" value="Disconnect"/>

Access Control Filters

Access control basics

Configuration > Security Setting

MAC Control

Configuration > Security Setting > MAC Control

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow only known MAC addresses to connect your network and deny all other unknown MAC addresses from connecting to your network.

Note: Denied MAC addresses will not be able to connect to your router management page, or access the Internet.

1. Log into your router management page (see “Access your router management page” on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **MAC Control**.

3. Add the MAC addresses to the MAC Table first before applying the MAC filter function.

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

To simplify configuration, click the **DHCP clients** drop-down list to select and computer or device that is currently connected to your router. Once you have selected the computer or device, click the **ID** drop-down list to select which entry to copy the selected DHCP client information and click **Copy To**. You can choose a DHCP client from the drop down list or you can manually enter the MAC/IP address information.

Note: If you are manually entering the MAC/IP address information, refer to your computer or device documentation to find the MAC address.

4. After the MAC address (e.g. 00:11:22:AA:BB:CC) and IP address (e.g. 192.168.10.101) information is entered, check the **Allow** option next to the entry to allow network access to this MAC address.

Note: Any unspecified MAC/IP addresses or entries without the **Allow** option checked will be denied network access.

ID	MAC Address	IP Address	Allow
1	00:14:D1:26:E4:76	192.168.10.101	<input checked="" type="checkbox"/>

5. Next to **MAC Address Control** at the top of the page, check the **Enable** option to enable MAC filtering. **Note:** Please add MAC/IP address entries first before enabling.

6. Click **Save** at the bottom of the page to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

- **Next** – Displays the next page to the current page of MAC filtering entries.
- **Previous** – Displays the previous page to the current page of MAC filtering entries.

URL Filters

Configuration > Security Setting > URL Filters

You may want to allow or 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).

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **URL Filters**.
3. Next to **URL Filter**, check the **Enable** option to enable URL filtering.

▶ URL Filter	<input type="checkbox"/> Enable
--------------	---------------------------------

4. In the entry list, choose an entry and under **URL**, enter the URL or domain name (e.g. www.trendnet.com) you would like to block access.

ID	URL	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

- **Drop** – Checking the option will drop or block access to the specific URL or domain.
- **Log** – Checking the option will log the access requests to the specific URL or domain in the router log. **Note:** *Checking the Log option only will not block access. You will need to check the Drop option to block access.*
- **Enable** – Check the enable option to enable the URL/domain filter.

5. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Additional URL filter options:

Log DNS Query – Checking the **Enable** option will log all URL or domain queries in the router log.

▶ Log DNS Query	<input type="checkbox"/> Enable
-----------------	---------------------------------

Privilege IP Addresses Range – Enter the IP address range (use last IP address number only such as 192.168.10.**101**-192.168.10.**110**) to exclude from Domain/URL filtering. IP addresses included in the range will not be blocked from accessing any of the URLs specified.

▶ Privilege IP Addresses Range	From <input type="text"/> To <input type="text"/>
--------------------------------	---

Keyword Blocking

Configuration > Security Setting > Keyword Blocking

You may want to allow or block computers or devices on your network access to web content with specific keywords instead of complete URL to generally allow or 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 [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Keyword Blocking**.
3. Next to **Keyword Blocking**, check the **Enable** option to enable keyword blocking.

▶ Keyword Blocking	<input type="checkbox"/> Enable
--------------------	---------------------------------

4. In the entry list, choose an entry and under **keyword**, enter the keyword you would like to block access and check the **Enable** option.

ID	Keyword	Enable
1	<input type="text"/>	<input type="checkbox"/>

5. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Packet Outbound/Inbound Filters

Configuration > Security Setting > Packet Filters

You may want specify inbound or outbound access control to allow/deny sources (or Internet IP addresses) to your network from the Internet or from computers or devices on your network to the Internet. Firewall rules may allow for more granular control of specific inbound and outbound access between your network and the Internet. It is recommended that these settings remain set to default unless you are knowledgeable about the effects of changing the firewall rule configuration. It is possible to have undesirable functionality from your router if these settings are improperly modified.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Packet Filters**.

Outbound Packet Filter

You may want apply outbound packet filters to allow or deny access of specific traffic from computers or devices on your local network to the Internet.

To configure outbound packet filters:

Next to **Outbound Packet Filter**, check the **Enable** option to enable outbound filtering.

▶ Outbound Packet Filter	<input type="checkbox"/> Enable
--------------------------	---------------------------------

- Select **Allow all to pass except those match the following rules** to allow all traffic and deny only the filters specified in the list.
- Select **Deny all to pass except those match the following rules** to deny all traffic and allow only the filter specified in the list.

<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.
--

Review the outbound packet filter settings.

ID	Source IP	Destination IP : Ports	Protocol	Enable	Use rule#
1	<input type="text"/>	0.0.0.0 : <input type="text"/>	Both ▾	<input type="checkbox"/>	(0) Always ▾

- **Source IP** – Enter the source IP address or computer/device IP address on your local network to apply the filter. (e.g. 192.168.10.101)
- **Destination IP : Ports** – Enter the destination IP address of the computer/device located on the Internet and port number to apply the filter. To specify all port numbers, do not specify any value for **Ports** field. For specific port numbers, enter a port number or range within the range of 1-65535 (e.g. 21 or 21-30) in the **Ports** field.

Note: Typically, you can specify 0.0.0.0 for any destination IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200)

- **Protocol** – Select the protocol type to filter. **TCP**, **UDP**, or you can select **Both** to choose both protocol types.
- **Enable** – Check the option to enable the filter.
- **Use rule#** - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule.

Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure Time Settings and see page 49 to create a schedule.

To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/>
--

Clicking **MAC Level** will bring you to the **MAC Control** configuration page. See **MAC Control** section.

Inbound Packet Filter

You may want apply inbound packet filters to allow or deny access of specific traffic from the Internet to computers or devices on your local network.

To configure inbound packet filters:

Click **Inbound Filter** at the bottom of the outbound packet filter page.

<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/>
--

Next to **Inbound Packet Filter**, check the **Enable** option to enable inbound filtering.

▶ Inbound Packet Filter	<input type="checkbox"/> Enable
-------------------------	---------------------------------

- Select **Allow all to pass except those match the following rules** to allow all traffic and deny only the filters specified in the list.
- Select **Deny all to pass except those match the following rules** to deny all traffic and allow only the filter specified in the list.

<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.
--

Review the inbound packet filter settings.

ID	Source IP	Destination IP : Ports	Protocol	Enable	Use rule#
1	<input type="text"/>	0.0.0.0 : <input type="text"/>	Both ▾	<input type="checkbox"/>	(0) Always ▾

- **Source IP** – Enter the source IP address or computer/device IP address on your located on the Internet to apply the filter. (e.g. 192.168.10.101)

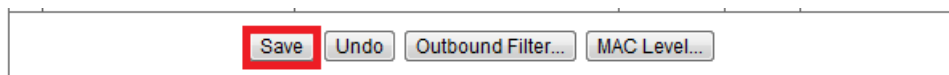
Note: Typically, you can specify 0.0.0.0 for any source IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200)

- **Destination IP : Ports** – Enter the destination IP address of the computer/device located on your local network and port number to apply the filter. To specify all port numbers, do not specify any value for **Ports** field. For specific port numbers, enter a port number or range within the range of 1-65535 (e.g. 21 or 21-30) in the **Ports** field.
- **Protocol** – Select the protocol type to filter. **TCP**, **UDP**, or you can select **Both** to choose both protocol types.
- **Enable** – Check the option to enable the filter.
- **Use rule#** - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule.

Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure Time Settings and see page 49 to create a schedule.

To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



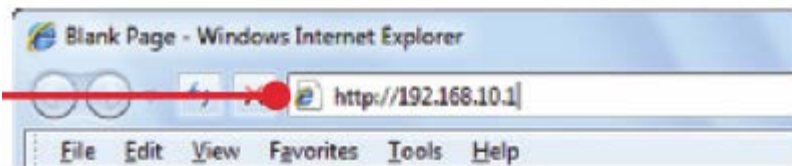
Clicking **MAC Level** will bring you to the **MAC Control** configuration page. See **MAC Control** section.

Advanced Router Setup

Access your router management page

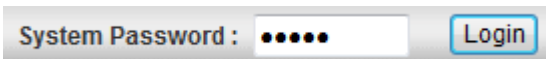
Note: Your router management page <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

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 password.



2. Enter the default user name and password and then click **Login**.

Default System Password: **admin**

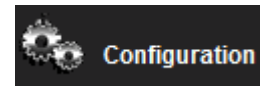


Change your router login password

Configuration > Basic Setting > Password

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **Password**.



3. In the **Old Password** field, enter the current password (default: admin). **New Password** field, enter the new password and in the **New Password** field, and in the **Reconfirm** field, retype the new password again to confirm.

Password	
Item	Setting
▶ Old Password	<input type="password"/>
▶ New Password	<input type="password"/>
▶ Reconfirm	<input type="password"/>

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



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

Set your router date and time

Configuration > Advanced Setting > System Time

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **System Time**.

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

▶ Time Zone	(GMT-08:00) Pacific Time (US & Canada) ▼
-------------	--

4. You can choose one of the following options to set the System Time:

- **NTP (Network Time Protocol Server)** - Next to **Auto-Synchronization**, check the **Enable** option and click the drop-down list and select on one of the options to configure your time server. You can choose **Auto** to set the router to automatically select a predefined time server or **Manual** to manually enter a time server (e.g. pool.ntp.org) that is not listed.

*Note: If you do not choose **Manual** or **Auto**, choose one of the predefined time server is the list.*

▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable
	Time Server (RFC-868):
	Auto ▼
	Auto

Next to **Daylight Saving**, check the **Enable** option and configure **Start** and **End** of your daylight savings duration.

▶ Daylight Saving	<input checked="" type="checkbox"/> Enable
Start :	2 ▼ / 13 ▼ / Mar ▼ (Hour/Day/Month)
End :	2 ▼ / 6 ▼ / Nov ▼ (Hour/Day/Month)

Click **Save** at the bottom of the page to save the changes, then click **Sync with Time Server** and wait for a status result.

*Note: If you would like to discard the changes, click **Undo** before you click **Save**.*

Save	Undo
Sync with Time Server	Sync with my PC (Friday November 04, 2011 16:35:27)

OR

- **Sync with your computer time** - Click **Sync with my PC (Date & Time of your computer)** and wait for a status result, then click **Save** to save the changes.

5. To verify the current system time, click on **Configuration**, click on **Advanced Setting**, and click **Setting Overview** to check the system time.

• Setting Overview	System Time [Modify]
• System Log	Item Status
• Dynamic DNS	System Time 2011/11/03 13:41:06
• QoS	Dynamic DNS [Modify]
• SNMP	Item Status
• Routing	DDNS Disable
• System Time	Provider -
• Scheduling	Routing [Modify]

Manually configure your Internet connection

Configuration > Basic Setting > Network Settings

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **Network Settings**.
3. In the **WAN Type** drop-down list, select the type of Internet connection provided by your ISP (Internet Service Provider).

WAN Type: Dynamic IP Address

- Static IP Address
- Dynamic IP Address
- PPP over Ethernet
- PPTP
- L2TP

4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Save**.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Save Undo
Virtual Computers...

Note: If you are unsure which Internet connection type you are using, please contact your ISP (Internet Service Provider).

Clone a MAC address

Configuration > Basic Setting > Network Settings

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs (Internet Service Providers) 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 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **Network Settings**.
3. Next to **ISP registered MAC Address**, click **Clone** to clone your computer's MAC address or manually enter the 12-digit MAC address of your old router. (e.g. 00:11:22:AA:BB:CC)

ISP registered MAC Address: [] Clone

6. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Change your router IP address

Configuration > Basic Setting > Network 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.

Note: For VPN (Virtual Private Network) configuration, it is required that each router should have a different router or LAN IP address/network on each end of the VPN tunnel.

Default Router or LAN IP Address: 192.168.10.1

Default Router or LAN IP Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **Network Settings**.
3. Next to **LAN IP Address** and **Subnet Mask**, enter the router IP address settings.

▶ LAN IP Address	<input type="text" value="192.168.10.1"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0"/>

- **IP Address** – Enter the new router IP address.
(e.g. 192.168.100.1)
- **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.

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



The screenshot shows a rectangular box containing three buttons. The 'Save' button is highlighted with a red border. To its right is the 'Undo' button. Below these two buttons is a button labeled 'Virtual Computers...'. The 'Save' button is a red rectangle with white text, while 'Undo' and 'Virtual Computers...' are grey buttons with black text.

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://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access your router management page.

Set up the DHCP server on your router

Configuration > Basic Setting > DHCP Server

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 [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **DHCP Server**.

3. Review the DHCP Server settings.

▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	<input type="text" value="101"/>
▶ IP Pool Ending Address	<input type="text" value="199"/>
▶ Lease Time	<input type="text" value="86400"/> Seconds
▶ Domain Name	<input type="text"/>

- **DHCP Server** – Enable or Disable the DHCP server.
- **IP Pool Starting Address** – Changes the starting address for the DHCP server range. (e.g. 192.168.10.20)
- **IP Pool Ending Address** – Changes the last address for the DHCP server range. (e.g. 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** – Enter the lease time in seconds that DHCP client will hold their automatically assigned IP address before requesting a new IP address.
- **Domain Name (Optional)** – Specifies a domain name to assign to computers or devices. (e.g. trendnet.com)

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.

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Note: Clicking the **More>>** option will allow you to configure additional parameters for your DHCP server on your router to assign to computers or devices on your network.

▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Primary WINS	<input type="text"/>
▶ Secondary WINS	<input type="text"/>
▶ Gateway	<input type="text"/> (optional)

Clients List – If you click **Clients List**, 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.

The DHCP Clients List will allow you to select and manage multiple clients and accomplish tasks in your router such as sending WoL (Wake on LAN) or Wake Up messages, allow access or deny access by adding the DHCP client to MAC address control configuration or assign DHCP reservation or Fixed Mapping.

DHCP Clients List					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.10.101	trendnet1	00-14-D1-26-E4-76	Wired	23:59:27	<input type="checkbox"/>

The DHCP Client List will display the following information:

- **IP Address** – Displays the current IP address assigned to the client device by your router DHCP server.
- **Host Name** – Displays the client device name or computer name.
- **MAC Address** – Displays the MAC address of the client device or computer.
- **Type** – Displays how the client device is connected.
- **Lease Time** – Displays the lease time of the client device IP address assigned by your router DHCP server.
- **Back** – (At the bottom of the page) Returns you to the main DHCP server configuration page.
- **Refresh** – (At the bottom of the page) Refreshes the DHCP Clients List.

Check the **Select** option next to the DHCP client you want to configure and review the options below.

- **Wake up** – Send WoL (Wake on LAN) messages to the selected DHCP client device. **Note:** This will require your client device to support WoL and configured properly on the client device.
- **Delete** – Deletes the selected DHCP client device from the DHCP Clients List table.

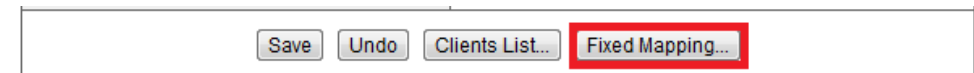
- **Access** – Enables the MAC Address Control feature and adds the selected DHCP client device to be allowed under the MAC Address Control configuration page.
- **Deny** – Enables the MAC Address Control feature and adds the selected DHCP client device to be denied under the MAC Address Control configuration page.
- **Fixed Mapping** – Adds the selected DHCP client device to the DHCP Reservation list.

Set up DHCP reservation

Configuration > Basic Setting > DHCP Server > Fixed Mapping

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, see “Virtual Server” on page 46) or special application (also called port triggering, see “Special Application” on page 47).

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, then click on **DHCP Server**, and click on **Fixed Mapping**.



4. You can choose one of the following options to add a DHCP reservation:
 - **Select an existing DHCP client from drop-down menu** - If the device or computer are adding is already connected to your router and is assigned an IP address automatically from the DHCP server on your router, click the **DHCP clients** drop-down menu and select computer or device. Then click the **ID** drop-down menu and select the ID you would like to assign the DHCP client and click **Copy to**.

DHCP clients ID

The DHCP client will be copied to the ID you selected in the list. Check the **Enable** option next to the entry.

ID	MAC Address	IP Address	Enable
1	<input type="text" value="00:18:E7:88:31:C8"/>	<input type="text" value="192.168.10.102"/>	<input checked="" type="checkbox"/>

Click **Save** at the bottom of the page to save the changes.
Note: If you would like to discard the changes, click **Undo** before you click **Save**. If you click **Back**, this will return you to the main DHCP Server page.

OR

Enter the DHCP reservation manually – Select one of the empty/available IDs in the list and next to the **ID #** click on **MAC Address** and enter the MAC address (e.g. 00:11:22:AA:BB:CC) of the computer or device for which you are creating the reservation. Then click on the **IP Address** field and enter the IP address (e.g. 192.168.10.101) to assign for the reservation and check the **Enable** option.

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 Address & IP Pool Starting Address) in the main DHCP Server page.

ID	MAC Address	IP Address	Enable
1	<input type="text" value="00:18:E7:88:31:C8"/>	<input type="text" value="192.168.10.102"/>	<input checked="" type="checkbox"/>

Click **Save** at the bottom of the page to save the changes.
Note: If you would like to discard the changes, click **Undo** before you click **Save**. If you click **Back**, this will return you to the main DHCP Server page.

Enable/disable UPnP on your router

Configuration > Forwarding Rules > DMZ

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 [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **DMZ**.
3. Next to **UPnP** setting, check the **Enable** option to enable UPnP.

	Enable
▶ UPnP setting	<input checked="" type="checkbox"/>

Note: It is recommended to leave this 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. To save changes, click **Save** at the bottom of the page.
Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Allow/deny VPN connections through your router

Configuration > Forwarding Rules > DMZ

VPN (Virtual Private Network) 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 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 34](#)).
2. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **DMZ**.
3. Next to **PPTP**, **L2TP**, or **IPsec** (depending the VPN protocol your corporation requires) check the **Enable** option next to VPN protocol to turn on the VPN pass through feature.

Note: It is recommended to leave these settings enabled.

	Enable
▶ PPTP Pass through	<input checked="" type="checkbox"/>
▶ L2TP Pass through	<input checked="" type="checkbox"/>
▶ IPsec Pass through	<input checked="" type="checkbox"/>

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Save Undo

Allow/deny multicast streaming through your router

Configuration > Forwarding Rules > DMZ

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications. Multicast streaming is enabled by default on your router to allow applications that require multicast communication through your router which typically does not require and additional configuration changes. The router can allow or deny IGMPv1/2 (Internet Group Multicast Protocol) traffic to pass through.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **DMZ**.
3. Next to **IGMP setting**, check the **Enable** option to turn on IGMP/multicast pass through.

	Enable
▶ IGMP setting	<input type="checkbox"/>

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Save Undo

Enable/disable DoS (Denial of Service) Prevention

Configuration > Security Setting > Management

To provide additional security, your router offers DoS (Denial of Service) attack prevention to protect your network against well-known DoS attacks. You may want to enable the DoS feature for additional network security.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Management**.
3. To enable DoS prevention, next to **DoS Attack Detection**, check the **Enable** option.

▶ DoS Attack Detection	<input checked="" type="checkbox"/>	Enable
------------------------	-------------------------------------	--------

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Allow/deny ping requests to your router from the Internet

Configuration > Security Setting > Management

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 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 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Management**.
3. To deny ping requests from the Internet, next to **Discard PING from WAN side**, check the **Enable** option.

▶ Discard PING from WAN side	<input type="checkbox"/>	Enable
------------------------------	--------------------------	--------

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Identify your network on the Internet

Configuration > Advanced Setting > Dynamic DNS

If you want to remotely access computers or devices on your network attached to your router, you will need to be able to identify your network or router on the Internet. The DDNS (Dynamic DNS) feature allows you to identify your network on the Internet even if your Internet IP address changes as the DDNS service providers allow you to create a domain name you can use to easily identify your network on the Internet.

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

1. Sign up for one of the DDNS available service providers list under **Provider**. (e.g. *dyndns.com*, *no-ip.com*, etc.)
2. Log into your router management page (see "Access your router management page" on [page 34](#)).
3. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Dynamic DNS**.
4. Next to **DDNS**, click **Enable**.

▶ DDNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
--------	---

5. In the **Provider** drop-down list and select the provider for DDNS service you registered.

▶ Provider	DynDNS.com(Dynamic) ▼
------------	-----------------------

6. Enter your DDNS information in the fields provided.

▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

- **Host Name** – The domain name or URL you created with your DDNS service provider. (e.g. *trendnet.dyndns.biz*)
Note: This will be the domain or URL you use to identify your router or network on the Internet. This can be used when configuring the VPN (Virtual Private Network) feature on your router for instead of using the WAN IP address/remote gateway IP address.
- **Username / E-mail** – The user name or e-mail address used to log into your DDNS account. (e.g. *trendnet* or [user@trendnet.com](#))
- **Password / Key** – The password used to log into your DDNS account.

7. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Allow remote access to your router management page

Configuration > Security Setting > Management

You may want to make changes to your router from a remote location such as 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 34](#)).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Management**.
3. Review the items for **Remote Administrator Host : Port**.

			Enable
▶ Remote Administrator Host : Port	0.0.0.0 / 0	: 8080	<input checked="" type="checkbox"/>

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

- **Subnet Mask (CIDR notation)** – Enter the subnet mask in CIDR (Classless Inter-Domain Routing) notation for IP address or IP network you would like to allow. For example, if you are specifying a single IP address, use 32 which is equivalent to a subnet mask of 255.255.255.255 and specifies a single IP address.
Note: It is recommended to leave this setting as 0, to allow remote access from anywhere on the Internet.

- **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 or special application, please change the port to use. (Recommended port range 1024-65534)

7. To save changes, click **Save** at the bottom of the page.

*Note: If you would like to discard the changes, click **Undo** before you click **Save**.*

Save Undo

This section also provides the option to configure the idle timeout period before automatically logging you out of the router management page. Next to **Administrator Time-out**, you can enter the idle timeout in seconds before automatically logging you out of the router management page.

Item	Setting	Enable
▶ Administrator Time-out	300 seconds (0 to disable)	

Open a device on your network to the Internet

DMZ

Configuration > Forwarding Rules > 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 also very **insecure** method.

It is strongly recommended to use **virtual server** (also called port forwarding, see "Virtual Server" on page 46) instead, to allow access to your computers or network devices from the Internet.

1. Make sure to configure your computer or network device to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 39).
2. Log into your router management page (see "Access your router management page" on [page 34](#)).
3. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **DMZ**.
4. Next to **IP Address of DMZ Host**, enter the IP address (e.g. 192.168.10.250) you assigned to the computer or network device to expose to the Internet and click **Enabled**.

	Enable
▶ IP Address of DMZ Host <input type="text"/>	<input checked="" type="checkbox"/>

6. To save changes, click **Save** at the bottom of the page.

Virtual Computers

Configuration > Basic Setting > Network Settings > Virtual Computers

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. This is also known as the Multi-DMZ feature. Your router includes the Virtual Computers feature that makes all the ports and services available on the WAN/Internet IP side IP address and forwards them to specified IP address (computers or network devices) on your network. Using this feature can allow you to different computers or devices on your network from the Internet using specific WAN/Internet IP addresses assigned by your ISP. **Note:** First, verify if you have multiple static WAN/Internet IP addresses by your ISP. The Virtual Computers feature requires multiple static WAN/Internet IP addresses. Contact your ISP for details.

1. Make sure to configure your computer or network device to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 39).
2. Log into your router management page (see "Access your router management page" on [page 34](#)).
3. Click on **Configuration** at the top of the page, click on **Basic Setting**, then click on **Network Settings**, and click on **Virtual Computers**.
4. Select an **ID #** to modify and under **Global IP** (e.g. 10.10.10.10) enter an additional static WAN/Internet IP address assigned by your ISP. Then under **Local IP**, enter the IP address (e.g. 192.168.10.251) to map and check **Enable**.

ID	Global IP	Local IP	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

6. To save changes, click **Save** at the bottom of the page.

Virtual Server

Configuration > Forwarding Rules > 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 45) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an network/IP camera (typically on TRENDnet IP cameras use HTTP TCP port 80 for remote access web requests) on your network for to allow remote access to it.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **Virtual Server**.

To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify by clicking the **Well known services** drop-down list, otherwise, you can choose to manually add a new virtual server.



3. Review the virtual server settings.

ID	Server IP	Public Port	Private Port	Protocol	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both ▾	<input type="checkbox"/>	(0) Always ▾

- **Server IP** – Enter the IP address of the device to forward the port. (e.g. 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.
- **Public Port** – 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.*
- **Private Port** – Enter the port number required by your device.
- **Protocol** – Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP.
Note: Please refer to the device documentation to determine which ports and protocols are required.
- **Enable** – Checking the **Enable** option turns on the virtual server.
- **Use Rule#** – Allows you to specify a pre-defined schedule when the virtual server is activated.
Note: To define a schedule, see the "Create schedules" section.

To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



Example: To forward TCP port 80 to your network/IP camera

1. 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 39).

Note: You may need to reference your camera documentation on configuring a static IP address.

2. Log into your router management page (see "Access your router management page" on [page 34](#)).

3. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **Virtual Server**.

4. In the **Well known services** drop-down list, select the pre-defined virtual server entry named **WEB (80)**. In the **ID** drop-down list, select **1**. Click **Copy to**.

5. **ID 1** fields will be populated with the selected pre-defined virtual server entry.

ID	Server IP	Public Port	Private Port	Protocol	Enable	Use Rule#
1		80	80	TCP	<input checked="" type="checkbox"/>	(0) Always

6. Under **Server IP**, enter the IP address assigned to the camera. (e.g. 192.168.10.101)

7. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Special Applications

Configuration > Forwarding Rules > Special Application

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 40.

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 34](#)).

2. Click on **Configuration** at the top of the page, click on **Forwarding Rules**, and click on **Special Application**.

To simplify configuration, there is a list of commonly used pre-defined special application entries to modify by clicking the **Popular applications** drop-down list, otherwise, you can choose to manually add a new special application.

3. Review the special application settings.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **Trigger** – Port or port range requested by the device.
(e.g. 2000-2001 or 2000)
Note: Please refer to the device documentation to determine which ports are required.
- **Incoming Ports** – Port(s) forwarded to the device.
(e.g. 2000-2038,2069,2081,2200-2210)
Note: Please refer to the device documentation to determine which ports are required.
- **Enable** – Checking the **Enable** option turns on the special application.

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

To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Prioritize traffic using QoS (Quality of Service)

Configuration > Advanced Setting > QoS

You may want to prioritize outbound traffic for specific computers or devices on your network to have higher priority.

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **QoS**.
3. Next to **QoS Control**, check the **Enable** option.

▶ QoS Control	<input checked="" type="checkbox"/> Enable
---------------	--

4. Next to **Bandwidth of Upstream**, enter the maximum upload speed in kbps you have available from you ISP (Internet Service Provider).

Note: You can check your ISP for the maximum available upload speed you have available or you can run an Internet speed tests available on the Internet to determine the estimated value.

▶ Bandwidth of Upstream	<input type="text"/>	kbps (Kilobits per second)
-------------------------	----------------------	----------------------------

5. Review the QoS rule settings below.

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input type="checkbox"/>	(0) Always ▾

- Local IP : Ports** – The IP address and port of the local device on your network.
(Port range to use: 1-65535)
Note: Typically, for the local device, it is recommended to specify all ports. To specify all ports, do not enter a value in the Port field.
- Remote IP : Ports** – The IP address and port of the remote device on destination on the Internet. *(Port range to use: 1-65535)*
Note: You will need to specify the ports to apply QoS.
- QoS Priority** – Choose from three priority queues to apply, **High**, **Normal**, and **Low**.
- Enable** – Check the option to enable the QoS rule.
- Use Rule#** – Allows you to specify a pre-defined schedule when the QoS rule is activated.
Note: To define a schedule, see the “Create schedules” section.

To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Create schedules

Configuration > Advanced Setting > Scheduling

For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly. See page 35 to configure the system time.

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

- Virtual Server
- Packet Filters
- QoS

To create a schedule to define a time period when a feature should be activated:

- Log into your router management page (see “Access your router management page” on [page 34](#)).
- Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Scheduling**.
- Next to **Schedule**, check the **Enable** option.

▶ Schedule Enable

- Click **Save** at the bottom of the page.

- Next to a schedule entry, click **New Add**.

Rule#	Rule Name	Action
1		<input type="button" value="New Add"/>

6. Next to **Name of Rule #**, enter a name for the schedule.

▶ Name of Rule 1	<input type="text"/>
------------------	----------------------

7. Next to one of the entries, click **Week Day** and choose the day you would like to apply the schedule. In the **Start Time (hh:mm)** field, enter the start time. (e.g. 05:00) and in the **End Time (hh:mm)** field, enter the end time. (e.g.15:00).

Time Range: 00:00 (12:00AM) - 23:59 (11:59PM)

Note: Under *Week Day*, you can choose every day to apply the schedule to every day of the week.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --	<input type="text"/>	<input type="text"/>

8. To save changes, click **Save** at the bottom of the page.

<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>

9. Apply the schedule to one of the applicable features (Virtual Server, Packet Filters, or QoS) in the drop-down list option **Use Rule#**.

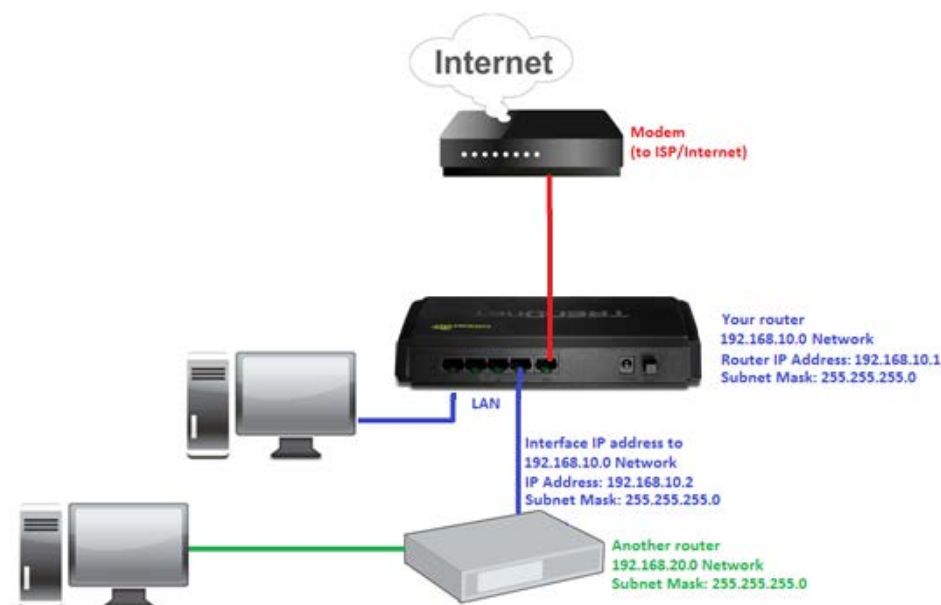
Note: The feature will be activated during the time period specified in the schedule and deactivated during the time period not specified.

Add static routes to your router

Configuration > Advanced Setting > 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, 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 34](#)).

2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Routing**.

3. Next to **Static Routing**, check the **Enable** option to enable static routing.

▶ Static Routing	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
------------------	---

4. Review the static route settings.

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **Destination** – 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)
- **Hop** – Enter the number of hops (routers) required to reach the destination network. The hop count range that can be specified is 0-99.
- **Enable** – Check the option to enable the route and uncheck the option to disable the route.

5. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Enable dynamic routing on your router

Configuration > Advanced Setting > Routing

You may want set up 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 34](#)).

2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Routing**.

3. Select the appropriate dynamic routing protocol and version communicate with other routers.

▶ Dynamic Routing	<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2
-------------------	--

- **Disabled** – Disable sending and receiving or exchange of routing information dynamically between your router and other routers.
- **RIPv1** - Enables sending and receiving or exchange of routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 1 protocol.
- **RIPv2** – Enables sending and receiving routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 2 protocol.

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>

Enable route mode on your router

Configuration > Basic Setting > Network Settings

You may want set up your router to route computers or devices on your network to other local networks through other routers on your internal network only and not connected to the Internet. This will disable NAT (Network Address Translation) on your router for LAN to WAN (Internet) traffic and only allow access to internal networks only using static or dynamic routing.

Note: Configuring this feature assumes that you have some general networking knowledge. This feature is only available when the following WAN (Internet) types are configured: Dynamic IP Address, Static IP Address, PPP over Ethernet.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Basic Setting**, and click on **Network Settings**.
3. Click the **WAN Type** drop-down list and select one of the following: **Dynamic IP Address**, **Static IP Address**, or **PPP over Ethernet**.

▶ WAN Type	Static IP Address ▼
------------	---------------------

4. Next to **NAT Disable**, check the **Enable** option.

▶ NAT disable	<input checked="" type="checkbox"/> Enable
---------------	--

5. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input checked="" type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Virtual Computers..."/>

Using WoL (Wake on LAN) on your router

Configuration > Toolbox > Miscellaneous

You may want to use your router to power on devices using WoL (Wake on LAN). In order for this feature to work, the computer or device should support WoL and this feature should be enabled and configured properly. Please refer to your computer or device User's Guide/Manual for instructions on using WoL.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Miscellaneous**.
3. Next to **MAC Address for Wake-on-LAN**, enter the MAC address of the device with WoL enabled and configured. (e.g. 00:11:22:AA:BB:CC) click **Wake up** to send WoL messages to the MAC Address specified.

▶ MAC Address for Wake-on-LAN	<input type="text"/>	<input type="button" value="Wake up"/>
-------------------------------	----------------------	--

4. Click **Save** at the bottom of the page to save the MAC address configured for WoL.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.


<input checked="" type="button" value="Save"/> <input type="button" value="Undo"/>
--

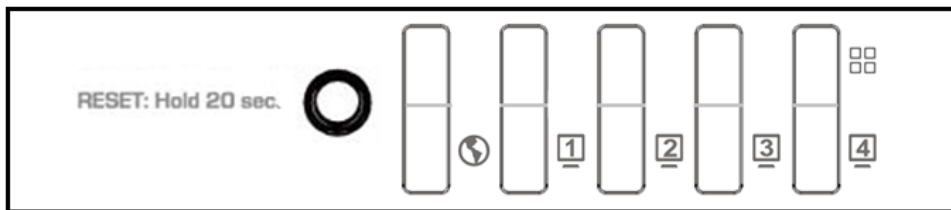
Router Maintenance & Monitoring

Reset your router to factory defaults

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 54.

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

-  **Reset Button** – Located on the front panel of your router. Use this method if you are encountering difficulties with accessing your router management page. Push and hold this button for 20 seconds and release to reset your router to its factory defaults. The LEDs will blink rapidly when the reset process is activated.



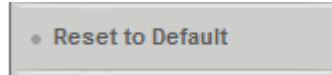
Front Panel Button and LEDs

OR

- Router Management Page**
Configuration > Toolbox > Reset to Default

1. Log into your router management page (see “Access your router management page” on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Reset to Default**.



3. You will be prompted to reset your router to factory defaults. Click **Yes** or **OK**.

Router Default Settings

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

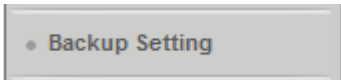
Configuration > Toolbox

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:

Configuration > Toolbox > Backup Setting

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Backup Setting**.

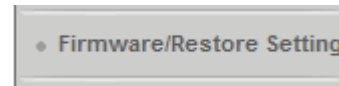


3. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *config.bin*)
4. Save the configuration file to location on your computer.

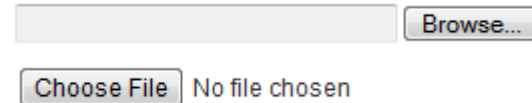
To restore your router configuration:

Configuration > Toolbox > Firmware/Restore Setting

1. Log into your router management page (see "Access your router management page" on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Firmware/Restore Setting**.



3. Under **Firmware/Configuration Filename**, depending on your web browser, click on **Browse** or **Choose File**.



A separate file navigation window should open.

4. Navigate to the location of the router configuration file to restore . (Default Filename: *config.bin*).
5. Select the router configuration file to restore and click **Upgrade**. (Default Filename: *cfg.bin*). If prompted, click **Yes** or **OK**.



6. Wait for the router to restore settings.

Upgrade your router firmware

Configuration > Toolbox > Firmware/Restore Setting

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 below. <http://www.trendnet.com/downloads/>

In addition, it is also important for you to check the firmware version and compare it to the version your router is currently running. 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.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Firmware/Restore Setting**.

Note: This page also displays the current firmware version of your router.

Current firmware version is **1.00.01**.

Choose File No file chosen
Current firmware version is **1.00.01**.

3. Under **Firmware/Configuration Filename**, depending on your web browser, click on **Browse** or **Choose File**.

Browse...

Choose File No file chosen

A separate file navigation window should open.

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

6. Click **Upgrade**. If prompted, click **Yes** or **OK**.
(Default Filename: <firmwarefilename>.bin).

Upgrade Cancel

7. Wait for the router to complete the firmware upgrade process.

Restart your router

Configuration > Toolbox

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.

- **Disconnect the power adapter** – 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. This is also known as a hard reboot or power cycle.

Disconnect the power adapter from the power port of your router for 10 seconds, then, plug the power adapter back into the power of your router. Wait for your router Status light to begin flashing.

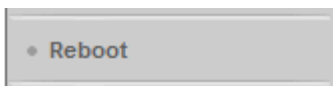
OR

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

Configuration > Toolbox > Reboot

1. Log into your router management page (see “Access your router management page” on [page 34](#)).

2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Reboot**.



3. You will be prompted to reboot your router. Click **Yes** or **OK**.

Check connectivity using the router management page

Configuration > Toolbox > Miscellaneous

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

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **Miscellaneous**.
3. Next to **Domain Name or IP address for Ping Test**, enter in the IP address (e.g. *192.168.10.101*) or host name (e.g. *www.trendnet.com*) to test and click **Ping**.

4. You will receive a *success* or *fail* result message of the address you entered providing a basic indicating of the router's connectivity to the Internet or devices that are connected to your network.

Ping Result

```
PING trendnet.com (192.168.1.249): 56 data bytes
64 bytes from 192.168.1.249: icmp_seq=0 ttl=127 time=0.0 ms
64 bytes from 192.168.1.249: icmp_seq=1 ttl=127 time=0.0 ms
64 bytes from 192.168.1.249: icmp_seq=2 ttl=127 time=0.0 ms
64 bytes from 192.168.1.249: icmp_seq=3 ttl=127 time=0.0 ms

--- trendnet.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5. Click **Save** at the bottom of the page to save the domain name or IP address.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

Check the router status information

Status

You may want to check the system information of your router such as WAN (Internet) connectivity, wired network settings, router MAC address, packet statistics, and current sessions.

1. Log into your router management page (see "Access your router management page" on [page 34](#)).

Note: The Status page will appear first when accessing the router management so you will be able to view the Status page information without logging in.

2. Click on **Status** at the top of the page.



3. Review the device information.

System Status or WAN (Internet) Information

System Status [Help]		
Item	WAN Status	Sidenote
MAC Address		
Remaining Lease Time		
IP Address		
Subnet Mask		
Gateway		
Domain Name Server		

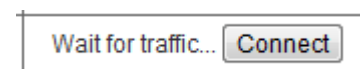
- **MAC Address** – The current MAC address used by your router's WAN port or interface configuration.
- **Remaining Lease Time:** If you are using a dynamic IP address Internet connection type, this will display the time remaining of your IP address leave from the ISP until your router will request for a new IP address.
- **IP Address** – The current IP address assigned to your router WAN port or interface configuration.

Note: If you are using a dynamic IP address Internet connection type, and you are logged into the router management page, you will have the Renew & Release options available.



- **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.
- **Domain Name Server** – The current DNS address(es) assigned to your router WAN (Internet) port or interface configuration.
- **Connection Time** – Displays the current WAN (Internet) connection status when using other Internet connection types such as PPPoE.

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



Wired LAN Status Information

LAN Status		
Item	LAN Status	Sidenote
MAC Address		
IP Address	192.168.10.1	
Subnet Mask	255.255.255.0	
DHCP Server	Enable	

- **MAC Address** – The current MAC address of your router's wired LAN or interface configuration.
- **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.

Packet Statistics Information

The table displays the amount of octets, unicast, and multicast packets sent and received on your router's WAN (Internet) interface.

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	97882746	16906516
Unicast packets	82070	84468
Multicast packets	0	0

There is information at the bottom of the page that displays your router status uptime, the device time/date and estimated device load.

Device Time: Thu, 01 Jan 2009 02:44:13 +0000

After Time: 02:44:13 up 2:44, load average: 0.00, 0.01, 0.00

Clicking **Refresh** at the bottom of the page will refresh the information on the status page.

Clicking **View Log** will bring you to log page (Configuration > Toolbox > System Information). See the "View your router log" section.

Clicking **Clients List** will bring you to the DHCP Clients List (Configuration > Basic Setting > DHCP Server > Clients List). See "Set up the DHCP server on you router" section.

Current Sessions

Status > NAT Status

The router will also display the current TCP/UDP sessions. To view the current sessions, click **NAT Status**.

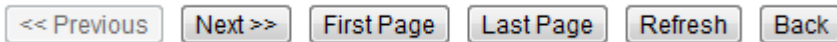
NAT Status					
ID	Protocol	Internal	NAT	External	Time-out
1	tcp	192.168.10.101:63258	10.10.10.101	50.18.169.214:80	89
2	tcp	192.168.10.101:63335	10.10.10.101	204.0.5.42:80	505
3	tcp	192.168.10.101:63264	10.10.10.101	50.18.169.214:80	89
4	tcp	192.168.10.101:63332	10.10.10.101	74.125.227.91:80	39
5	tcp	192.168.10.101:63314	10.10.10.101	75.126.109.204:80	24
6	tcp	192.168.10.101:63257	10.10.10.101	63.146.126.10:80	22
7	tcp	192.168.10.101:63266	10.10.10.101	173.192.226.215:80	22
8	tcp	192.168.10.101:63339	10.10.10.101	8.17.87.173:80	27
9	tcp	192.168.10.101:63254	10.10.10.101	74.125.227.90:80	39
10	tcp	192.168.10.101:63242	10.10.10.101	208.50.81.155:80	39
11	tcp	192.168.10.101:63225	10.10.10.101	204.0.5.51:80	495
12	tcp	192.168.10.101:63240	10.10.10.101	208.50.81.155:80	39
13	tcp	192.168.10.101:63333	10.10.10.101	74.125.227.90:80	505
14	tcp	192.168.10.101:63329	10.10.10.101	64.210.61.130:80	39
15	tcp	192.168.10.101:63336	10.10.10.101	64.210.61.144:80	39

Page: 1/8 (Active Session Number: 107)

- **ID** – Displays the session number.
- **Protocol** – Displays the protocol used in the session established, TCP or UDP.

- **Internal** – Displays the internal IP address of the session and the local port number used in the session established.
- **NAT** – Displays the NAT IP used in the session established.
- **External** – Display the destination IP address and port of the session established.
- **Timeout** – Displays the TTL (Time to Live) of the session established.
- **Page: (Active Session Number:)** - Displays the current session page you are viewing and number of active sessions.

Session Log Navigation



- **First Page** – Displays the first page of the session log.
- **Last Page** – Displays the last page of the session log.
- **Previous Page** – Display the session log page previous to the current. The **Page: 1/1** will display the current page.
- **Next Page** – Displays the session log page next to the current. The **Page: 1/1** will display the current page.
- **Refresh** – Refreshes the information displayed on the log page.
- **Download** - Allows you to download the current log to your local computer. (Default Filename: system.log)
- **Clear logs** - Clears all logging

View your router log

Configuration > Toolbox > System Information

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 34](#)).
2. Click on **Configuration** at the top of the page, click on **Toolbox**, and click on **System Information**.
3. Review the device log information.

Under **System Information**, the current WAN (Internet) connection type is displayed along with the current date and time set on the router.

System Information	
Item	Setting
▶ WAN Type	Dynamic IP Address
▶ Display time	2011/11/07 15:57:56

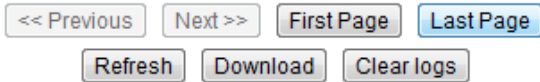
You can view the router log under **System Log**.

System Log	
Time	Log
Nov 7 13:14:01	udhcpd: Warning: No specify Hostname
Nov 7 13:14:11	commander: sync-date success.
Nov 7 15:36:06	udhcpd: Warning: No specify Hostname

Page: 1/1 (Log Number: 3)

- **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 35)
- **Log** – Displays the log message.
- **Page: (Log Number)** – Displays the current log page you are viewing and number of logs.

Router Log Navigation



- **First Page** – Displays the first page of the log.
- **Last Page** – Displays the last page of the log.
- **Previous Page** – Display the log page previous to the current. The **Page: 1/1** will display the current page.
- **Next Page** – Displays the log page next to the current. The **Page: 1/1** will display the current page.
- **Refresh** – Refreshes the information displayed on the log page.
- **Download** - Allows you to download the current log to your local computer. (Default Filename: system.log)
- **Clear logs** - Clears all logging

Configure your router log

Configuration > Advanced Setting > System Log

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 an external log server

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **System Log**.

3. Next to **IP address for syslogd**, enter the IP address (e.g. 192.168.10.250) of the external log server to send router logging and check the **Enable** option.

Item	Setting	Enable
▶ IP address for syslogd	<input type="text"/>	<input checked="" type="checkbox"/>

4. Click **Save** to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



Clicking **View Log** will bring you to log page (Configuration > Toolbox > System Information). See the “View your router log” section.

Send router logs to your e-mail address

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **System Log**.
3. Review the e-mail log settings.

		Enable
▶ Setting of Email alert		<input checked="" type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

- **SMTP Server : port** – Enter the IP address (e.g. 10.10.10.10) or domain name (e.g. mail.trendnet.com) of your e-mail server. Enter the port used by your e-mail service. (e.g. Default SMTP Server Port: 25)
- **SMTP Username** – Enter your account user name for your e-mail service.
- **SMTP Password** – Enter your password for your e-mail service.
- **E-mail addresses** – Enter the e-mail addresses to send the log file. (e.g. user1@trendnet.com, user2@trendnet.com)

4. Click **Save** to save the changes.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.

<input type="button" value="Save"/> <input type="button" value="Undo"/>
<input type="button" value="View Log..."/> <input type="button" value="Email Log Now"/>

5. Click **Email Log Now** to send an e-mail of the current router log using your email alert settings.

Clicking **View Log** will bring you to log page (Configuration > Toolbox > System Information). See the “View your router log” section.

Enable SNMP on your router

Configuration > Advanced Setting > SNMP

SNMP (Simple Network Management Protocol) is a network management protocol used to monitor (read) and/or manage (write) multiple network devices on a network. This feature requires a preconfigured external SNMP server.

1. Log into your router management page (see “Access your router management page” on [page 34](#)).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **SNMP**.
3. Review the options for SNMP.

▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>

- **Enable SNMP** – Check the **Local** option to allow SNMP access on the router wired LAN interface. Check the **Remote** option to allow SNMP access on the router WAN (Internet) interface.
- **Get Community** – Enter the community name to match the settings with the external SNMP server. This community will have SNMP read access only.
- **Set Community** – Enter the community name to match the settings with the external SNMP server. This community will have SNMP write access.

- **IP 1-4** – Enter up to four IP addresses of external SNMP servers. (e.g. 192.168.10.250)
- **SNMP Version** – Select the correct SNMP version to match the SNMP version of your external SNMP server(s), **V1** or **V2c**.
- **WAN Access IP Address** – You can specify a single IP address from the Internet to allow to connect your router using SNMP. (optional)

Note: When allowing Remote SNMP access, leaving this setting blank will allow access from any IP address from the Internet. It is recommended to specify an IP address if allowing Remote SNMP access.

4. To save changes, click **Save** at the bottom of the page.

Note: If you would like to discard the changes, click **Undo** before you click **Save**.



Save Undo

Router Management Page Structure

Status

- System Status
- LAN Status
- Statistics Information

Wizard

- Setup Wizard

Configuration

- Basic Setting
 - Network Settings
 - LAN & WAN (Internet)
 - DHCP Server
 - Password
- Forwarding Rules
 - Virtual Server
 - Special Application
 - DMZ
- Security
 - Setting Overview
 - Packet Filters
 - URL Filters
 - Keyword Blocking
 - MAC Control
 - VPN-IPsec

- VPN-L2TP Client
- VPN-L2TP Server
- VPN-PPTP Client
- VPN-PPTP Server
- Management
 - Remote Management

- Advanced Setting

- Setting Overview
- System Log
- Dynamic DNS
- QoS
- SNMP
- Routing
- System Time
- Scheduling

- Toolbox

- System Info
- Firmware/Restore Setting
 - Upgrade Firmware
 - Restore Configuration
- Backup Setting
- Reset to Default
- Reboot
- Miscellaneous

Logout

- Logout of router management page

Technical Specifications

Hardware	
Standards	IEEE 802.3 (10BASE-T), IEEE 802.3u (100BASE-TX)
WAN	1 x 10/100Mbps Auto-MDIX port (Internet)
LAN	4 x 10/100Mbps Auto-MDIX ports
Power Switch	On/off power switch
Reset Button	Reset button - Factory Default (Hold for 20 seconds)
Connection Type	Dynamic IP, Static (fixed) IP, PPPoE, PPTP, L2TP
Firewall	NAT, SPI, and DoS prevention
VPN	IPsec/PPTP/L2TP– Up to 80* tunnels PPTP/L2TP Server and Client – Define up to 5 user accounts each (multiple logins per account) IPsec/L2TP/PPTP VPN pass through – Up to 100 sessions
IPsec VPN Protocols	Encryption (DES, 3DES, AES-128/192/256 bit), Authentication (MD5, SHA1), DH/PFS Groups (1-18), Key Management (Manual/IKE), Preshared Key (PSK), Encapsulation (ESP, AH, ESP+AH), Mode (Main/Aggressive), NAT Traversal, NetBIOS over IPsec, XAUTH, Keep-Alive, Dead Peer Detection (DPD), Local/Remote ID (FQDN, E-Mail, Key ID)
PPTP/L2TP VPN Protocols	Authentication (PAP, CHAP, MS-CHAP v1/2), Encryption (MPPE-40/56/128 bit)
Access Control	Virtual Servers, Packet MAC/IP Packet Filters, URL/Keyword Filters, DMZ host, Multi-DMZ, UPnP, and IGMPv1/2 pass through
Time/Schedule	Set time via NTP or manually and define schedules: virtual server, packet filters, and QoS
Routing	Static and Dynamic RIP v1/2
Quality of Service	Service-Based IP/(TCP/UDP) port with 3 priority queues (High, Normal, Low)

Management/ Monitoring	Local/remote configuration, upgrade firmware, Backup/Restore configuration via Web browser Internal System Log, Syslog, E-Mail Alert, SNMPv1/v2c, Ping Test Tool, and Wake-on-LAN (WoL)
LED Indicator	Status, LAN1~LAN4, WAN (Internet)
Power	Input: 100~240V AC, 50~60Hz Output: 12V DC, 1A
Power Consumption	4.08 Watts (max.)
Dimension (L x W x H)	189 x 118 x 33 mm (7.4 x 4.6 x 1.3 in)
Weight	249 g (8.8 oz)
Temperature	Operation: 0~ 40°C (32°F~ 104°F); Storage: -10~ 90°C (14°F~158 °F)
Humidity	Max. 95% (non-condensing)
Certifications	CE, FCC

*The number of supported concurrent VPN tunnels is dependent upon available bandwidth

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 7](#).
2. Make sure the LAN and Status 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).

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.*

4. Press on the factory reset button on the front panel for 20 seconds, the release.

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. What should I do?

Answer:

1. Click on Wizard at the top of the router management page.
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.
2. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.
3. 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.

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 **ipconfig getifaddr <en0 or en1>** to display the wired or wireless IP address settings.

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

Graphical Method

Windows 7

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings** double-click the **Local Area Connection** icon, and click **Details**.

Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, double-click the **Local Area Connection** icon and click **Details**.

Windows XP

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Double-click the **Local Area Connection** icon and the click the **Support** tab. Click on **Details** for more IP address information.

MAC OS 10.6/10.5

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

MAC OS 10.4

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

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

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

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

Windows 7

- 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

- a. Go into the **Control Panel**, double-click the **Network Connections** icon

- b. Right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

MAC OS 10.4/10.5/10.6

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Ethernet connection.
 - In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
 - In MAC OS 10.5/10.6, in the left column, select **Ethernet**.
- e. Configure TCP/IP to use DHCP.
 - In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
 - In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
 - In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
- f. Restart your computer.

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

How to find your MAC address?

Windows 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 **getmac -v** to display your MAC addresses.

MAC OS 10.6/10.5

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

MAC OS 10.4

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

Additional IPsec VPN options

There are additional parameters in your router that you can configure to increase the encryption or authentication strength of the IPsec VPN Tunnel. Any additional security options enabled and configured must be configured on both sides of the IPsec VPN tunnel. Adding additional security strength to your VPN may significantly degrade the performance of transmitting or receiving data through the VPN tunnel.

▶ Method	IKE
----------	-----

- **Method** – You can choose between **IKE** or **Manual**.
 - **IKE (Internet Key Exchange)** – (Recommended) Compared to the older Manual method, this method is more secure as it can provide endpoint security, security against replay attacks or anti-replay, and dynamic session rekeying using a PSK (preshared key) meaning that the session key between the two endpoints will change after a specified period of time.
 - **Manual** – Manual Key is an older with several limitations compared to IKE. Since the same session key is always used and never changes, the VPN is vulnerable to replay attacks.

▶ Phase1 Key Life Time	28800	seconds
▶ Phase2 Key Life Time	3600	seconds

- **Phase 1/Phase 2 Key Life Time** – Using the IKE method, you can specify the period of time in seconds for each phase of the tunnel before a new session key is created between the VPN endpoints. There is an SA (security association) created for each phase, one for Phase 1 (IKE phase) phase and another for Phase 2 (IPsec phase). It is recommended that these values are left at default settings.

Note: If you are changing these values, it is strongly recommended to have different time values for each, never the same and assign a longer time value to Phase 1 than Phase 2. Assigning the same value may cause VPN connectivity problems between the VPN endpoints.

▶ Encapsulation Protocol	ESP
--------------------------	-----

- **Encapsulation Protocol** - You can choose between **ESP, AH, or ESP+AH**.
 - **ESP (Encapsulating Security Payload)** – (Recommended) This protocol is recommended as it can provide both authentication and encryption of the data and maintain and acceptable performance.
 - **AH (Authentication Header)** – This protocol is less secure compared to ESP as it can only provide authentication of the data, no encryption.
 - **ESP+AH (Encapsulating Security Payload + Authentication Header)** – This protocol is the most secure because it combines the security mechanism of both ESP and AH, however, performance may degrade significantly if used due to the additional security encapsulation of both protocols.

▶ PFS Group	Disable
-------------	---------

- **PFS (Perfect Forward Secrecy) Group** – You can choose between **Group 1, Group 2, Group 5, or Same Phase 1**. This provides an additional layer of security in Phase 2 (IPsec phase) by ensuring that if any session keys are compromised, no other keys can be derived from the compromised key. The group options are based of a security algorithm known as the DH (Diffie-Hellman) algorithm. As the DH group numbers increase, the security also increases. Adding this option may significantly decrease performance.
 - **Group 1** – DH group 1 (768-bit)
 - **Group 2** – DH group 2 (1024-bit)
 - **Group 5** – DH group 5 (1536-bit)
 - **Same as Phase 1** – Chooses the same DH group selected under the IKE proposal section.

▶ Aggressive Mode	<input checked="" type="checkbox"/> Enable
-------------------	--

- **Aggressive Mode** –By default, the IKE negotiation will use Main mode. Checking this option will change negotiation to Aggressive. Aggressive mode will increase the speed of establishing a connection between the VPN endpoints by sending fewer messages than in Main mode. The disadvantage of

using Aggressive mode would decrease security as the identity of the endpoints would be sent unencrypted and/or authenticated, along with disabling negotiation of additional security parameters such as PFS (Perfect Forward Secrecy) and DH (Diffie-Hellman) groups between the VPN endpoints.

Note: It is recommended only to leave Aggressive mode disabled, unless you are experiencing difficulties establishing a VPN connection and require more compatibility typically between VPN gateways from two different manufacturers.

▶ Connecting Type	On demand ▼
-------------------	-------------

- **Connecting Type** – This option is only available in Site-to-Site IPsec VPN tunnel configurations. You can choose between **On demand**, **Always on**, or **Manual**.

Note: It is recommended to leave this setting at default and use the DPD (Dead Peer Detection) feature to control the connection timeout.

- **On demand** – This will automatically disconnect the connection between VPN endpoints after an idle period of time when there is no traffic exchange through the VPN tunnel. If traffic is detected, the connection between VPN endpoints will automatically be re-established to exchange traffic.
- **Always on** – The connection between VPN endpoints will always be established.
- **Manual** – Controlled through the IPsec main configuration page, the connection between the VPN endpoints will only be established or disconnected when clicking **Connect** or **Disconnect** on the IPsec main configuration page.

▶ Remote ID	Type: Username ▼ ID: <input type="text"/>
▶ Local ID	Type: Username ▼ ID: <input type="text"/>

- **Remote / Local ID** – This provides an additional layer of identification or authentication on the VPN tunnel. You can choose **Username**, **FQDN**, **User@FQDN**, or **Key ID**. These settings must match on both VPN endpoints.

- **Username** – Create and enter a user name. (e.g. trendnetuser)
- **FQDN (Fully Qualified Domain Name)** – Enter a domain name. (e.g. trendnet.com)
- **User@FQDN** – Enter an e-mail address. (e.g. site1@trendnet.com)
- **Key ID** – Create and enter a password or key. (e.g. 1234567890)

▶ Dead Peer Detection (DPD)	<input type="checkbox"/> Enable ▶ Timeout: <input type="text" value="180"/> Second(s) ▶ Delay: <input type="text" value="30"/> Second(s)
-----------------------------	--

- **DPD (Dead Peer Detection)** – This feature ensures that the tunnel between VPN endpoints is only connected when it is in use and disconnected during an idle period of time increasing security using “hello” and “acknowledge” messages. Instead of constantly sending messages between VPN endpoints such as using Keep Alives, this allows for more efficiency utilizing the VPN connection.
 - **Enable** – Checking this option enables DPD.
 - **Timeout** - Enter the time interval in seconds that the router will send “hello” messages before disconnecting the VPN connection. For every “acknowledge” message, the timer will reset. The connection will be re-established when there is an attempt to communicate through the VPN connection and the timer will restart.
 - **Delay** – Enter the time interval in seconds between each “hello” message sent. If the timeout period is reached and VPN connection is disconnected, delay messages will no longer be sent until the connection is re-established.

▶ XAUTH	<input checked="" type="radio"/> None <input type="radio"/> Server <input type="radio"/> Client ▶ Username: <input type="text"/> ▶ Password: <input type="text"/>
---------	---

- **XAUTH (Extended Authentication)** – This provides an additional layer of identification or authentication on the VPN tunnel. Unlike the Remote / Local ID feature, XAUTH allows you to authentication from a separate database of

user accounts. Your router supports an internal user account database for XAUTH authentication in the IPsec main configuration page. For XAUTH configuration between VPN endpoints, one endpoint must be configured as the XAUTH Server and the other configured as the XAUTH client. **Note:** Your router does not support external authentication to external servers such as a RADIUS server.

- **Server** – Configures your VPN tunnel as the XAUTH Server.
- **Client** – Configures your VPN tunnel as the XAUTH Client. Enter your **Username** and **Password** for authentication.

If your VPN tunnel is configured as the XAUTH server, to configure the user account in the internal authentication database, click on **Configuration** at the top of the page, click on **Security Setting**, then click on **VPN-IPsec**, and click on **XAUTH** at the bottom of the page.

You can enter the user account information (Username, Password) for XAUTH.

IPsec XAUTH Server side setting		
ID	Username	Password
1	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="password"/>

For the IKE and IPsec proposals, you can select different **Encryption** and **Authentication** methods. You are also able to create a second IKE and IPsec proposal in case the first proposal cannot be negotiated with the VPN endpoint, it will use the second proposal defined.

Set IKE Proposal		<input checked="" type="checkbox"/> Enable		
ID	Encryption	Authentication	DH Group	Enable
1	3DES	SHA1	Group1	<input checked="" type="checkbox"/>
2	3DES	SHA1	Group1	<input type="checkbox"/>

Set IPsec Proposal		<input checked="" type="checkbox"/> Enable	
ID	Encryption	Authentication	Enable
1	3DES	SHA1	<input checked="" type="checkbox"/>
2	3DES	SHA1	<input type="checkbox"/>

- **Encryption** – Select the encryption method. You can choose between **DES**, **3DES**, **AES-128**, **AES-192**, or **AES-256**.
 - **DES (Data Encryption Standard)** – Weaker encryption strength. It uses a symmetric key algorithm with 56-bit key size.
 - **3DES (Triple DES, TDEA Triple Data Encryption Algorithm)** –Applies DES three times to each data block resulting in 168-bit key size. Better encryption strength than DES but lower performance than AES.
 - **AES-128/192/256 (Advanced Encryption Standard 128/192/256-bit key sizes)** – (Recommended) Provides the strongest encryption strength and best performance. You can choose 128, 192, or 256-bit key size. As the bit and key size increase, the security strength also increases.
 - **Null** – IPsec only. Weaker encryption strength. And offers better performance.
- **Authentication** – Select the authentication method. You can choose between **SHA1** or **MD5**.
 - **SHA1 (Secure Hash Algorithm)** – (Recommended) Stronger than MD5 as it produces a longer hash key but slightly lower performance.
 - **MD5 (Message Digest 5)** - Weaker than SHA1 as the hash key is slightly shorter than SHA1 and provides higher performance.
- **DH (Diffie-Hellman) Group** - As the DH group numbers increase, the security also increases. You can choose between **Group 1**, **Group 2**, or **Group 5**. This is to configure the IKE proposal only. To configure the DH Group for the IPsec proposal, configure PFS (Perfect Forward Secrecy)
 - **Group 1** – DH group 1 (768-bit)
 - **Group 2** – DH group 2 (1024-bit)
 - **Group 5** – DH group 5 (1536-bit)

▶ NetBIOS over IPsec	<input type="checkbox"/> Enable
----------------------	---------------------------------

- **NetBIOS (Network Basic Input/Output System) over IPsec** – Checking the **Enable** option allows computer and network devices to communicate using NetBIOS computer or host names instead of IP addresses over the VPN tunnel.

▶ VPN Statistic	<input type="checkbox"/> Enable
-----------------	---------------------------------

- **VPN Statistic** – Check the **Enable** option allows you to view the IPsec VPN tunnel uptime and the number of incoming and outgoing packets. Check the **Enable** option and click **Save** at the bottom of the page.

Click **Statistic** at the bottom of the page.

<input style="border: none;" type="button" value=" << Previous "/> <input style="border: none;" type="button" value=" Next >> "/> <input style="border: none;" type="button" value=" Save "/> <input style="border: none;" type="button" value=" Undo "/> <input style="border: none;" type="button" value=" XAUTH account "/> <input style="border: none;" type="button" value=" Statistic "/> <input style="border: none;" type="button" value=" Refresh "/>
--

View the IPsec VPN tunnel uptime and packet statistics.

ID	Tunnel Name	Elapsed Time	Incoming	Outgoing
1	Tunnel 1			

▶ Max. number of tunnels	<input type="text" value="5"/>
--------------------------	--------------------------------

Max. number of tunnels – Enter the maximum amount of *concurrent VPN tunnels your router can establish. Regardless of how many entries and enable, your router will only be able to activate the maximum amount of tunnels entered for this setting.

*The number of supported concurrent VPN tunnels is dependent upon available bandwidth

Additional PPTP/L2TP options

▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS_CHAP <input type="checkbox"/> MS_CHAPv2
---------------------------	--

- **Authentication Protocol**
 - **PAP (Password Authentication Protocol)** – Provides basic password authentication. Weak security protocol as it does not provide data encryption. MPPE Encryption Mode will not be available for this option.
 - **CHAP (Challenge Handshake Authentication Protocol)** – Provides stronger authentication capabilities than PAP, but still does not provide data encryption. MPPE Encryption Mode will not be available for this option.
 - **MS-CHAP (Microsoft Challenge Handshake Authentication Protocol Version 1)** – (Recommended) Provides authentication and data encryption. MPPE Encryption Mode will be available for this option.
 - **MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2)** – (Recommended) Provides authentication and data encryption. Strongest PPTP/L2TP security protocol supported by your router. MPPE Encryption Mode will be available for this option.


▶ Encryption Length	<input type="checkbox"/> 40 bits <input type="checkbox"/> 56 bits <input type="checkbox"/> 128 bits
---------------------	---

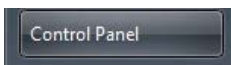
- **Encryption Length** – Enable MPPE Encryption Mode will allow you to choose which key lengths to support **40 bits**, **56 bits**, or **128 bits**. The longer the key length, the stronger the security.

Connecting to your router using the built-in PPTP VPN client software

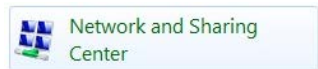
Note: Below are the examples according to the examples provided in the Virtual Private Networking PPTP section. Please ensure that your VPN client computer is able to access the Internet from a remote location.

Windows 7

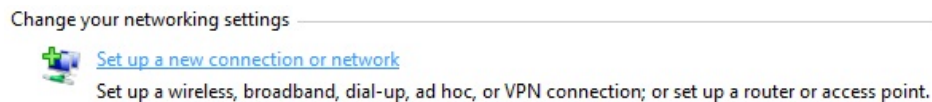
1. Click Start  and then click **Control Panel**.



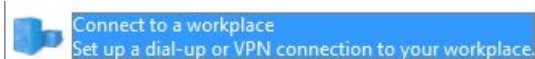
2. In the Control Panel window, click on **Network and Sharing Center**.



3. Under Change your networking settings, click on **Set up a new connection or network**.



4. In the window, click on **Connect to a workplace** and then click **Next**.



5. In the window, click on **Use my Internet Connection (VPN)**.



6. Next to Internet address, enter the remote router WAN (Internet) IP address and then click **Next**.

Internet address:

7. Enter the user name and password account information you configured in your router and check **Show characters** to verify and **Remember this password** to save the credentials. Click **Connect**.

User name:

Password:

Show characters

Remember this password


8. Your computer will attempt to connect to the PPTP VPN server (router).

Verifying user name and password...



9. If successful, you will receive a message that indicates you are connected.


You are connected

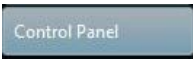
10. To verify connectivity, you can use the ping connectivity test. Click **Start**  + **R** key at the same time to bring up the run command window. Type `cmd` in the run command window and click **OK**. In the command prompt, type `ping <IP address>` of remote computer or device over the VPN. If you receive replies, the connectivity is successful. If you receive time outs, there may be problems with IP configuration or firewall/security settings of the remote computer or device you are trying to communicate.

```
C:\>ping 192.168.10.101

Pinging 192.168.10.101 with 32 bytes of data:
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
```

Windows Vista

1. Click Start  and then click **Control Panel**.



2. In the Control Panel window, click on **Network and Sharing Center**.



3. Under Tasks on the left panel, click on **Set up a connection or network**.



4. In the window, click on **Connect to a workplace** and then click **Next**.



5. In the window, click on **Use my Internet Connection (VPN)**.



6. Next to Internet address, enter the remote router WAN (Internet) IP address and then click **Next**.



7. Enter the user name and password account information you configured in your router and check **Show characters** to verify and **Remember this password** to save the credentials. Click **Connect**.

User name:

Password:

Show characters

Remember this password


8. Your computer will attempt to connect to the PPTP VPN server (router).

Verifying user name and password...



9. If successful, you will receive a message that indicates you are connected.

You are connected

10. To verify connectivity, you can use the ping connectivity test. Click **Start**  + **R** key at the same time to bring up the run command window. Type `cmd` in the run command window and click **OK**. In the command prompt, type `ping <IP address>` of remote computer or device over the VPN. If you receive replies, the connectivity is successful. If you receive time outs, there may problems with IP configuration or firewall/security settings of the remote computer or device you are trying to communicate.

```
C:\>ping 192.168.10.101

Pinging 192.168.10.101 with 32 bytes of data:
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
```

Windows XP

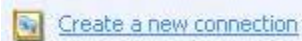
1. Click Start  and then click **Control Panel**.



2. In the Control Panel window, click on **Network Connections**.



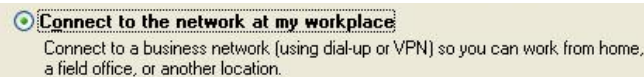
3. Under Network Tasks on the left panel, click on **Create a new connection**.



4. In the New Connection Wizard window, click **Next**.



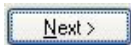
5. In the window, click on **Connect to the network at my workplace** and then click **Next**.



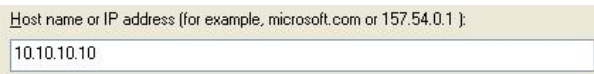
6. In the window, click on **Virtual Private Network connection** and then click **Next**.



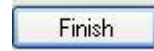
7. In the Connection Name window, click **Next**.



8. Next to Host name or IP address, enter the remote router WAN (Internet) IP address and then click **Next**.



9. In the Completing the New Connection Wizard window, click **Finish**.




10. Enter the user name and password account information you configured in your router and check **Save this user name and password for the following users: Me only** to save the credentials. Click **Connect**.



8. Your computer will attempt to connect to the PPTP VPN server (router) and if successful, you receive a message that indicates that you are connected.



10. To verify connectivity, you can use the ping connectivity test. Click Start  + **R** key at the same time to bring up the run command window. Type *cmd* in the run command window and click **OK**. In the command prompt, type *ping <IP address>* of remote computer or device over the VPN. If you receive replies, the connectivity is successful. If you receive time outs, there may be problems with IP configuration or firewall/security settings of the remote computer or device you are trying to communicate.

```
C:\>ping 192.168.10.101

Pinging 192.168.10.101 with 32 bytes of data:
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
Reply from 192.168.10.101: bytes=32 time=2ms TTL=127
```

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
- EN 61000-3-3 : 2008
- EN 55024 : 1998 + A1 : 2001 + A2 : 2003
- EN 61000-3-2 : 2006 + A2 : 2009



 Český [Czech]	TRENDnet tímto prohlašuje, že tento TW100-BRV214 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2004/108/ES.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TW100-BRV214 overholder de væsentlige krav og øvrige relevante krav i direktiv 2004/108/EF.
 Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TW100-BRV214 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2004/108/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TW100-BRV214 vastavust direktiivi 2004/108/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this TW100-BRV214 is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el TW100-BRV214 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2004/108/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΤΡΕΝΔΝΕΤ ΔΗΛΩΝΕΙ ΟΤΙ ΤΩ100-ΒΡV214 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2004/108/ΕΚ.
 Français [French]	Par la présente TRENDnet déclare que l'appareil TW100-BRV214 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2004/108/CE.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo TW100-BRV214 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2004/108/CE.
 Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TW100-BRV214 atbilst Direktīvas 2004/108/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TW100-BRV214 atitinka esminius reikalavimus ir kitas 2004/108/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TW100-BRV214 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2004/108/EG.
 Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TW100-BRV214 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 2004/108/EC.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TW100-BRV214 megfelel a vonatkozó alapvető követelményeknek és az 2004/108/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym TRENDnet oświadcza, że TW100-BRV214 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2004/108/EC.
 Português [Portuguese]	TRENDnet declara que este TW100-BRV214 está conforme com os requisitos essenciais e outras disposições da Directiva 2004/108/CE.
 Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TW100-BRV214 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2004/108/ES.
 Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TW100-BRV214 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2004/108/ES.
 Suomi [Finnish]	TRENDnet vakuuttaa täten että TW100-BRV214 tyyppinen laite on direktiivin 2004/108/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar TRENDnet att denna TW100-BRV214 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-BRV214 – 3 Years Warranty

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

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

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

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

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

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

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

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

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

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

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

PWP05202009v2

2012/05/11



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