INSTALLATION AND SET-UP GUIDE

Setting up the L2TP WAN connection type on the Linksys LRT214 and LRT224

The **Layer 2 Tunneling Protocol (L2TP)** WAN connection type is a legacy feature originally designed for specific ISPs in **Europe**. The legacy feature does not support advanced security options such as MPPE encryption and L2TP over IPSec. Without the advanced security options, the current implementation on LRT routers cannot work with third-party VPN services that employ L2TP.

This article will guide you on how to set up the L2TP WAN connection type on the Linksys Gigabit VPN routers, LRT214 and LRT224. Before you proceed, make sure you have completed the following in your L2TP Server:

NOTE: The images may vary according to your L2TP server.

- Enable the L2TP Server.
- Disable the **Use MPPE encryption**.

- Disable the **L2TP over IPSec Setting**.

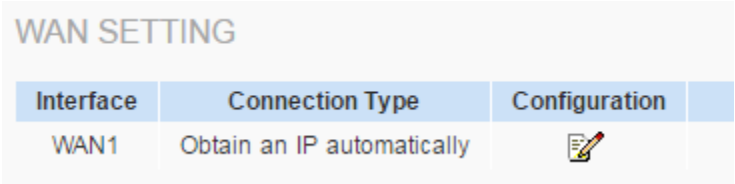
Follow the steps below to set up the L2TP WAN connection type on the Linksys Gigabit VPN router.

Step 1:
Open a web browser and access the router's web-based setup page. To learn how, click here.

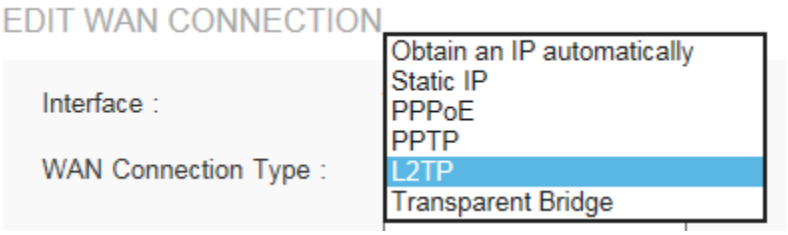
Step 2:
Click on the **Configuration** tab.

Step 3:

In the **Setup** > **Network** > **WAN SETTING**, click  under **Configuration**.

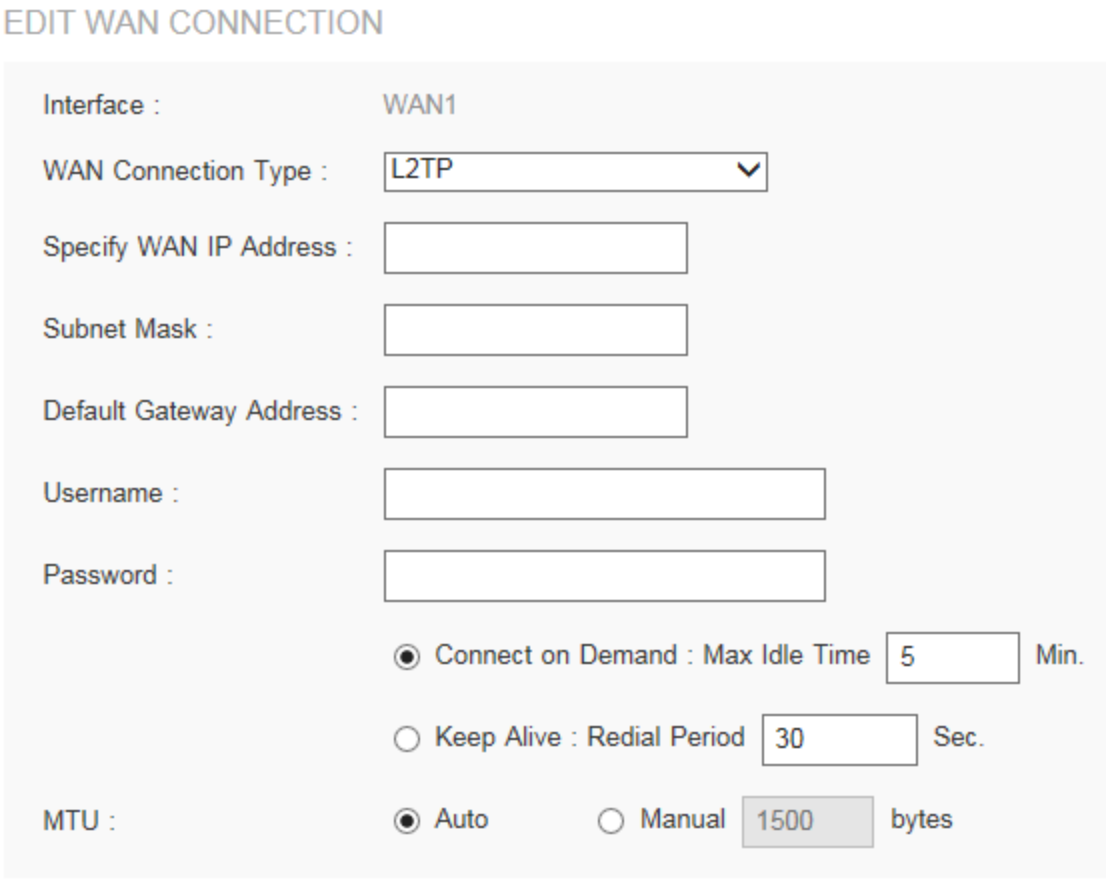


Step 4:
In the **WAN Connection Type**, click the dropdown menu and select **L2TP**.



Step 5:
Enter the information from your L2TP server in the succeeding fields.

NOTE: You may choose **Connect on Demand** if you want to enable auto-dialing for a dial connection. Select **Keep Alive** if you want the dial connection to redial automatically when disconnected. The default setting for **Maximum Transmission Unit (MTU)** is **Auto**. The default manual setting is 1500 bytes.



Step 6:
Click **Save**.

You should now have successfully set up the L2TP WAN connection type on your Linksys LRT214 or LRT224.

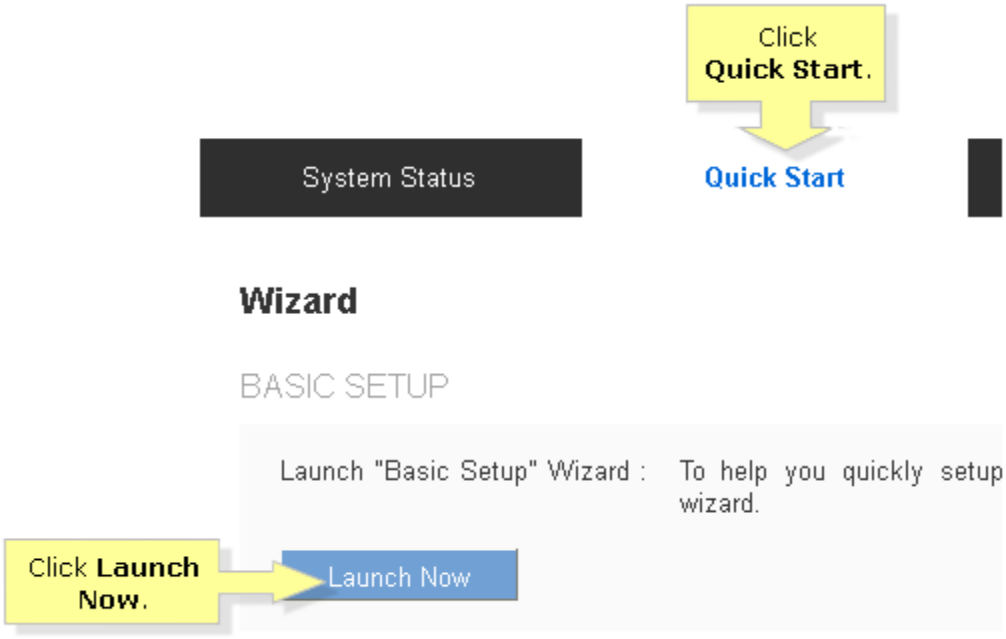
Setting up the Linksys Gigabit VPN Router using the Basic Setup Wizard

Setting up the Linksys Gigabit VPN Router is easy using the **Basic Setup Wizard** to configure the basic network settings of your router. You can find this software by accessing the web-based setup page of your VPN router. For instructions, click here.

Setting up your Router

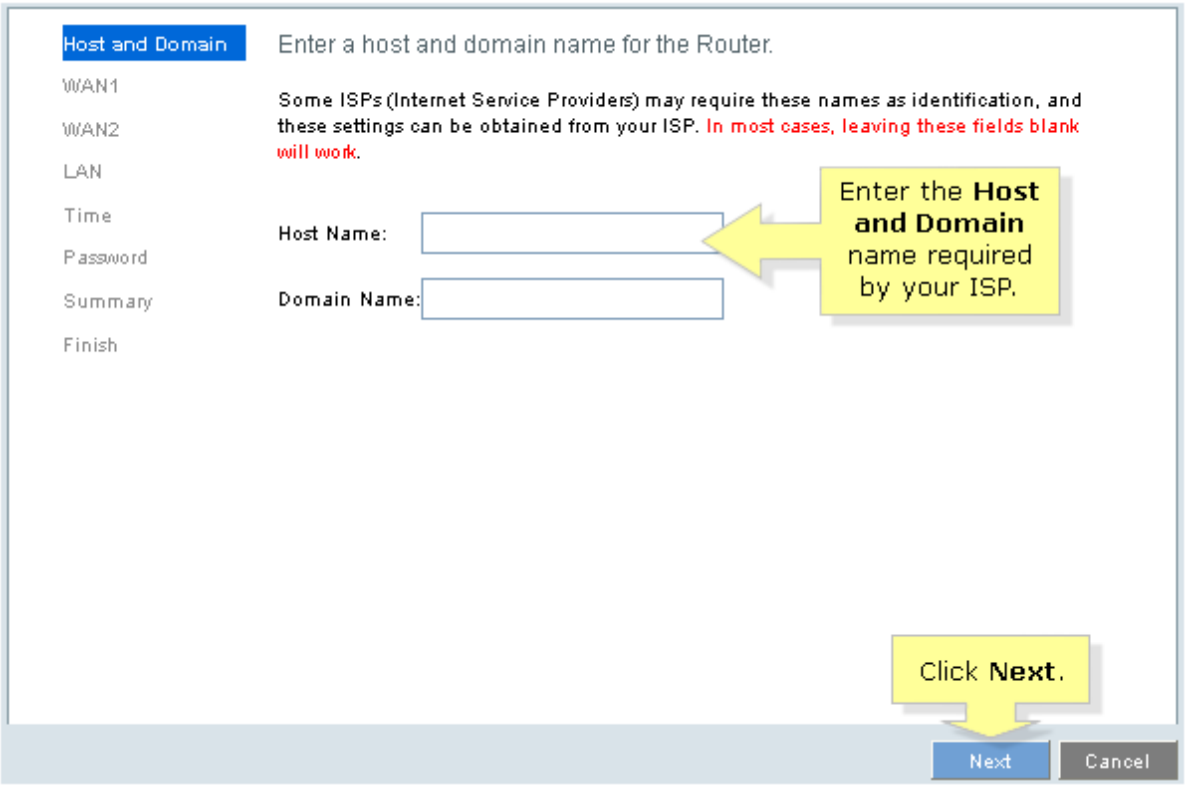
Once you have access the web-based setup page of your router, you may proceed with the setup.

Step 1:
On the web-based setup page, click **Quick Start** tab. Then, click the **Launch Now** button to immediately start the set up process.



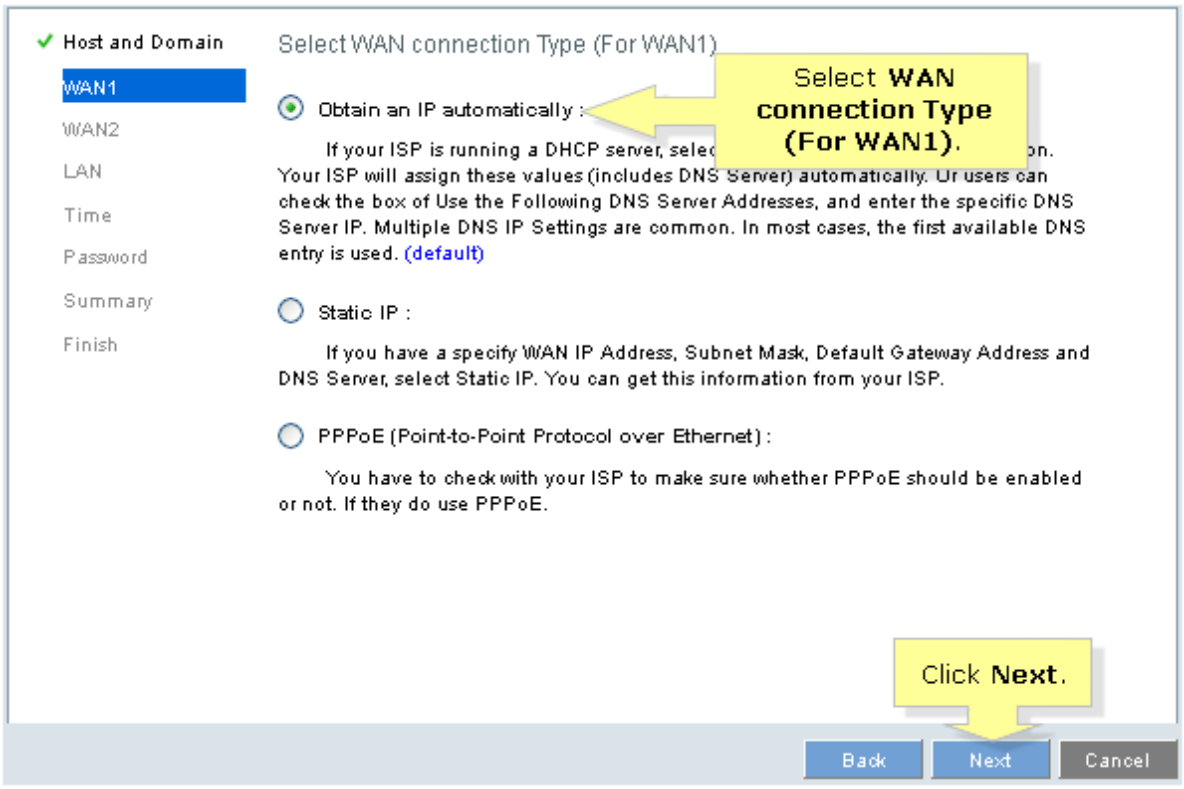
Step 2:
Under **Host Name** and **Domain Name**, enter the host and domain name required by your **Internet Service Provider (ISP)** and then click **Next**.

NOTE: If your ISP does not require a Host Name and a Domain Name, just leave the fields blank instead.



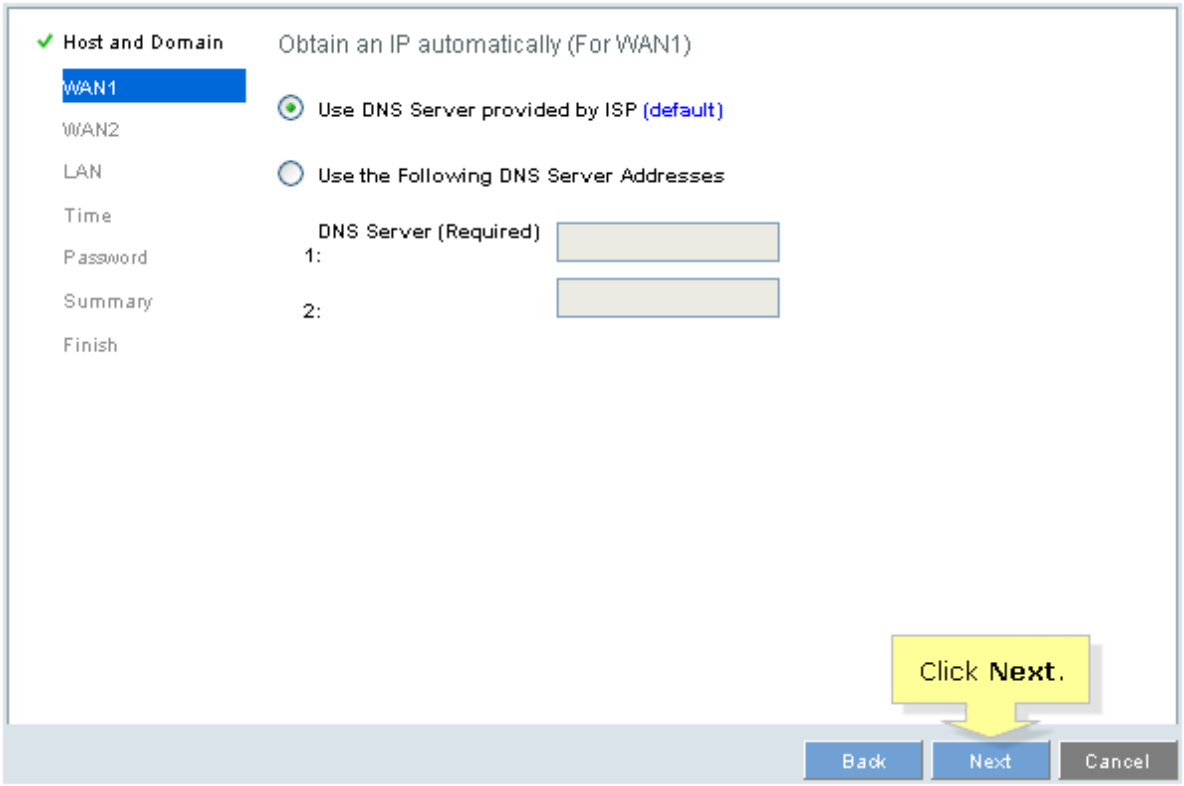
Step 3:
Select your **WAN connection Type** under **WAN1**. Then, click **Next**.

NOTE: In this example, **Obtain an IP automatically** is used.



Step 4:

Select the DNS settings on your router. If you have a specific DNS you would like to use, select **Use the Following DNS Server Addresses** and enter your DNS Server Addresses. Otherwise, select **Use DNS Server provided by ISP (default)** then click **Next**.



QUICK TIP: If you have a Dual-WAN Router, Model LRT224 and are using both WAN ports, enter the settings for your second ISP under **WAN2** then click **Next**.

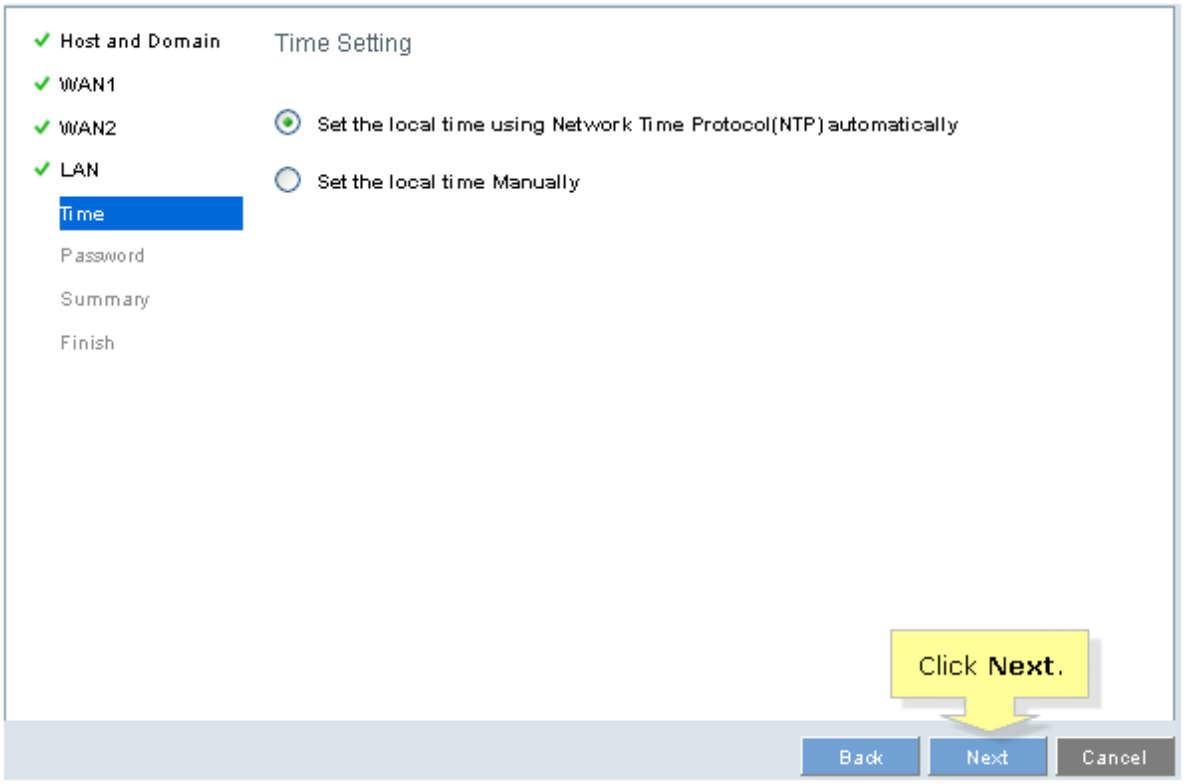
NOTE: WAN2 will not be an option on the LRT214 since it only has one WAN port

Step 5:

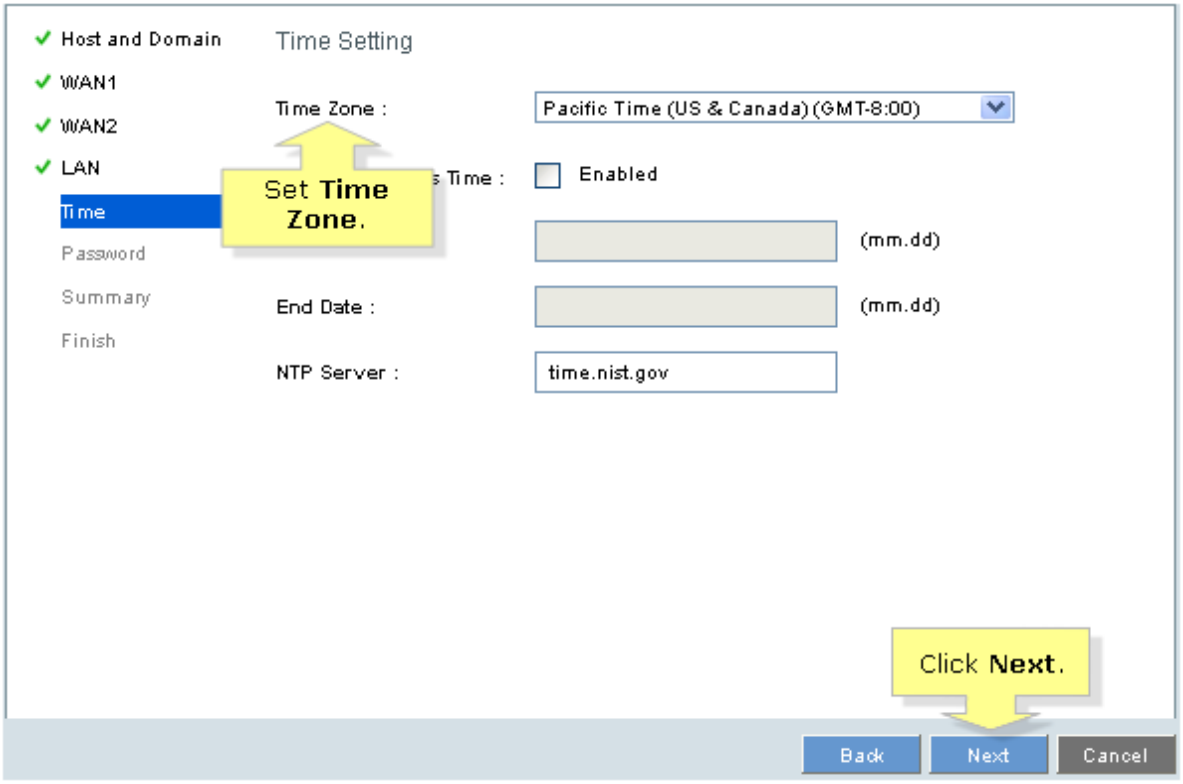
Enter the **Device IP Address** of your VPN router under **LAN**. Click **Next**.

NOTE: In this example, "192.168.1.1" is the local IP Address of the VPN router.

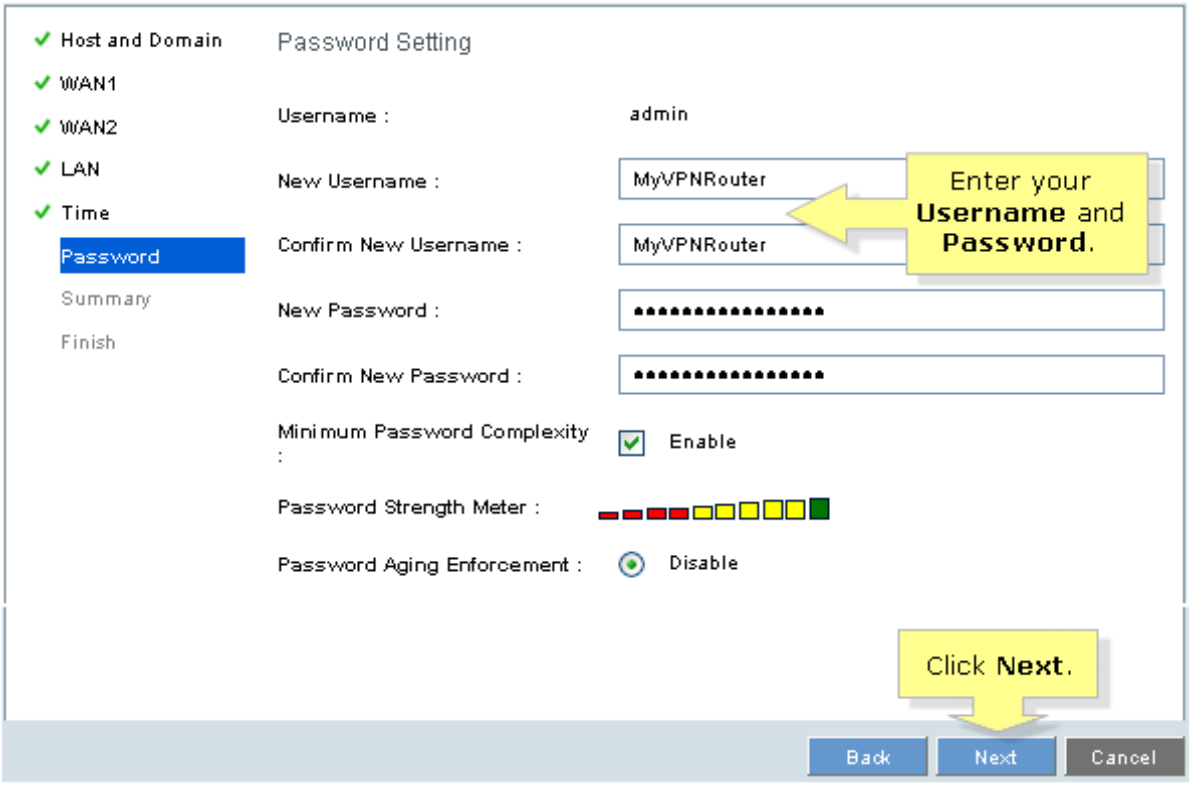
Step 6:
Under **Time** option, select your preferred time then click **Next**.



Step 7:
Set **Time Zone** that you will be using for your router. Click **Next** to proceed.

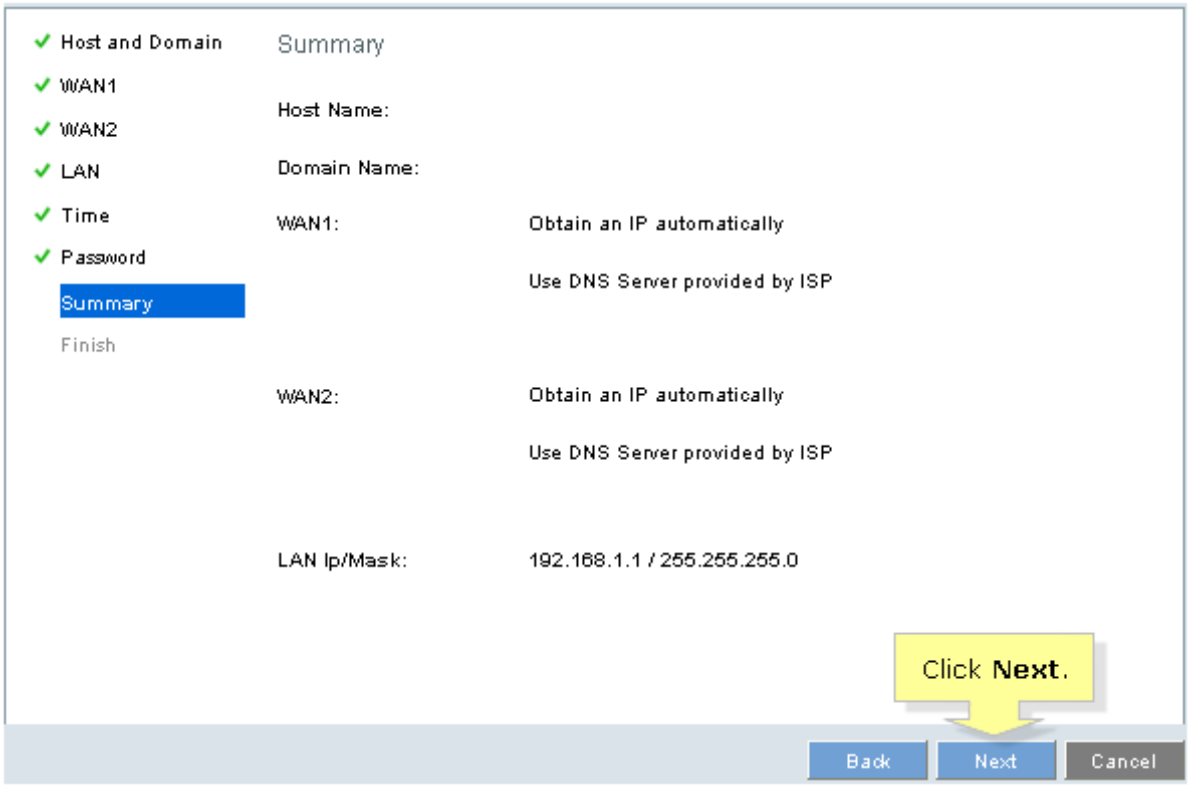


Step 8:
Enter your **Username** and **Password** for your router. It is recommended to change your router Username and Password according to your preference to avoid any compromise with regards to your network security. Then, click **Next**.



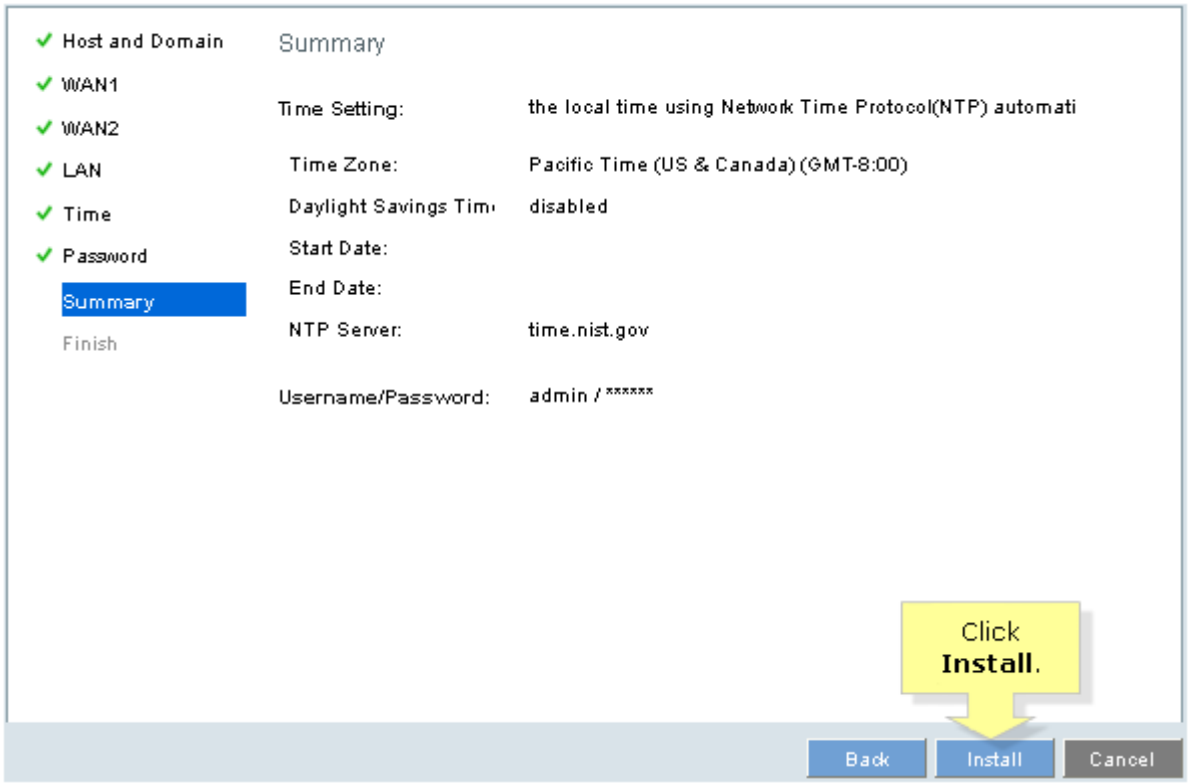
QUICK TIP: The **Password Strength Meter** describes how secure your password is. The higher the meter, the more secure it becomes. Use a combination of upper-case letters, lower-case letters and numbers to maximize the strength of your password.

Step 9:
This window will give you a summary of the settings that was set up for the router. Click **Next** to proceed.



Step 10:

Click **Install** to apply the settings to your VPN router.



Congratulations! You have now successfully set up your Linksys Gigabit VPN Router.

Configuring Internet Connection for the Linksys Gigabit VPN router using manual setup

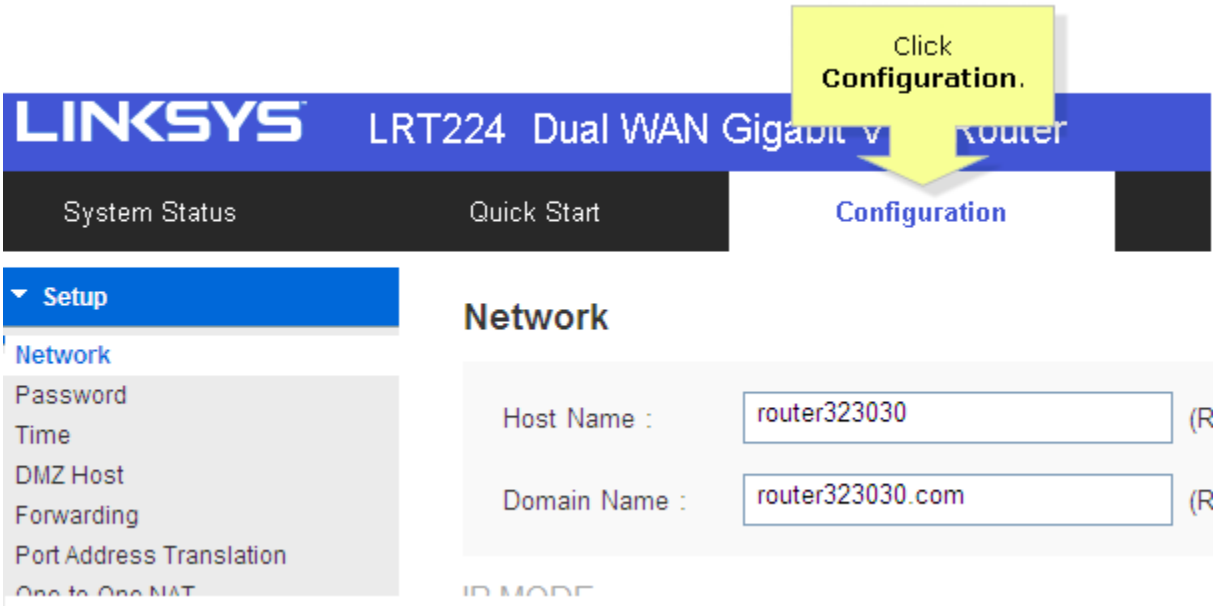
There are two ways to configure the router for Internet Connection:

- By using the Setup Wizard, for instructions click here.
- Through manual setup.

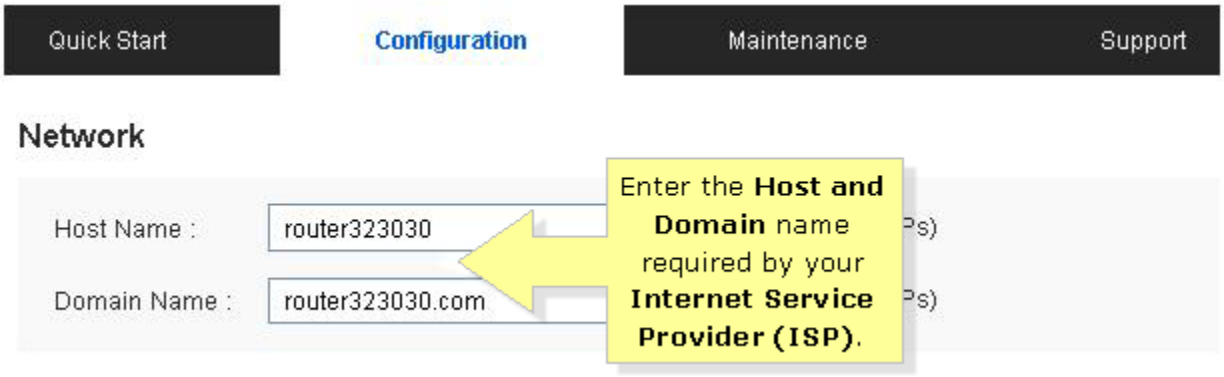
This article will guide you on how to configure the router for internet connection using manual set up.

Step 1:
Access the router's web-based setup page. For instructions, click here.

Step 2:
On the web-based setup page, click **Configuration** > **Setup** > **Network**.

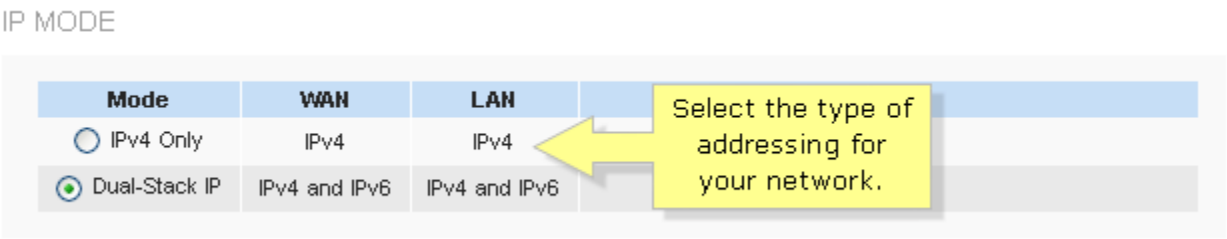


Step 3:
Enter the **Host Name** and **Domain Name** required by your **Internet Service Provider (ISP)**.

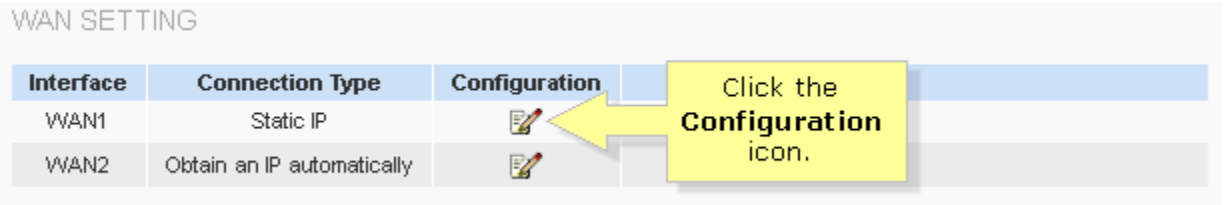


NOTE: If your ISP does not require a Host Name and a Domain Name, just leave the fields blank instead.

Step 4:
Select the type of addressing for your network under **IP MODE**. In this example, we will use the default **Dual-Stack IP** settings. Then, click the Save button.

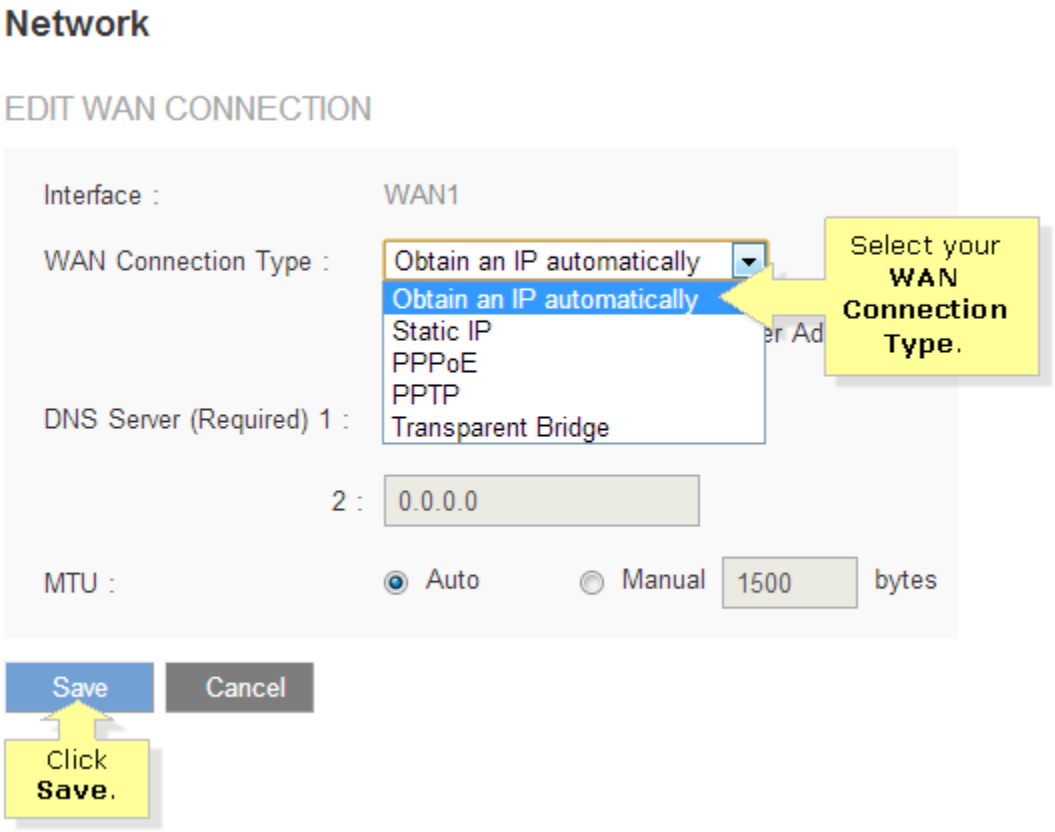


Step 5:
Under the **WAN SETTING** option click on the **Configuration** icon.

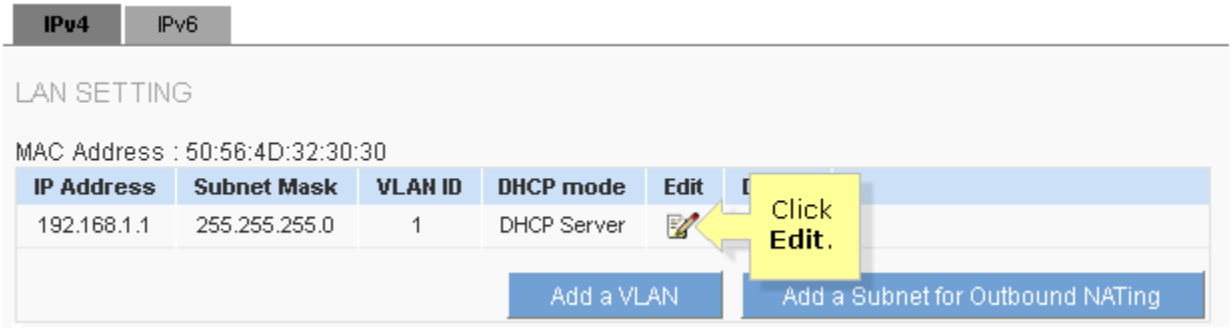


Step 6:
Select your **WAN Connection Type** then click **Save**.

NOTE: In this example, we used **Obtain an IP automatically** for the WAN Connection Type.



NOTE: If you need to change the LAN IP address of the router, under LAN Setting click on the **Edit** icon and make the necessary changes.



NOTE: By default, the settings under **LAN SETTING** section are the following:

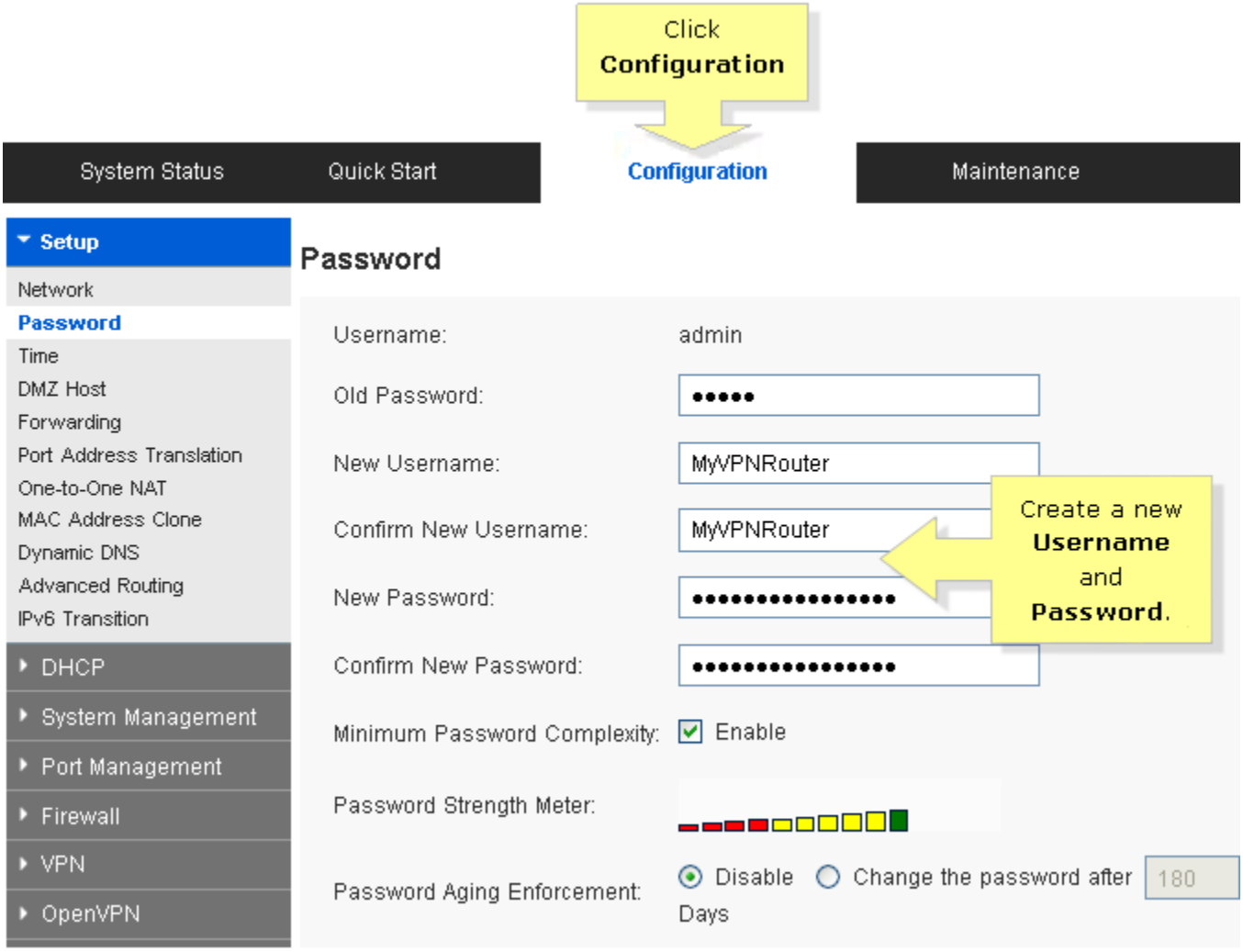
- **IP Address:** 192.168.1.1
- **Subnet Mask:** 255.255.255.0
- **VLAN ID:** 1

Step 7:

To change the router's **Password**. Click **Configuration > Setup > Password** to set the router

administrator **Username** and **Password**.

NOTE: It is strongly recommended to change the default Username and Password (admin/admin). This is to avoid any compromise with regards to your network security.

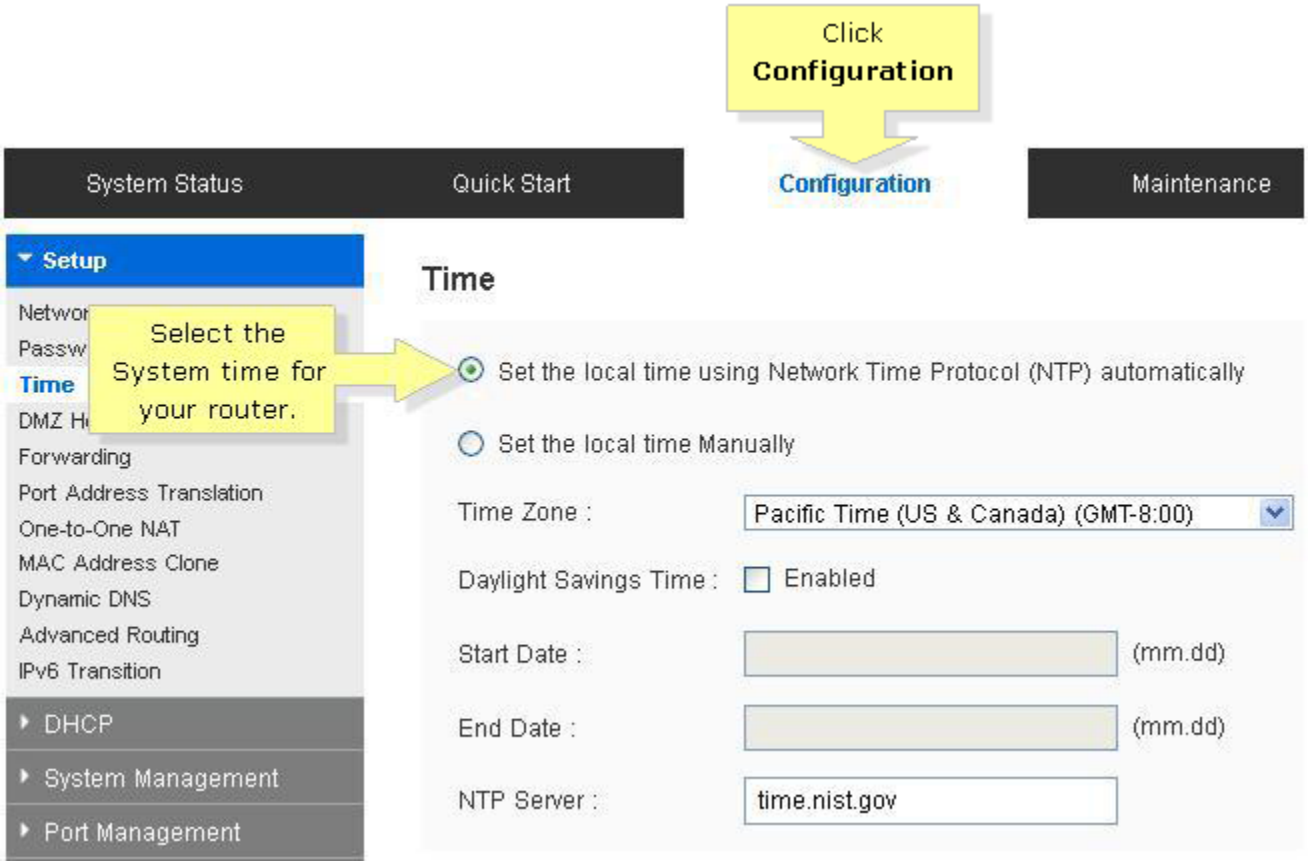


QUICK TIP: The **Password Strength Meter** describes how secure your password is. The higher the meter, the more secure it becomes. Use a combination of upper-case letters, lower-case letters and numbers to maximize the strength of your password.

Step 8:
Click **Save**.

Step 9:
To change the **Time** setting. Click **Configuration** > **Setup** > **Time** to configure the System time for the router depending on your preference.

NOTE: This option is used know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources.



Step 10:
Click **Save**.

Congratulations! You have now successfully set up your Linksys VPN router.

Configuring the LRT2x4 router and VPN Clients using OpenVPN

OpenVPN is an application that implements **Virtual Private Network (VPN)** for creating secure point-to-point connections, which allow OpenVPN clients such as laptops, smartphones, and tablets to connect using two-factor authentication. It supports SSL/TLS for key exchange as part of the authentication, in addition to username or password. It also has the capability to support up to **five (5)** OpenVPN Tunnels.

QUICK TIP: OpenVPN Tunnel can be either **full** or **split**. The **Full Tunnel** forces all traffic to be forwarded to the OpenVPN Server, whereas a **Split Tunnel** allows an OpenVPN client to access Internet-bound resources via local Internet Service Provider (ISP).

The steps below will show you how OpenVPN works on a local setup with your Linksys Gigabit VPN Router.

IMPORTANT: Make sure you have downloaded the OpenVPN Client. Click here to get one.

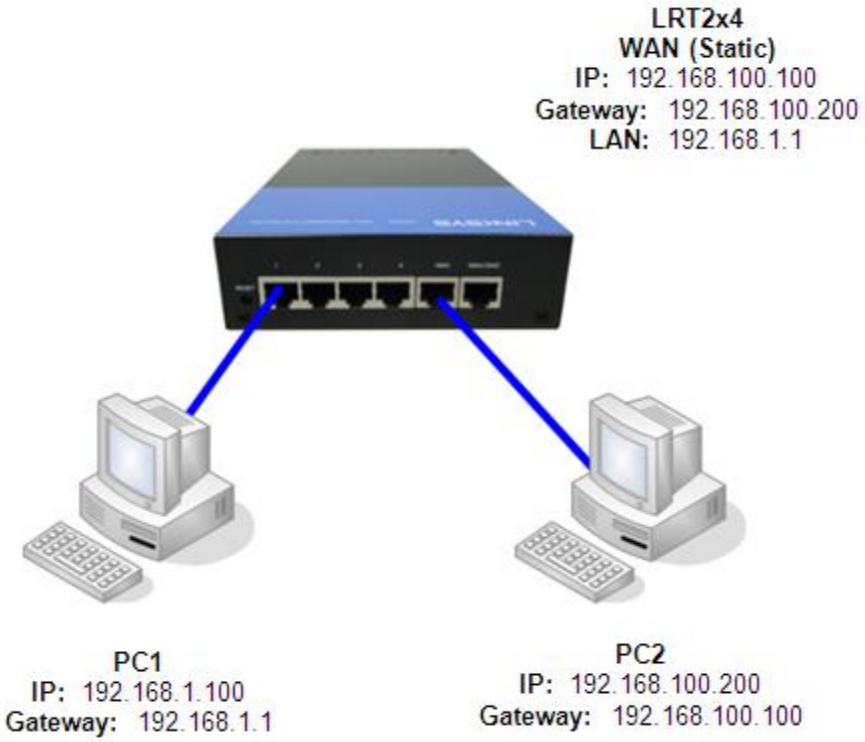
i. Setting up OpenVPN
ii. Installing OpenVPN Client
iii. Verifying IP addresses

Setting up OpenVPN

Step 1:
Reset the router to its factory default settings.

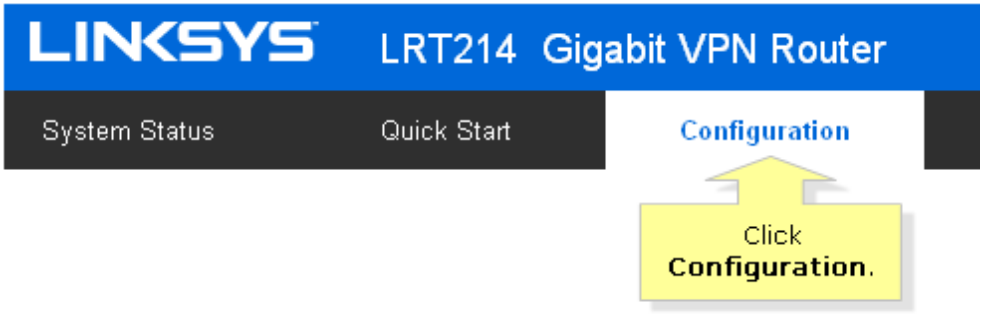
Step 2:
Connect all devices as the topology below where **PC1** is on the LAN side and **PC2** is on the WAN side.

NOTE: PC2 serves as an OpenVPN client that is trying to access PC1 in the LAN of LRT2x4.



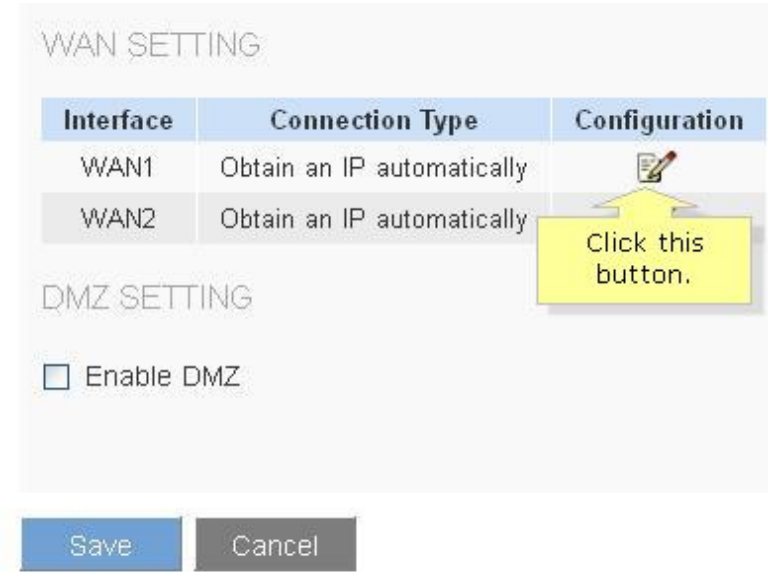
Step 3:
Access the router's web-based setup page. To learn how, click here.

Step 4:
Click **Configuration**.



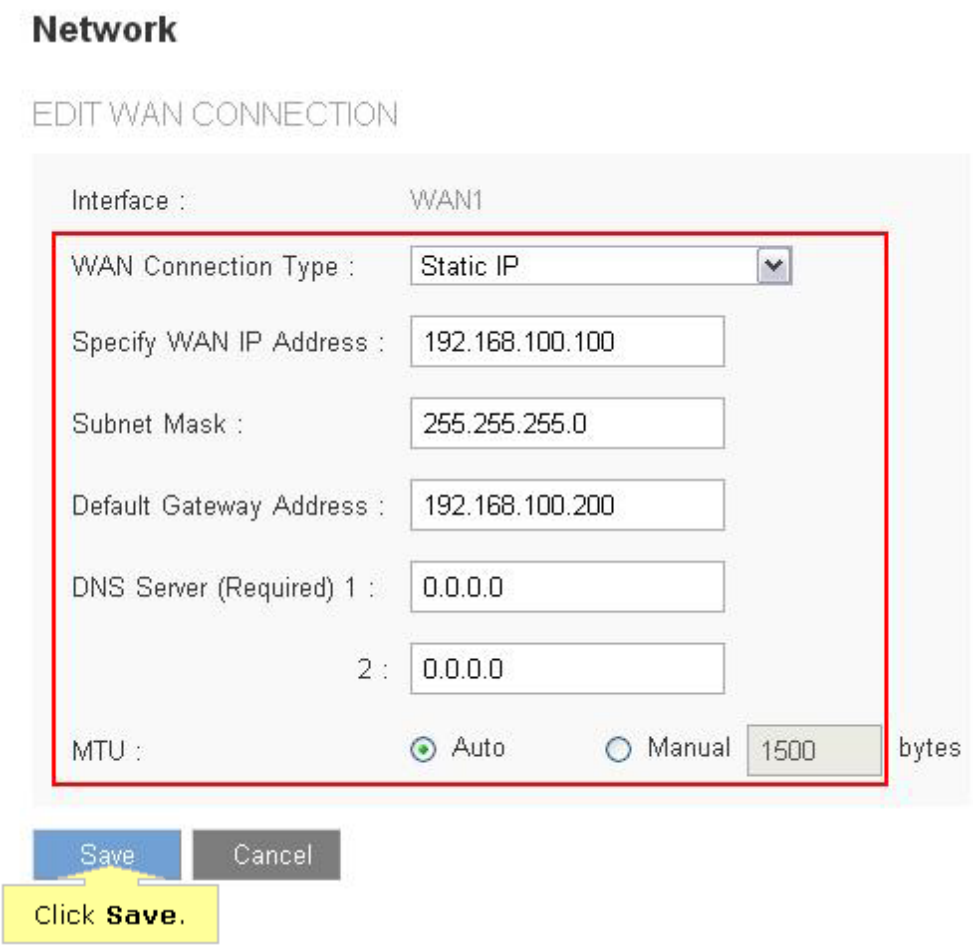
Step 5:

Click **Network**. Under the **WAN SETTING** section, click the configuration button of **WAN1**.

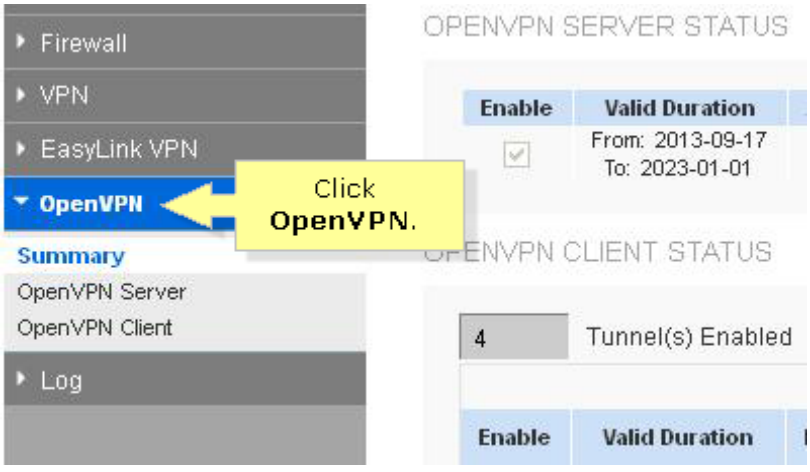


Step 6:

Configure the **WAN CONNECTION** according to the following information. Click **Save**.

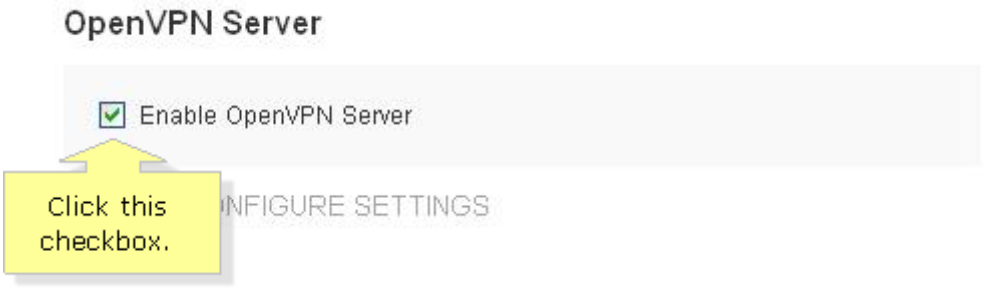


Step 7:
Click **OpenVPN**.

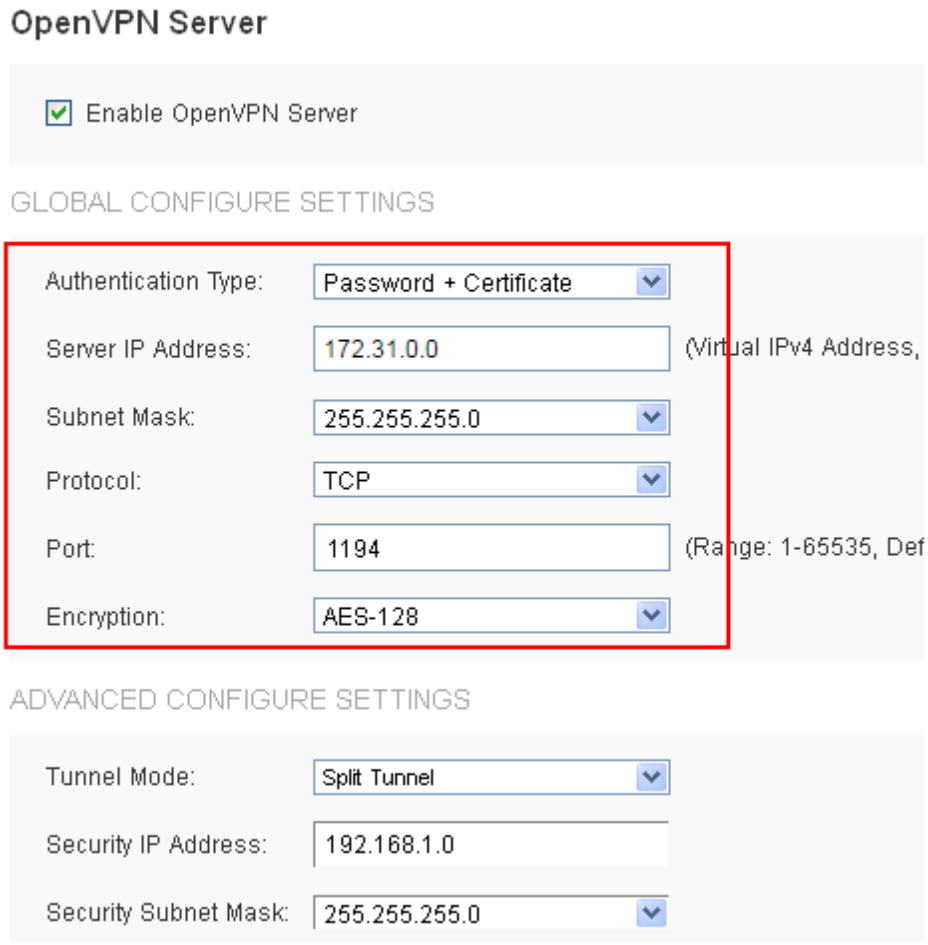


Step 8:
Under **OPENVPN SERVER STATUS** of the **Summary** page, click the **Config.** button.

Step 9:
Click the **Enable OpenVPN Server** checkbox.



Step 10:
Select **Password + Certificate** as the **Authentication Type**. Enter your configuration settings.

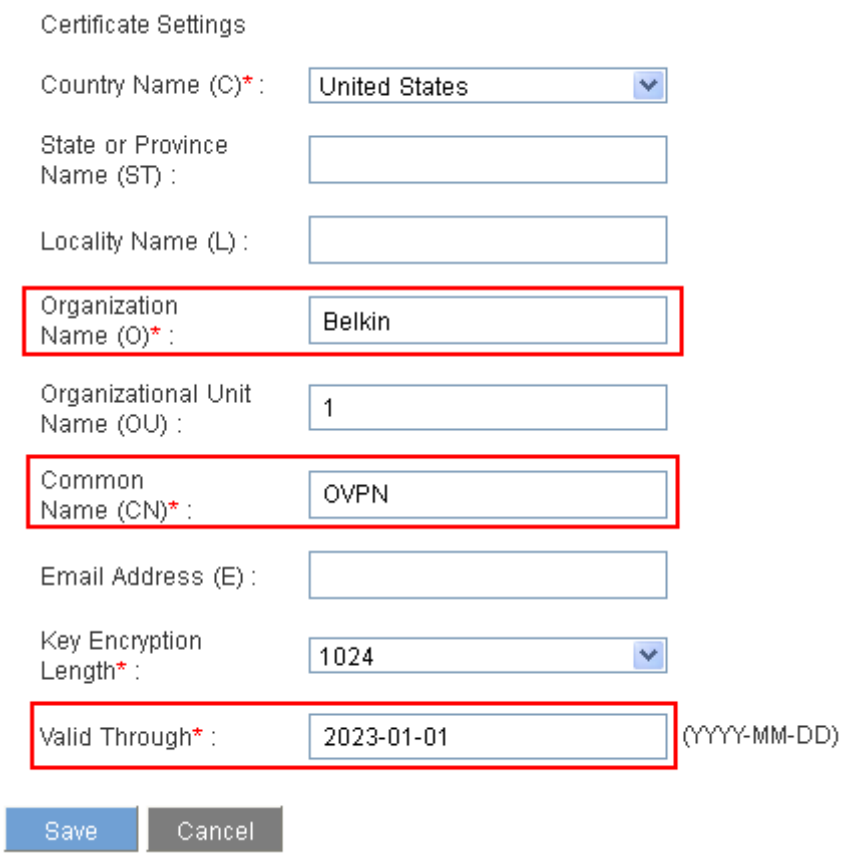


NOTE: This option is only applicable if you selected **Certificate** or **Password + Certificate** as the authentication type.

- **Authentication Type** – Select **Password**, **Certificate or Password + Certificate**. When you change authentication type, all client configurations and current used certificates will be cleaned up.
- **Server IP Address** – Enter a virtual IPv4 address for the server. The default IP address is **172.31.0.0**.
- **Subnet Mask** - Enter the IPv4 subnet mask.
- **Protocol** - Select either **TCP** or **UDP** protocol.
- **Port** - Configure OpenVPN server listen port. The the default value is **1194**.
- **Encryption** - Select encryption mode: **NULL**, **DES**, **3DES**, **AES-128**, **AES-192** or **AES-256**.

Step 11:
Scroll down to the **Certificate Settings** section, then enter the necessary information in the fields provided. Click **Save**.

QUICK TIP: Make sure the following fields are filled out: **Organization Name**, **Common Name**, and **Valid Through**.

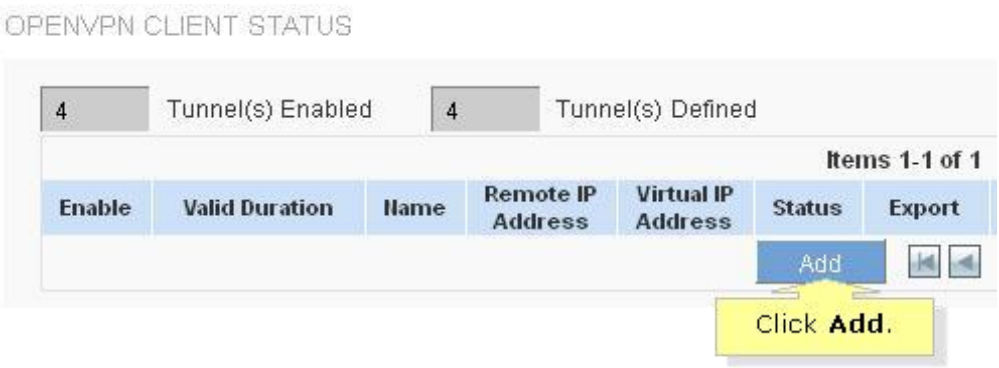


NOTE: This option is only applicable if you selected **Certificate** or **Password + Certificate** as authentication type.

- **Country Name (C)*** - Select a country for server certificate.
- **State or Province Name (ST)** - Enter the state or province name.
- **Locality Name (L)** - Enter locality name.
- **Organization Name (O)*** - Enter the organization name.
- **Common Name (CN)*** - Enter a common name for the certificate.
- **Email Address (E)** - Enter an Email address.
- **Key Encryption Length*** - Select either 1024 or 2048 for the key encryption length.
- **Valid Through*** - Enter a date for when the certificate should expire. The start date will be the date the certificate was created.

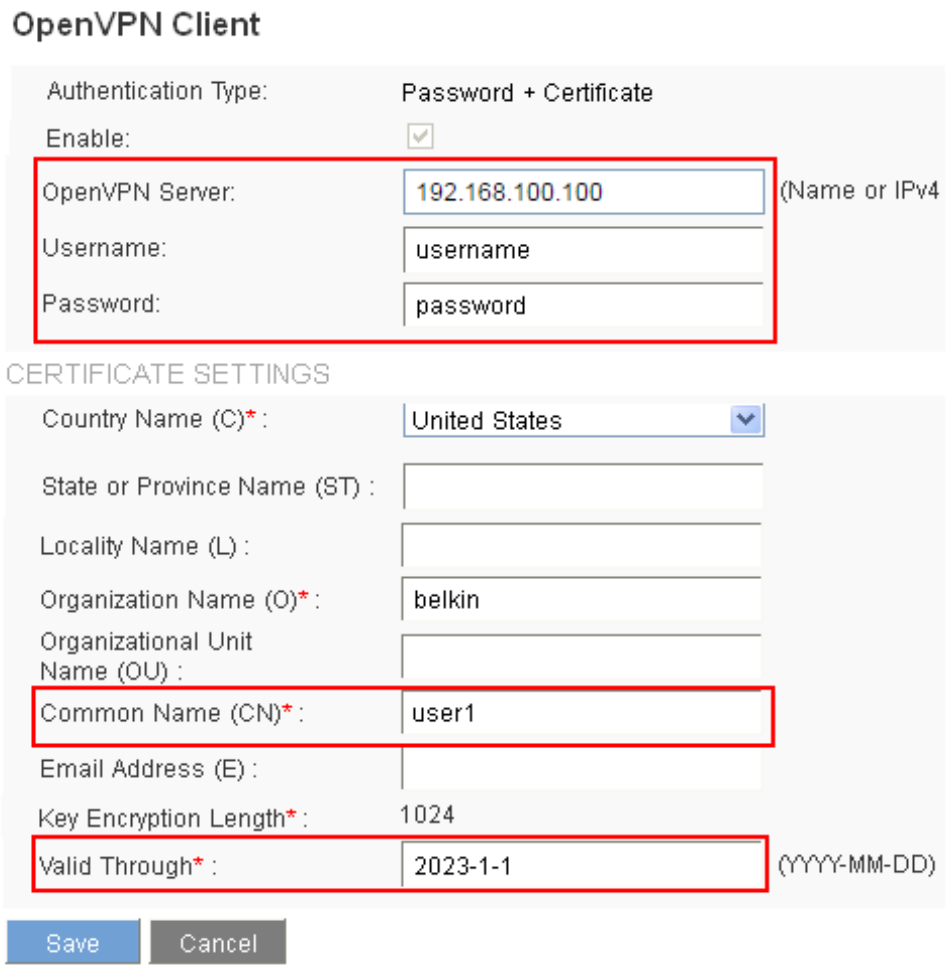
Step 12:

Under **OPENVPN CLIENT STATUS** of the Summary page, click the **Add** button.



Step 13:
Enter the necessary information in the fields provided. Click **Save**.

QUICK TIP: Make sure the following fields are filled: **OpenVPN Server**, **Username**, **Password**, **Common Name**, and **Valid Through**.



- **Authentication Type** - Displays current authentication type.
- **Enable** - Indicates whether this client is enabled or not.

- **OpenVPN Server** – Enter OpenVPN server IPv4 address or DNS resolved name. This is the Router's WAN IP address or FQDN name.

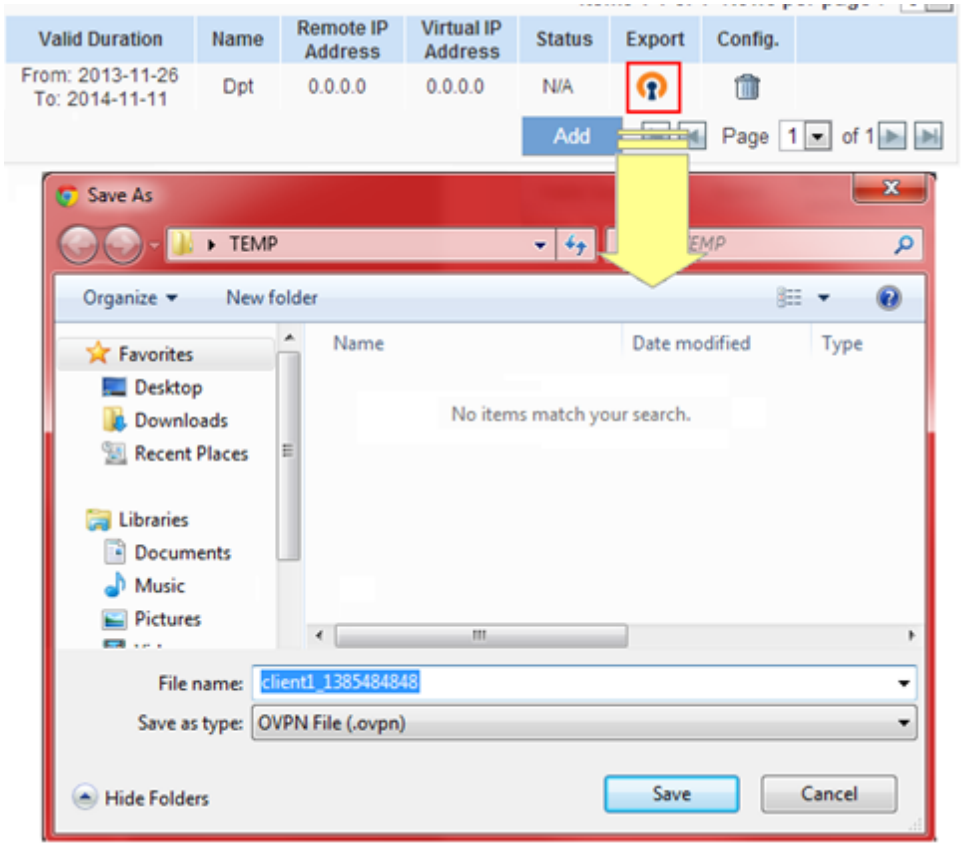
NOTE: The OpenVPN Server of LRT2x4 needs a virtual IPv4 address, which has a default **172.31.0.0** with subnet mask of **255.255.255.0**.

- **Username** – Enter a username for the OpenVPN client. This option is only available if Password or Password + Certificate is selected under the authentication type.
- **Password** – Enter a password for the OpenVPN client. This option is only available if Password or Password + Certificate selected under the authentication type.

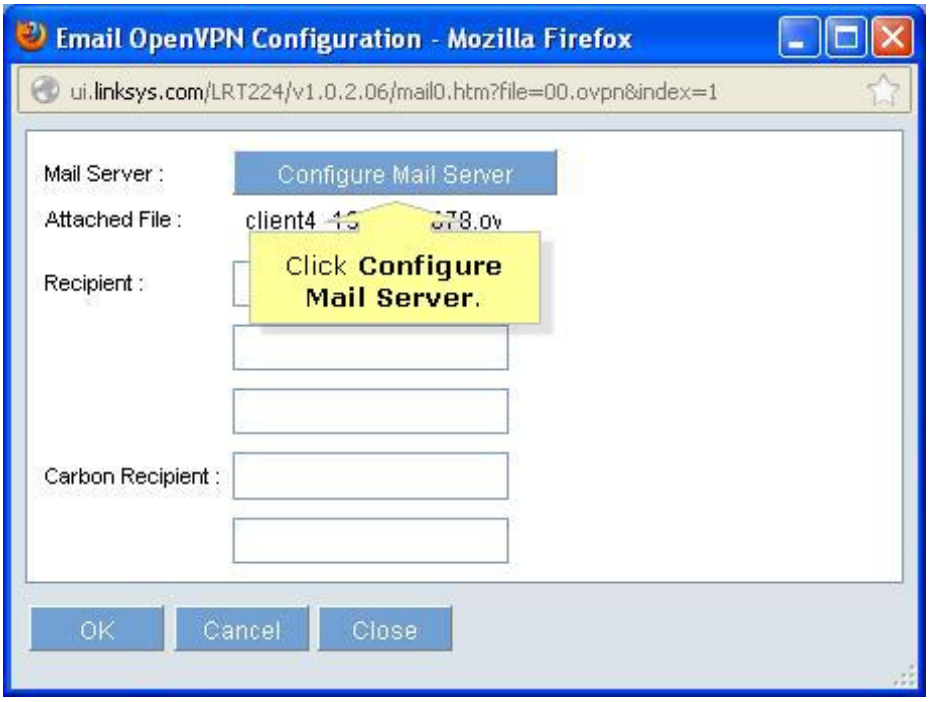
Step 14:

Under **OPENVPN CLIENT STATUS** section of the **Summary** page, click the **Export** or **Email** button.

- **Export** – Export the OpenVPN Client configuration file, you don't need to do any configuration for the OpenVPN client.

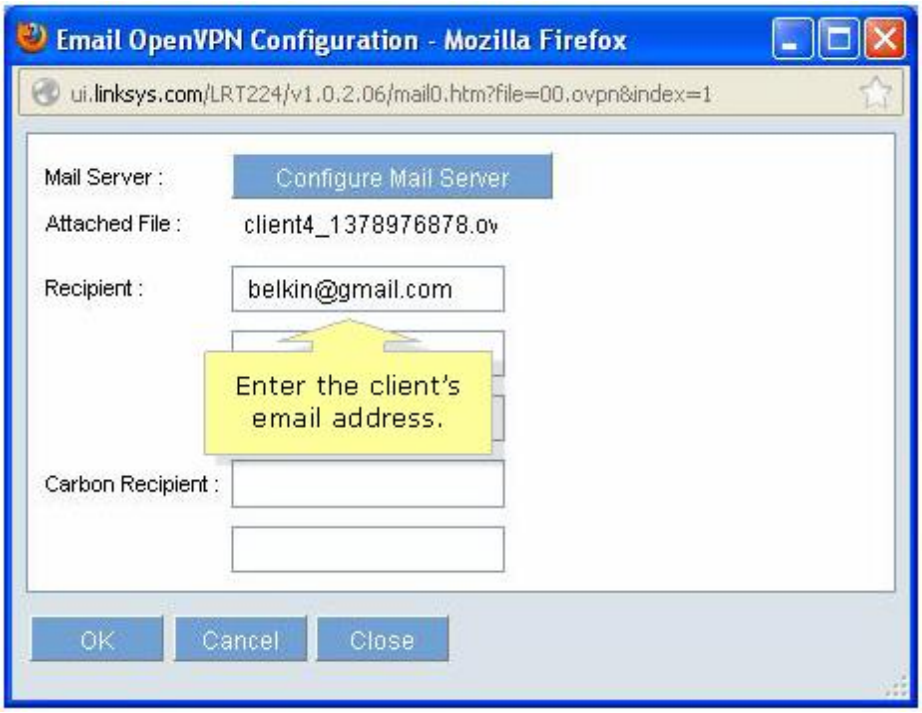


- **Email** – The OpenVPN Client configuration file can be sent through Email. Configure the Outgoing Mail Server to proceed.

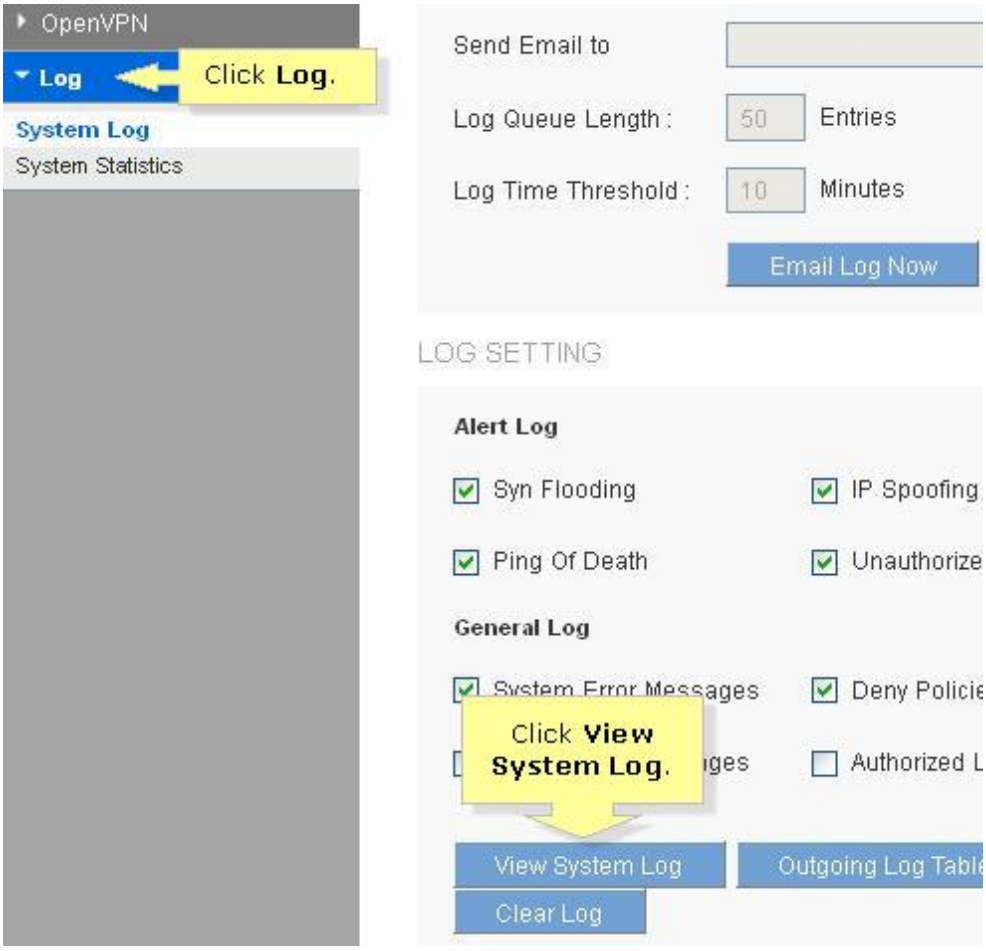


For instance, use the Google SMTP server for sending the mail. The **Sender** will be the email address of sender shown on the email. The **Mail Server** would be the name of Google SMTP server. Google SMTP server is with SSL Authentication type and 465 SMTP Port. **Username** and **Password** are the sender's login email account information. Save the provided details.

Once you're finished configuring the **MAIL SERVER**, enter the client's email address in the Recipient or Carbon Recipient field. The email recipient can download the OVPN file from the email.



To check if the email has been successfully sent, you can check it under **Log > System Log > View System Log**.



If the mail has been successfully sent, you will see a message similar to the message below.

Time	Event-Type	Message
Feb 7 02:03:13 2014	VPN Log	OPEN VPN: client1_1389947551.ovpn sent successfully

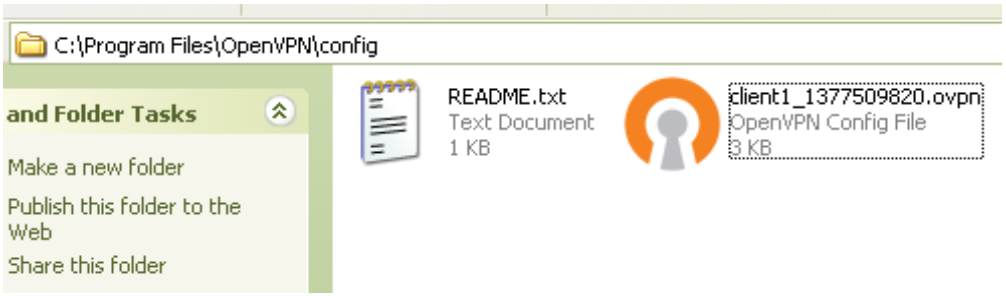
Installing OpenVPN Client

Step 1:
Install the OpenVPN Client on **PC2**. Click here to download the installer.

Step 2:
Go to **Start > All Programs > OpenVPN > Shortcuts > OpenVPN configuration file directory**. Open the **OpenVPN client configuration** folder.

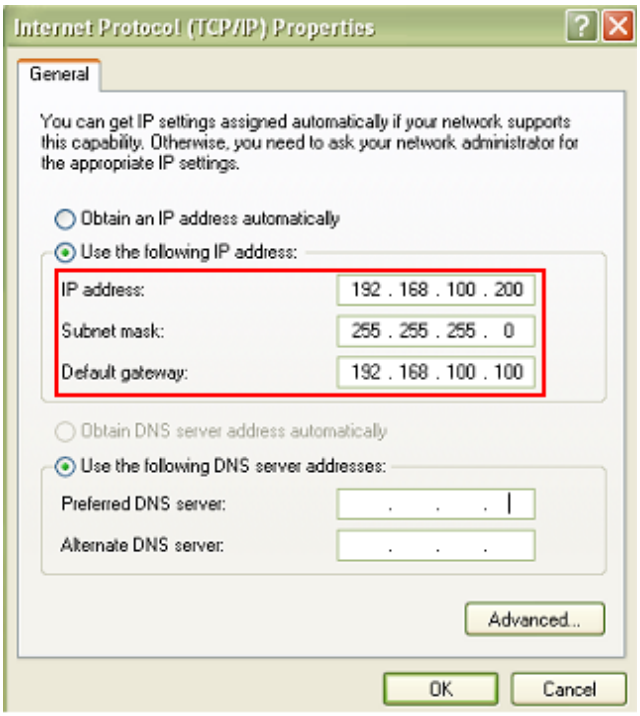
Step 3:

Copy and paste the OpenVPN client configuration file in the folder.



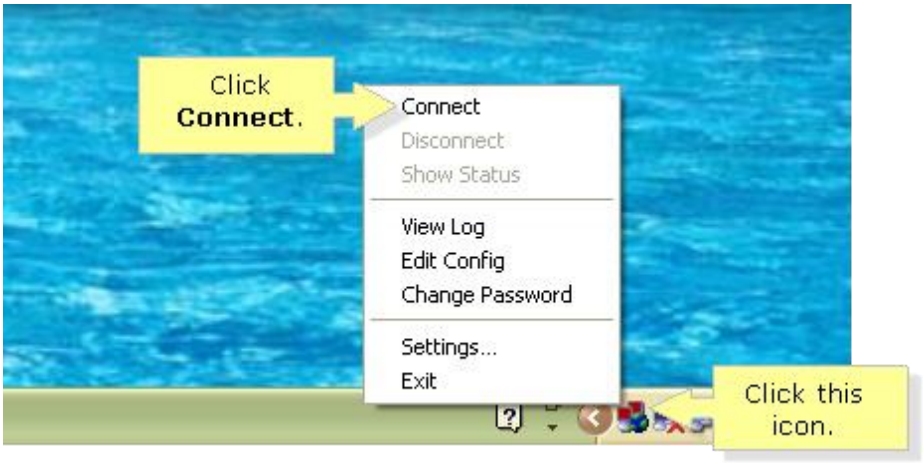
Step 4:

Make sure the IP addresses configuration is correct on **PC2**.



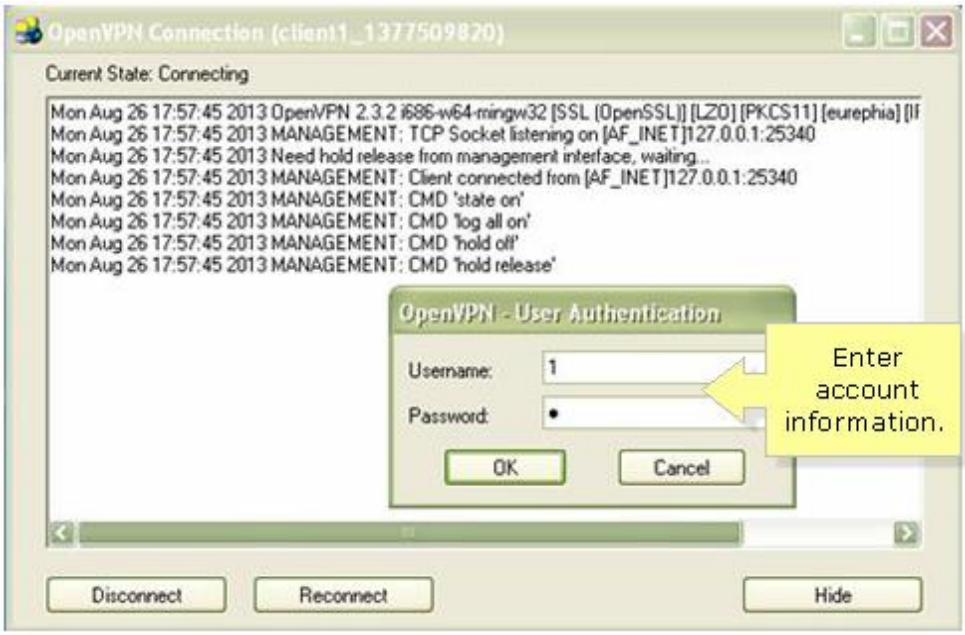
Step 5:

Click the OpenVPN client icon then click **Connect**. The OpenVPN client will auto connect to the OpenVPN server without extra settings.



If all the configurations and connection are OK, the OpenVPN client will prompt for User Authentication.

Step 6:
Enter the account information provided from Step 13 above. Click **OK**.

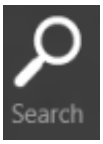


If the username and password are correct, the OpenVPN will be established successfully.

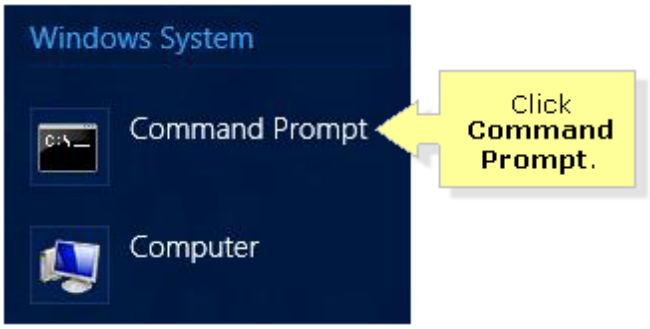
Verifying IP addresses

Verify that PC2 got the Virtual IPv4 address.

Step 1:

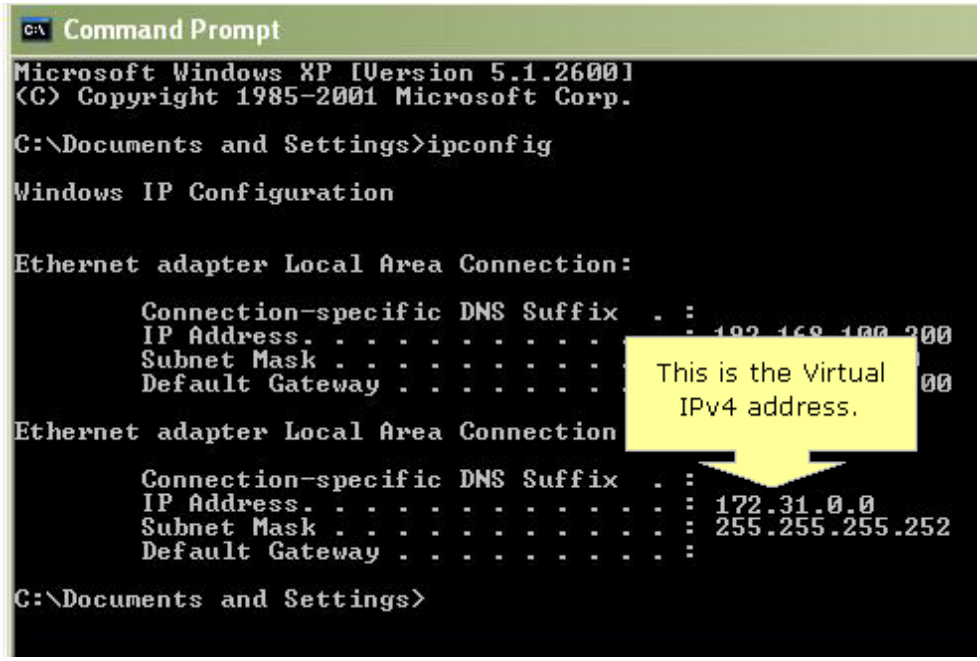
Click the 

icon in the Charms bar. Enter "command prompt" in the search field and then, click **Command Prompt** from the search results.



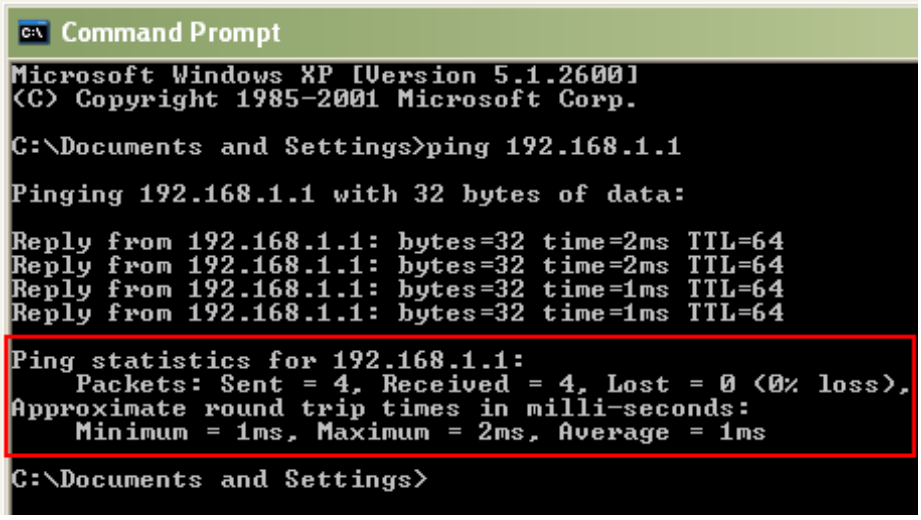
Step 2:

Type "ipconfig" then press **Enter**.



Step 3:

Make sure PC2 can PING the LAN gateway. Type "ping 192.168.1.1" then press **Enter**.



Once the local setup passes the testing, you can now plug the LRT2x4 into the modem and let OpenVPN client connect from the Internet. You may now also connect your laptops, smartphones and tablets to access the VPN connection. To know how to configure OpenVPN on an iOS device, click here. For Android™ devices, click here.

Configuring a Gateway-To-Gateway VPN tunnel between two Linksys Business Gigabit VPN Routers

A **Gateway-To-Gateway VPN** is used to form a secure connection between two networks over the Internet. The secure connection, also known as a VPN tunnel, allows computers in the two networks to be accessible to each other, while keeping the data being exchanged from potential hackers in the Internet.

Configuration must be done on both routers to enable a gateway-to-gateway VPN. The configurations done in the **Local Group Setup** and **Remote Group Setup** sections should be reversed between the two routers so that the local group of one is the remote group of the other.

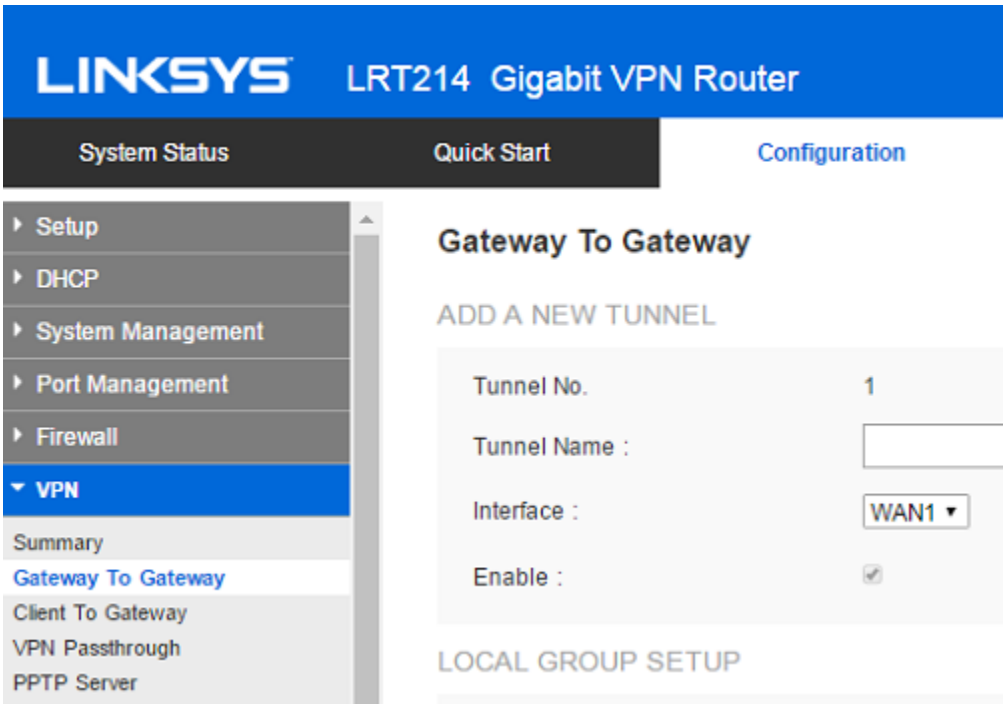
NOTE: This configuration is ONLY applicable to the Linksys LRT214 and LRT224 Business Gigabit VPN Routers. It can be in the following setup:

- **LRT214 to LRT214**
- **LRT224 to LRT224**
- **LRT214 to LRT224**

Below are the steps for configuring a gateway-to-gateway VPN tunnel where one router has a **static WAN IP** and the other has a **dynamic IP** with a DDNS domain name.

Step 1:

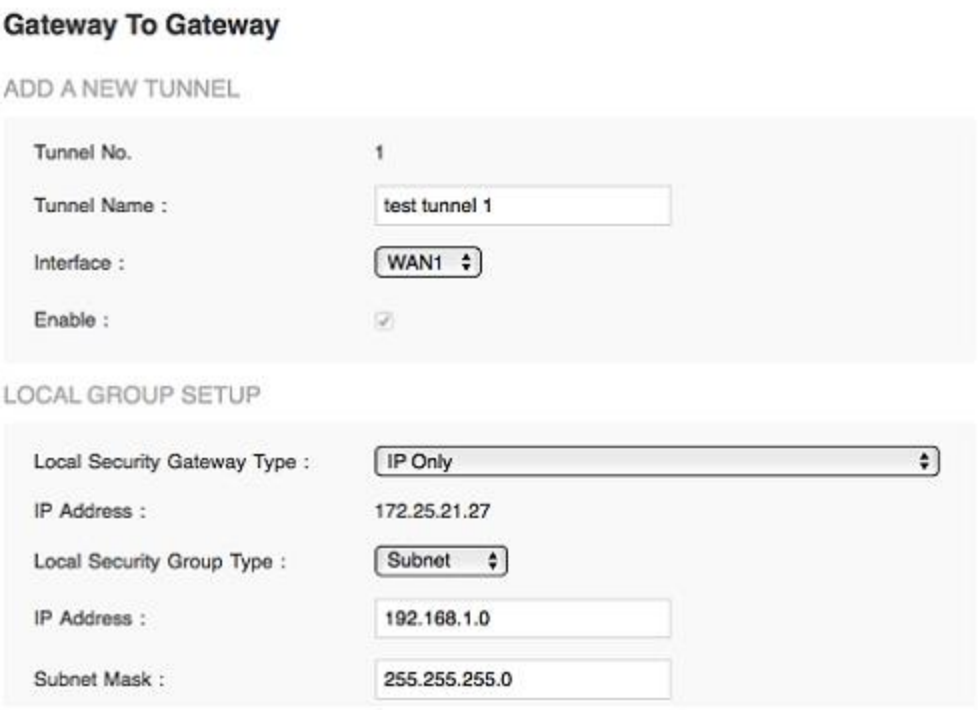
Log in to the web administrative interface of the router with a static WAN IP and go to **Configuration > VPN > Gateway To Gateway**. When the **Gateway To Gateway** page opens, enter a name for the tunnel. The name is optional but will make it easier to identify a tunnel if the router will be configured with multiple tunnels later on.



Step 2:

Configure **LOCAL GROUP SETUP**. Since the router has a static WAN IP in this example, select **IP Only** for the **Local Security Gateway Type**. If the WAN port is up and running, the WAN IP should automatically display in the **IP Address** field. The rest of the fields can be left as default.

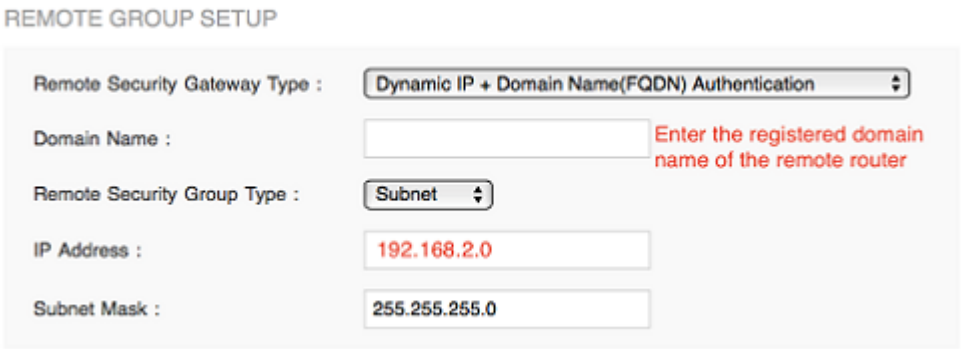
NOTE: In this example, the Tunnel Name **test tunnel 1** is used.



Step 3:

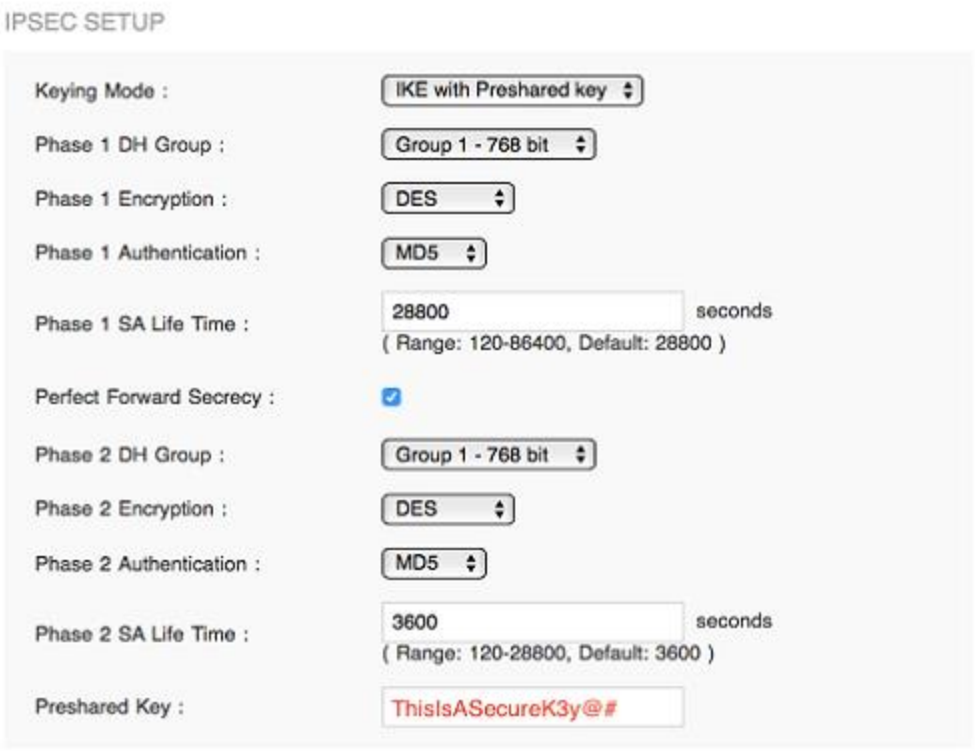
Configure the **REMOTE GROUP SETUP**. Since the remote router in this example has a dynamic IP and a DDNS domain name, select **Dynamic IP + Domain Name(FQDN) Authentication**. Enter the registered domain name of the remote router in the **Domain Name** field. And then, enter the network address of the remote network in the IP Address field. In this example, the remote router's LAN IP is 192.168.2.0 and the subnet mask is 255.255.255.0.

NOTE: If the domain name is entered incorrectly, the tunnel will NOT be able to connect successfully.



Step 4:

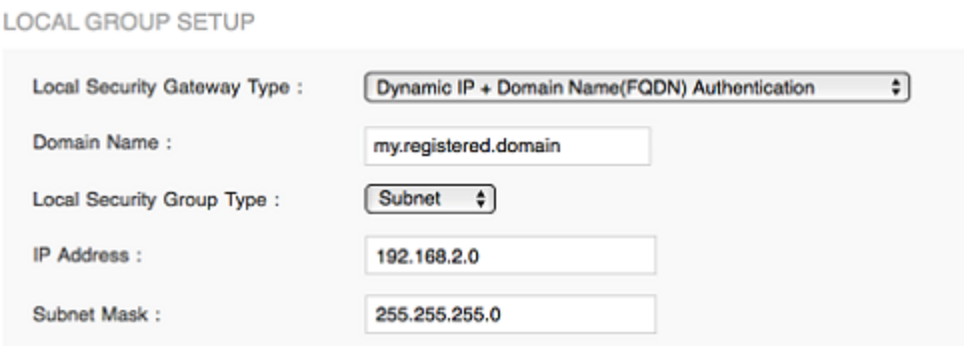
Configure the **IPSEC SETUP**. In this section, the only mandatory field for configuration is a **Preshared Key**, which is a shared secret between the two sides of the VPN tunnel. Therefore, the preshared key needs to be copied into the other router's tunnel configuration.



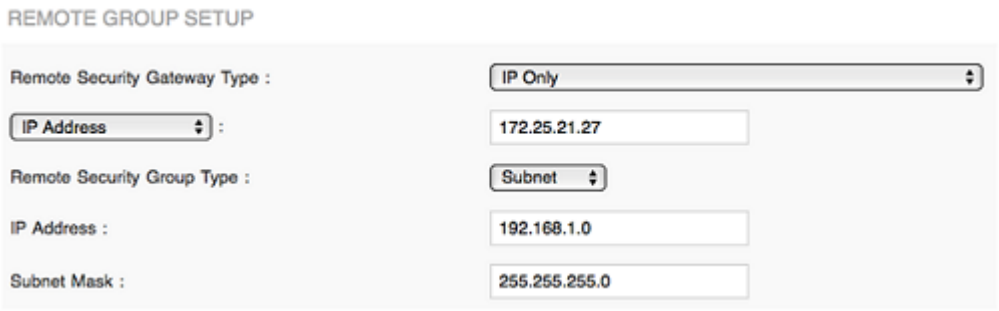
Step 5:
Click the **Save** button, then go to the **VPN > Summary** page to see the tunnel status. At this point, the status is **waiting for connection**, since the other router has not been configured yet.

Step 6:
Log in to the web administrative interface of the router with a dynamic IP and DDNS domain name. On the **Configuration** page, choose **VPN > Gateway To Gateway**. When the **Gateway To Gateway** page opens, enter a name for the tunnel. The name is optional as previously stated.

Step 7:
Configure the **LOCAL GROUP SETUP**. Select **Dynamic IP + Domain Name(FQDN) Authentication** for the **Local Security Gateway Type**. Enter the registered domain name into the **Domain Name** field.



Step 8:
Configure the **REMOTE GROUP SETUP**. Since the first router in this example has a static IP (172.25.21.27), select **IP Only** for the **Remote Security Gateway Type** and enter its static IP Address into the **IP Address** field. The **Remote Security Group Type** can use the default (**Subnet**), and enter the Subnet Address of the first router (192.168.1.0) into the **IP Address** field.



Step 9:
Configure **IPSEC SETUP**. Enter the identical preshared key into the **Preshared Key** field.

Step 10:
Click the **Save** button. The tunnel is ready for testing.

Step 11:
Go to **the VPN > Summary** page to check the tunnel status.

You should now have configured the Gateway-To-Gateway VPN tunnel.