

EnGenius®

ESR300H / ESR150H

11N X-TRA RANGE Wireless Router

V1.1



Table of Contents

1. Product Overview	5
1.1. Package Contents	6
1.2. Product Layout.....	6
1.3. Wall Mounting	8
2. Installation	8
2.1. System Requirements.....	8
2.2. Setup Notes	8
3. Getting Started.....	9
3.1. Using your CD.....	9
3.2. Setup your network cables	10
3.3. Login your Router	12
3.4. Configuring your Internet	13
Dynamic IP Address (DHCP)	14
Static IP	14
Point-to-Point Protocol over Ethernet (PPPoE)	14
Layer 2 Tunneling Protocol (L2TP).....	15
4. Parental Control.....	18
5. Advanced Networking Setting	22
System	22
6. Internet	30
7. Wireless LAN Setup	40
Wireless > Basic	40
Wireless > Advanced	41

Wireless > Security.....	43
Wireless > WPS.....	47
Wireless > Client List.....	48
8. Parental Control Section.....	49
Parental Control > Wizard.....	49
Parental Control > Web Monitor.....	52
9. Firewall Section.....	53
Firewall > Basic.....	53
Firewall > Advanced.....	54
Firewall > DMZ (Demilitarized Zone).....	55
Firewall > DoS (Denial of Service).....	56
Firewall > ACL.....	57
10. VPN (Virtual Private Network) Section.....	58
VPN > Status.....	58
11. Advanced Section.....	74
Advanced > NAT (Network Address Translation).....	74
Advanced > Port Mapping.....	75
Advanced > Port Forwarding.....	76
Advanced > Port Triggering (Special Application).....	77
Advanced > ALG (Application Layer Gateway).....	78
Advanced > UPnP (Universal Plug and Play).....	79
Advanced > IGMP (Internet Group Multicast Protocol).....	80
Advanced > QoS (Quality of Service).....	81
Advanced > Routing.....	85

Advanced > WOL (Wake on LAN)	87
12. Tools Section	88
Tools > Admin	88
Tools > Time	90
Tools > DDNS (Dynamic DNS)	91
Tools > Diagnosis	92
Tools > Firmware	93
Tools > Back-Up	94
Tools > Reset	95
Appendix A – FCC Interference Statement	96
Appendix B – Industry Canada statement	98

1. Product Overview

Thank you for purchasing the ESR300H High Power Wireless N Router from EnGenius Technologies.

By applying the latest in 802.11n technology, the ESR300H provides users with high speed (up to 300Mbps) to stream HD multimedia, play games online, or download large files. With 200mW of high output power, it has up to twice the range compared to other wireless routers and has better coverage to reach what would be normally weak or dead spots.

The **ESR300H** also has all the standard security features contained in routers today. Multiple SSIDs, Firewall Mapping, DMZ, IP Filtering, ICMP Blocking, and VPN Pass Through are all standard features within the **ESR300H**. Content filtering is easily managed by basing it on MAC Addresses, URLs, or other such features. These features are easily accessed and set up in the easy to use User Interface.

With the User Friendly Setup Wizard, setting up internet connectivity, Wireless LAN, and security is a breeze.

Features

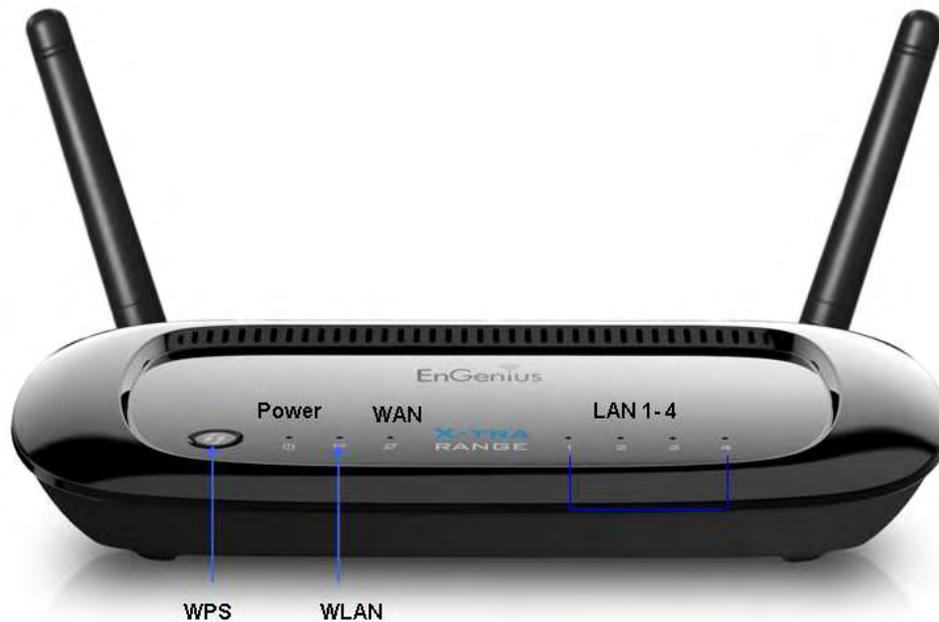
- 300Mbps High Speed Wireless Networking: The ESR300H provides up to 300Mbps to allow you to watch online multimedia such as Netflix®, play games online, music, and download large files.
- 200mW High Output Power: Extend your home network area with longer wireless range and better coverage.
- WEP/WPA/WP2 Security: Secure your wireless network to prevent unauthorized access
- Advanced Firewall: Provides advanced SPI firewall, Denial of Service (DoS) attack blocking, MAC filtering, and URL filtering to secure high-speed network connections.
- Up to 4 SSIDs to highly secure your wireless network while sharing it to different groups.
- QoS to prioritize the multimedia streaming of data.
- Parental Control: Enable centralized control to restrict some Internet access for different computers on the network

- VPN: Support up to 5 VPN tunnels to better secure your network from remote access
- Easy Smart Wizard Setup

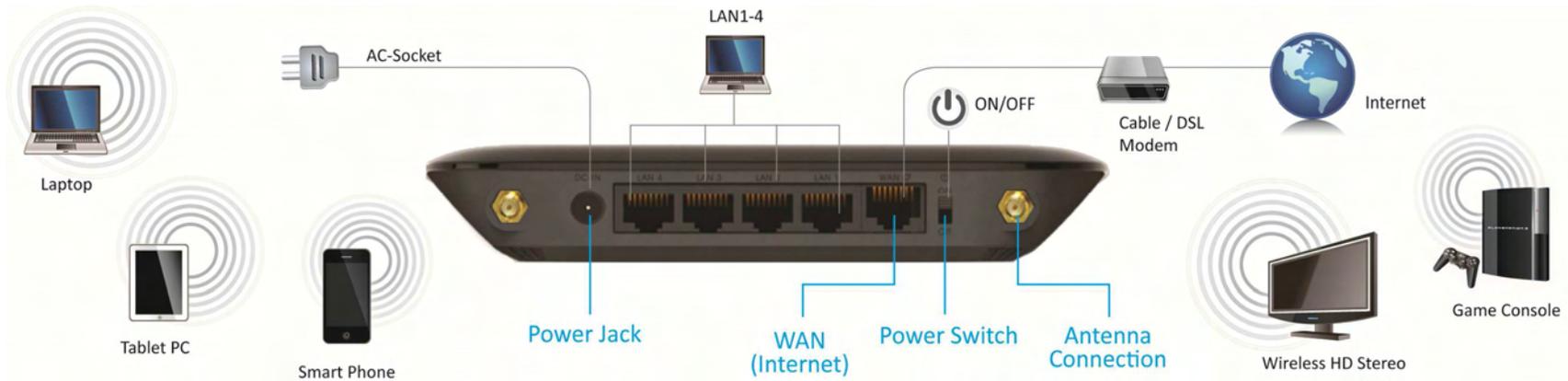
1.1. Package Contents

1. ESR300H Wireless N Router
2. 2dBi Antenna
3. ESR300H Quick Installation Guide
4. 12V/1A Power Adaptor
5. Ethernet Cable
6. ESR300H User CD (with User Manual)
7. Technical Supporting Card

1.2. Product Layout



Front Panel Components	Description
Power LED	This LED goes ON when the power is being supplied to the router.
WLAN LED	This LED goes ON when the RF (wireless LAN) feature is enabled.
WAN LED	This LED goes ON when an Ethernet cable is connected to the router's WAN port.
LAN (1 – 4) LEDs	These LEDs go ON when an Ethernet cable is connected to the corresponding router LAN port.
WPS Button	Press 0 to 5 seconds to activate the router's Wi-Fi Protected Setup (WPS) feature. Press 10 to 15 seconds to reboot the router. Press longer than 15 seconds to reset the router to the factory default settings.



Back Panel Components	Description
LAN Ports (1 – 4)	Use an Ethernet cable to connect each port to a computer on your Local Area Network (LAN).
WAN /Internet Port	Use an Ethernet cable to connect this port to a cable or DSL modem.
DC-Jack (POWER)	Connect the power adapter to this connector.
Power Switch	Turns the router on or off.
Antenna Connector	Interface for the antennas.

1.3. Wall Mounting

Mounting the **ESR300H** to a wall will allow the wireless range to be optimized. To mount the device in the wall, measure the distance of the mounting holes of the **ESR300H** and drill the appropriate holes on the wall location. Once the nails are secure, firmly lock the mounts onto the **ESR300H**.

2. Installation

2.1. System Requirements

To begin installing the **ESR300H**, you need the following:

- Computer (Windows, Linux, OSX Operating System)
- CD-ROM*
- Web Browser (Internet Explorer, FireFox, Chrome, Safari)
- Network Interface Card with an open RJ-45 Ethernet Port
- WiFi Card or USB WiFi Dongle (802.11 B/G/N)**
- External xDSL (ADSL) or Cable Modem with an open RJ-45 Ethernet Port
- CAT5 Ethernet Cables

Windows Only: Using **ESR300H Setup CD*

***Optional*

2.2. Setup Notes

When considering the placement of the **ESR300H** remember the following:

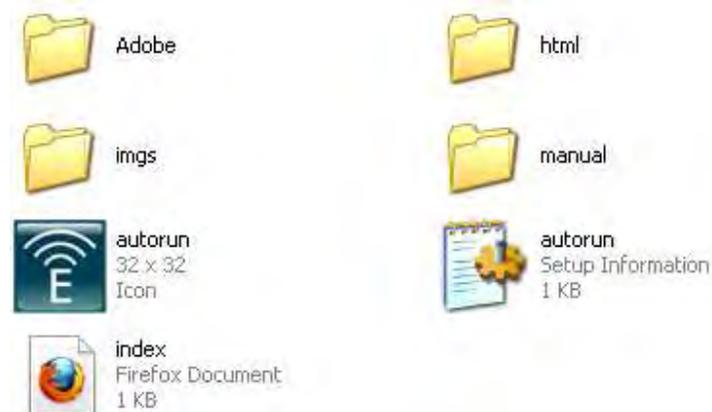
- The **ESR300H** must be close to the DSL or Cable Modem and a Power Source. Initially, it needs to be closed to the computer that is used to set up the **ESR300H**.
- Placing the **ESR300H** in the center of the office space will result in the most optimal wireless range.
- The higher the placement of the **ESR300H**, the better wireless range it will have.
- Other electronic devices can cause interference, which will cause the wireless range of the **ESR300H** to diminish.

3. Getting Started

3.1. Using your CD

Before getting started, please power off your cable modem or the DSL.

1. Insert the ESR300H Installation CD into your CD-ROM drive. The CD should automatically start in a few seconds. If you are not using **Windows (Internet Explorer)**, please browse the CD and open the file names **index.html (it can be found from the "html" folder)** to start.



2. Click **Quick Start**. The wizard will guide you through setting up your ESR300H.

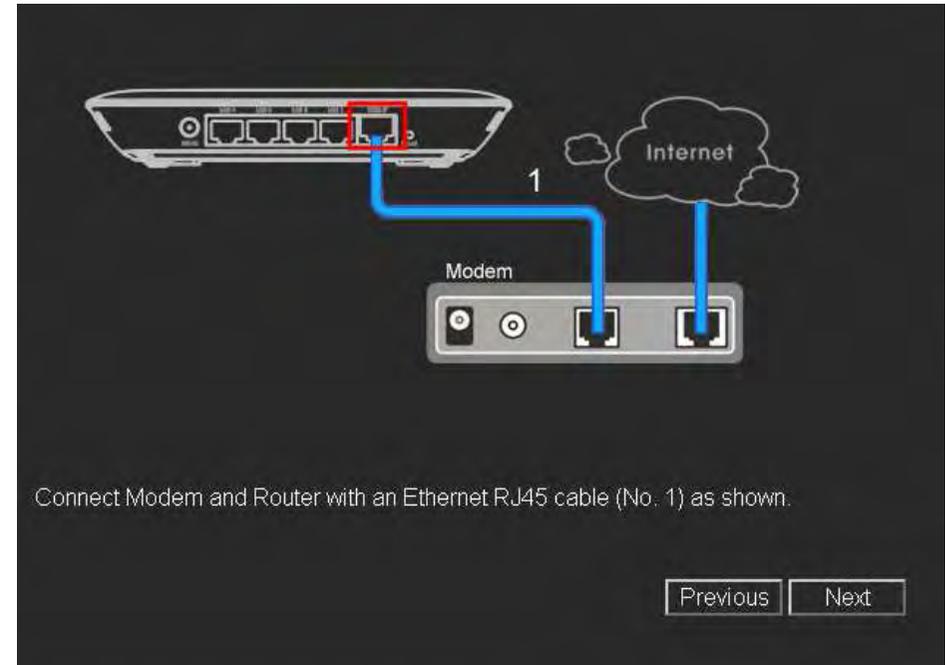


3.2. Setup your network cables

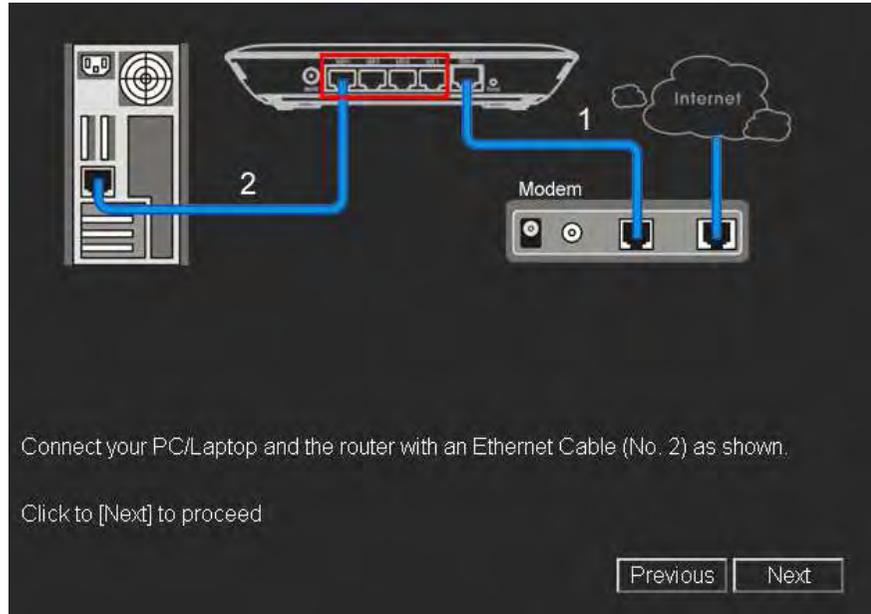
1. Power on ESR300H.



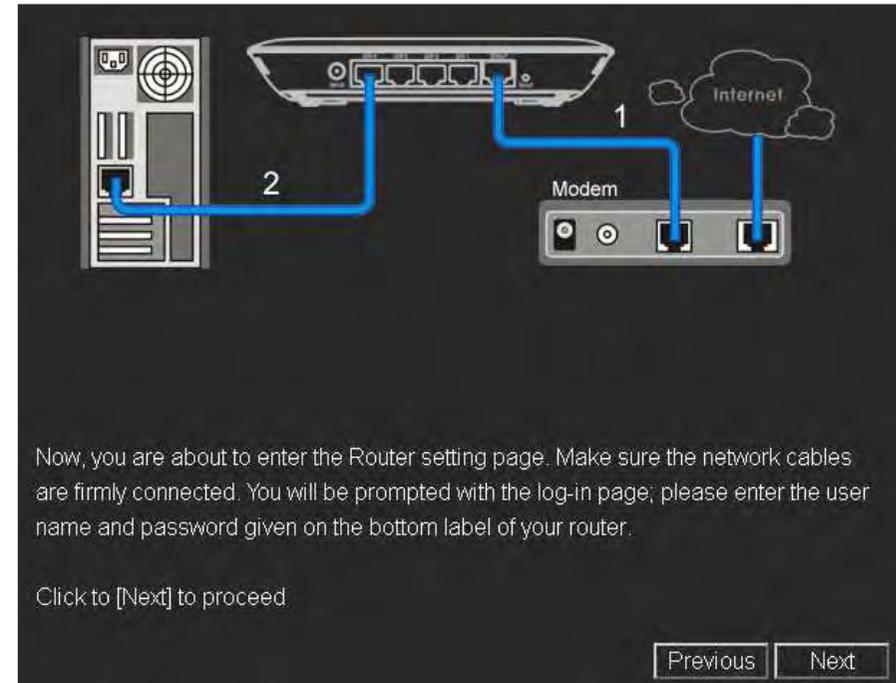
2. Plug either end of an Ethernet cable into the WAN port on the back panel of the router (see CABLE 1). Plug the other end of the cable into your cable/DSL modem.



3. Plug either end of an Ethernet cable into the LAN port on the back panel of the router (see **CABLE 2**). Plug the other end of the cable into your computer.

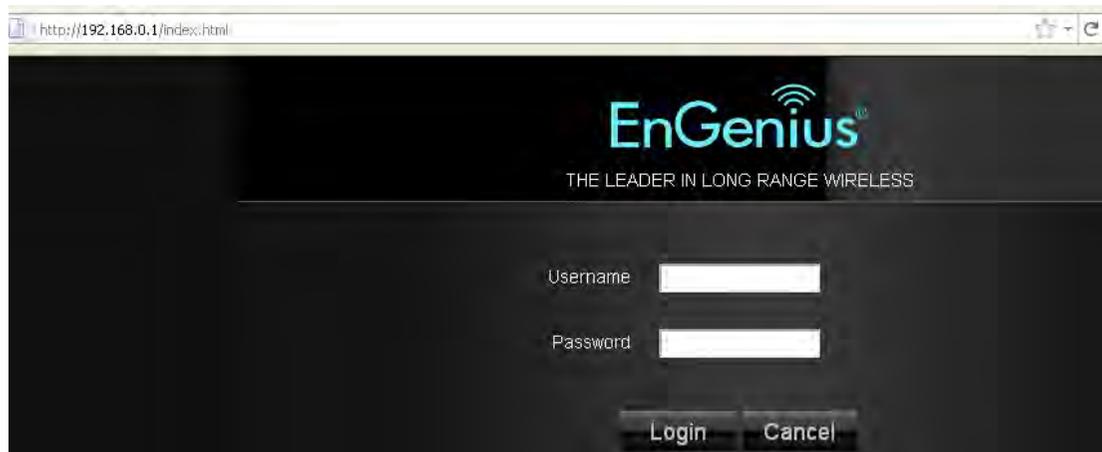


4. Make sure the network cable and power adapter are firmly connected. Click Next. You will then be prompted with the login screen. Please enter the default user name as admin and the default password as **admin** for your router.



NOTE: If the browser is not automatically prompted. Please manually enter the default router IP address **192.168.0.1** into your browser.

3.3. Login your Router

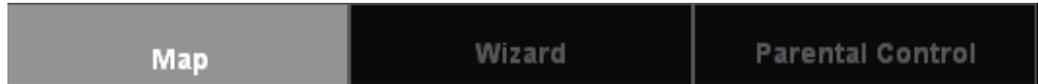


1. Once logged in, the landing page will display information about the **ESR300H**.
2. Icon introduction

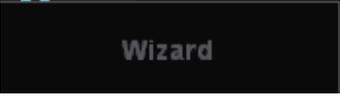
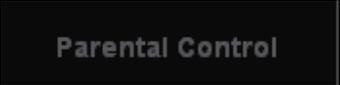
On the top right, you will see four icons:



-  Home
-  Setup Wizard Mode
-  Advanced Networking Setting
-  Exit



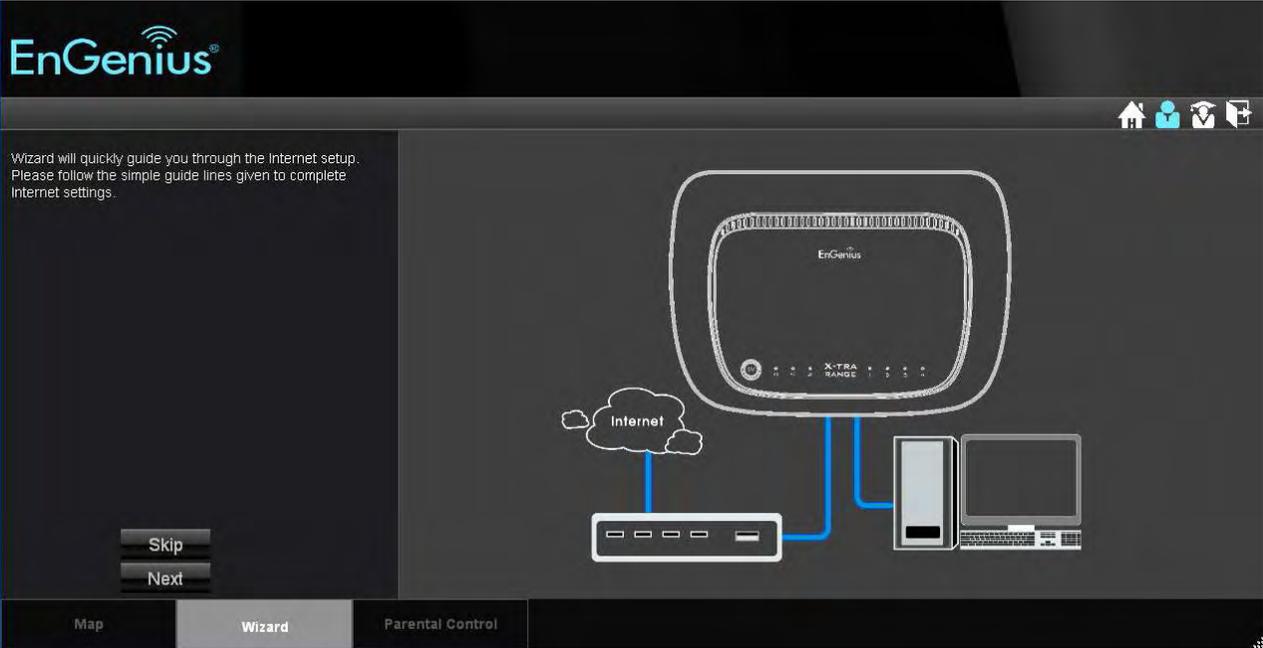
On the bottom left, you will see:

-  Map
-  Wizard
-  Parental Control

- View the router information and connection status
- Open the setup wizard by clicking **Wizard** button
- Customize the parent control setting by clicking **Parent Control** button

3.4. Configuring your Internet

1. Select **Wizard** on the bottom left hand corner of the landing page.
2. The wizard will then explain to you that it will set up the internet connection. Click **Next**.



3. The **Wizard** will then proceed to automatically detect the type of internet connection being used based on the connection on the WAN port of the **ESR300H**. Please wait a few seconds to finish detecting the internet connection.
4. If the **ESR300H** does not detect the appropriate internet connection, you can select the correct one on the drop down menu of **Login Method (also known as WAN protocol / Internet Connection method)**.

Dynamic IP Address (DHCP)

A DHCP type of connection is where your internet connection is usually always on and your internet service provider automatically provides you with an IP address. A DHCP connection is usually from a Cable internet service.

Static IP

To set up a Static IP connection, enter the following: IP Address of the Internet Connection, Subnet Mask, Default Gateway, and both DNS Servers. This information can be obtained by either your Internet Service provider or Network Administrator. If your internet service provider requires a username and password to connect, you will then be prompted to enter the correct information.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.

Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE): To set up a PPPoE connection, enter the Username, Password, and Service (name) of the internet connection provided by your ISP. Click Next and the **ESR300H** should connect to the internet successfully. A PPPoE connection is usually from a DSL internet service.

1. Login: The username or e-mail address that the internet connection uses to access internet connectivity.
2. Password: The password that corresponds to the username or e-mail address used to connect to the internet in the PPPoE.
3. Service Name: The Service Name is optional. This is to signify the name of the Internet Service Provider.
4. MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.
5. Point-to-Point Tunneling Protocol (PPTP)

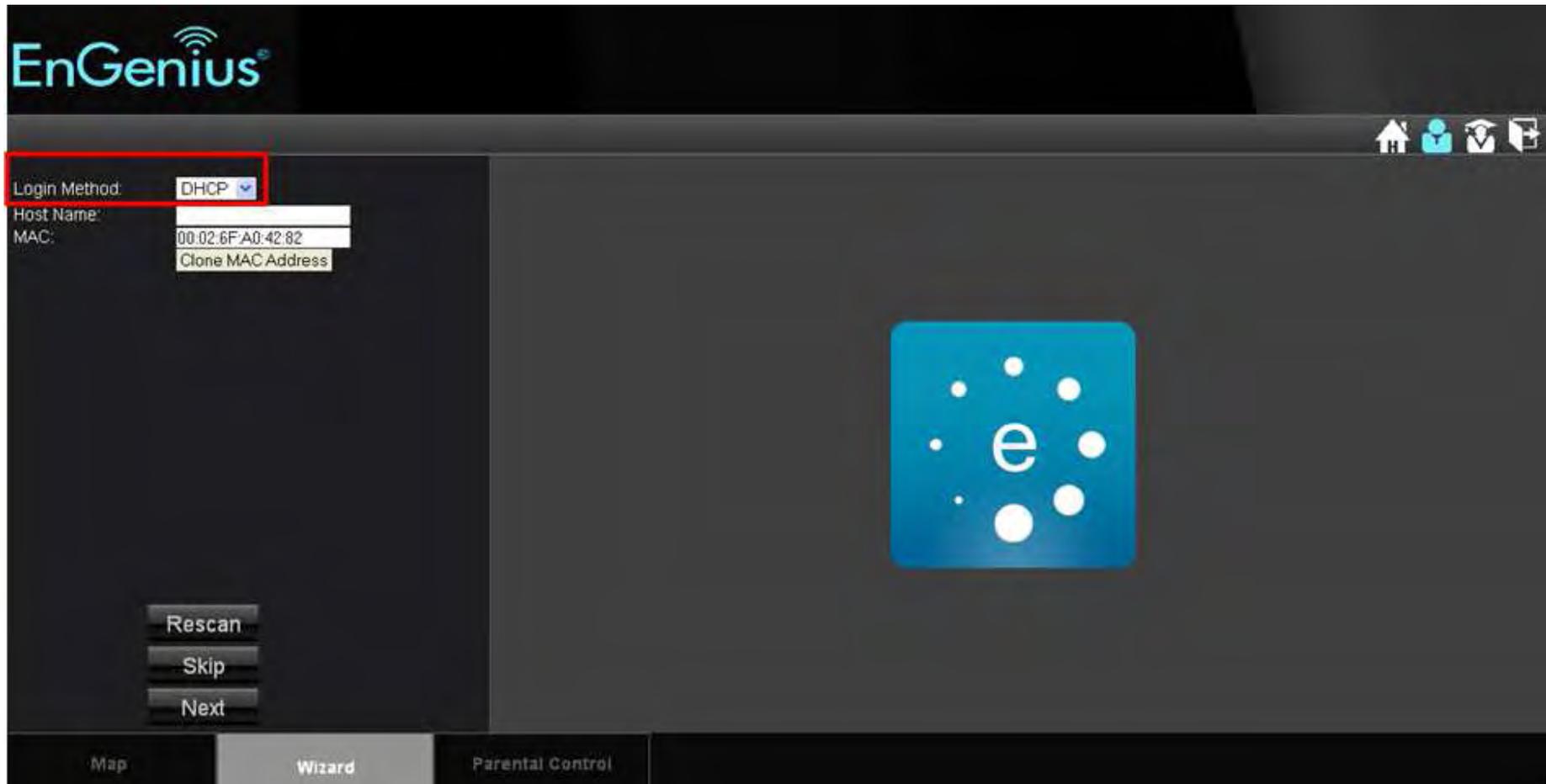
To set up a PPTP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, Service, and Connection ID of the PPTP internet connection. Once completed, click **Next**. Once configured, the internet connection will successfully connect.

Layer 2 Tunneling Protocol (L2TP)

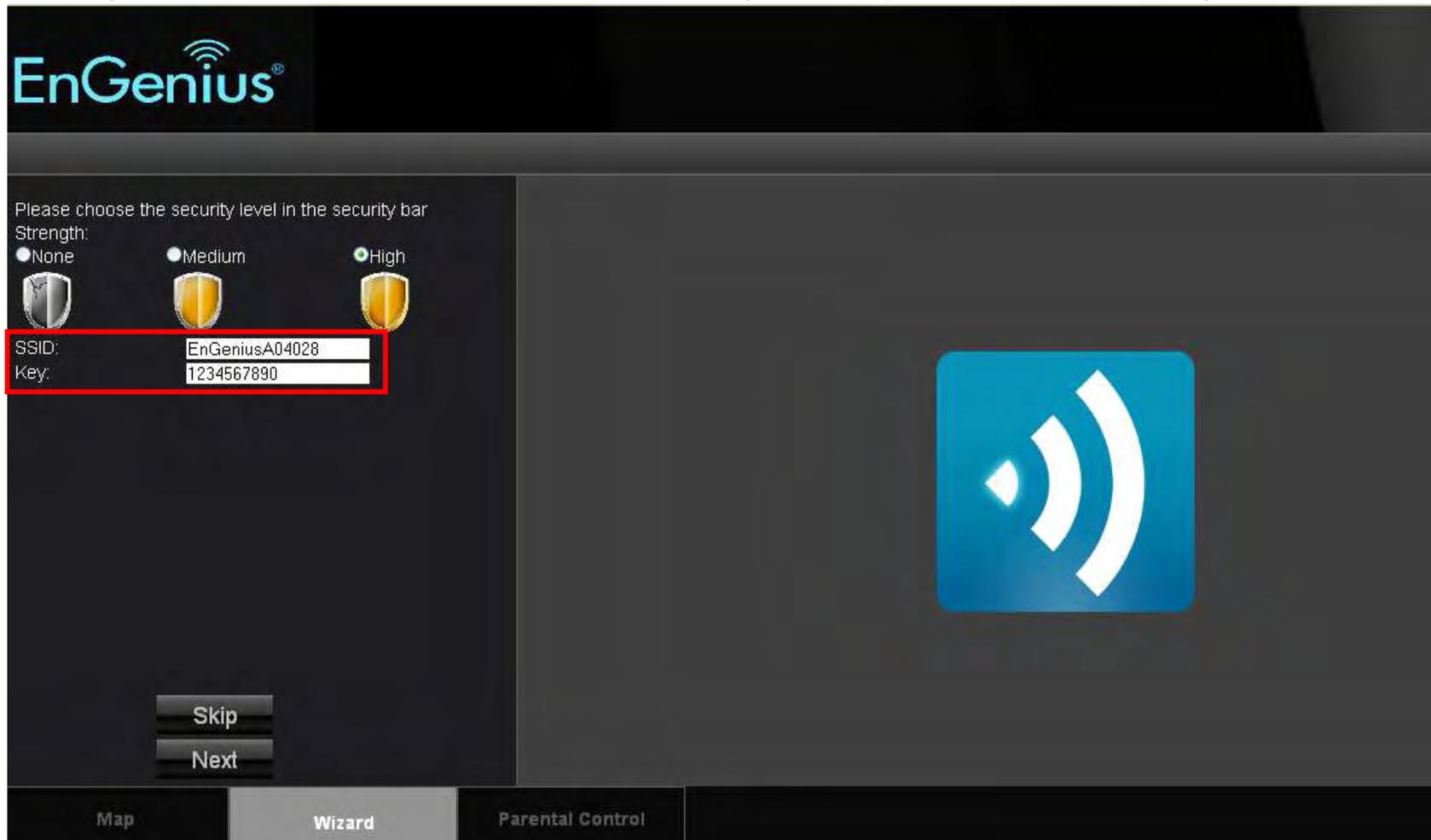
To set up an L2TP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, and Service. Click next when completed. Once configured, the internet connection will successfully connect.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.

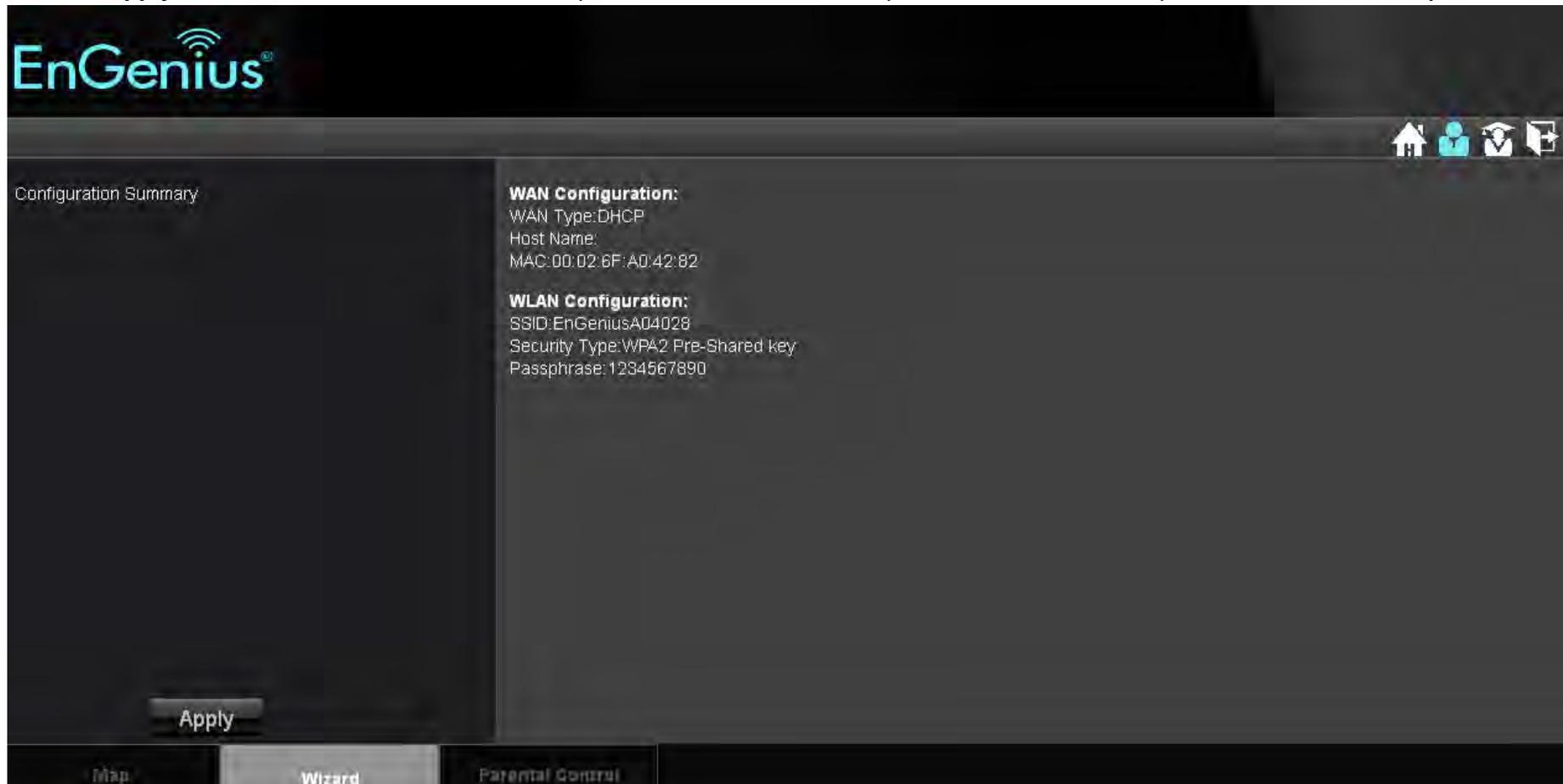
5. When the internet connection is detected, click **Next**.



6. It is highly recommended to select High as the security level to better secure your router and prevent outside intrusion.
7. Enter your desired router name in the column of SSID, and enter your desired password in the column of Key.



8. Click **Apply** to save the information entered in step 13 -14. You have now completed the ESR300H setup. Now ESR300H is ready for use.



4. Parental Control

Parent Control: Parental control enables centralized control on the Internet access restriction for each connected computer. You can make the access policies for a keyword or URL filtered based on weekdays or weekend.

The screenshot displays the EnGenius web interface for Parental Control. At the top left is the EnGenius logo. The main area is divided into several sections:

- Policy List:** A table with columns 'Policy', 'Action', and 'Member'. It lists 'Web Monitor' with 'Allow' action for 'carina-PC,D1M0QTK1', and 'weekday' and 'weekend' with 'Allow' action.
- Buttons:** 'Add Policy' and 'Edit' buttons are located below the policy list.
- Policy Configuration:** A section for the 'Web Monitor' policy showing 'Status Enabled', 'Block URL', and 'Schedule' (Always, 00:00-24:00). It includes a 'Member' list with a device icon and the name 'carina-PC, D1M0QTK1', and an 'Apply' button.
- Device List:** A large area on the right with the instruction: 'Please use your mouse to [drag and drop] add or remove device from the list.'
- Navigation:** A bottom bar contains 'Map', 'Wizard', and 'Parental Control' (highlighted with a red box).
- URL:** The address bar shows 'http://192.168.0.1/eg_parent_ctrl.html'.

You can add policies by clicking **Add Policy**. You will then be prompted to:

1. Name the Policy. Click **Next**.
2. Select the device (by its MAC Address) to apply the policy to. Click **Next**.

Step 2: Select Target Device

Specify a device with its IP or MAC address.

Filtering Type MAC IP

Member List

Device Name	MAC Address	
		Add

Prev Next Save Cancel

3. Schedule when the policy will be active. Click **Next**.

Step 3: Select Schedule

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

Schedule Deny Allow

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time of day All Day (use 24-hour clock)
From 0 : 0 To 0 : 0

Prev Next Save Cancel

4. Enter Keywords and URLs to be filtered/ blocked. Check **Enable Application Filter** if you would like the application filtering. Click **Next**.

Step 4: Web/Keyword Filter

You can block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site

Filtering Deny Allow

URL/Keyword

URL List

No.	URL/Keyword
-----	-------------

Enable Application Filter

5. Enable or disable **Web Access Logging**. Click **Save** for your settings.

Step 6: Configure Web Access Logging

Web Access Logging Disabled Enabled

6. If you would like to proceed to the advanced **Networking Setting**, please click:



The screenshot displays the EnGenius web interface. At the top left is the EnGenius logo. In the top right corner, there are navigation icons: a home icon, a user profile icon, a graduation cap icon (highlighted with a red box), and a refresh icon. The main content area is divided into three sections:

- System Information:** A list of system details including Application Version (1.0.2), Hardware Version (1.0.0), Serial Number (000000001), MAC Address (00:AA:BB:CC:DD:11), Attain IP Protocol (Dynamic IP Address), IP Address (---), Subnet Mask (---), Default Gateway (---), SSID (EnGenius888890), and Security type (WPA Pre-Shared key).
- Status:** A central column showing network status: Internet (Offline), WAN Cable (Disconnected), and Wireless (On).
- Device List:** A table listing connected devices, with one device shown: D1M0QTK1.

At the bottom of the interface, there are four tabs: Map, Wizard, Parental Control, and an unlabeled tab.

5. Advanced Networking Setting

If you would like to manually configure the advanced Networking Settings please open your browser (Internet Explorer or Firefox), and type in the default IP **192.168.0.1** to get access to the web-based management utility. Once open, click  to start the configuration.

There are 8 main tabs in the Advanced Networking Setting. They are System, Internet, Wireless, Parent Control, Firewall, VPN, Advanced, and Tools.

System

Status: You can review the router information and setting status

System

Model: The model name of ESR300H

Mode: The operation mode you choose

Uptime: The duration which ESR300 is connected

Hardware Version: The hardware version number of your ESR300H

Serial Number: The serial number of your ESR300H. The serial number is required when you need customer support or repair for your ESR300H.

Application Version: The software version of your ESR300H. You can always update to the latest firmware of your ESR300. The latest firmware can be found on the EnGenius website. (please visit www.engeniustech.com for the latest firmware and the related documents)

WAN Settings

Attain IP Protocol: Displays the IP Protocol in use for the ESR300H. It can be Dynamic IP address or Static IP Address.

IP Address: Your router's WAN IP address

Submask: Your router's WAN Submask

Default Gateway: Your ISP's Gateway IP address

MAC Address: Your router's WAN MAC address. You can also find your router's MAC address on the label on the back side of the router

Primary DNS: Primary DNS of your ISP provider

Secondary DNS: Secondary DNS of your ISP provider

LAN Settings

IP address: Your router's local IP address. The default LAN IP address is 192.168.0.1

Submask: Your router's local submask

DHCP Server: The status of your router's DHCP server function. Enable or disable.

MAC address: Your router's LAN MAC address

WLAN Settings

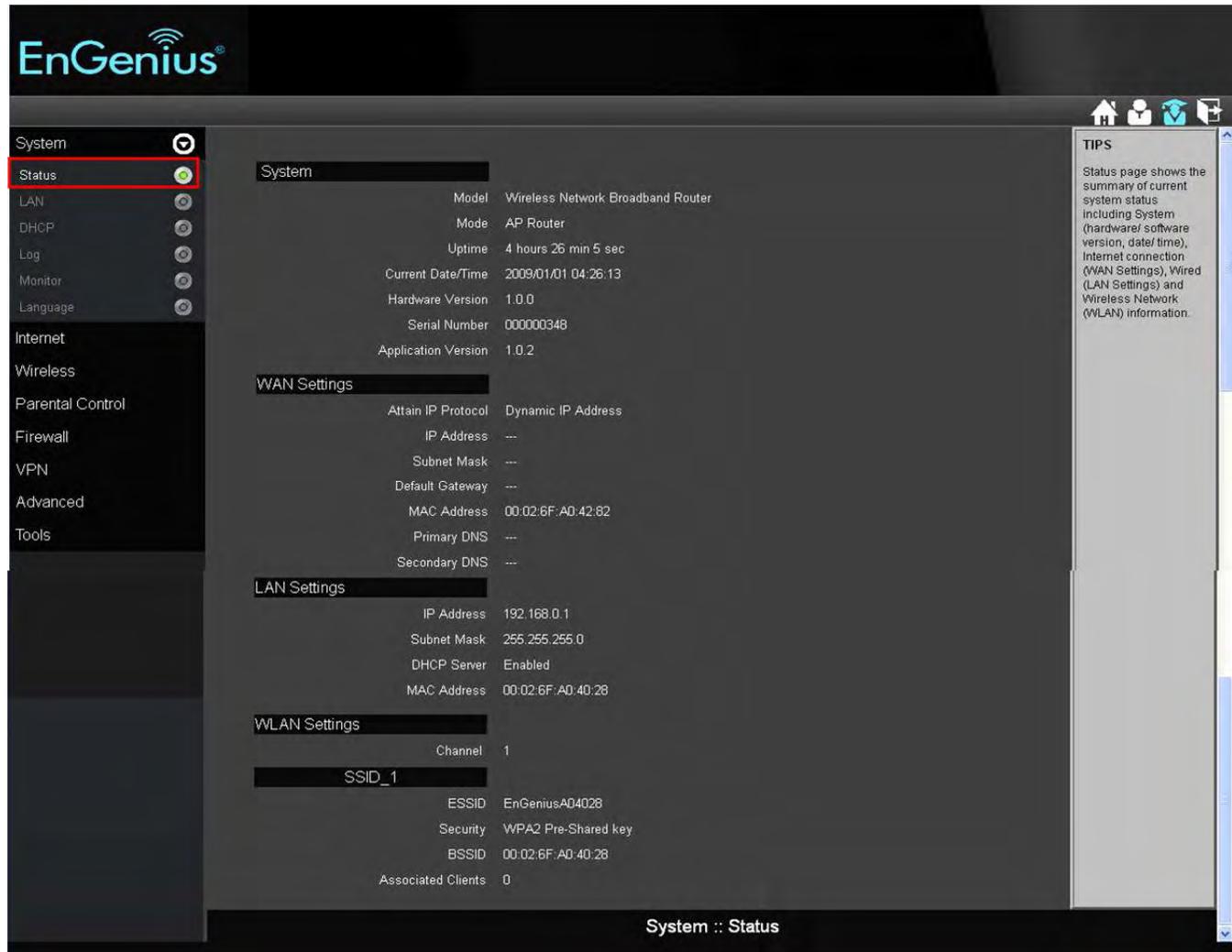
Channel: The wireless channel number used is shown

SSID: Up to 4 SSIDs (network groups) for the ESR300H

ESSID: Your router's name

Security: Security level utilized by your ESR300H

Associated Client: The number of clients connected to your router



LAN

LAN IP

IP Address: Your router's LAN IP address

IP Subnet Mask: Your router's LAN Subnet Mask

802.1d Spanning Tree: 802.1d Spanning Tree is disabled by default. When enabled, the spanning tree protocol is applied to prevent network loops (transmissions won't pass the same node twice to reach the destination).

DHCP Server: DHCP server automatically assigns IP address to computers on your network. Enabling this function allows your router to automatically assign IP address to the connected devices.

DHCP Server: DHCP Server is enabled by default. If you do not need a DHCP server, please select disabled.

Lease Time: If your DHCP Server is enabled, the Lease Time function allows you to assign the desired amount of time for each connected client.

Start IP: The starting IP address for the range of addresses assigned by your router

End IP: The last IP address for the range of addresses assigned by your router

Domain Name: The domain name of your router

DNS Server: DNS server can translate the domain or website names into internet address or URL. Typically, your ISP will provide you with one or more DNS Server IP addresses. You can also assign your desired DNS Server IP address by selecting **User-Defined**.

First DNS Server: DNS Relay is set by default. If your ISP provides you with a DNS Server IP address, please select From ISP, and type in the assigned IP address. Select User-Defined if you wish to assign a DNS Server IP by yourself. Select **None** if you do not have any.

Second DNS Server: If you get a second DNS Server IP or you wish to assign a second DNS Server IP, please type in the desired IP address in the field.

Click **Apply** to save your settings.

EnGenius

System

Status

LAN

DHCP

Log

Monitor

Language

Internet

Wireless

Parental Control

Firewall

VPN

Advanced

Tools

LAN IP

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

802.1d Spanning Tree: Disabled

DHCP Server

DHCP Server: Enabled

Lease Time: Forever

Start IP: 192.168.0.100

End IP: 192.168.0.200

Domain Name: esr300h

DNS Servers

DNS Servers Assigned by DHCP Server

First DNS Server: DNS Relay, 192.168.0.1

Second DNS Server: None, 0.0.0.0

Apply Cancel

TIPS

LAN Settings allows you to configure your wired network. Your router IP is defined by [IP address] field. By default, the DHCP server is enabled so that your network clients can be assigned with a virtual IP address in order to share the Internet connection. For advanced users, you may also change DNS server to meet special requirements. Usually, you do not need to make any changes on this section. Please keep the default value if you are uncertain about these settings.

System :: LAN

DHCP

DHCP Client Table: Displays all the connected DHCP clients whose IP addresses are assigned by the DHCP Server in your network. Click Refresh to update the table.

Enable Static DHCP IP: Check Enable Static DHCP IP if you wish to add more Static DHCP IP addresses. Click Reset if you would like to erase IP address or MAC address.

Current Static DHCP Table: Once the desired DHCP IP address is added in the previous step, it will be listed in the Current Static DHCP Table. You can delete any added Static DHCP IP address from the table if you do not need one.

Click **Apply** to save the settings.

The screenshot displays the EnGenius DHCP configuration interface. On the left is a sidebar with navigation options: System, Status, LAN, DHCP (highlighted with a red box), Log, Monitor, Language, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, and Tools. The main content area is titled 'DHCP Client Table' and contains a table with the following data:

IP Address	MAC Address	Expiration Time
192.168.0.100	00:1B:24:5A:CD:72	Forever
192.168.0.101	00:25:64:4A:8A:E8	Forever

Below the table is a 'Refresh' button. Underneath is a checkbox labeled 'Enable Static DHCP IP'. Below this is a table for adding static IP addresses:

IP Address	MAC Address
<input type="text"/>	<input type="text"/>

Buttons for 'Add' and 'Reset' are located below this table. Further down is the 'Current Static DHCP Table' with the following structure:

No.	IP Address	MAC Address	Select
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Buttons for 'Delete Selected', 'Delete All', and 'Reset' are located below this table. At the bottom right of the main content area are 'Apply' and 'Cancel' buttons. On the right side of the interface, there is a 'TIPS' section with the following text:

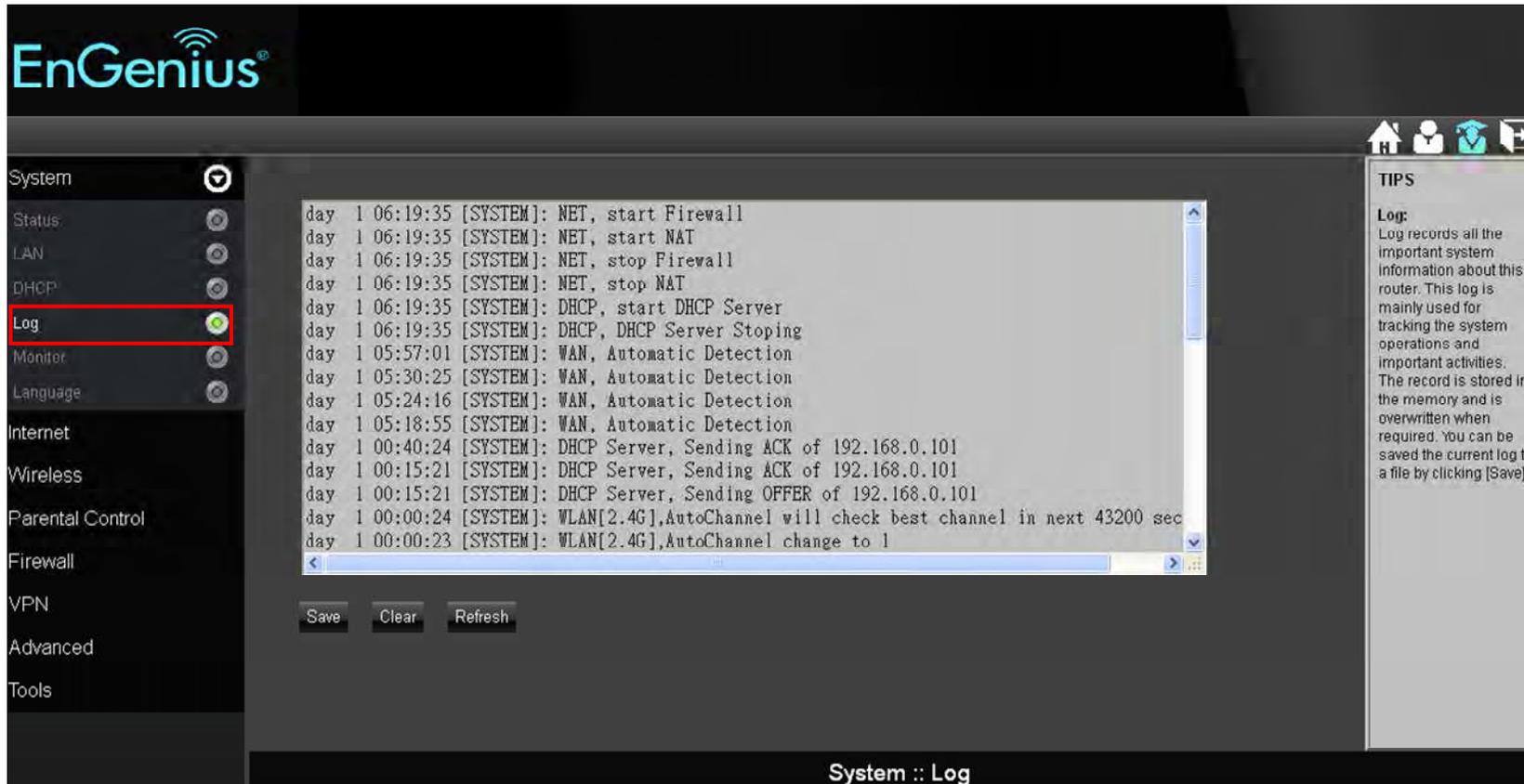
TIPS

DHCP Client Table: This table shows all the IP addresses that are currently being used. Each IP is assigned to a device which can be identified by MAC address. You can obtain the latest IP assignment by clicking [Refresh].

Enable Static DHCP IP: This feature allows for static leases to be assigned to a client based on a MAC address. Usually, you do not need to make any changes on this section. Please keep the default value if you are uncertain about these settings.

At the bottom of the page, the text 'System :: DHCP' is displayed.

Log: Records the system log of the router. The log displays any event that occurred after your router starts up. Click **Save** if you wish to save the log in a local file for further analysis. Click **Clear** if you wish to erase the current log. Click **Refresh** to get the most updated information. If the router is powered off, the system log will disappear if it is not saved in a local file



The screenshot displays the EnGenius router's web management interface. On the left, a navigation menu lists various system settings, with 'Log' highlighted in red. The main area shows a scrollable log of system events. Below the log are three buttons: 'Save', 'Clear', and 'Refresh'. On the right side, a 'TIPS' box provides additional information about the log's function.

```
day 1 06:19:35 [SYSTEM]: NET, start Firewall
day 1 06:19:35 [SYSTEM]: NET, start NAT
day 1 06:19:35 [SYSTEM]: NET, stop Firewall
day 1 06:19:35 [SYSTEM]: NET, stop NAT
day 1 06:19:35 [SYSTEM]: DHCP, start DHCP Server
day 1 06:19:35 [SYSTEM]: DHCP, DHCP Server Stopping
day 1 05:57:01 [SYSTEM]: WAN, Automatic Detection
day 1 05:30:25 [SYSTEM]: WAN, Automatic Detection
day 1 05:24:16 [SYSTEM]: WAN, Automatic Detection
day 1 05:18:55 [SYSTEM]: WAN, Automatic Detection
day 1 00:40:24 [SYSTEM]: DHCP Server, Sending ACK of 192.168.0.101
day 1 00:15:21 [SYSTEM]: DHCP Server, Sending ACK of 192.168.0.101
day 1 00:15:21 [SYSTEM]: DHCP Server, Sending OFFER of 192.168.0.101
day 1 00:00:24 [SYSTEM]: WLAN[2.4G],AutoChannel will check best channel in next 43200 sec
day 1 00:00:23 [SYSTEM]: WLAN[2.4G],AutoChannel change to 1
```

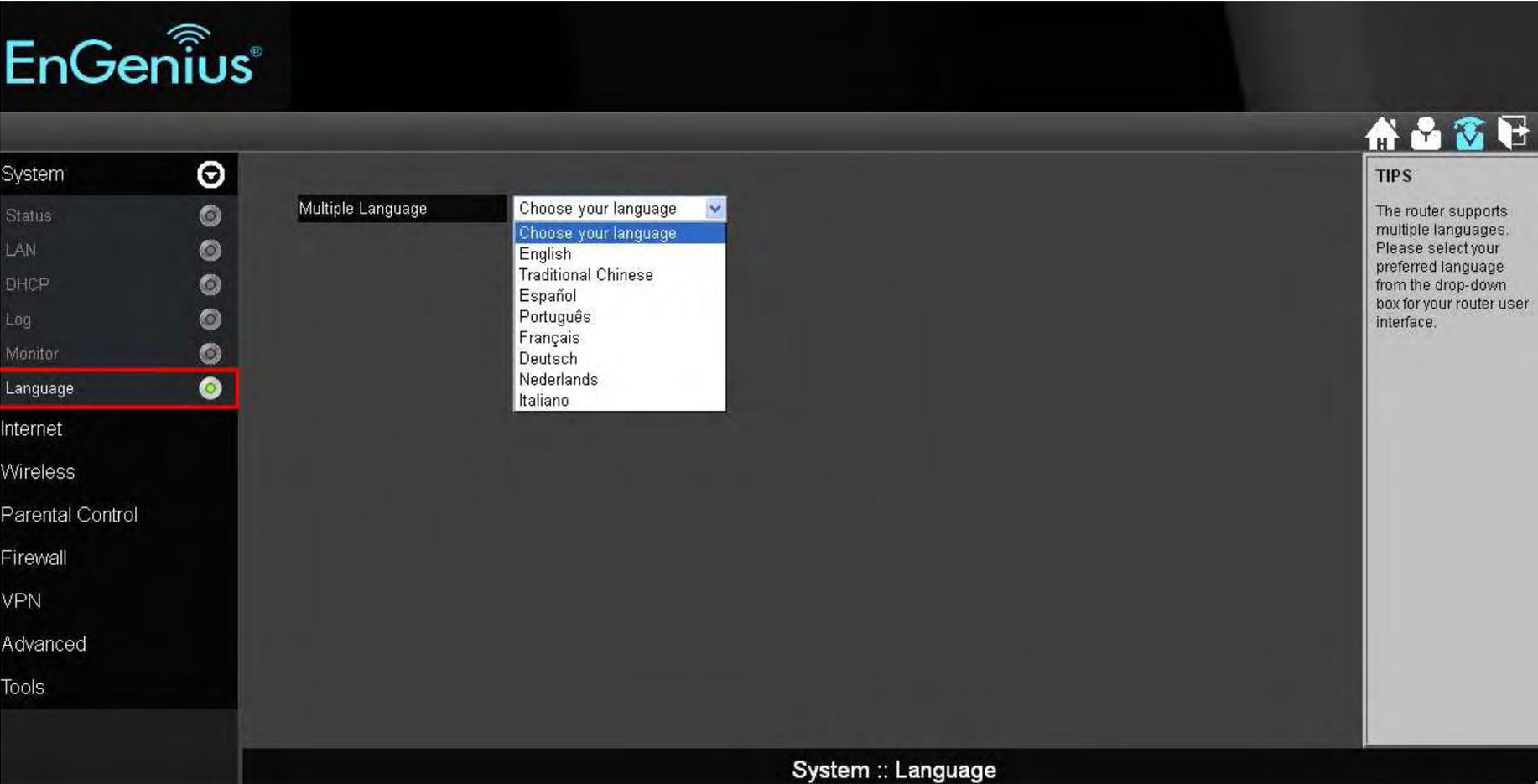
TIPS
Log:
Log records all the important system information about this router. This log is mainly used for tracking the system operations and important activities. The record is stored in the memory and is overwritten when required. You can be saved the current log to a file by clicking [Save].

System :: Log

Monitor: Displays the bandwidth utilized on WAN and WLAN.



Language: ESR300 supports multiple languages. Please select your preferred language.



6. Internet

Status: Displays the internet connection type and status

WAN Setting

Attain IP Protocol: Displays the IP Protocol currently used by the ESR300H. It can be Dynamic IP address or Static IP Address.

IP Address: Your router's WAN IP address

Submask: Your router's WAN Submask

Default Gateway: Your ISP's Gateway IP address

MAC Address: Your router's WAN MAC address. You can also find your router's MAC address on the label on the back side of the router

Primary DNS: Primary DNS of your ISP provider

Secondary DNS: Secondary DNS of your ISP provider

The screenshot shows the EnGenius router's web interface. The left sidebar has a menu with categories: System, Internet, Dynamic IP, Static IP, PPPoE, PPTP, L2TP, Wireless, Parental Control, Firewall, VPN, Advanced, and Tools. Under the 'Internet' category, the 'Status' option is highlighted with a red box and a green checkmark. The main content area is titled 'WAN Settings' and shows the following configuration:

Attain IP Protocol	Dynamic IP Address
IP Address	---
Subnet Mask	---
Default Gateway	---
MAC Address	00:02:6F:A0:42:82
Primary DNS	---
Secondary DNS	---

A 'Renew' button is located at the bottom right of the settings area. The bottom status bar reads 'Internet :: Status'. On the right side of the interface, there is a 'TIPS' section with the following text: 'WAN Settings (Internet Status) page shows the summary of current Internet connection information. This section is also shown on the System Status page.'

Dynamic IP: A DHCP type of connection where your internet connection is usually always on and your internet service provider automatically provides you with a dynamic IP address. A DHCP connection is usually from a Cable internet service.

Hostname: Assign a name for your internet connection type. You can leave it blank.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Dynamic IP (DHCP) is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.



Clone MAC:

Some ISPs require you to register the MAC address of your network interface card (NIC) connected directly to your cable or DSL modem during installation. Clone MAC will mask the router's MAC address with the MAC address of your NIC. Enter the MAC address of the NIC in the MAC address field and click the Clone MAC button. Now, the correct MAC address is used for communication to the ISP.

DNS Server: A DNS server can translate the domain or website names into internet address or URL. Typically your ISP will provide you with one or more DNS Server IP addresses. You can also assign your desired DNS Server IP address by selecting **User-Defined**.

First DNS Server: DNS Relay is set by default. If your ISP provides you with a DNS Server IP address, please select From ISP, and type in the assigned IP address. Select **User-Defined** if you wish to assign a DNS Server IP by yourself.

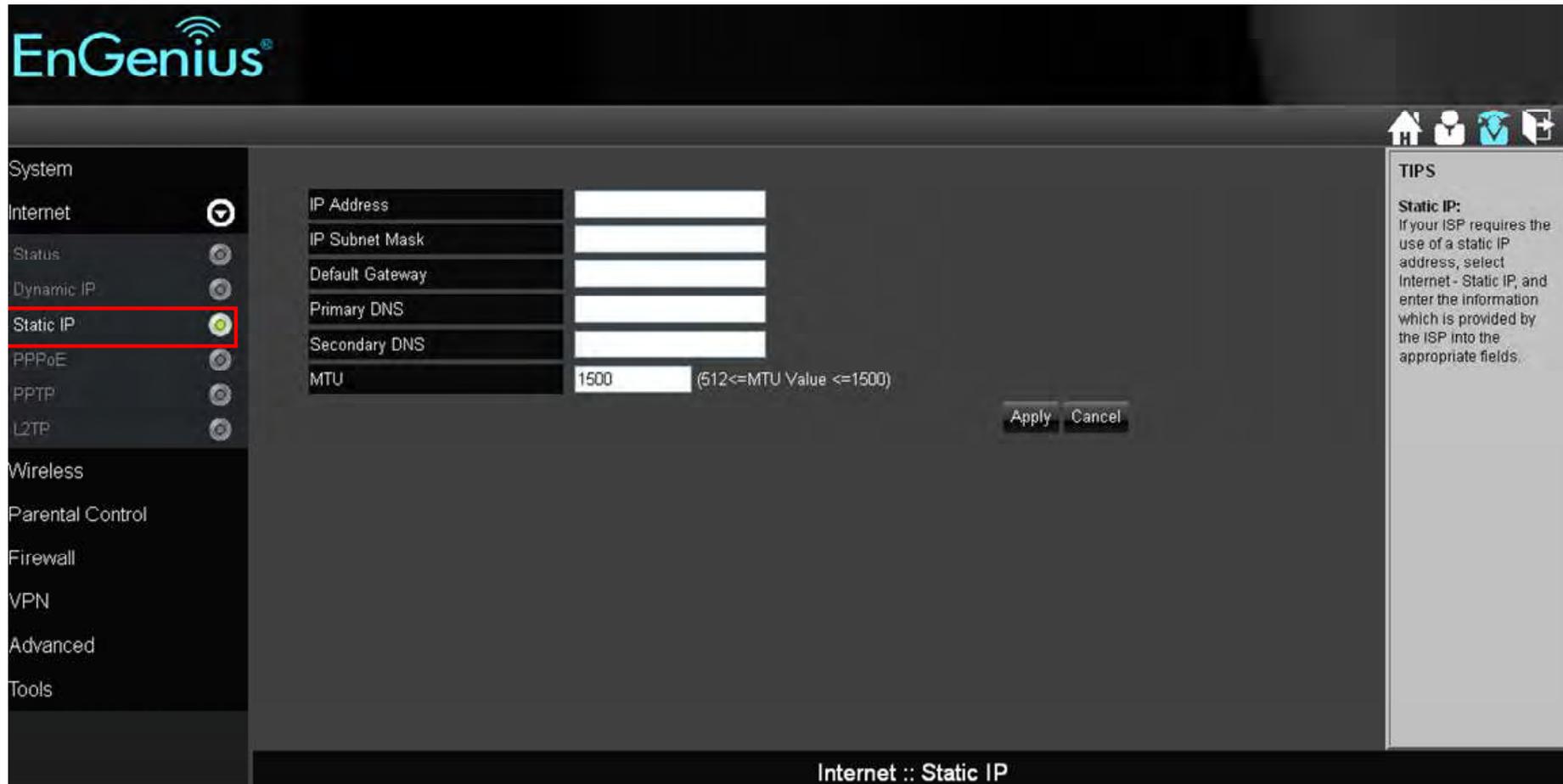
Second DNS Server: If you have a second DNS Server IP or you wish to assign a second DNS Server IP, please type in the desired IP address in the field.

Click **Apply** to enable your settings.

Static IP

To set up a Static IP connection, enter the following: IP Address of the Internet Connection, Subnet Mask, Default Gateway, and both DNS Servers provided by your Internet Service provider (ISP) or Network Administrator.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.



The screenshot displays the EnGenius router's web-based configuration interface. The left sidebar contains a navigation menu with categories: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, and Tools. Under the 'Internet' category, several options are listed: Status, Dynamic IP, Static IP (highlighted with a red box), PPPoE, PPTP, and L2TP. The main content area is titled 'Internet :: Static IP' and contains the following configuration fields:

IP Address	<input type="text"/>
IP Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
MTU	<input type="text" value="1500"/> (512<=MTU Value <=1500)

At the bottom right of the configuration area, there are 'Apply' and 'Cancel' buttons. On the far right, a 'TIPS' section provides instructions: 'Static IP: If your ISP requires the use of a static IP address, select Internet - Static IP, and enter the information which is provided by the ISP into the appropriate fields.'

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE): To set up a PPPoE connection, enter the Username, Password, and Service (name) of the internet connection provided by your ISP. A PPPoE connection is usually from a DSL internet service.

The screenshot shows the EnGenius web interface for configuring a PPPoE connection. The left sidebar lists various settings, with 'PPPoE' highlighted in red. The main configuration area includes the following fields and options:

Username	<input type="text"/>
Password	<input type="password"/>
Service Name	<input type="text"/>
MTU	<input type="text" value="1492"/> (512<=MTU Value <=1492)
Authentication Type	Auto <input type="button" value="v"/>
Type	Keep Connection <input type="button" value="v"/>
Idle Timeout	<input type="text" value="10"/> (1-1000 Minutes)
MAC Address	<input type="text" value="00:02:6F:A0:42:82"/> <input type="button" value="Clone MAC"/>

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

TIPS
If your Internet is PPPoE based, your ISP will provide you with the user name and password. Please obtain this data from the ISP and enter the information into the appropriate fields. Usually Username and Password are the only two fields you need to enter. Please keep the other fields if you are uncertain about them.

MTU:
Maximum Transmission Unit (MTU) is the largest packet size permitted for internet transmission.

Authentication Type:
Please select the authentication type (Auto / PAP / CHAP) provided by your ISP.

Type:
This is the type of

Login: The username or e-mail address that the internet connection uses to access internet connectivity.

Password: The password that corresponds to the username or e-mail address used to connect to the internet in the PPPoE.

Service Name: The Service Name is optional. This is to signify the name of the Internet Service Provider.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of PPPoE is 1492. If you wish to manually change the MTU size, set it between 1200 and 1492.

Authentication Type: Auto, PAP, or CHAP. Select the authentication type provided by your ISP. If you are not sure, please select Auto.

Type: Connection type. You can select Keep Connection, Automatic Connection, or Manual Connection.

Idle Timeout: Maximum amount of time for inactive internet connection. The internet connection will be dropped when the maximum idle time is reached.

Clone MAC:

Some ISPs require you to register the MAC address of your network interface card (NIC) connected directly to your cable or DSL modem during installation. Clone MAC will mask the router's MAC address with the MAC address of your NIC. Enter the MAC address of the NIC in the MAC address field and click the Clone MAC button. Now, the correct MAC address is used for communication to the ISP.

Click **Apply** to enable your settings.

PPTP

To set up a PPTP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, and Service IP address provided by your ISP.

WAN Interface Settings

WAN Interface Type: Dynamic IP Address

Hostname: _____

MAC Address: 00:00:00:00:00:00

PPTP Settings

Username: _____

Password: _____

Service IP Address: _____

Connection ID: 0 (Optional)

MTU: 1400 (512<=MTU Value <=1492)

Type: Keep Connection

Idle Timeout: 10 (1-1000 Minutes)

TIPS

Your ISP will provide you with the user name and password. Please enter them accordingly.

WAN Interface Type: Select either Dynamic IP Address or Static IP address provided by your ISP.

Service IP Address: This is your ISP's PPTP server IP address. Contact your ISP for more information.

MTU: Maximum Transmission Unit (MTU) is the largest packet size permitted for internet transmission. Note: This setting should be only changed by experienced users.

Type: This is the type of connection between the router and ISP.

Clone MAC:

Some ISPs require you to register the MAC address of your network interface card (NIC) connected directly to your cable or DSL modem during installation. Clone MAC will mask the router's MAC address with the MAC address of your NIC. Enter the MAC address of the NIC in the MAC address field and click the Clone MAC button. Now, the correct MAC address is used for communication to the ISP.

Connection ID: you can leave it blank

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of PPTP is 1400. If you wish to manually change the MTU size, set it between 1200 and 1500.

Type: Connection type, you can select Keep Connection, Automatic Connection, or Manual Connection.

Idle Timeout: Maximum amount of time for inactive internet connection. The internet connection will be dropped when the maximum idle time is reached.

L2TP

To set up an L2TP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, and Service IP Address provided by your ISP.



The screenshot displays the EnGenius router's web management interface. The left sidebar contains a menu with the following items: System, Internet (selected), Status, Dynamic IP, Static IP, PPPoE, PPTP, L2TP (highlighted with a red box), Wireless, Parental Control, Firewall, VPN, Advanced, and Tools. The main content area is titled "WAN Interface Settings" and includes the following fields:

- WAN Interface Type: Dynamic IP Address (dropdown menu)
- Hostname: [Empty text field]
- MAC Address: 00:00:00:00:00:00 (with a "Clone MAC" checkbox)
- L2TP Settings section:
 - Username: [Empty text field]
 - Password: [Empty text field]
 - Service IP Address: [Empty text field]
 - MTU: 1460 (with a note: (512<=MTU Value <=1492))
 - Type: Keep Connection (dropdown menu)
 - Idle Timeout: [Empty text field] (with a note: (1-1000 Minutes))

At the bottom right of the settings area are "Apply" and "Cancel" buttons. A "TIPS" box on the right side of the interface provides the following information:

TIPS
L2TP is a WAN type through which some Internet Service Provider (ISP) may use for the Internet service. Please enter the Username and Password provided by your ISP to be authenticated. Do not change any other settings unless specific requested by your ISP.

Clone MAC:
You may need to use [Clone MAC] if your ISP requires your PC/Laptop MAC address as part of authentication. The router will clone your PC/Laptop MAC address to login.

Internet :: L2TP

Clone MAC:

Some ISPs require you to register the MAC address of your network interface card (NIC) connected directly to your cable or DSL modem during installation. Clone MAC will mask the router's MAC address with the MAC address of your NIC. Enter the MAC address of the NIC in the MAC address field and click the Clone MAC button. Now, the correct MAC address is used for communication to the ISP.

Connection ID: you can leave it blank

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of L2TP is 1460. If you wish to manually change the MTU size, set it between 1200 and 1492.

Idle Timeout: maximum amount of time for inactive internet connection. The internet connection will be dropped when the maximum idle time is reached.

Click Apply to enable your settings.

7. Wireless LAN Setup

Wireless > Basic

In the Basic Wireless Setup (Located in the **Wireless** section in the **Main Menu**), select **Basic**, and you can quickly enable and configure the Wireless network.

The screenshot shows the EnGenius web interface for configuring the wireless network. The left sidebar contains a menu with the following items: System, Internet, Wireless, Basic (highlighted with a red box and a green status indicator), Advanced, Security, WPS, Client List, Parental Control, Firewall, VPN, Advanced, and Tools. The main content area is titled "Wireless :: Basic" and contains the following settings:

- Radio: Enable Disable
- Mode: AP
- Band: 2.4 GHz (B+G+N)
- Enable SSID#: 1
- SSID1: EnGeniusA04028
- Auto Channel: Enable Disable
- Check Channel Time: Half Day

At the bottom right of the settings area are "Apply" and "Cancel" buttons. On the right side of the page, there is a "TIPS" section with the following text:

TIPS

Mode:
Select AP/Router mode or WDS mode for the wireless network connection. Note: AP is: AP/Router mode. And WDS is Wireless Distribution System (WDS) mode.

Enable SSID#:
The router supports up to 4 SSIDs, allowing you to secure your private local network by assigning a different SSID to each group of users. For example, guests may be placed on a secondary SSID.

SSID:
This is the broadcasted wireless network name.

Radio: You can turn on/off the wireless radio. If wireless Radio is off, you cannot set an access point through wireless.

Mode: Select Access Point mode or Wireless Distribution Service (WDS) mode for your router.

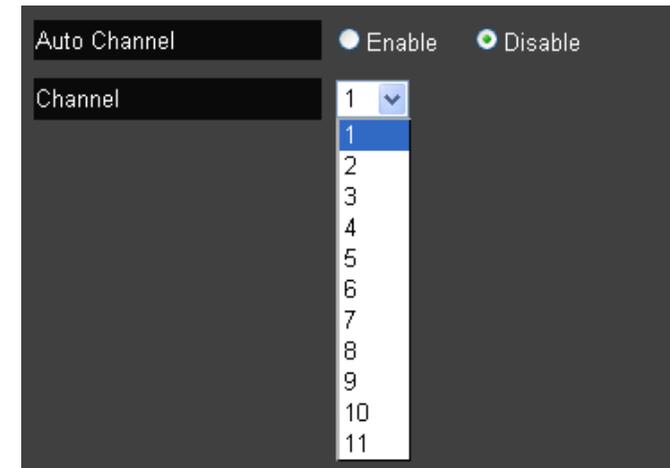
- AP: Use the **ESR300H** as a Wireless Access Point for wireless devices to connect.
- WDS: In a WDS, access points are used to expand the wireless area by connecting to each other, without all of them having a wired backbone. To set up a WDS, enter the MAC Addresses of the other Access Points configured for WDS (up to 4 maximum) and set the WDS rate.

Set Security: you can select disable, WEP, or WPA for WDS security.

Band: You can select one of the wireless standards for your wireless network. The options are:

- 2.4 GHz (B)
- 2.4 GHz (G)
- 2.4 GHz (N)
- 2.4 GHz (B+G)
- 2.4 GHz (B+G+N)

1. **Enable SSID#:** Set the number of Wireless Groups. Up to 4 can be set.
2. **SSID[#]:** The Name of the wireless network.
3. **Auto Channel:** Auto channel is enabled by default. If you wish to select an appropriate channel for your wireless network, please disable Auto Channel, and select Channel from 1 – 11.
4. **Check Channel Time:** if Auto Channel is enabled, please select time period you wish the system check the appropriate channel for your router.



Wireless > Advanced

To change more advanced wireless features of the **EAS300H**, select the **Advanced** option of the Wireless section.

In the **Advanced** option, you can change the following:

1. **Fragment Threshold:** This specifies the maximum size of a packet during data transmission. A value too low could lead to low performance.
2. **RTS Threshold:** If the packet size is smaller than the RTS threshold, the **ESR300H** will not use RTS/CTS to send the data packet.
3. **Beacon Interval:** This is the amount of time that the **ESR300H** will resynchronize the network.
4. **Delivery Traffic Indication Message (DTIM) Period:** The DTIM is a countdown informing clients of the next point of broadcast and multicast messages over the network. This is a value between 1 and 255.

5. **Data Rate:** This is the rate in which the **ESR300H** will transmit data packets.
6. **N Data Rate:** This is the rate in which the **ESR300H** will transmit data packets to Wireless N compatible devices.
7. **Channel Bandwidth:** The factory default enables Auto 20/40MHz to optimize the best performance by auto selecting channel bandwidth.
8. **Preamble Type:** Select either Long Preamble (better LAN compatibility) or Short Preamble (better wireless performance).
9. **CTS Protection:** CTS Protection is recommended. It can lower the data collisions between Wireless B and Wireless G devices. Enabling CTS protection will lower data throughput of the **ESR300H**.

Click **Apply** to save your settings.

The screenshot displays the EnGenius wireless configuration interface. On the left, a sidebar lists various system settings, with 'Advanced' highlighted in red. The main content area is titled 'Wireless :: Advanced' and contains the following settings:

- Fragment Threshold:** 2346 (range 256-2346)
- RTS Threshold:** 2347 (range 1-2347)
- Beacon Interval:** 100 (range 20-1024 ms)
- DTIM Period:** 1 (range 1-255)
- N Data Rate:** Auto
- Channel Bandwidth:** Auto 20/40 MHz 20 MHz
- Preamble Type:** Long Preamble Short Preamble
- CTS Protection:** Auto Always None

At the bottom right of the settings area are 'Apply' and 'Cancel' buttons. On the far right, a 'TIPS' section provides additional information:

TIPS
Usually, you do not need to make any changes on this section. Please keep the default value if you are uncertain about these settings.

Fragment Threshold:
This is the packet size for each fragment.

RTS Threshold:
When the packet size is smaller than the RTS Threshold, then the packet will be sent without RTS/CTS handshake.

Beacon Interval:
This is the time interval that the router broadcasts a beacon. The beacon is used to inform about the AP existence.

Wireless > Security

To change the wireless security of the **ESR300H**, select the Security option of the Wireless section.

It is recommended to enable security options on the wireless network to prevent intrusions to systems on your wireless network.

1. **SSID Selection:** Choose the wireless network group to change the wireless security settings for.
2. **Broadcast SSID:** Choose whether or not you want the Wireless Group to be visible to other members.
3. **WiFi Multimedia (WMM):** Enable Quality of Server (QoS) to optimize the streaming for bandwidth sensitive data such as HDTV video streaming, online gaming, VoIP, videoconferencing, and etc.
4. **Encryption:** encrypt your router with passwords in different security level.



The screenshot displays the EnGenius router's configuration interface for the Wireless Security section. The left sidebar shows the navigation menu with 'Security' highlighted. The main content area contains the following settings:

- SSID Selection: EnGeniusA04028
- Broadcast SSID: Enable
- WMM: Enable
- Encryption: WPA Pre-Shared key
- WPA Type: WPA(TKIP) WPA2(AES) WPA2 Mixed
- Pre-Shared Key Type: Passphrase
- Pre-Shared Key: 1234567890

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the settings area. The status bar at the bottom of the page reads 'Wireless :: Security'.

TIPS

WMM:
Wi-Fi Multi-Media (WMM) is a Quality of Service protocol which prioritizes video, voice and bandwidth sensitive data over other types of data on the wireless network.

Encryption:
Not enabling encryption is strongly discouraged because unauthorized parties may access your network. Encrypt your router with WEP/WPA/WPA2 and select a strong passphrase. A strong passphrase is greater than 8 characters and may be composed of letters, numbers, and symbols. Note: WPA/WPA2 offer much stronger security than WEP.

Wired Equivalent Privacy (WEP)

To enable WEP security on your wireless network, select **WEP** in the encryption type.

The screenshot shows a configuration window for WEP security. The settings are as follows:

SSID Selection	EnGenius888890
Broadcast SSID	Enable
WMM	Enable
Encryption	WEP
Authentication Type	<input type="radio"/> Open System <input checked="" type="radio"/> Shared Key <input type="radio"/> Auto
Key Length	64-bit
Key Type	ASCII (5 characters)
Default key	Key 1
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****
<input type="checkbox"/> Enable 802.1x Authentication	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

1. **Authentication Type:** You can select between Open System (wireless stations can associate with this **ESR300H** wirelessly without WEP encryption) or Shared Key (devices must provide the corresponding WEP key [up to 4] when trying to connect to the **ESR300H** wirelessly).
2. **Key Length:** You can select between 64-bit encryption or 128-encryption keys.
3. **Key Type:** You can set the characters used for the WEP Key (ASCII or Hexadecimal).
4. **Encryption Key [#]:** The encryption keys used to encrypt the data packets during data transmission.

Click **Apply** when all settings are configured.

Wi-Fi Protected Access (WPA) Pre-Shared Key

To enable **WPA** on your wireless network, select **WPA-Pre-Shared Key** in the encryption type.

SSID Selection	EnGenius888890 ▾
Broadcast SSID	Enable ▾
WMM	Enable ▾
Encryption	WPA Pre-Shared key ▾
WPA Type	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-Shared Key Type	Passphrase ▾
Pre-Shared Key	TPHS5QNZNMGB

1. **WPA Type:** You can select between WPA (TKIP) (Temporal Key Integrity Protocol; a 128-bit key is user per packet and is generates a new key for each packet sent), WPA2(AES) (Advanced Encryption Standard; government standard packet encryption and stronger than TKIP), or WPA2 Mixed.
2. **Pre-Shared Key Type:** You can select Passphrase (ASCII) or Hexadecimal for the Pre-Shared Key.
3. **Pre-Shared Key:** Enter the Pre-Shared Key of your choice.

WPA Radius

You can use a **RADIUS** server to authenticate wireless stations and provide a session key to encrypt data during communication. You will just need to provide the Server IP Address, Server Port, and Server Password of the RADIUS server to the **ESR300H**.

SSID Selection	EnGeniusA04028
Broadcast SSID	Enable
WMM	Enable
Encryption	WPA RADIUS
WPA Type	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP Address	
RADIUS Server port	1812
RADIUS Server password	

Apply Cancel

Wireless > WPS

To configure the WiFi Protected Setup information, select the **WPS** option from the Wireless section.

WPS is an easy way to allow wireless clients to connect to the **ESR300H**. This can automate connection between the device and the **ESR300H** by use of a button or a PIN.

1. **WPS:** Check the box if you want to enable WPS.
2. **WPS Current Status:** A notification if the wireless security is configured or not configured.
3. **Self Pin Code:** This is the Wireless PIN of this **ESR300H**.
4. **SSID:** This is the wireless network name you are currently configuring.
5. **Authentication Mode:** The current security settings for the corresponding SSID.
6. **Passphrase Key:** The randomly generated key created by the **ESR300H** during WPS.
7. **WPS via Push Button:** Start the WPS process via a button.
8. **WPS via PIN:** Start the WPS process by entering the PIN of the wireless device.

The screenshot displays the EnGenius router's web interface for WPS configuration. The left sidebar contains navigation links: System, Internet, Wireless (selected), Basic, Advanced, Security, WPS (highlighted with a red box), Client List, Parental Control, Firewall, VPN, Advanced, and Tools. The main content area is titled 'Wi-Fi Protected Setup Information' and includes the following settings:

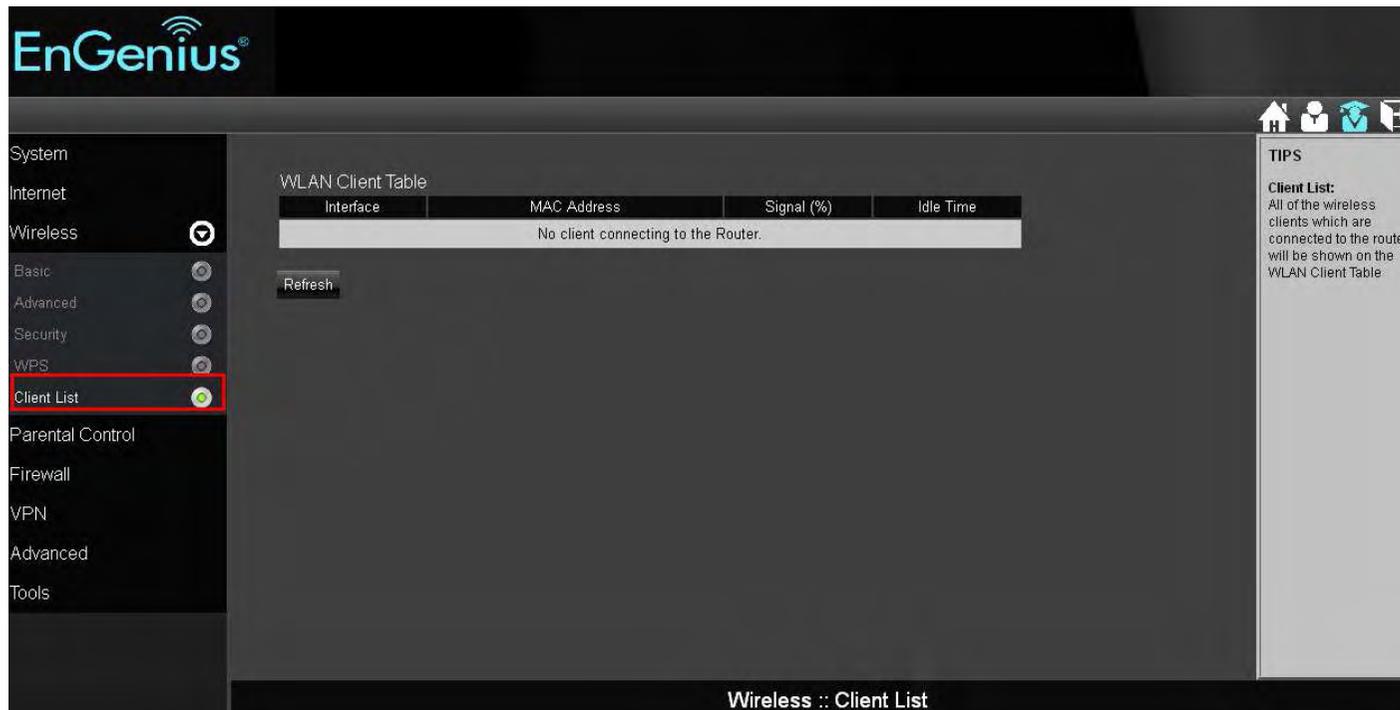
WPS	<input checked="" type="checkbox"/> Enable
WPS Current Status	Configured Release Configuration
Self Pin Code	05021840
SSID	EnGeniusA04028
Authentication Mode	WPA2 Pre-Shared key
Passphrase Key	1234567890
WPS Via Push Button	Start to Process
WPS via PIN	<input type="text"/> Start to Process

A 'TIPS' section on the right states: 'Self Pin Code: This is an 8-digit PIN which is required when configuring the router for the first time in Windows 7 or Vista.'

At the bottom of the page, the breadcrumb 'Wireless :: WPS' is visible.

Wireless > Client List

To view the wireless devices currently connected to the **ESR300H**, select the **Client List** option in the Wireless section.



The screenshot shows the EnGenius web interface. The left sidebar contains a menu with the following items: System, Internet, Wireless (selected), Basic, Advanced, Security, WPS, Client List (highlighted with a red box), Parental Control, Firewall, VPN, Advanced, and Tools. The main content area displays the 'WLAN Client Table' with the following columns: Interface, MAC Address, Signal (%), and Idle Time. The table is currently empty, showing the message 'No client connecting to the Router.' Below the table is a 'Refresh' button. The right sidebar contains a 'TIPS' section with the following text: 'Client List: All of the wireless clients which are connected to the router will be shown on the WLAN Client Table'. The bottom status bar shows 'Wireless :: Client List'.

Interface	MAC Address	Signal (%)	Idle Time
No client connecting to the Router.			

Refresh

TIPS
Client List:
All of the wireless clients which are connected to the router will be shown on the WLAN Client Table

Wireless :: Client List

8. Parental Control Section

Parental control enables centralized control on the Internet access restriction for each connected computer. You can make the access policies for keywords or URLs filtered based on weekdays or weekend.

Parental Control > Wizard

To access the Parental Control Wizard, select the **Wizard** option in the Parental Control section.

The **Parental Control Wizard** will bring up simple network monitoring controls. You can add policies and then limit keyword usages or block specific URLs during specified times.

Enable	Policy Name	Target Device	Schedule	Logged	Modify
<input checked="" type="checkbox"/>	Web Monitor	carina-PC, D1MQQTK1	Always	Yes	
<input checked="" type="checkbox"/>	weekday		From 12:00 To 22:00--Mon, Tue, Wed, Thu, Fri	Yes	
<input checked="" type="checkbox"/>	weekend		From 06:00 To 22:00--Sat, Sun	Yes	

TIPS
Parental Control is a feature that allows parents to filter out and control the Internet access. By adding keywords, the parental control engine checks the web contents and make sure it does not contain the specified content. Also, parents can limit the Internet access within the specified time and day (this is known as Schedule). Policy is a rule profile which describes the keyword filter and Internet access schedule. For example, a policy can be created to filter out the pages containing "XXX" or "SEX". You can apply the policy to multiple users. Those users are known as the policy member. Parental control engine will screen these member user(s) based on the applied...

You can add policies by clicking **Add Policy**. You will then be prompted to:

6. Name the **Policy**. Click **Next**.

7. Select the device (by its MAC Address) to apply the policy to. Click **Next**.

Step 2: Select Target Device

Specify a device with its IP or MAC address.

Filtering Type MAC IP

Member List

Device Name	MAC Address	
		Add

Prev Next Save Cancel

8. Schedule when the policy will be active. Click **Next**

Step 3: Select Schedule

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

Schedule Deny Allow

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time of day All Day (use 24-hour clock)
From 0 : 0 To 0 : 0

Prev Next Save Cancel

9. Enter Keywords and URLs to be filtered/ blocked. Check **Enable Application Filter** if you would like to enable application filtering. Click **Next**.

Step 4: Web/Keyword Filter

You can block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site

Filtering Deny Allow

URL/Keyword

URL List

No.	URL/Keyword
-----	-------------

Enable Application Filter

10. Enable or disable **Web Access Logging**. Click Save for your settings.

Step 6: Configure Web Access Logging

Web Access Logging Disabled Enabled

Parental Control > Web Monitor

To quickly view the Parental Control policies you already made in Parent Control Wizard, select the **Web Monitor** option from the Parental Control section.



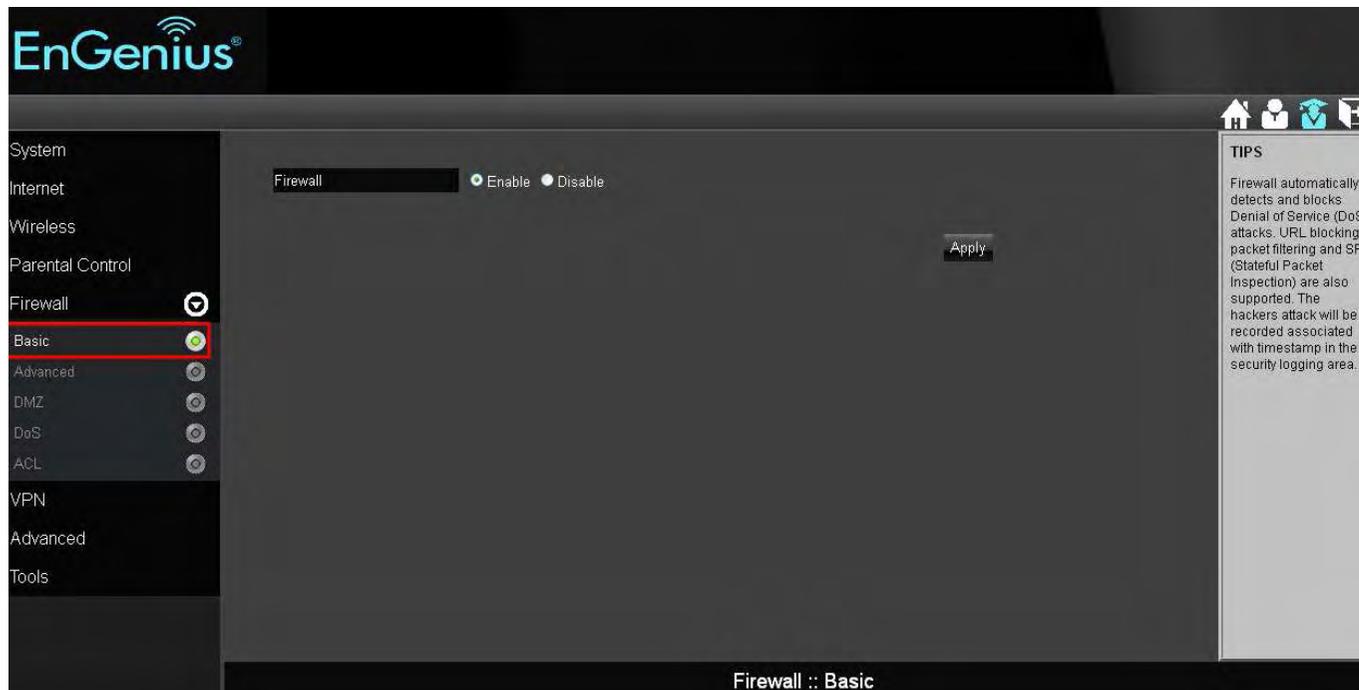
9. Firewall Section

To access the **Firewall** Section of the Expert Menu, select **Firewall** on the left hand side.

Firewall > Basic

To enable or disable firewall, select the **Basic** option in the Firewall section.

In the **Basic** option, select whether or not you want to Enable or Disable the firewall settings of the **ESR300H**.



Firewall > Advanced

VPN Passthrough: Allows VPN (Virtual Private Network) packets to pass through the Firewall. If you are not using VPN, these options can be disabled. VPN L2TP Passthrough, VPN PPTP Passthrough, and VPN IPSec Passthrough are enabled by factory default for better security.

The screenshot displays the EnGenius Firewall configuration interface. The left sidebar shows the navigation menu with 'Advanced' highlighted. The main content area features a table with the following data:

Description	Select
VPN L2TP Pass-Through	<input checked="" type="checkbox"/>
VPN PPTP Pass-Through	<input checked="" type="checkbox"/>
VPN IPSec Pass-Through	<input checked="" type="checkbox"/>

Below the table are 'Apply' and 'Cancel' buttons. On the right, a 'TIPS' box contains the following text:

VPN Pass-Through: This router supports VPN pass-through which allows VPN (Virtual Private Network) packets to pass through the Firewall. If you are not using VPN, the options can be disabled.

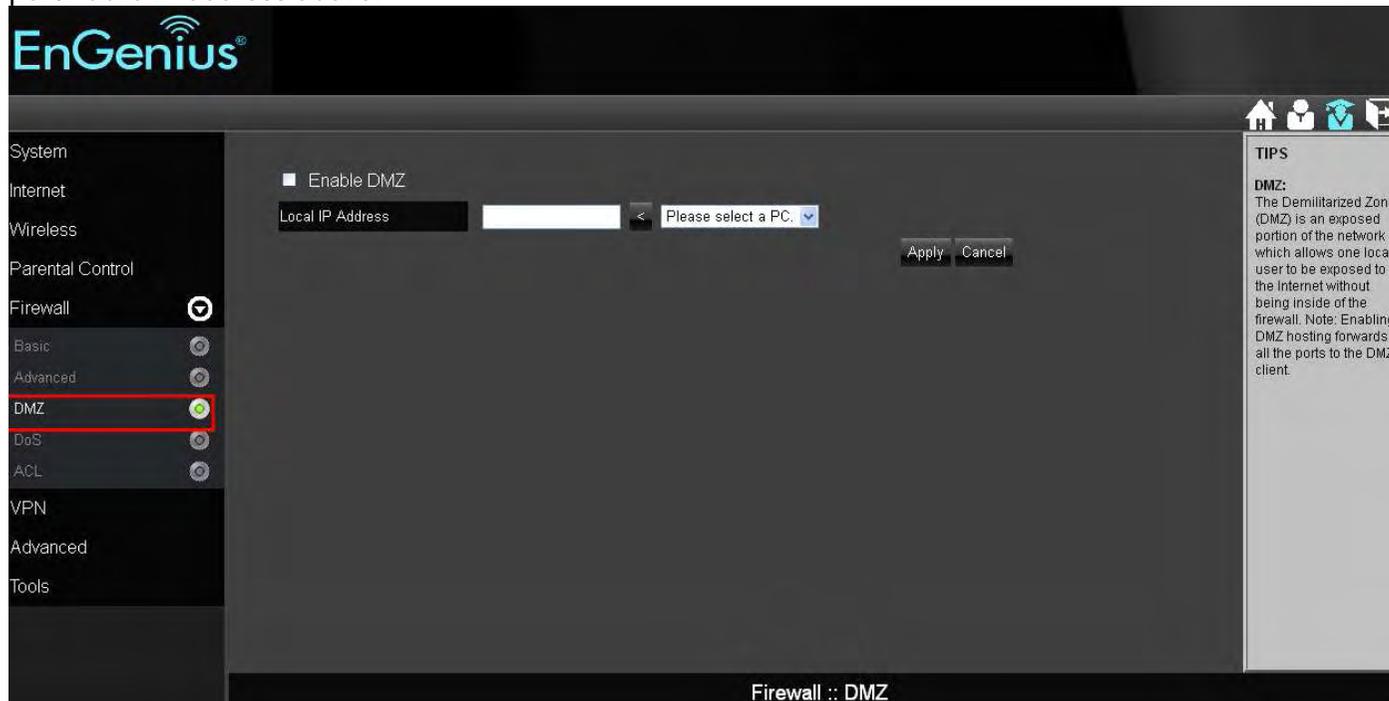
The status bar at the bottom of the page reads 'Firewall :: Advanced'.

Firewall > DMZ (Demilitarized Zone)

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to allow unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas a DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

A DMZ allows a computer to have all its connections and ports completely open during data transmission. **Warning: Computer will be completely vulnerable to any malicious attacks.**

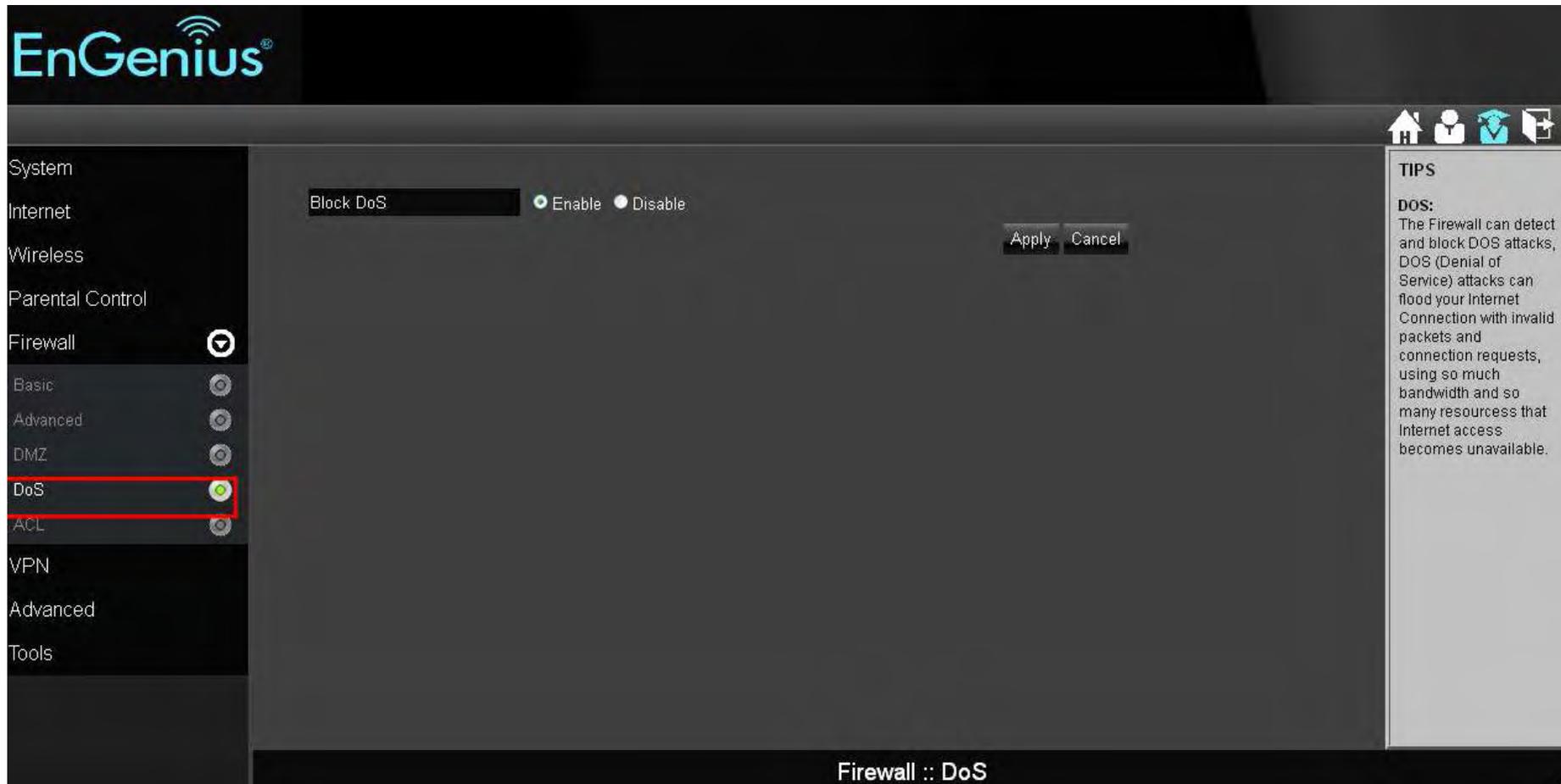
LAN IP Address: Fill-in the IP address of a particular host in your LAN Network that will receive all the packets originally going to the WAN port/Public IP address above.



Firewall > DoS (Denial of Service)

To enable blocking of DoS attacks, select the **DoS** option in the Firewall section.

DoS attacks can flood your internet connection with continuous transmission of data. Blocking these attack can ensure that the internet connection will always be available.



Firewall > ACL

To manage Parental Control settings (either through the Parental Control Wizard or the ACL option), select the ACL option in the Firewall section. Please refer to Parental Control Section for details.



EnGenius®

System
Internet
Wireless
Parental Control
Firewall **ACL**
Basic
Advanced
DMZ
DoS
VPN
Advanced
Tools

Enable Parental Control (Access Control)

Add Policy

Policy Table

Enable	Policy Name	Target Device	Schedule	Logged	Modify
<input checked="" type="checkbox"/>	Web Monitor	D1M0QTK1	Always	Yes	 
<input checked="" type="checkbox"/>	weekday		From 12:00 To 22:00--Mon, Tue, Wed, Thu, Fri	Yes	 
<input checked="" type="checkbox"/>	weekend		From 06:00 To 22:00--Sat, Sun	Yes	 

Apply Cancel

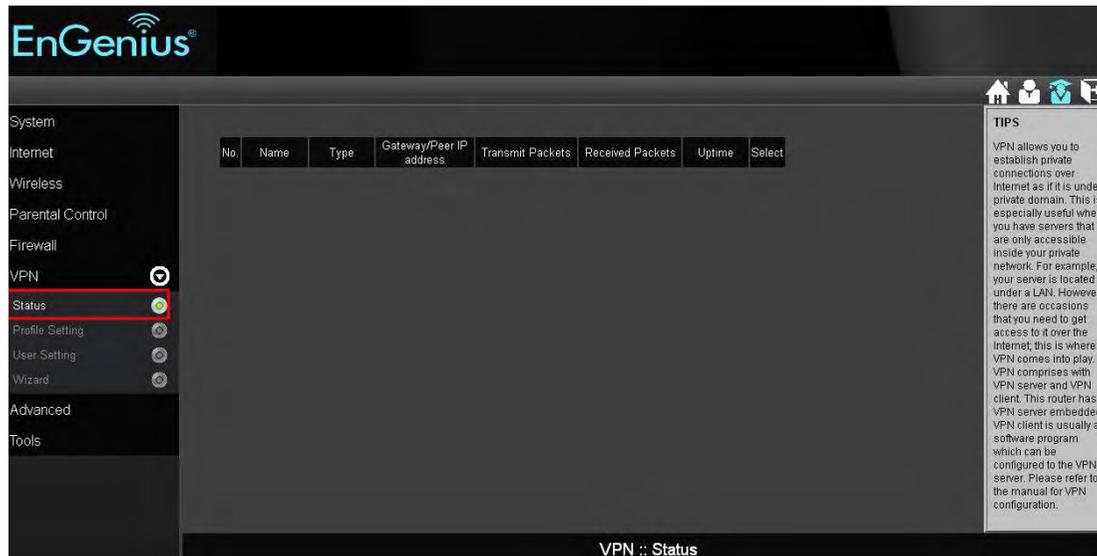
TIPS
Parental Control is a feature that allows parents to filter out and control the Internet access. By adding keywords, the parental control engine checks the web contents and make sure it does not contain the specified content. Also, parents can limit the Internet access within the specified time and day (this is known as Schedule). Policy is a rule profile which describes the keyword filter and Internet access schedule. For example, a policy can be created to filter out the pages containing "XXX" or "SEX". You can apply the policy to multiple users. Those users are known as the policy member. Parental control engine will screen these member user(s) based on the applied

10. VPN (Virtual Private Network) Section

VPN > Status

A Virtual Private Network (VPN) provides a secure connection between two remote locations or two users over the public Internet. It provides authentication to securely encrypt the data communicated between the two remote endpoints. The ESR300H supports up to 5 VPN tunnels, making it ideal for small-office and home-office (SOHO) users.

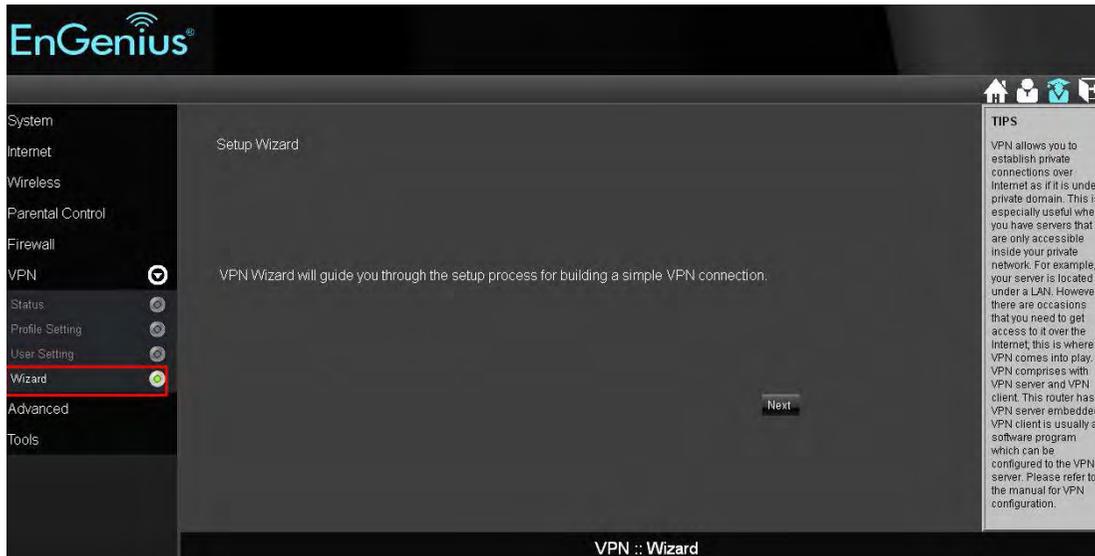
To view the status of your VPN tunnels that were configured on the **ESR300H**, select the Status option in the VPN section. The status table will show the name of the VPN, the VPN type, the Gateway/Peer IP address, how many packets have been transmitted and received, and how the VPN has been up.



You can set the VPN tunnels by either the user friendly **Wizard** or the manual **Profile Setting**. It is highly recommended to start with the **Wizard** to establish VPN tunnels. If you are an advanced user and would like to manually configure VPN Settings, select **Profile Setting** for advanced VPN setting.

VPN Wizard

Click **Next** to start VPN Wizard



Create a name for the VPN tunnel in the Name field. Click **Next**.

The screenshot shows the "Step 1: VPN Policy Name" configuration screen. It contains the text "Please enter the policy name" and a label "VPN policy name". Below the label is a text input field with the label "Name" and a placeholder "(eg: OfficeVPN)". At the bottom right of the screen are three buttons: "Back", "Next", and "Cancel".

You can select either **L2TP** or **PPTP** as the VPN Connection Type. Then click **Next**.

Step2: VPN Connection Type

Please choose VPN connection type

L2TP Choose this if you are using L2TP client for connection

PPTP Choose this if you are using PPTP client for connection

Back Next Cancel

L2TP Settings

User Name: Enter the user name used to connect to L2TP server

Password: Enter the password used to connect to L2TP server

VPN Server IP Setting

Server IP: Enter an IP address which is different from your router's LAN IP address. (example: the default LAN IP of ESR300H is 192.168.0.1. You could create a Server IP address as 10.0.174.45)

Remote IP Range: Enter an IP range under the same subnet as the above Server IP. (example: if your Server IP address is 10.0.174.45, you could create the remote IP Range as 10.0.174.66 – 100. The remote IP range should not include Server IP address to avoid duplicate IP Addresses within the same network.)

Click **Next**.

Step4: VPN L2TP Setting

Please enter the setting of L2TP

L2TP Settings

Authentication: MSCHAP_V2

User Name: (eg: guest)

password: (eg: nk9543)

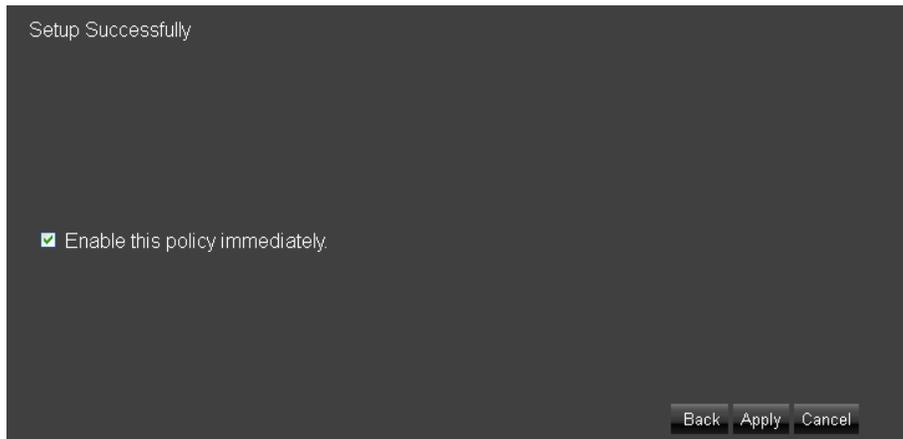
VPN Server IP Setting

Server IP: (eg: 10.0.174.45)

Remote IP Range: - (eg: 10.0.174.66 - 100)

Back Next Cancel

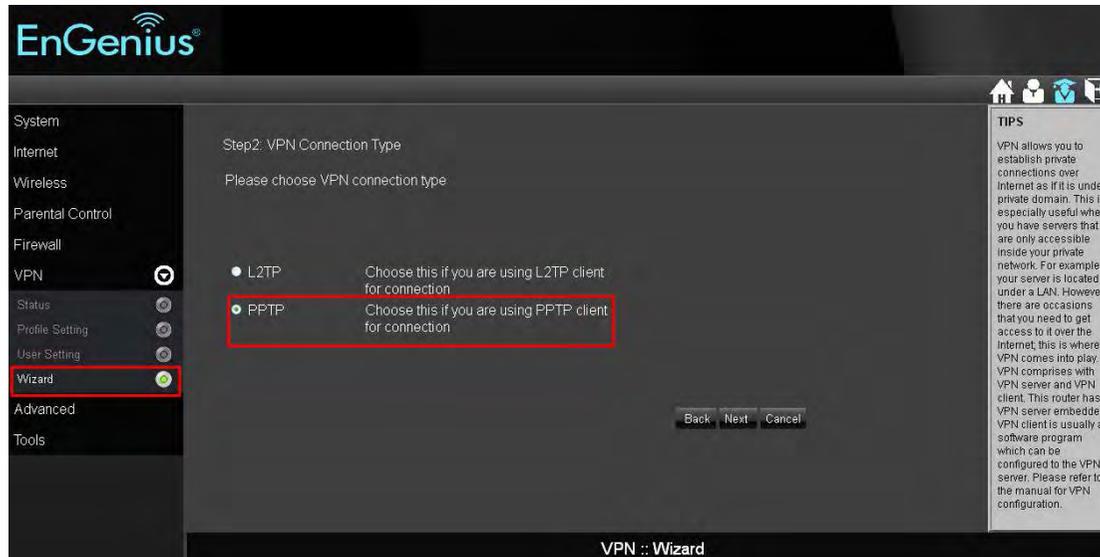
The L2TP VPN profile should be completed successfully. Click **Apply** to save the L2TP VPN Profile setting. To connect to the VPN tunnel, now you can use your native Windows VPN client to connect the L2TP tunnel.



PPTP Setting

If you want to setup a PPTP VPN tunnel, please select PPTP VPN Connection Type after selecting the Wizard in the VPN option.

Click **Next**.



User Name: Enter the user name to connect to the PPTP server

Password: Enter the password to connect to the PPTP server

VPN Server IP Setting

Server IP: Enter an IP address which is different from your router's LAN IP address. (example: the default LAN IP of ESR300H is 192.168.0.1. You could create a Server IP address as 10.0.174.45)

Remote IP Range: Enter an IP range under the same subnet of the above Server IP. (example: if your Server IP address is 10.0.174.45, you could create the remote IP Range as 10.0.174.66 – 100. The remote IP range should not include Server IP address to avoid duplicate IP addresses within the same network.)

Click **Next**.

Step4: VPN PPTP Setting

Please enter the setting of PPTP

PPTP Settings

Authentication

User Name (eg: guest)

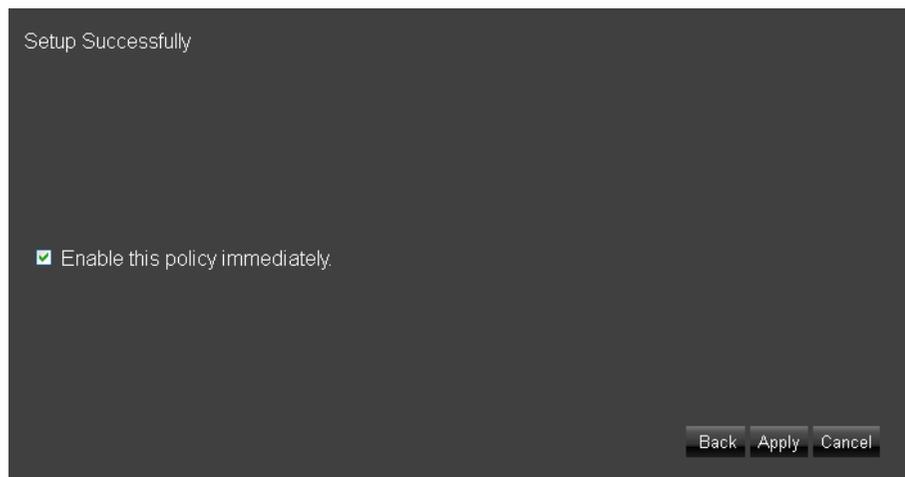
Password (eg: nk9543)

VPN Server IP Setting

Server IP (eg: 10.0.174.45)

Remote IP Range - (eg: 10.0.174.66 -100)

The PPTP VPN profile should be created successfully. Click **Apply** to save your setting. To connect VPN tunnel, now you can use your native Windows VPN client.



Profile Setting: If you wish to manually setup a VPN tunnel, you can go to **Profile Setting** in the VPN section. Before getting started, please select **User Setting** to create the user profile ahead of time.

User Setting:

Name: Enter the name to connect to L2TP or PPTP VPN tunnels.

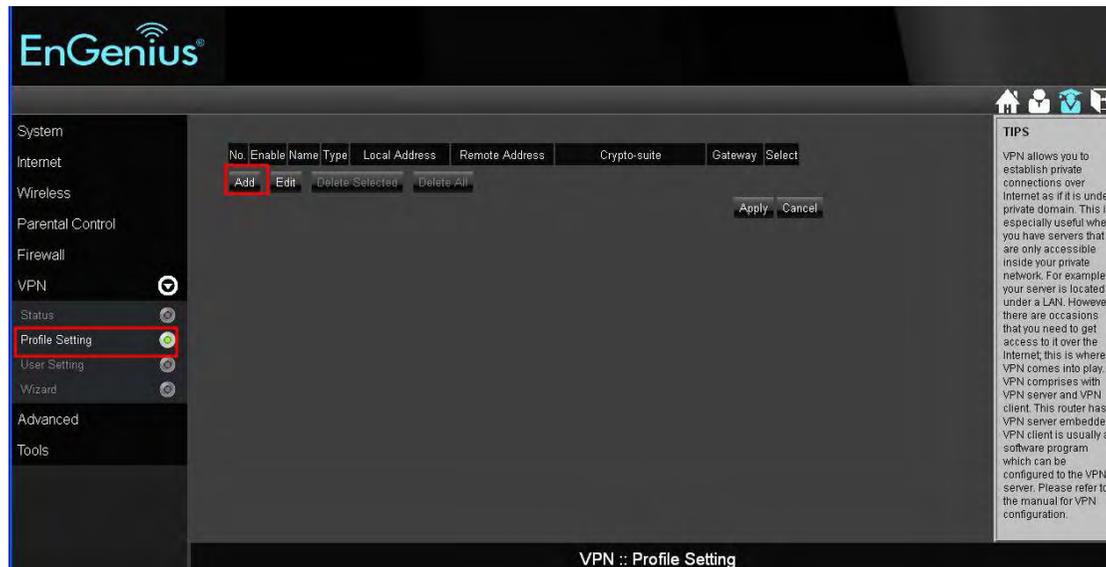
Password: Enter the password to connect to L2TP or PPTP VPN tunnels.

Confirm: Enter the password again to confirm the password entered above.

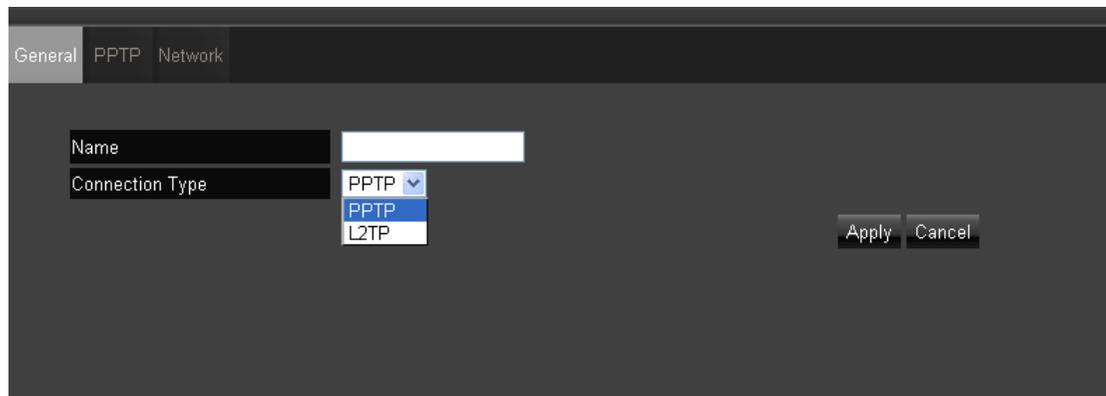
Click **Add** to enter the VPN user to the **Current VPN User Table**.



After completing the **User Setting**, please go to **Profile Setting** to start a manual VPN tunnel configuration. Click **Add** to get started.



In the **General** tab, enter a name for the VPN tunnel in the Name field. Select PPTP or L2TP for the **Connection Type**.

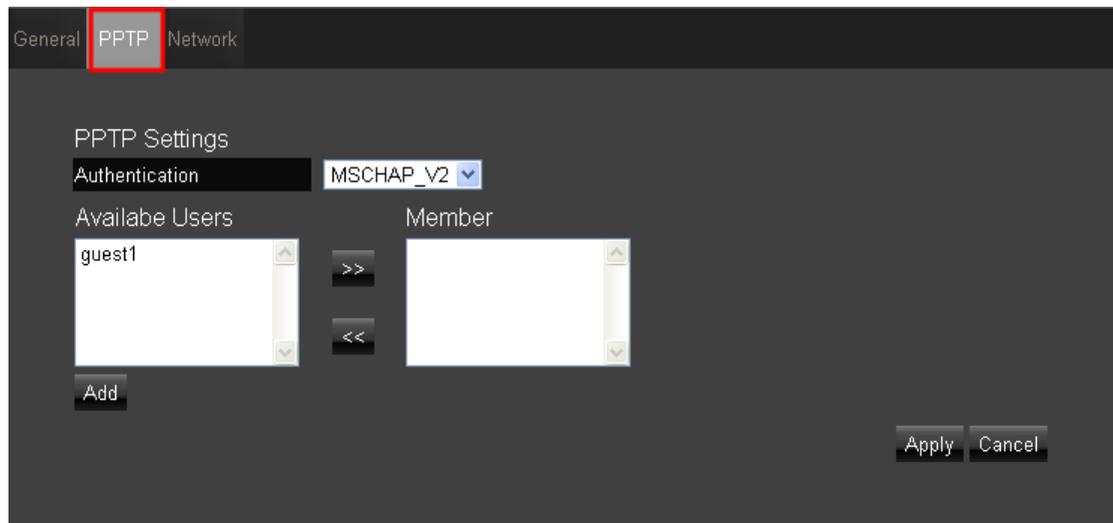


PPTP through Profile Setting

If you select PPTP as VPN Connection Type, go to PPTP tab.

Authentication: There are three authentication algorithms. Please select CHAP, PAP, or MSCHAP_V2.

Available Users: The users who you created in the User Setting to connect to PPTP server will be displayed. Select the users in the list who you wish to include in the VPN tunnel, and click the forward arrow to then add them to the **Member Box**. Click the backward arrow if you want to remove users from the **Member box**.



Go to the **Network** tab.

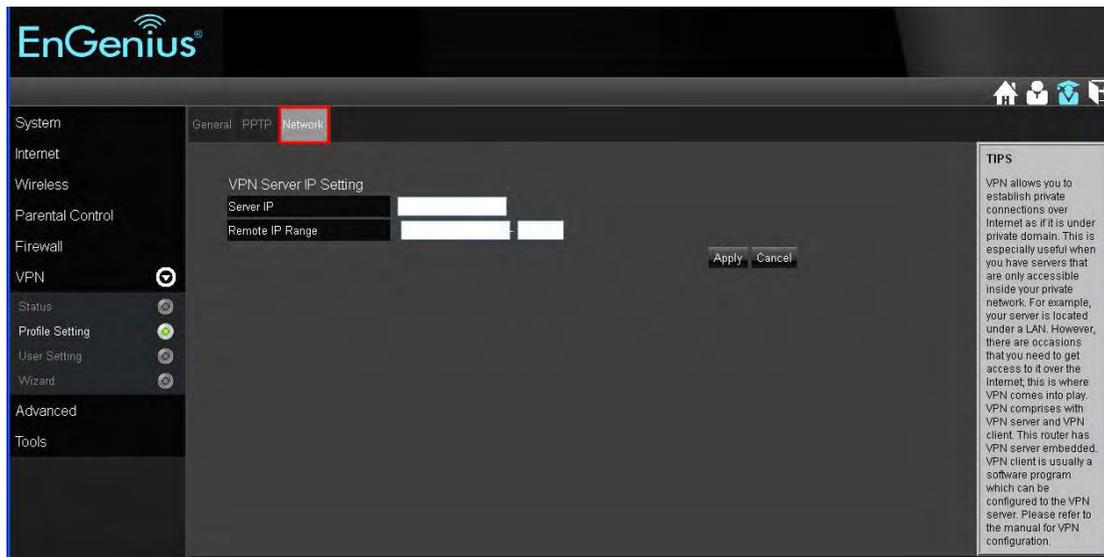
VPN Server IP Setting

Server IP: Enter an IP address which is different from your router's LAN IP address. (example: the default LAN IP of ESR300H is 192.168.0.1. You could create a Server IP address as 10.0.174.45)

Remote IP Range: Enter an IP range under the same subnet of the above Server IP. (example: if your Server IP address is 10.0.174.45, you could create the remote IP Range as 10.0.174.66 – 100. The remote IP range should not include Server IP address to avoid duplicate IP Addresses within the same network.)

Click **Apply** to save the PPTP VPN profile setting.

To connect to the VPN tunnel, you can use your native Windows VPN client.



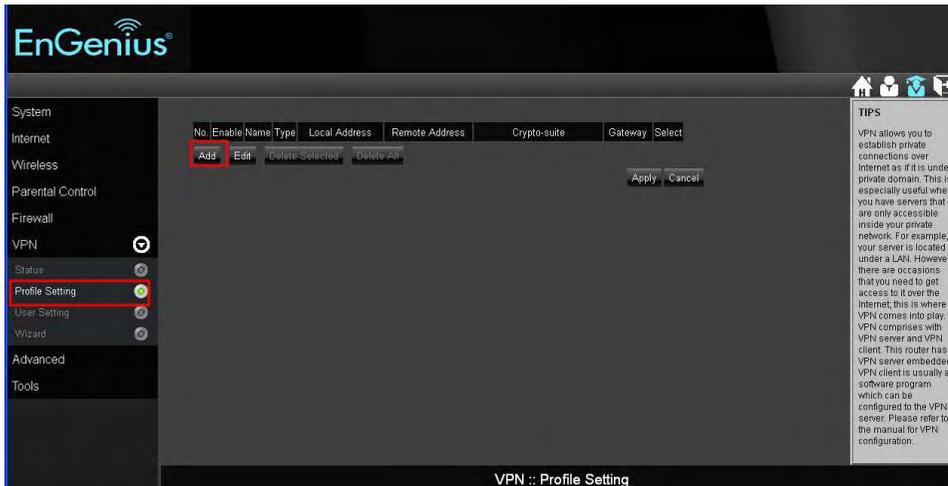
No.	Enable	Name	Type	Local Address	Remote Address	Crypto-suite	Gateway	Select
1	<input type="checkbox"/>	EnGenius	PPTP	192.168.0.0/24	10.1.1.10-20	N/A	10.1.1.1	<input type="checkbox"/>

Add Edit Delete Selected Delete All

Apply Cancel

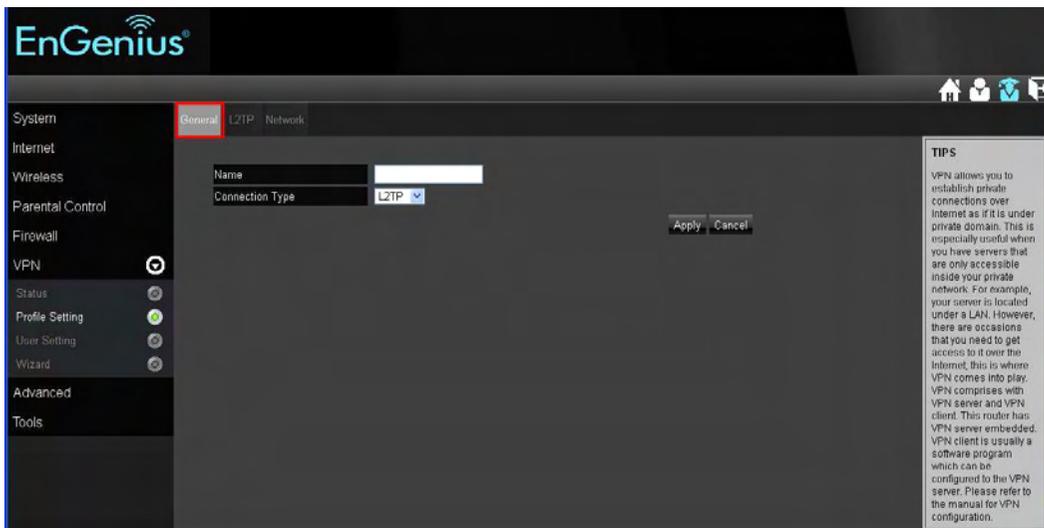
L2TP through Profile Setting

Click **Add** in the Profile Setting to start a L2TP VPN profile setting



Go to the **General** tab. Enter the L2TP profile name in the Name Field.

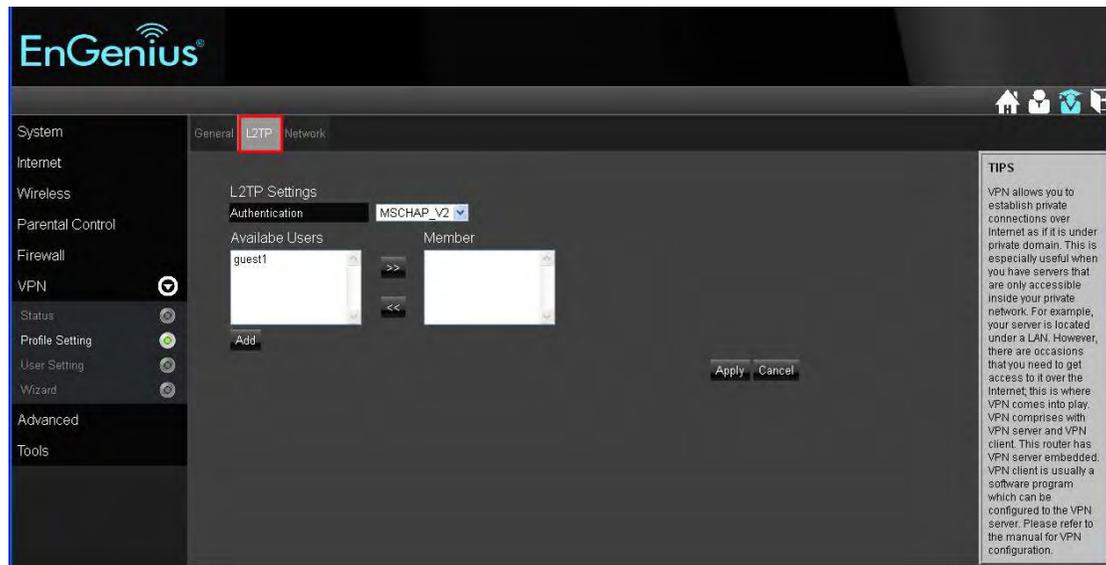
Select **L2TP** as the Connection Type.



Then go to the **L2TP** tab

Authentication: there are three authentication algorithms. Please select CHAP, PAP, or MSCHAP_V2.

Available Users: The users who you created in the User Setting to connect to PPTP server will be displayed. Select the users in the list who you wish to include in the VPN tunnel, and click the forward arrow to then add them to the **Member Box**. Click the backward arrow if you want to remove users from the **Member box**.



Go to the **Network** tab

VPN Server IP Setting

Server IP: enter an IP address which is different from your router's LAN IP address. (example: the default LAN IP of ESR300H is 192.168.0.1. You could create a Server IP address as 10.2.2.1)

Remote IP Range: enter an IP range under the same subnet of the above Server IP. (example: if your Server IP address is 10.2.2.1, you could create the remote IP Range as 10.2.2.10 – 20. The remote IP range should not include Server IP address to avoid duplicate IP addresses within the same network.)

Click **Apply** to save the L2TP VPN profile setting.

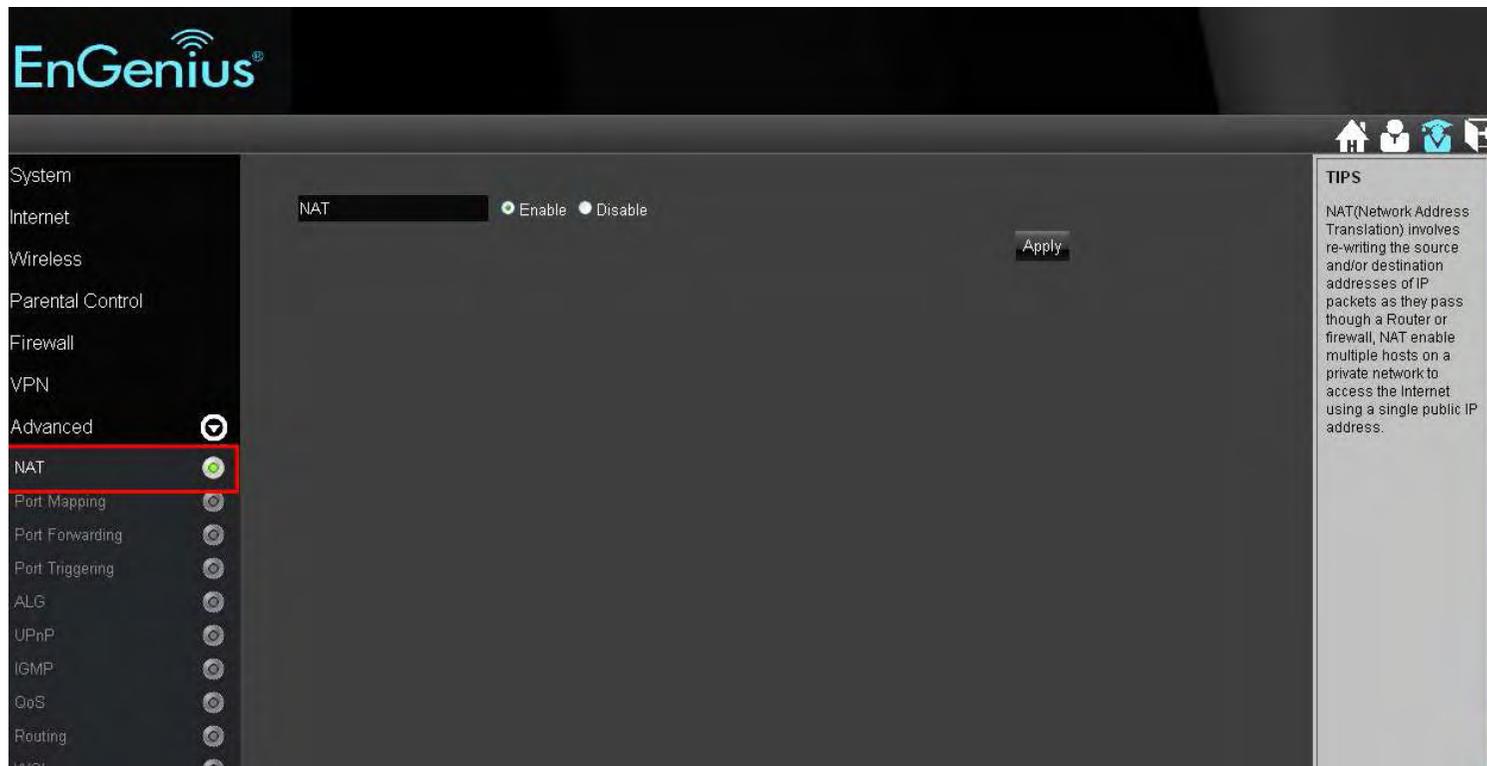
To connect to the VPN tunnel, you can use your native Windows VPN client.

11. Advanced Section

To access the **Advanced** section of the Expert Menu, select **Advanced** on the left hand side.

Advanced > NAT (Network Address Translation)

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP.

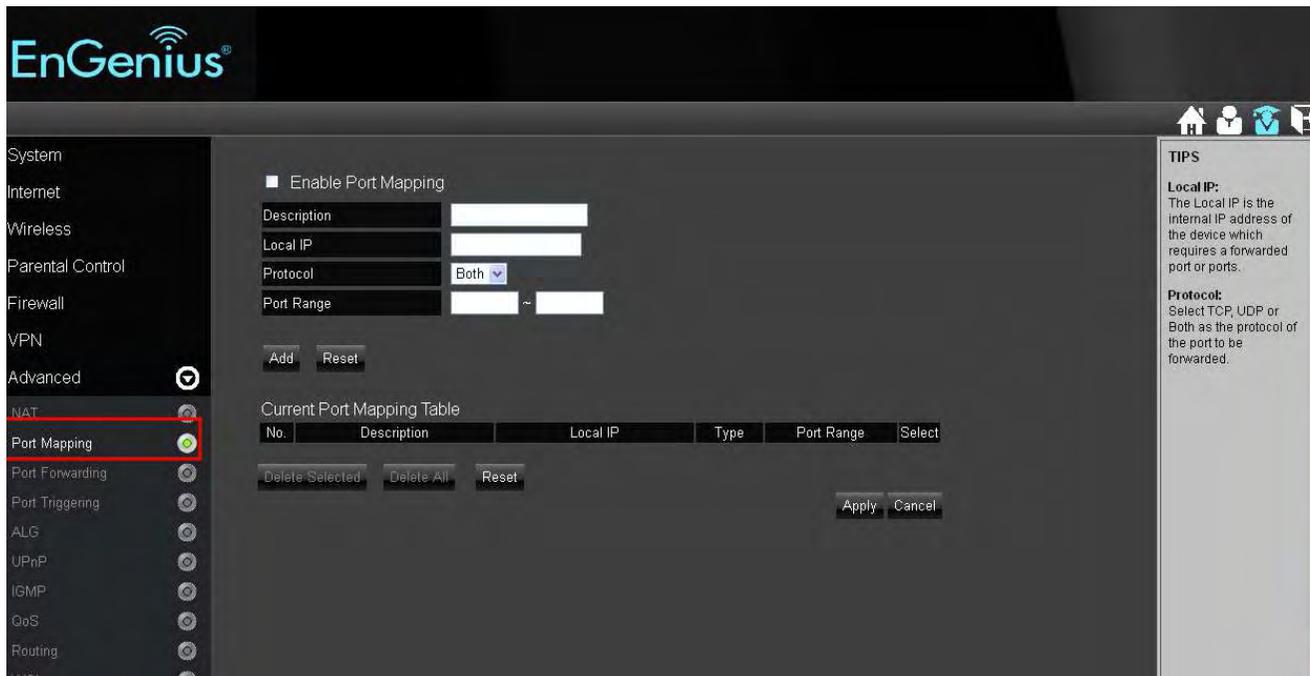


Advanced > Port Mapping

Port Mapping allows you to re-direct a particular range of service port numbers (from the Internet / WAN Port) to a particular LAN IP address.

1. **Enable Port Mapping:** Mark the checkbox to Enable Port Mapping.
2. **Description:** Enter the description on why the ports will be mapped.
3. **Local IP:** The local IP address of the server behind the NAT firewall.
4. **Protocol:** Select whether TCP, UDP, or Both ports will be mapped.
5. **Port Range:** Enter the range of ports to be forwarded to the private IP.

Click **Add** when finished with the configuration. Then the added **Port Mapping** setting will be listed on the **Current Port Mapping Table**. Click **Apply** to enable your setting.



Advanced > Port Forwarding

Use the **Port Forwarding** (Virtual Server) function when you want different servers/clients in your LAN to handle different internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use port numbers to recognize a particular internet application type. The Virtual Server allows you to re-direct a particular port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. Enable Port Forwarding: Mark the checkbox to Enable Port Forwarding.

1. **Description:** Enter the description on why the ports will be forwarded.
2. **Local IP:** Enter the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.
3. **Protocol:** Select whether TCP, UDP, or Both ports will be forwarded.
4. **Local Port:** This is the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.
5. **Public Port:** Port number will be changed to Local Port when the packet enters your LAN Network.



The screenshot displays the EnGenius web interface for configuring Port Forwarding. The left sidebar shows the navigation menu with 'Port Forwarding' highlighted in red. The main content area features a configuration form with the following fields:

- Enable Port Forwarding
- Description: [Text Input]
- Local IP: [Text Input]
- Protocol: [Both (Dropdown)]
- Local Port: [Text Input]
- Public Port: [Text Input]

Below the form are 'Add' and 'Reset' buttons. A table titled 'Current Port Forwarding Table' is shown below the form:

No.	Description	Local IP	Local Port	Type	Public Port	Select
-----	-------------	----------	------------	------	-------------	--------

Below the table are 'Delete Selected', 'Delete All', and 'Reset' buttons. At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons. A 'TIPS' sidebar on the right provides additional information:

TIPS

Local IP: The Local IP is the internal IP address of the device which requires a forwarded port or ports.

Protocol: Select TCP, UDP or Both as the protocol of the port to be forwarded.

Advanced > Port Triggering (Special Application)

Some applications require multiple connections, such as online games, videoconferencing, VoIP telephony and etc. You can configure port triggering function to support multiple connections if more than one local computer needs port forwarding for the same application or your application needs to open incoming ports that are different from the outgoing port.

1. **Enable Port Triggering:** Mark the checkbox to Enable Port Triggering.
2. **Description:** Enter the description on why the ports will be triggered.
3. **Popular Applications:** Select from default applications or add new applications in which to have their ports triggered.
4. **Trigger Port:** Enter the outgoing (Outbound) range of port numbers for your application.
5. **Trigger Type:** Select whether TCP, UDP, or Both for the outbound port trigger protocol.
6. **Public Port:** Enter the In-coming (Inbound) port or port range for your application (e.g. 2300-2400, 47624).
7. **Public Type:** Select whether TCP, UDP, or Both the for In-coming (Inbound) port trigger protocol (e.g. 2300-2400, 47624)

Once the setting of the triggered port is complete, it will be listed on the Current Trigger-Port Table.

The screenshot displays the EnGenius web interface for configuring Port Triggering. The left sidebar shows the navigation menu with 'Port Triggering' highlighted in red. The main content area features a configuration form with the following fields:

- Enable Trigger Port
- Description: [Text input field]
- Popular Applications: [Dropdown menu] Select an application [Add button]
- Trigger Port: [Text input field] ~ [Text input field]
- Trigger Type: [Dropdown menu] Both
- Public Port: [Text input field]
- Public Type: [Dropdown menu] Both

Below the form are 'Add' and 'Reset' buttons. The 'Current Trigger-Port Table' is currently empty. At the bottom of the table area are 'Delete Selected', 'Delete All', and 'Reset' buttons. To the right of the configuration area is a 'TIPS' sidebar with the following text:

TIPS
You can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. The outbound traffic triggers to which ports inbound traffic is directed.

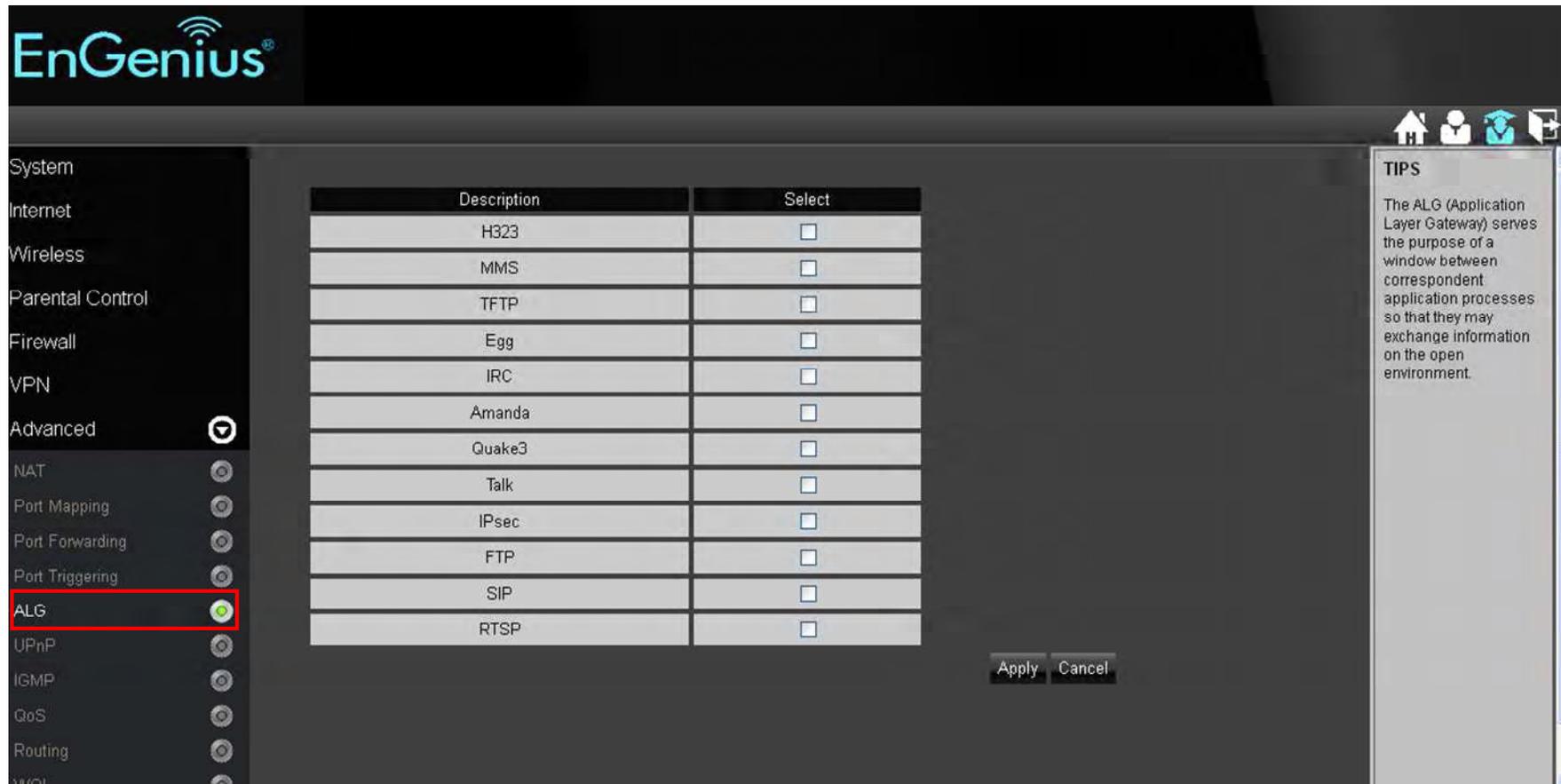
Popular applications:
Select an application which you desire to enable port triggering for.

Public Port:
This is the inbound (incoming) port for the selected application.

Advanced > ALG (Application Layer Gateway)

The **ALG** (Application Layer Gateway) serves as a window between correspondent application processes so that they may exchange information on an open environment.

Select the listed applications that need **ALG** support and then the router will authorize them to pass through the NAT gateway. Then click Apply.



The screenshot shows the EnGenius web interface. On the left sidebar, the 'Advanced' menu is expanded, and 'ALG' is selected and highlighted with a red box. The main content area displays a table with the following data:

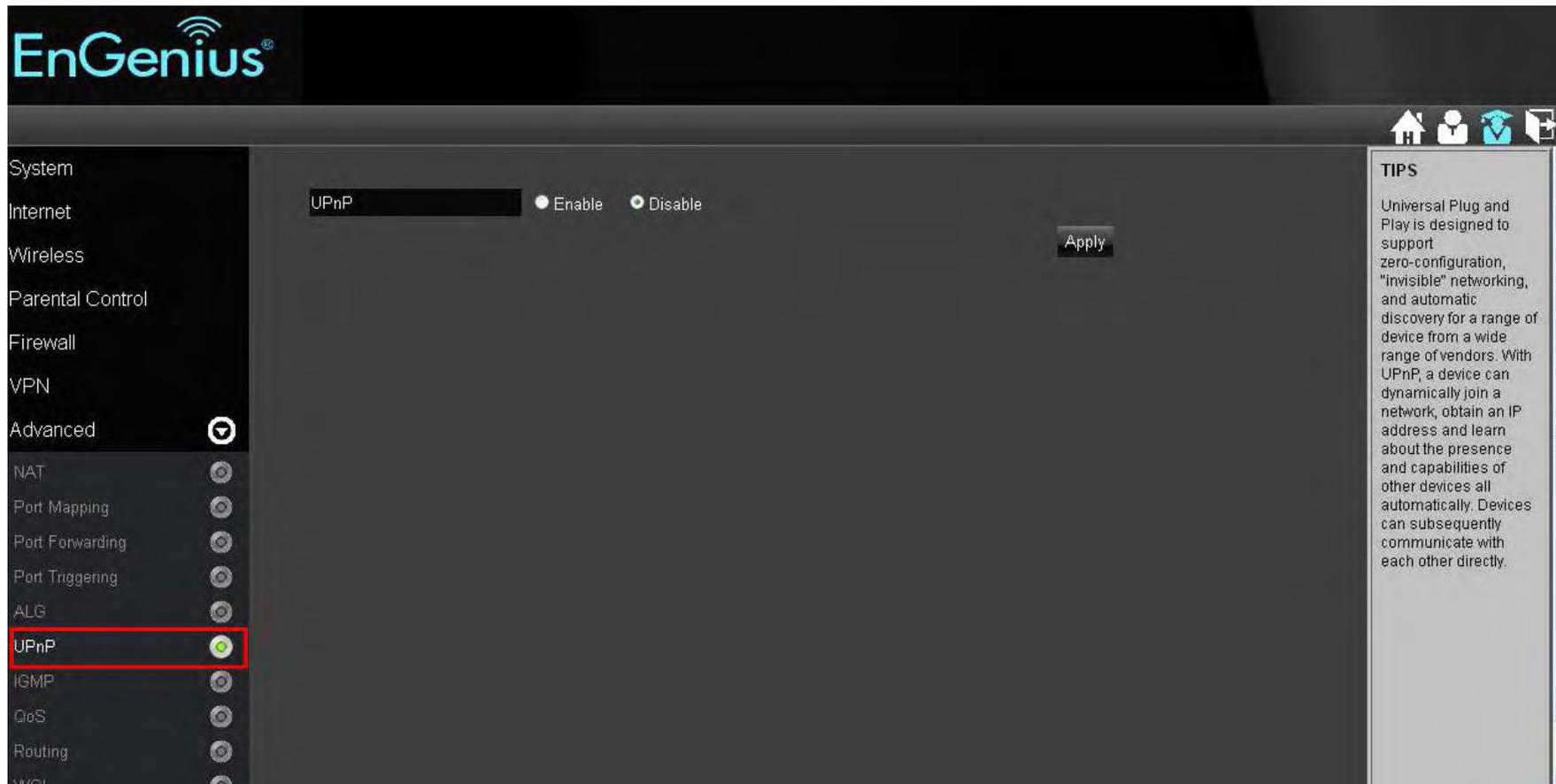
Description	Select
H323	<input type="checkbox"/>
MMS	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
Egg	<input type="checkbox"/>
IRC	<input type="checkbox"/>
Amanda	<input type="checkbox"/>
Quake3	<input type="checkbox"/>
Talk	<input type="checkbox"/>
IPsec	<input type="checkbox"/>
FTP	<input type="checkbox"/>
SIP	<input type="checkbox"/>
RTSP	<input type="checkbox"/>

At the bottom right of the table area, there are 'Apply' and 'Cancel' buttons. On the right side of the interface, there is a 'TIPS' box containing the following text:

TIPS
The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

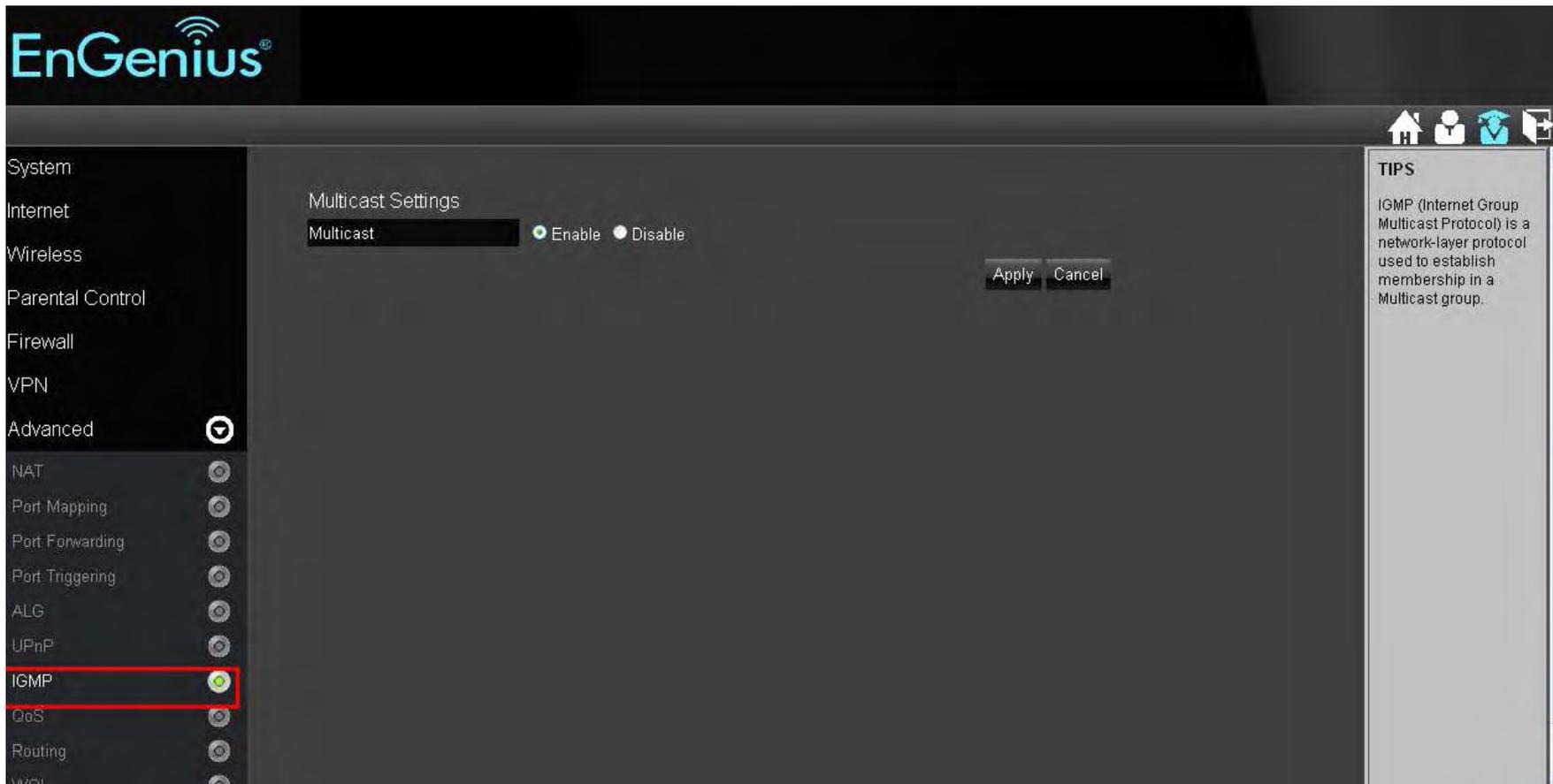
Advanced > UPnP (Universal Plug and Play)

UPnP helps internet devices, such as gaming and videoconferencing to access the network and connect to other registered UPnP devices



Advanced > IGMP (Internet Group Multicast Protocol)

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group.



The screenshot displays the EnGenius web management interface. On the left, a navigation menu lists various settings categories: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced (highlighted with a checkmark), NAT, Port Mapping, Port Forwarding, Port Triggering, ALG, UPnP, IGMP (highlighted with a red box and a green checkmark), QoS, Routing, and WLAN. The main content area is titled "Multicast Settings" and features a "Multicast" dropdown menu, two radio buttons for "Enable" (selected) and "Disable", and "Apply" and "Cancel" buttons. On the right side, a "TIPS" section provides a brief explanation: "IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group."

Advanced > QoS (Quality of Service)

Total Bandwidth Settings

QoS can prioritize the bandwidth use such as video streaming, online gaming, VoIP telephony, videoconferencing, and etc. to ensure the stable and efficient performance of the network.

Total Bandwidth Settings: You can specify the maximum value of the outgoing bandwidth of UpLink and Downlink for the application by selecting the speed from drop-down menus.

The screenshot displays the EnGenius web management interface. On the left is a navigation menu with categories: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced (expanded), NAT, Port Mapping, Port Forwarding, Port Triggering, ALG, UPnP, IGMP, QoS (highlighted with a red box), Routing, and WAN. The main content area is titled 'Total Bandwidth Settings' and shows 'Uplink' and 'Downlink' both set to 'Full' via dropdown menus. Below this, the 'QoS' section has three radio buttons: 'Priority Queue' (unselected), 'Bandwidth Allocation' (unselected), and 'Disabled' (selected). 'Apply' and 'Cancel' buttons are at the bottom right of the settings area. On the far right, a 'TIPS' sidebar contains three sections: 'Priority Queue' (explaining bandwidth priority), 'Bandwidth Allocation' (explaining bandwidth allocation), and 'Local IP Range' (explaining the internal IP address range).

QoS Type

Priority Queue:

- **Unlimited Priority Queue**

- Local IP Address: Enter the Local IP address which will have the highest priority to stream data and will not be bounded by the QoS limitation.
- High/Low Priority Queue: Specify the priority for different protocol. You can add and priority the desired protocol on the table.

EnGenius

Internet
Wireless
Parental Control
Firewall
VPN
Advanced
NAT
Port Mapping
Port Forwarding
Port Triggering
ALG
UPnP
IGMP
QoS
Routing
WOL
Tools

Total Bandwidth Settings
Uplink Full
Downlink Full

QoS Priority Queue Bandwidth Allocation Disabled

Unlimited Priority Queue

Local IP Address	Description
<input type="text"/>	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	<input type="radio"/>	<input type="radio"/>	20,21
HTTP	<input type="radio"/>	<input type="radio"/>	80
TELNET	<input type="radio"/>	<input type="radio"/>	23
SMTP	<input type="radio"/>	<input type="radio"/>	25
POP3	<input type="radio"/>	<input type="radio"/>	110
Name <input type="text"/>	<input type="radio"/>	<input type="radio"/>	Both <input type="text"/> ~ <input type="text"/>
Name <input type="text"/>	<input type="radio"/>	<input type="radio"/>	Both <input type="text"/> ~ <input type="text"/>
Name <input type="text"/>	<input type="radio"/>	<input type="radio"/>	Both <input type="text"/> ~ <input type="text"/>

Priority Queue:
As a feature of Quality of Service (QoS), bandwidth priority may be set to either High or Low for a local host or particular protocols and ports. Those hosts or protocols with a priority of High will be processed first.

Bandwidth Allocation:
You can allocate the maximum or minimum amount of bandwidth for a particular protocol.

Local IP Range:
This is the internal IP address range of the computers with QoS enabled.

Bandwidth Allocation: You can set the bandwidth allocation type (download and/or upload). You must provide the IP and Port ranges and select the type of protocol, policy, and rate (bps).

- **Type:** select Download or Upload which you want to reserve or limit the bandwidth
- **Local IP Range:** Enter the local IP range you wish to specify the bandwidth allocation.
- **Protocol:** Select the protocol you wish to reserve or limit the bandwidth
- **Port Range:** Enter the port range you wish to reserve or limit the bandwidth.
- **Policy:** Select either the Minimum or Maximum bandwidth you wish to specify
- **Rate (bps):** Select the desired bandwidth you would like to reserve or limit.

When the configuration is complete, click Add and your setting will be listed on the Current QoS Table.

The screenshot shows the EnGenius web interface for QoS configuration. The 'Bandwidth Allocation' radio button is selected and highlighted with a red box. The configuration fields are: Uplink (Full), Downlink (Full), QoS (Bandwidth Allocation), Type (Download), Local IP range (empty), Protocol (ALL), Port Range (1 ~ 65535), Policy (Min), and Rate(bps) (Full). Below the configuration are 'Add' and 'Reset' buttons. At the bottom, there is a 'Current QoS Table' with columns: No., Type, Local IP range, Protocol, Port Range, Policy, Rate(bps), and Select. Below the table are 'Delete Selected', 'Delete All', and 'Reset' buttons.

Disable **QoS** if you do not want to prioritize any data or protocol.

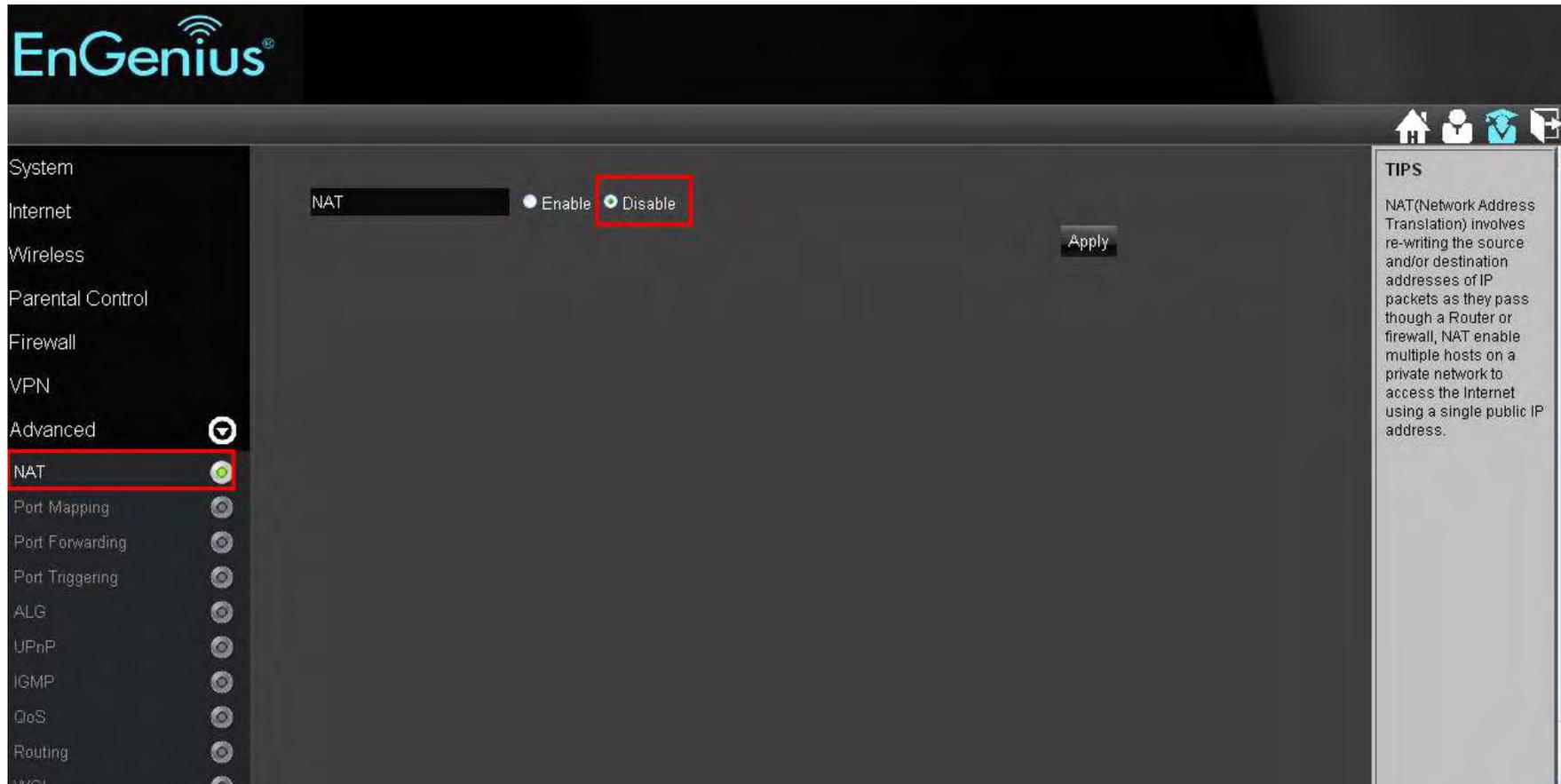
The screenshot shows the EnGenius web interface for configuring QoS. On the left is a navigation menu with categories: Internet, Wireless, Parental Control, Firewall, VPN, Advanced (selected), NAT, Port Mapping, Port Forwarding, Port Triggering, ALG, UPnP, IGMP, QoS (highlighted), Routing, WOL, and Tools. The main content area is titled 'Advanced :: QoS' and includes 'Total Bandwidth Settings' with 'Uplink' and 'Downlink' both set to 'Full'. Under 'QoS', three radio buttons are present: 'Priority Queue', 'Bandwidth Allocation', and 'Disabled' (which is selected and highlighted with a red box). 'Apply' and 'Cancel' buttons are located at the bottom right of the settings area. On the far right, a help sidebar contains information about 'Priority Queue', 'Bandwidth Allocation', and 'Local IP Range'.

Click **Apply** to save your settings.

Advanced > Routing

Typically you do not need to setup static routing since the ESR300H usually has adequate routing information after it has been configured for Internet access. You will only need to set up static routing if the router is connected with a network under a different subnet and you need the static routing to allow network connection in two different subnets.

Note: To enable a static routing, you need to disable the NAT function.



1. **Enable Static Routing:** Mark the checkbox to Enable Static Routing.
2. **Destination LAN IP:** Enter the static IP Address of the remote network to which you want to setup a static route.
3. **Subnet Mask:** Enter the Subnet Mask of the remote network to which you want to setup a static route.
4. **Default Gateway:** Enter the IP address of the Default Gateway which can connect your router with the remote network through the assigned static route.
5. **Hops:** Enter the maximum hops number of the assigned static route.
6. **Interface:** Enter the routing interface (LAN or WAN).

If you would like to enable Static Routing, please disable NAT function. Thus the packets can be forwarded based upon your routing policies.

Enable Static Routing

Destination LAN IP:

Subnet Mask:

Default Gateway:

Hops:

Interface: LAN

Current Static Routing Table

No.	Destination LAN IP	Subnet Mask	Default Gateway	Hops	Interface	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>						

TIPS

If the router is connected with a network under the different subnet, the routing setup allows the network connection in two different subnets.

Destination LAN IP:
This is the LAN IP address of the destination.

Subnet Mask:
This is the Subnet Mask of the destination.

Default Gateway:
This is the IP address of the Default Gateway for this destination LAN IP address and Subnet.

Hops:
This is the maximum number of hops in the static routing that a packet is allowed to travel.

Advanced > WOL (Wake on LAN)

WOL allows you to turn on a computer through the router. You will just need to provide the Server Port as well as the MAC address of the computer to utilize this feature.

The screenshot shows the EnGenius router's web interface. The left sidebar contains a menu with the following items: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced (highlighted with a checkmark), NAT, Port Mapping, Port Forwarding, Port Triggering, ALG, UPnP, IGMP, QoS, Routing, and WOL (highlighted with a red box). The main content area is titled 'WOL' and features the following settings:

- Enable WOL over WAN
- Server Port:
- Wake On LAN section:
 - Wake MAC Address:
 - Start button
- Apply button
- Reset button

On the right side, there is a 'TIPS' section with the following text:

TIPS
Wake on LAN (WOL) is a way to switch on a computer that is connected to a network. You make use this router to wake up a WOL-enabled computer using this feature. Enter the MAC address of the PC/Laptop and then click on [Start] to wake up the computer under sleeping mode. Your target PC/laptop motherboard must support WOL in order to use this function.

12. Tools Section

Tools > Admin

In the **Admin** option of the Tools section, you can change the password used to log in to the router at the login screen by entering the old password, followed by the new password twice. You can also allow only one computer to edit the settings on the **ESR300H** by supplying its static IP address.

Remote Management: This allows you to designate a host on the internet to configure the Broadband router and check the router's status from a remote site.

Select **Enable** to enable remote management.

Host Address: Enter the designated host IP Address in the Host IP Address field.

Port: Enter the port number for remote accessing management web interface. The default Port for remote management is 8080.

Click **Apply** to save the settings.

To access the settings of the ESR300H remotely, enter the router's WAN IP address and port number of the ESR300H. For example, if your router's WAN IP address is 24.24.247.100, and the default port number for remote access is selected, type in <http://24.24.247.100:8080> in the address bar of your browser and click Enter to start the remote access.

- System
- Internet
- Wireless
- Parental Control
- Firewall
- VPN
- Advanced
- Tools
- Admin**
- Time
- DDNS
- Diagnosis
- Firmware
- Back-up
- Reset

You can change the password that you use to access the router, this is not your ISP account password.

Old Password	<input type="password"/>
New Password	<input type="password"/>
Repeat New Password	<input type="password"/>

Host Address	port	Enable
<input type="text"/>	8080	<input type="checkbox"/>

Apply Cancel

TIPS

By enabling the remote management, users can access the Web-based management interface.

Host Address:

Leave this field blank to allow any host to perform remote management. Otherwise, specify a Host Address to allow only one host to access remote management on the router.

Port:

This is the port used for remote management. The default port for remote management is 8080.

Tools > Time

In the **Time** option of the Tools section, you can change the current time on the **ESR300H**. Enter the web address of the Network Time Protocol you want to have the **ESR300H** to match time with or have it synchronize with the PC accessing the **ESR300H**. You can also enable Daylight Savings.

The screenshot displays the EnGenius web management interface for the ESR300H device. The left sidebar contains a navigation menu with the following items: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, Tools (highlighted with a green circle), Admin, Time (highlighted with a red rectangle), DDNS, Diagnosis, Firmware, Back-up, and Reset. The main content area is titled 'Tools :: Time' and contains the following configuration options:

- Time Setup:** A dropdown menu set to 'Synchronize with the NTP Server'.
- Time Zone:** A dropdown menu set to '(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'.
- NTP Time Server:** An empty text input field.
- Enable Daylight Saving:** An unchecked checkbox.
- Start Time:** A series of dropdown menus set to 'January', '1st', 'Mon', and '12 am'.
- End Time:** A series of dropdown menus set to 'January', '1st', 'Mon', and '12 am'.

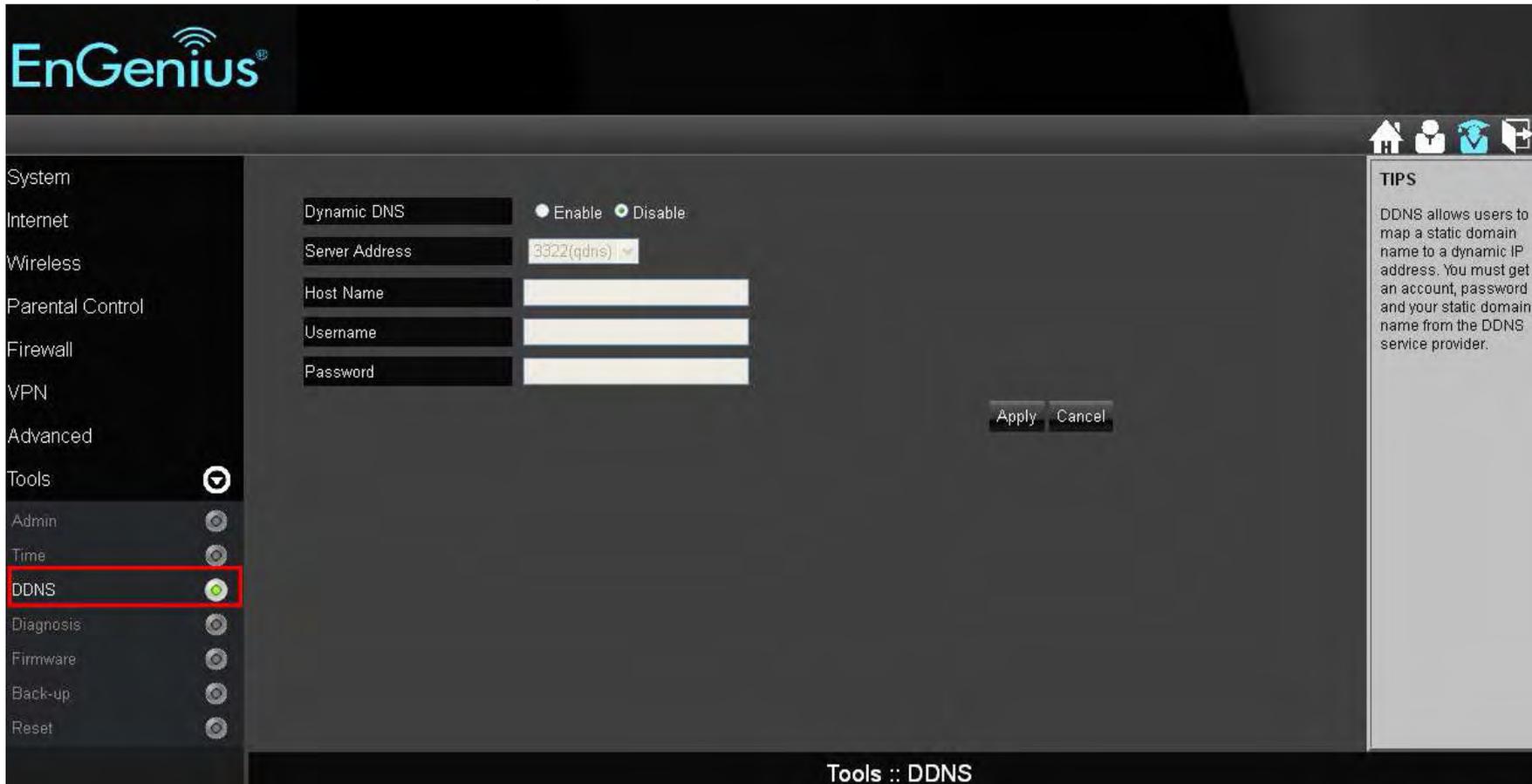
At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons. On the right side of the interface, there is a 'TIPS' section with the following text:

TIPS
NTP Time Server:
Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a time server on the Internet.

Tools > DDNS (Dynamic DNS)

DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password, and static domain name from the DDNS service provider such as DynDNS, ZoneEdit, CyberGate, and etc. to use this feature. DDNS benefits end users when they have their own websites or FTP sites.

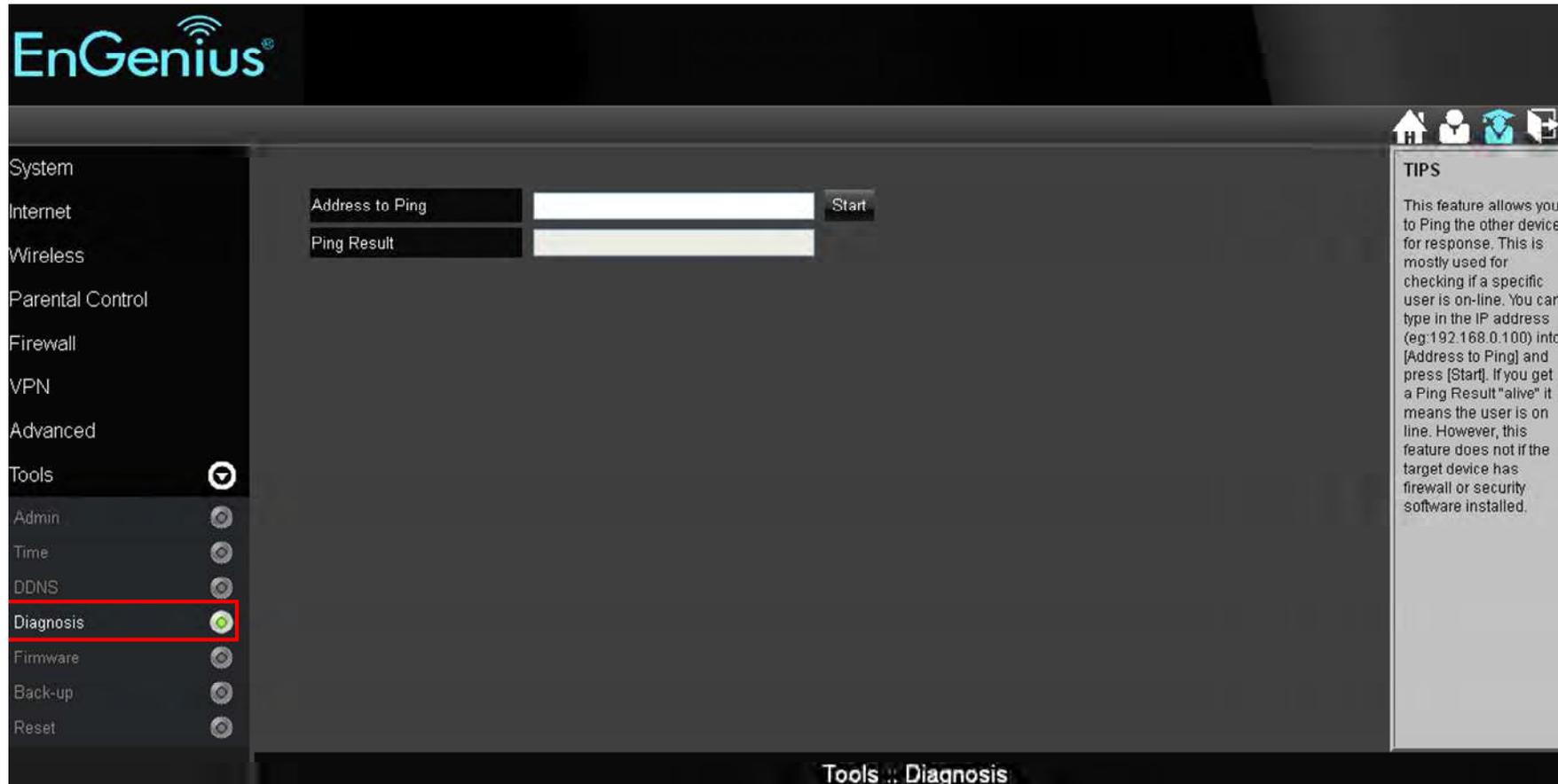
1. **Dynamic DNS:** Choose to Enable or Disable this feature.
2. **Server Address:** Select the Server Address in which to obtain the Dynamic DNS.
3. **Host Name:** Enter the static domain name which applies DDNS.
4. **Username:** Enter the username which you are given by DDNS service provider
5. **Password:** Enter the password you assign for your DDNS account



The screenshot shows the EnGenius web interface for configuring DDNS. The left sidebar contains a menu with categories: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, Tools (expanded), Admin, Time, DDNS (highlighted with a red box), Diagnosis, Firmware, Back-up, and Reset. The main content area is titled 'Dynamic DNS' and features a radio button selection for 'Enable' (selected) and 'Disable'. Below this are input fields for 'Server Address' (with a dropdown menu showing '3322(qdns)'), 'Host Name', 'Username', and 'Password'. 'Apply' and 'Cancel' buttons are located at the bottom right of the form. A 'TIPS' box on the right side of the page provides additional information: 'DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service provider.' The footer of the page reads 'Tools :: DDNS'.

Tools > Diagnosis

In the **Diagnosis** option of the Tools section, you can enter an IP Address of a computer on the LAN to check if it has established connection to the ESR300H.



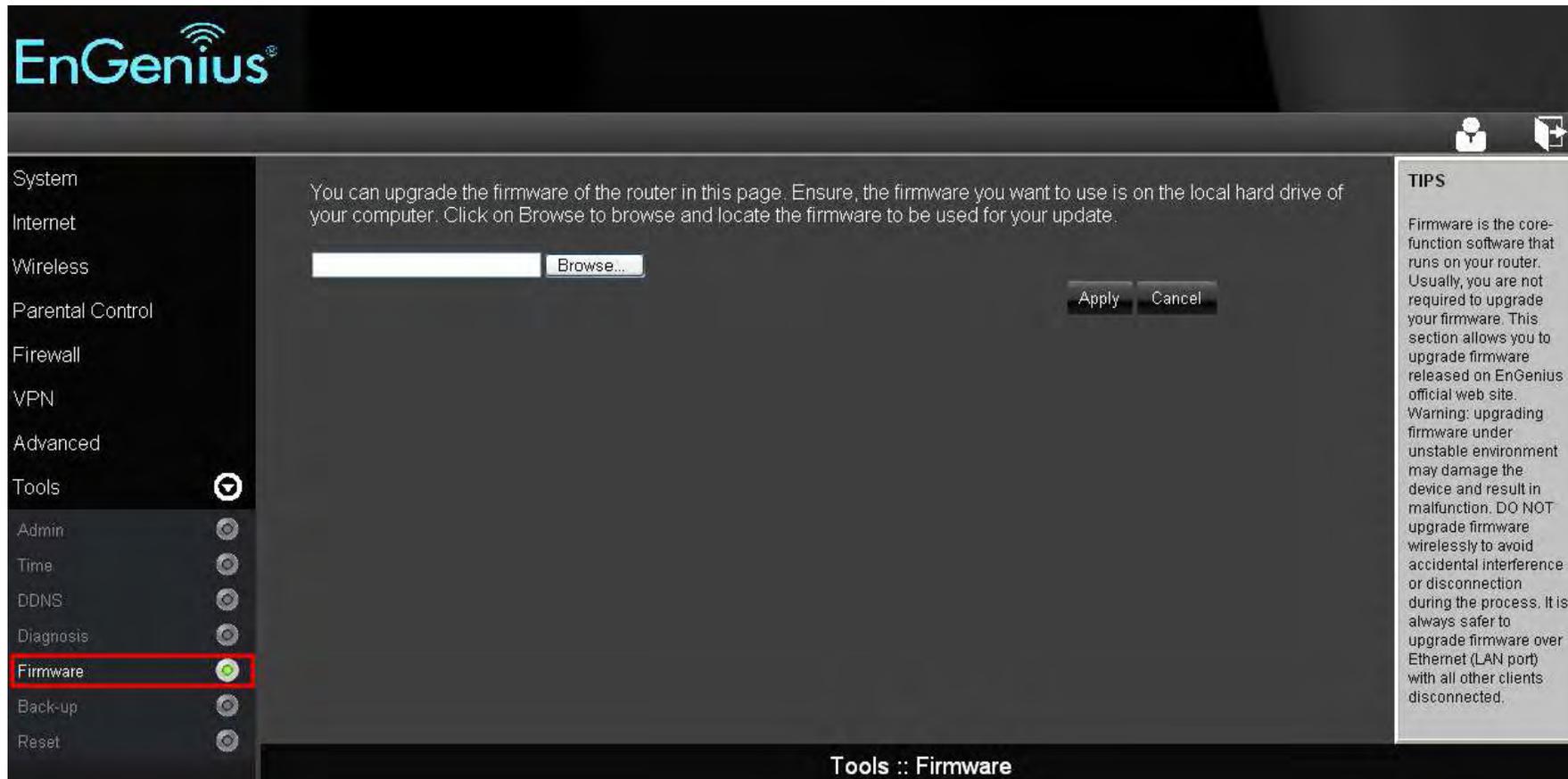
The screenshot displays the EnGenius web management interface. On the left, a navigation menu lists various system settings: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, Tools, Admin, Time, DDNS, Diagnosis (highlighted with a red box), Firmware, Back-up, and Reset. The 'Tools' section is expanded, showing the 'Diagnosis' tool. The main content area features a form with two input fields: 'Address to Ping' and 'Ping Result', with a 'Start' button next to the first field. A 'TIPS' box on the right provides instructions: 'This feature allows you to Ping the other device for response. This is mostly used for checking if a specific user is on-line. You can type in the IP address (eg:192.168.0.100) into [Address to Ping] and press [Start]. If you get a Ping Result "alive" it means the user is on line. However, this feature does not if the target device has firewall or security software installed.' The bottom status bar reads 'Tools :: Diagnosis'.

Tools > Firmware

In the **Firmware** option of the Tools section, you can update the firmware of the **ESR300H**. To update the firmware, follow these steps:

1. Download the appropriate firmware approved by Engenius® Technologies Inc. from an approved site.
2. Make sure the firmware file is in a known local location.
3. Select **Browse**.
4. Navigate through the file system and select the firmware file.
5. Select **Apply**.

This process may take a few minutes. The **ESR300H** will restart when completed.



The screenshot displays the EnGenius router's web management interface. The top left corner features the EnGenius logo. A left-hand navigation menu lists various system settings: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, Tools (highlighted with a green circle), Admin, Time, DDNS, Diagnosis, Firmware (highlighted with a red rectangle), Back-up, and Reset. The main content area is titled 'Tools :: Firmware' and contains the following text: 'You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.' Below this text is a file selection input field with a 'Browse...' button. To the right of the input field are 'Apply' and 'Cancel' buttons. On the far right, a 'TIPS' section provides additional information: 'Firmware is the core-function software that runs on your router. Usually, you are not required to upgrade your firmware. This section allows you to upgrade firmware released on EnGenius official web site. Warning: upgrading firmware under unstable environment may damage the device and result in malfunction. DO NOT upgrade firmware wirelessly to avoid accidental interference or disconnection during the process. It is always safer to upgrade firmware over Ethernet (LAN port) with all other clients disconnected.'

Tools > Back-Up

In the **Back-Up** option of the Tools section, you can:

1. Restore the **ESR300H** to factory defaults.
2. Save the current configuration on the **ESR300H** to a .dlf file.
3. Restore saved settings by:
 - a. Select **Browse**.
 - b. Browse location for the file with the saved settings of the **ESR300H**.
 - c. Select **Upload**.

The screenshot displays the EnGenius router's web management interface. The top left features the EnGenius logo. A navigation menu on the left lists various system settings, with 'Tools' expanded to show 'Back-up' highlighted in red. The main content area contains three sections: 'Restore to factory default' with a 'Reset' button, 'Backup Settings' with a 'Save' button, and 'Restore Settings' with a text input field, a 'Browse...' button, and an 'Upload' button. On the right, a 'TIPS' box provides instructions for each function: 'Restore to factory default' returns the router to its original state; 'Backup Settings' saves the current configuration to a file; and 'Restore Settings' loads a previously saved configuration file. The bottom status bar reads 'Tools :: Back-up'.

Tools > Reset

In the **Reset** option of the Tools section, you can manually restart the **ESR300H**.

The screenshot displays the EnGenius router's web management interface. The top left corner features the EnGenius logo. A navigation menu on the left lists various system settings: System, Internet, Wireless, Parental Control, Firewall, VPN, Advanced, Tools, Admin, Time, DDNS, Diagnostics, Firmware, Back-up, and Reset. The 'Reset' option is highlighted with a red rectangular border. The main content area contains the following text: "In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button." Below this text are two buttons labeled "Apply" and "Cancel". On the right side, a "TIPS" section provides additional information: "This feature allows you to reboot the router. If you encounter any unstable connection you may resolve it by resetting the device to release all the occupied system resource." The bottom status bar indicates "Tools :: Reset".

Table of Contents

Appendix A – FCC Interference Statement

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 device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Appendix B – Industry Canada statement

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC 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.

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device has been designed to operate with a Dipole antenna have a maximum gain of 2.0 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (IC: 3616C-SR300H / Model: ESR300H) has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de Dipole antenne avec dB 2.0. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio (IC: 3616C-SR300H / Model: ESR300H) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.