EnGenius®

ESR350H

11N X-TRA RANGE Wireless Router

V1.2

Table of Contents

1. Product Overview

Thank you for purchasing the ESR350H 300Mbps Wireless-N Gigabit Router from EnGenius Technologies.

By applying the latest in 802.11n technology, the ESR350H provides users with high speed (up to 300Mbps) to stream HD multimedia, play games online, or download large files. With 5dBi antenna, 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 **ESR350H** 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 **ESR350H**. 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

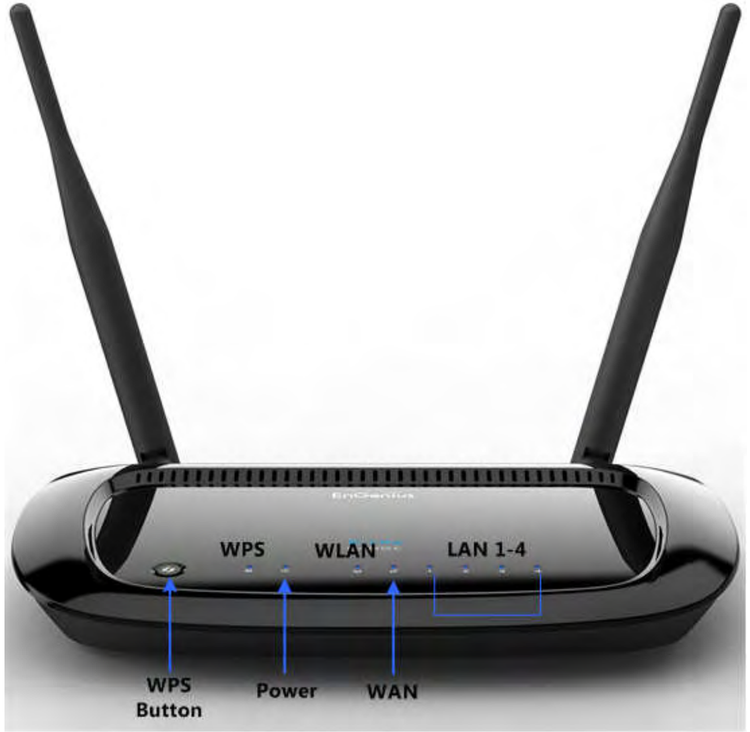
- High Performance Gigabit Connection: Offers one WAN and four LAN Gigabit connections.
- 300Mbps High Speed Wireless Networking: Provides up to 300Mbps to allow you to watch online multimedia such as Netflix®, play games online, music, and download large files.
- 5dBi antenna: Extend your home network 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: Supports up to 5 VPN tunnels to better secure your network from remote access.
- IPv6 Compliance: Supports the next generation IPv6 (Internet Protocol version 6) to enable highly reliable applications and enhanced security for safer Internet connectivity.
- Easy Smart Wizard Setup

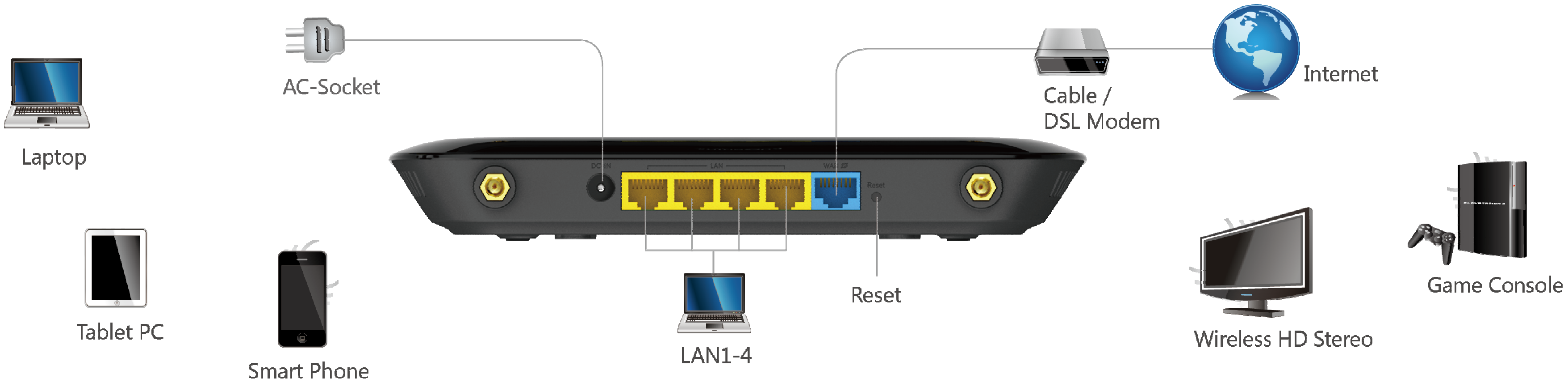
1.1. Package Contents

1. ESR350H Wireless N Router
2. 5dBi Antenna * 2
3. ESR350H Quick Installation Guide
4. 12V/1A Power Adaptor
5. Ethernet Cable
6. ESR350H User CD (with User Manual)
7. Technical Supporting Card

1.2. Product Layout



Front Panel Components	Description
WPS LED	This LED goes BLINK when the WPS feature is being triggered.
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	Click to activate the router's Wi-Fi Protected Setup (WPS) feature.



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.
Reset Button	Press 0 to 5 seconds to reboot the router. Press longer than 10 seconds to reset the router to the factory default settings.
Antenna Connector	Interface for the antennas.

1.3. Wall Mounting

Mounting the **ESR350H** 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 **ESR350H** and drill the appropriate holes on the wall location. Once the nails are secure, firmly lock the mounts onto the **ESR350H**.

2. Installation

2.1. System Requirements

To begin installing the **ESR350H**, you need the following:

- Computer (Windows, Linux, OS X 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

  ** You can only using **ESR350H** Installation CD for Windows operation system.*

  ***The Wi-Fi Card or Wi-Fi USB dongle is optional.*

2.2. Setup Notes

When considering the placement of the **ESR350H** remember the following:

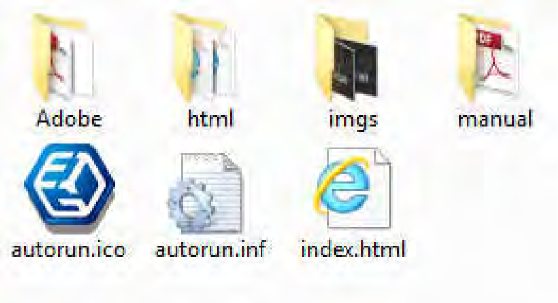
- The **ESR350H** must be close to the DSL or Cable Modem and a Power Source. Initially, it needs to be closed to the computer that is used to set up the **ESR350H**.
- Placing the **ESR350H** in the center of the office space will result in the most optimal wireless range.
- The higher the placement of the **ESR350H**, the better wireless range it will have.
- Other electronic devices can cause interference, which will cause the wireless range of the **ESR350H** to diminish.

3. Getting Started

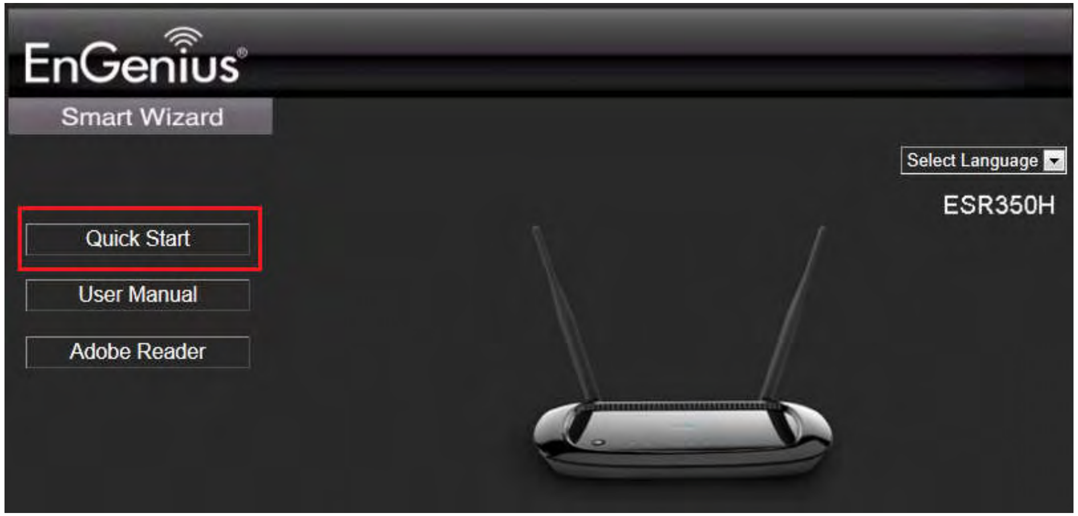
3.1. Using your CD

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

1. Insert the ESR350H 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** to start.

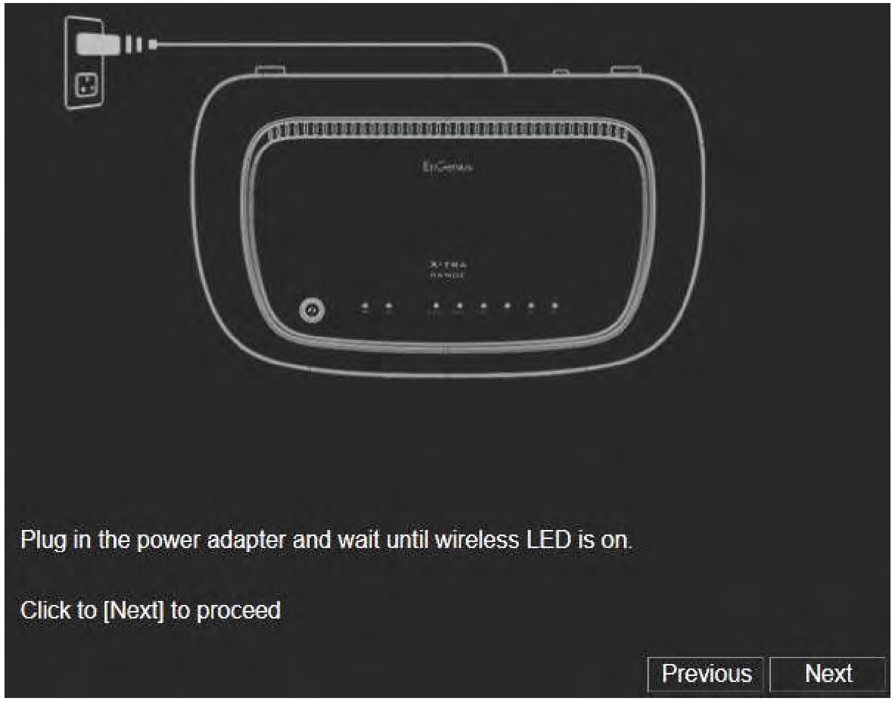


2. Click **Quick Start**. The wizard will guide you through setting up your ESR350H.



3.2. Setup your network cables

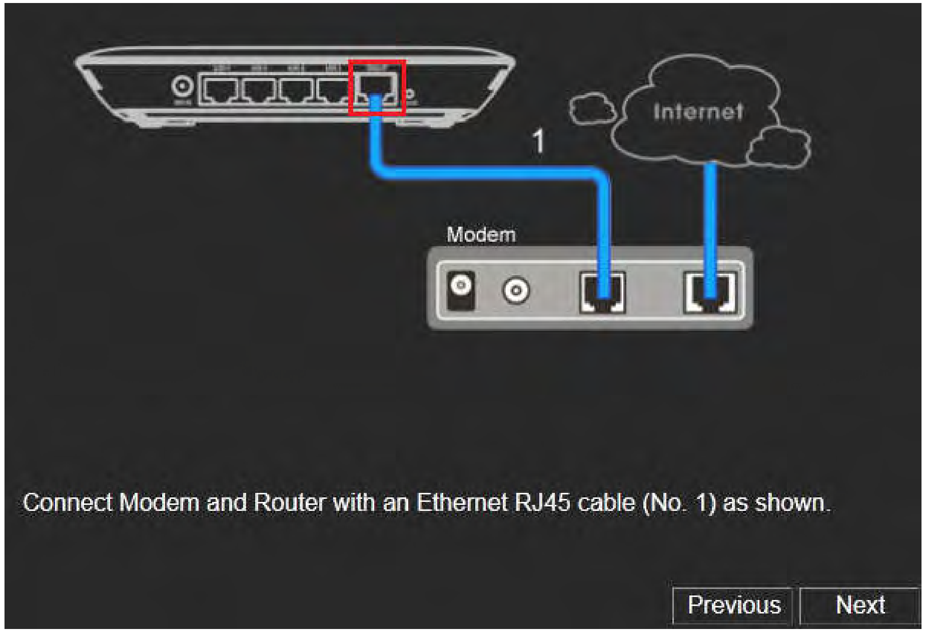
1. Power on ESR350H.



Plug in the power adapter and wait until wireless LED is on.

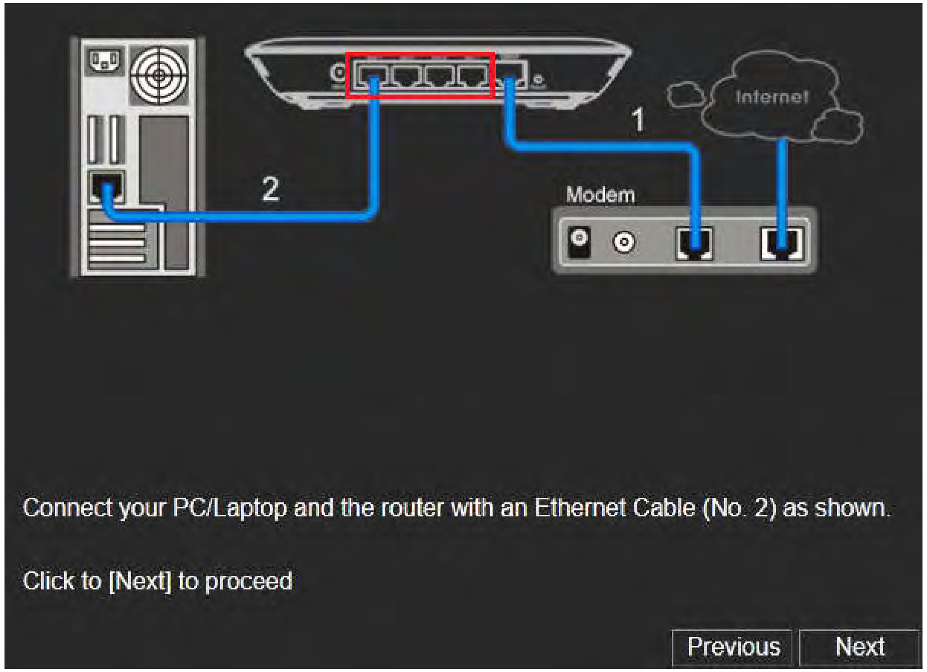
Click to [Next] to proceed

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.



Connect Modem and Router with an Ethernet RJ45 cable (No. 1) as shown.

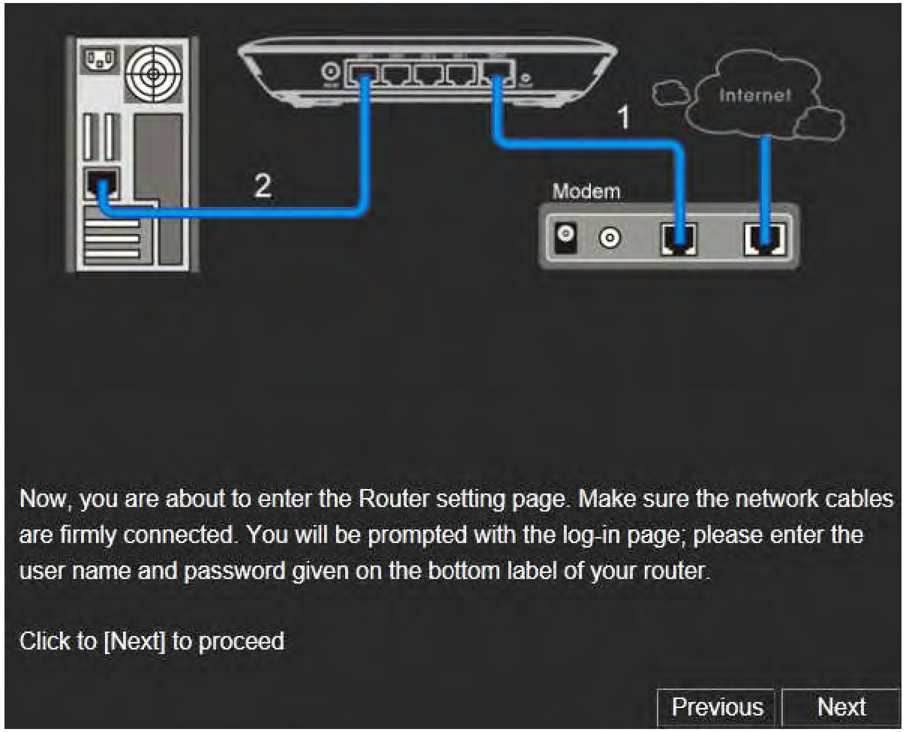
3. Plug either end of an Ethernet cable into the LAN port on the back panel of the router (see **CABLE 2**). Plug the other end of the cable into your computer.



Connect your PC/Laptop and the router with an Ethernet Cable (No. 2) as shown.

Click to [Next] to proceed

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.

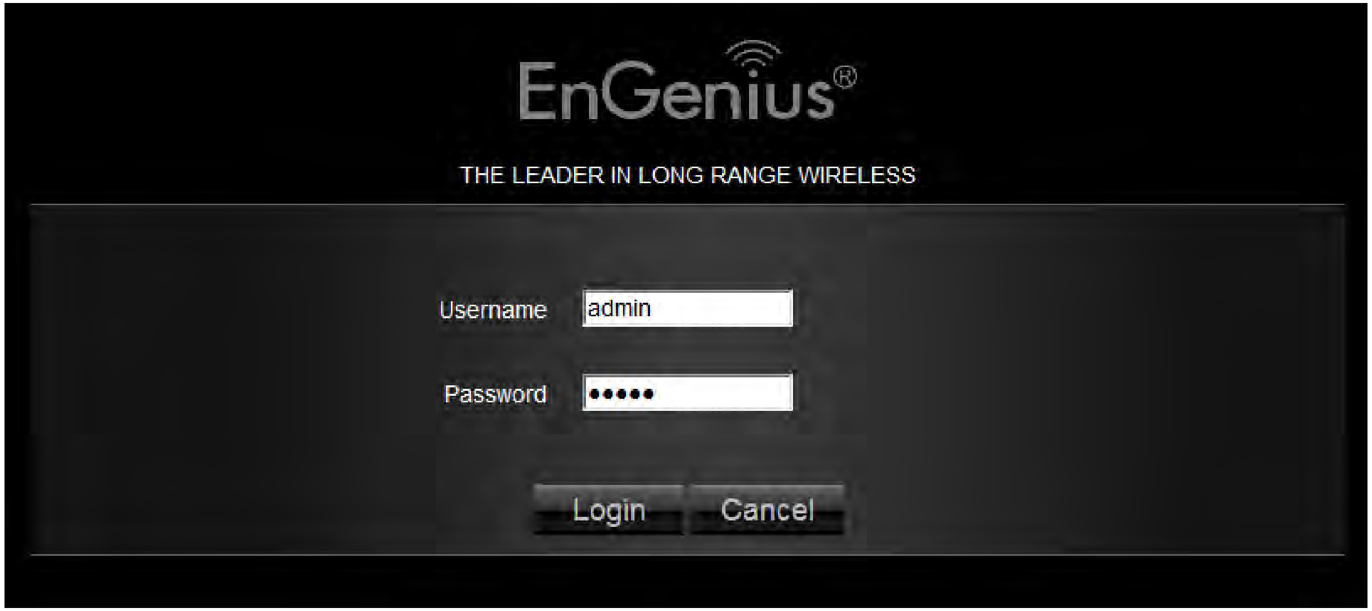


Now, you are about to enter the Router setting page. Make sure the network cables are firmly connected. You will be prompted with the log-in page; please enter the user name and password given on the bottom label of your router.

Click to [Next] to proceed

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



Username: admin

Password: •••••

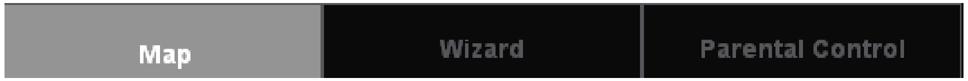
1. Once logged in, the landing page will display information about the **ESR350H**.

NOTE: The default user name is **admin** and the default password is **admin**.

2. Icon introduction

On the top right, you will see five icons:

- Home
- Setup Wizard Mode
- Advanced Networking Setting
- Language
- Logout

On the bottom left, you will see: 

-

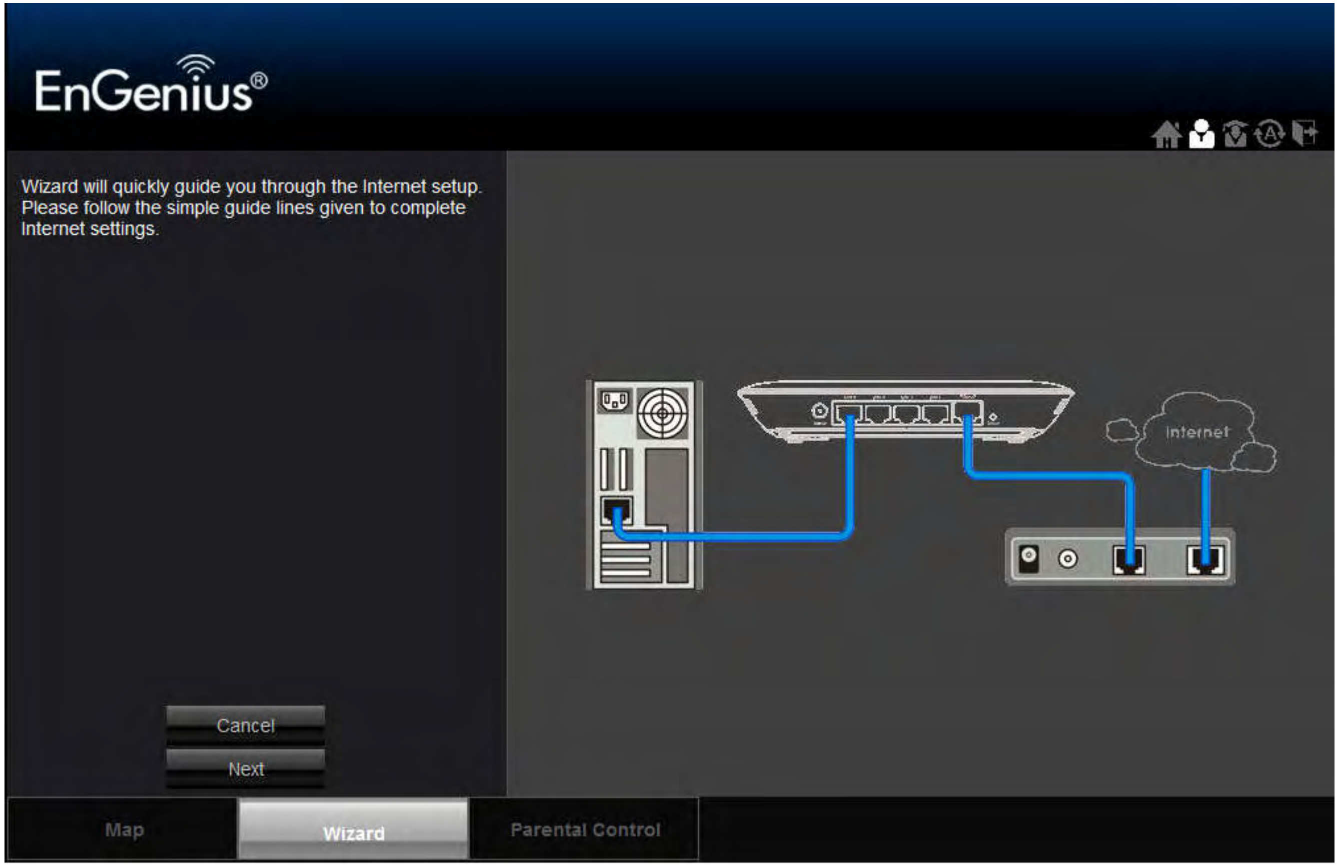
View the router information and connection status
-

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**.



Wizard will quickly guide you through the Internet setup. Please follow the simple guide lines given to complete Internet settings.

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 **ESR350H**. Please wait a few seconds to finish detecting the Internet connection.
4. If the **ESR350H** 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.

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 **ESR350H** should connect to the Internet successfully. A PPPoE connection is usually from a DSL Internet service.

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 1500.

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.

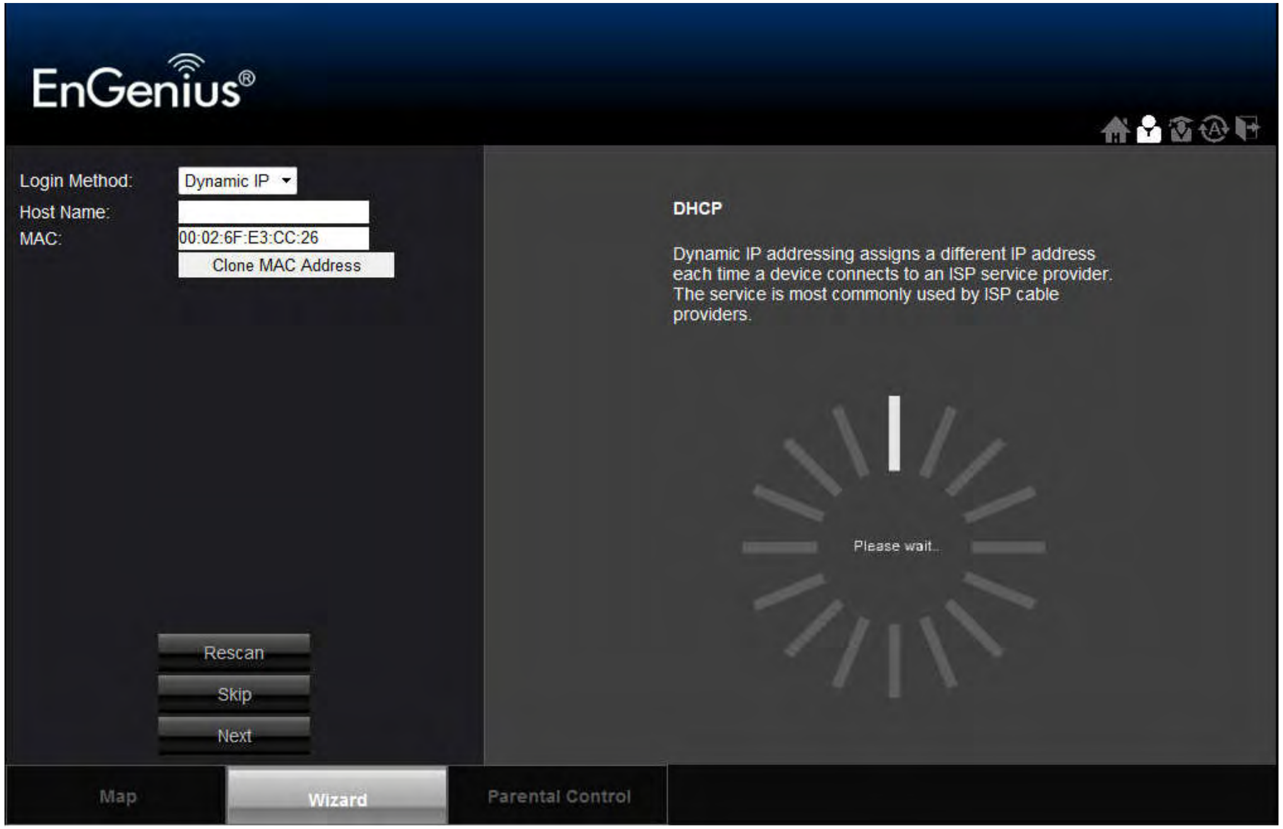
MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The factory default MTU size of PPTP is 1400. If you wish to manually change the MTU size, set it between 1200 and 1400.

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 L2TP is 1460. If you wish to manually change the MTU size, set it between 1200 and 1460.

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



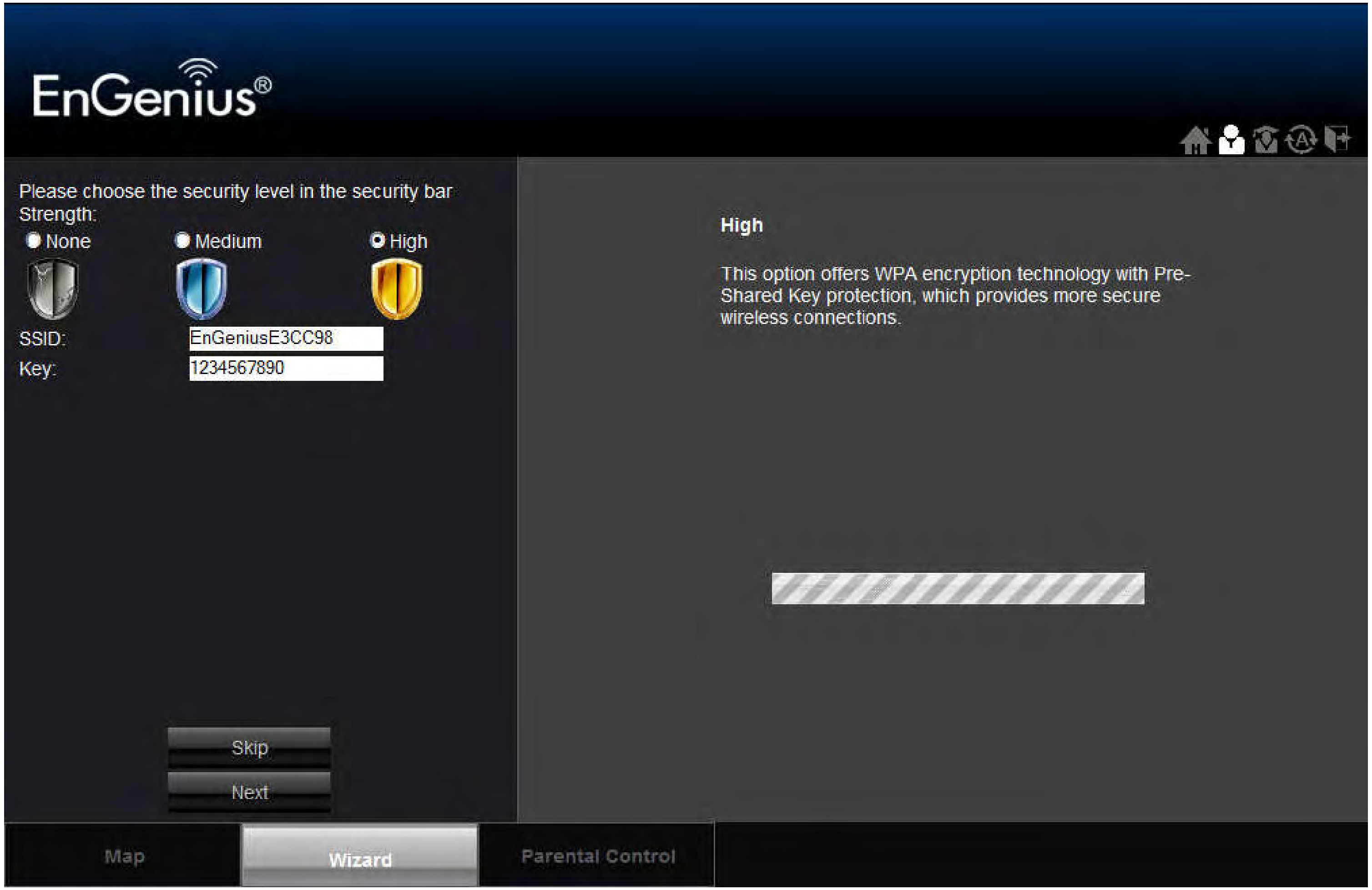
Login Method: Dynamic IP
Host Name:
MAC: 00:02:6F:E3:CC:26

DHCP

Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.

Please wait..

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.



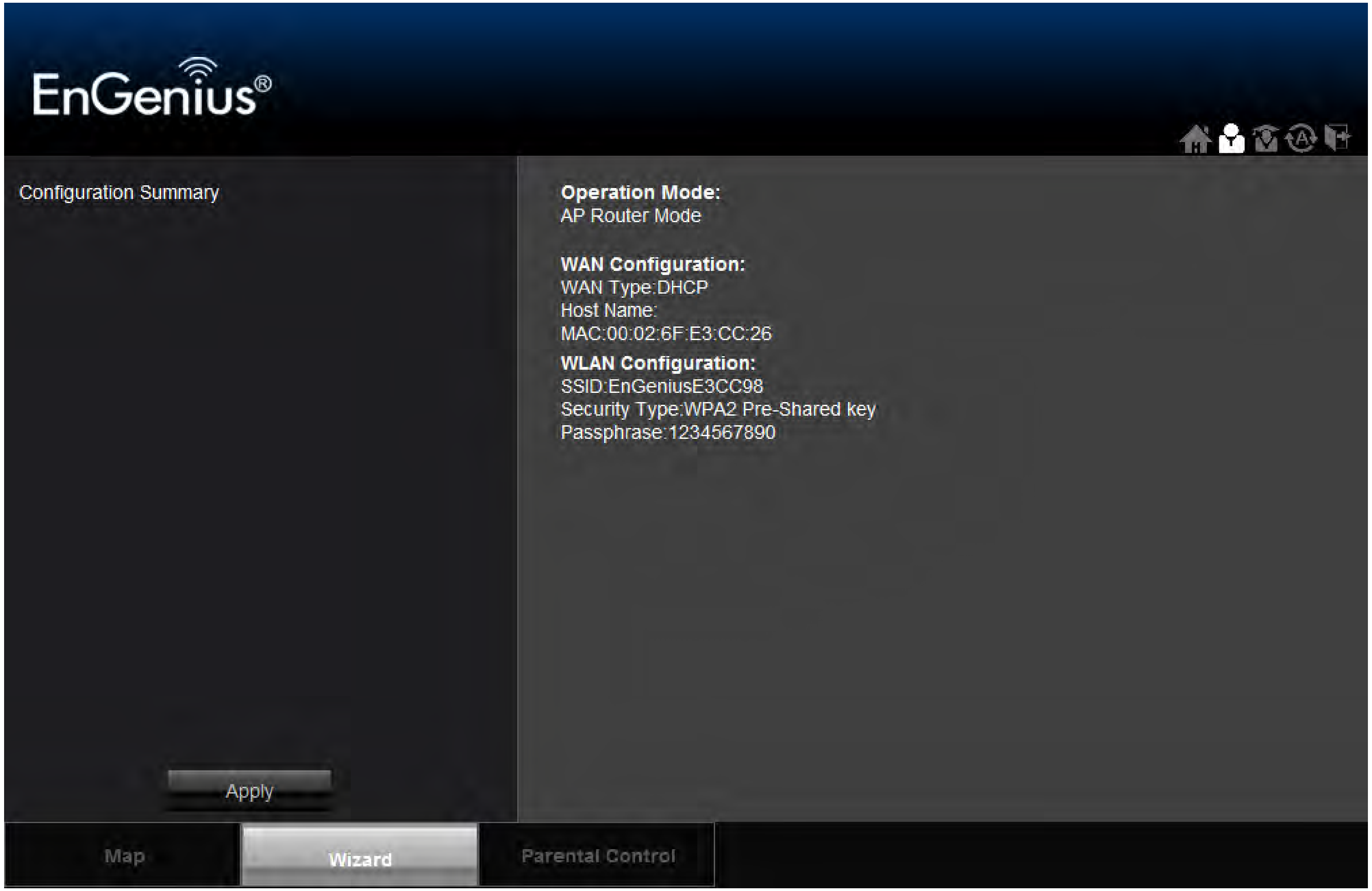
Please choose the security level in the security bar
Strength:
○ None ○ Medium ● High

SSID: EnGeniusE3CC98
Key: 1234567890

High

This option offers WPA encryption technology with Pre-Shared Key protection, which provides more secure wireless connections.

8. Click **Apply** to save the information. You have now completed the ESR350H setup. Now ESR350H is ready for use.



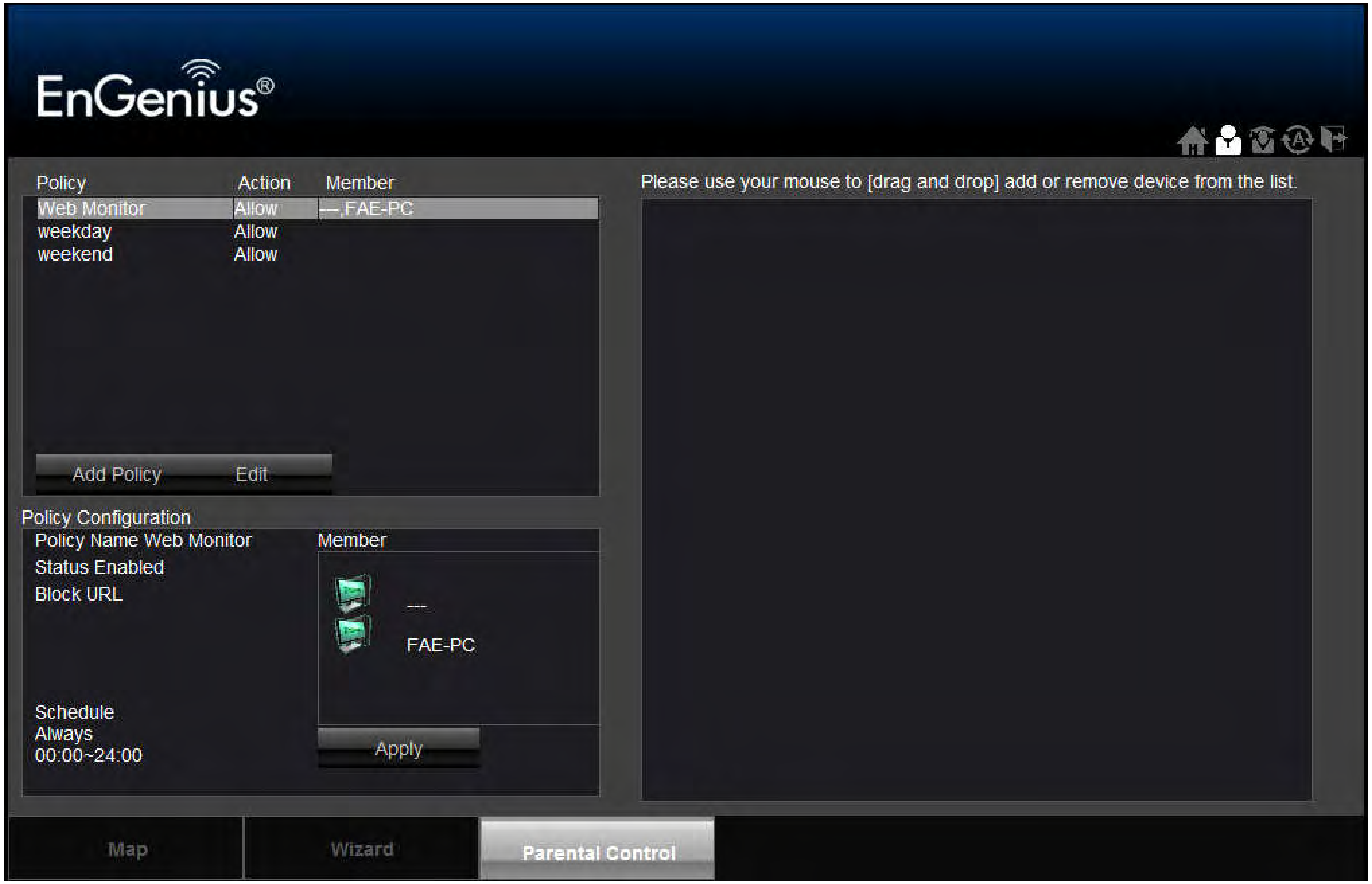
Operation Mode:
AP Router Mode

WAN Configuration:
WAN Type:DHCP
Host Name:
MAC:00:02:6F:E3:CC:26

WLAN Configuration:
SSID:EnGeniusE3CC98
Security Type:WPA2 Pre-Shared key
Passphrase:1234567890

4. Parental 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.



Policy	Action	Member
Web Monitor	Allow	---,FAE-PC
weekday	Allow	
weekend	Allow	

Policy Configuration

Policy Name Web Monitor

Status Enabled

Block URL

Schedule
Always
00:00~24:00

Member

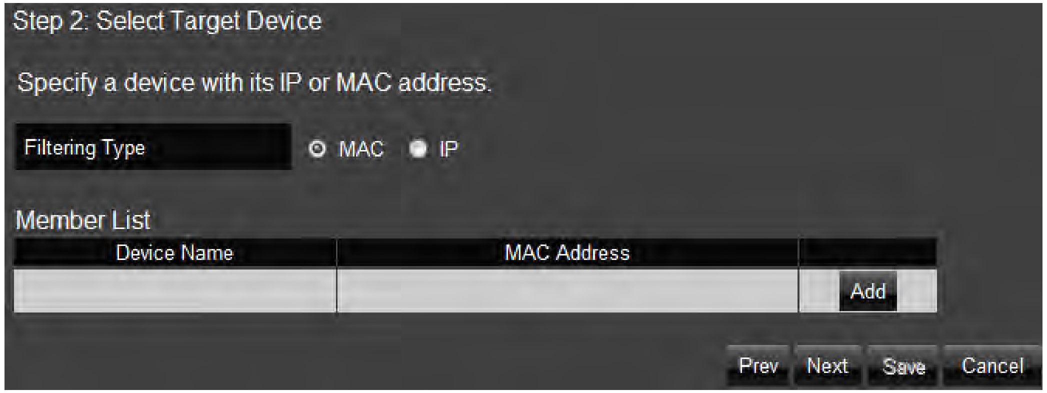
FAE-PC

Please use your mouse to [drag and drop] add or remove device from the list.

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

Name the Policy. Click **Next.**

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



Step 2: Select Target Device

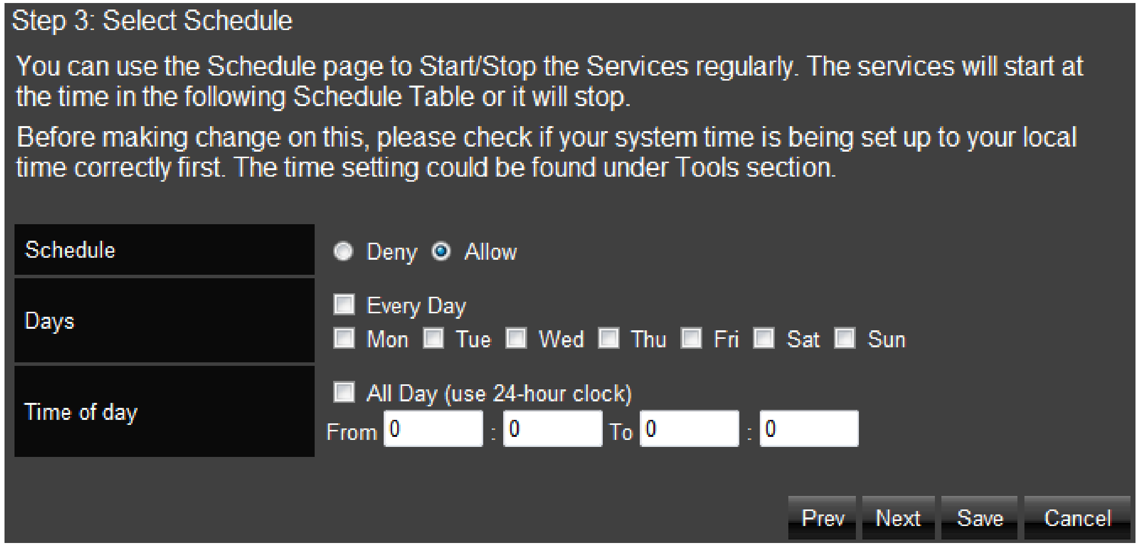
Specify a device with its IP or MAC address.

Filtering Type ● MAC ○ IP

Member List

Device Name	MAC Address	
		Add

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



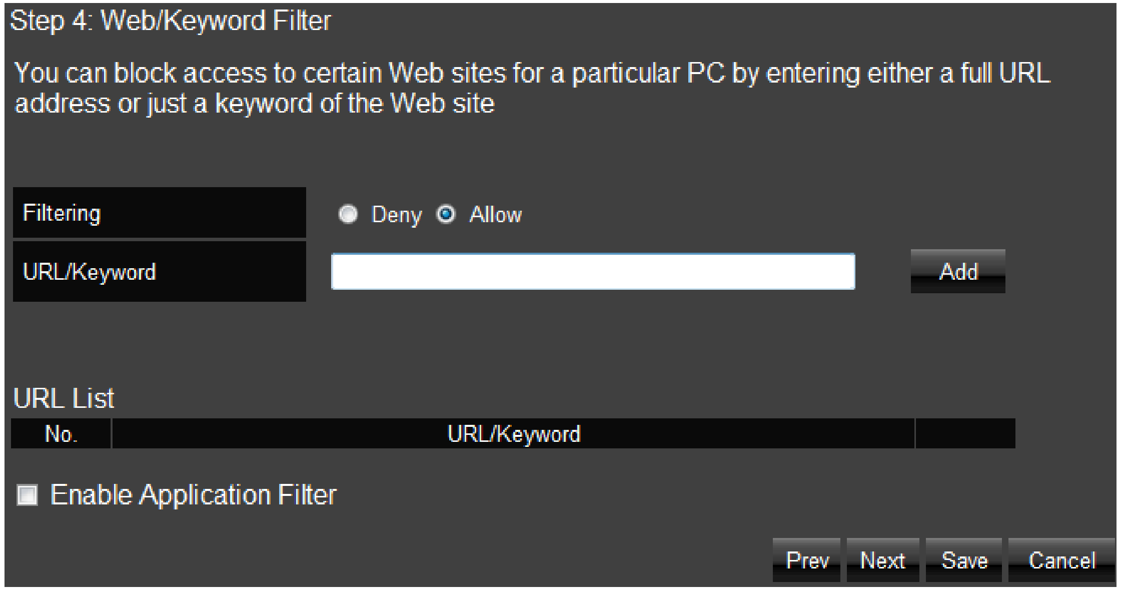
Step 3: Select Schedule

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.

Before making change on this, please check if your system time is being set up to your local time correctly first. The time setting could be found under Tools section.

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

3. 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

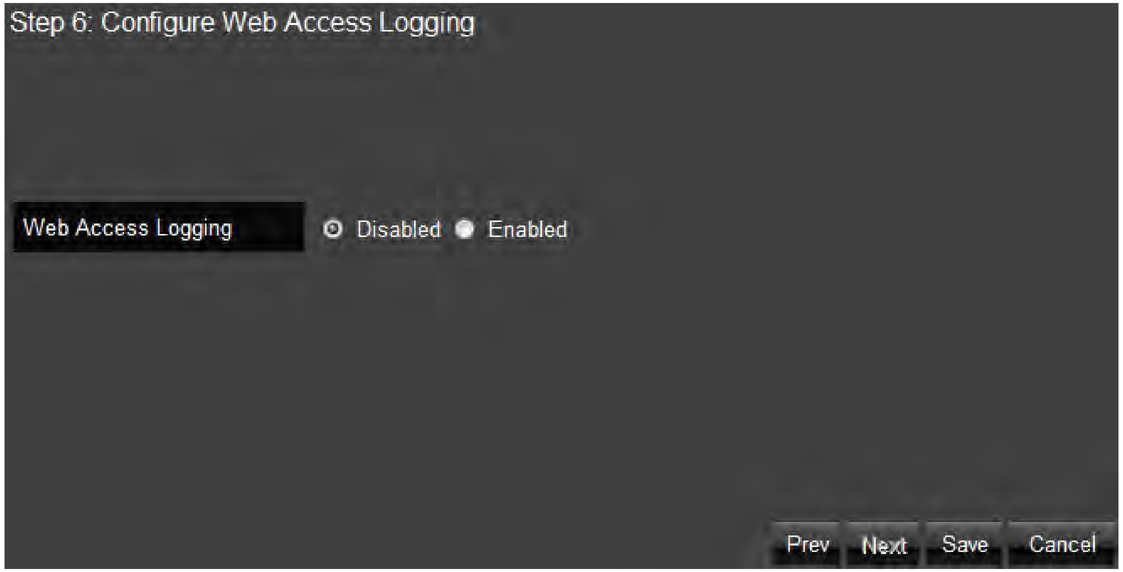
URL/Keyword

URL List

No.	URL/Keyword	

☐ Enable Application Filter

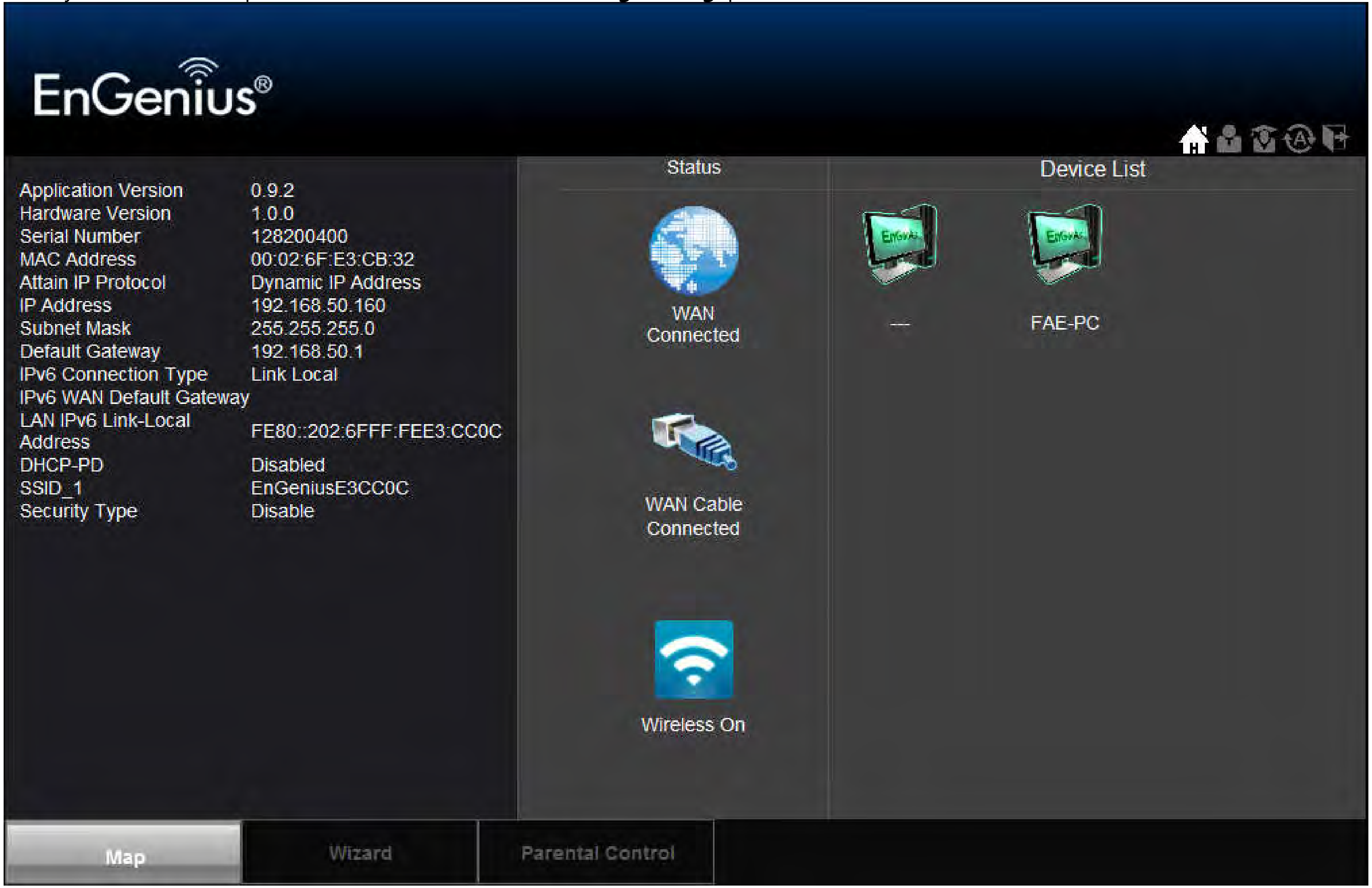
4. Enable or disable **Web Access Logging**. Click **Save** for your settings.



Step 6: Configure Web Access Logging

Web Access Logging ● Disabled ○ Enabled

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



Application Version	0.9.2
Hardware Version	1.0.0
Serial Number	128200400
MAC Address	00:02:6F:E3:CB:32
Attain IP Protocol	Dynamic IP Address
IP Address	192.168.50.160
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
IPv6 Connection Type	Link Local
IPv6 WAN Default Gateway	
LAN IPv6 Link-Local Address	FE80::202:6FFF:FEE3:CC0C
DHCP-PD	Disabled
SSID_1	EnGeniusE3CC0C
Security Type	Disable

5. 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 10 main tabs in the Networking Setting. They are System, Internet, Wireless, Parental Control, Guest Network, IPv6, Firewall, VPN, Advanced, and Tools.

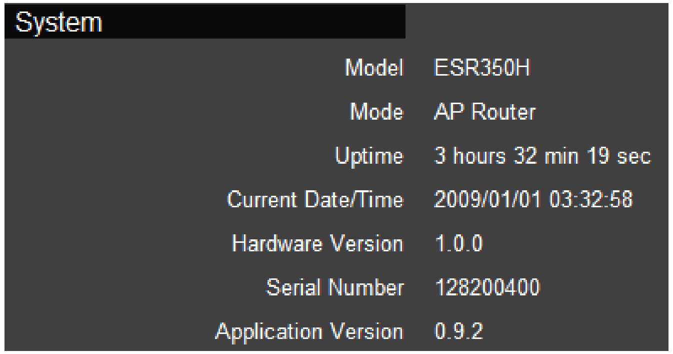
6. System

6.1. Status

You can review the router information and setting status.

System

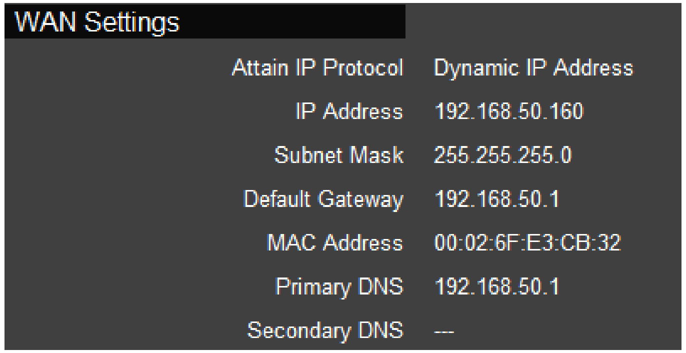
- **Model**: The model name.
- **Mode**: The operation mode you use.
- **Uptime**: The duration which ESR350H is powered on.
- **Hardware Version**: The hardware version number of your ESR350H
- **Serial Number**: The serial number of your ESR350H. The serial number is required when you need customer support or repair for your ESR350H.
- **Application Version**: The software version of your ESR350H. You can always update to the latest firmware of your ESR350H. The latest firmware can be found on the EnGenius website. (Please visit http://www.engeniusnetworks.com/ for the latest firmware and the related documents)



System	
Model	ESR350H
Mode	AP Router
Uptime	3 hours 32 min 19 sec
Current Date/Time	2009/01/01 03:32:58
Hardware Version	1.0.0
Serial Number	128200400
Application Version	0.9.2

WAN Settings

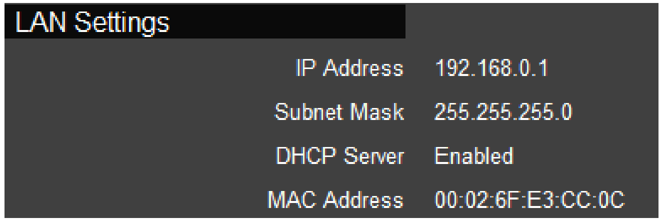
- **Attain IP Protocol**: Displays the IP Protocol in use for the ESR350H. It can be Dynamic IP address, Static IP Address, PPPoE, PPTP or L2TP.
- **IP Address**: Your router's WAN IP address
- **Subnet Mask**: Your router's WAN Subnet mask
- **Default Gateway**: Your ISP's Gateway IP address
- **MAC 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



WAN Settings	
Attain IP Protocol	Dynamic IP Address
IP Address	192.168.50.160
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
MAC Address	00:02:6F:E3:CB:32
Primary DNS	192.168.50.1
Secondary DNS	---

LAN Settings

- **IP Address**: Your router's local IP address. The default LAN IP address is 192.168.0.1
- **Subnet Mask**: Your router's local subnet mask
- **DHCP Server**: The status of your router's DHCP server function. Enable or disable.
- **MAC Address**: Your router's LAN MAC address

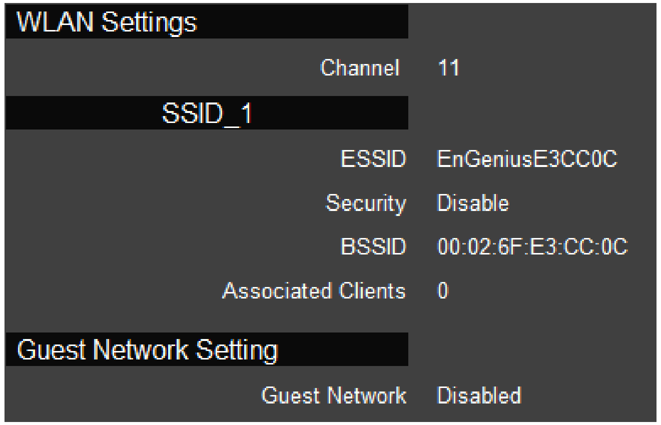


LAN Settings

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:02:6F:E3:CC:0C

WLAN Settings

- **Channel**: The wireless channel number used is shown
- **SSID_#**: Up to 4 SSIDs (network groups) for the ESR350H
- **ESSID**: Your router's name
- **Security**: Security level utilized by your ESR350H
- **BSSID**: Your router's WLAN MAC address
- **Associated Client**: The number of clients connected to your router
- **Guest Network Setting**: The information of Guest Network. Enable or disable.



WLAN Settings

Channel	11

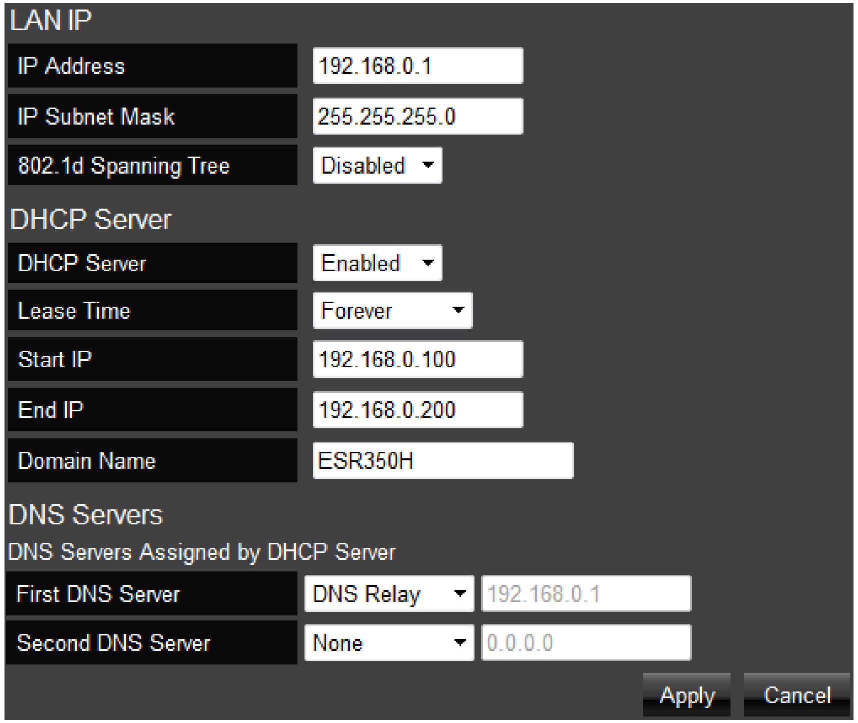
SSID_1

ESSID	EnGeniusE3CC0C
Security	Disable
BSSID	00:02:6F:E3:CC:0C
Associated Clients	0

Guest Network Setting

Guest Network	Disabled

6.2. LAN



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	ESR350H

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

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 Servers

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.

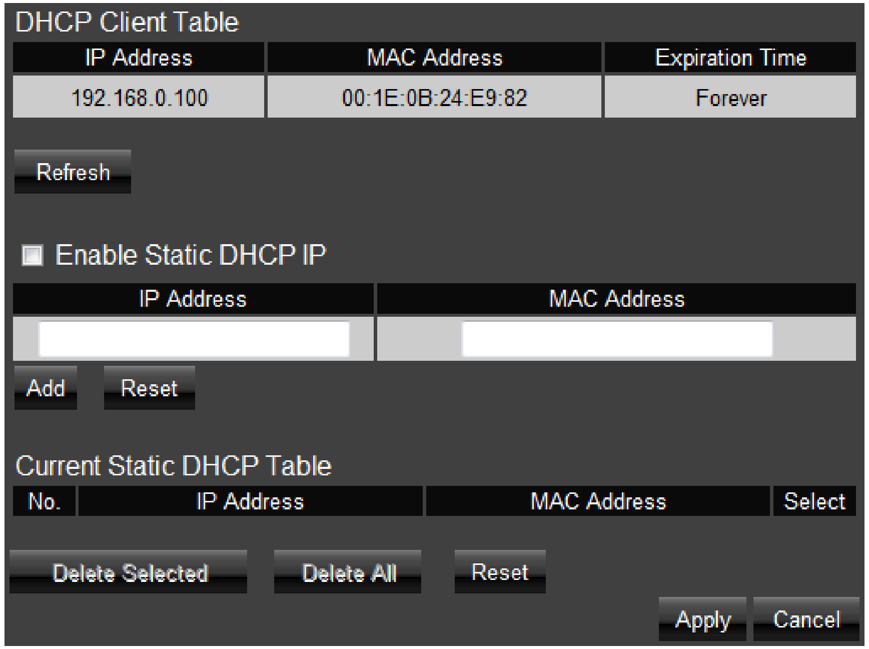
6.3. DHCP

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.



DHCP Client Table

IP Address	MAC Address	Expiration Time
192.168.0.100	00:1E:0B:24:E9:82	Forever

□ Enable Static DHCP IP

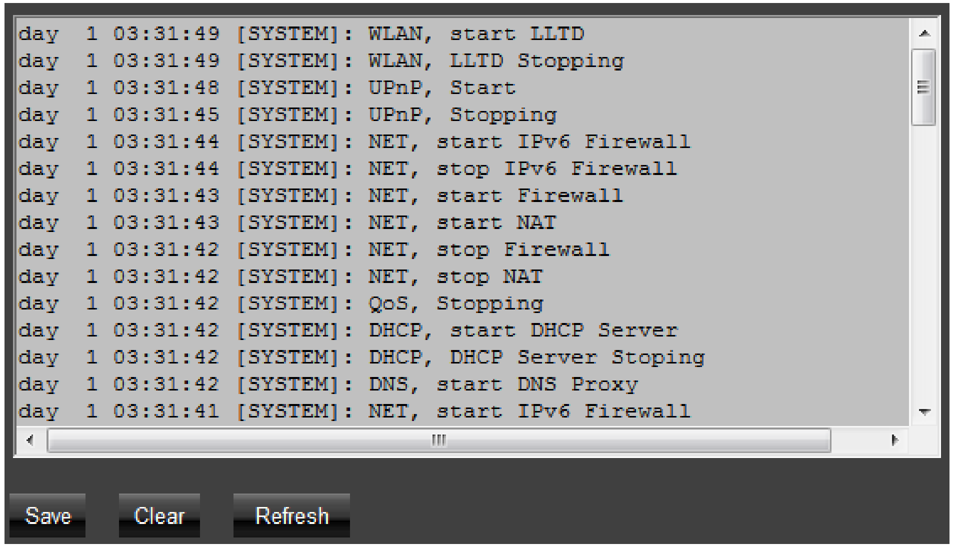
IP Address	MAC Address

Current Static DHCP Table

No.	IP Address	MAC Address	Select

6.4. Log

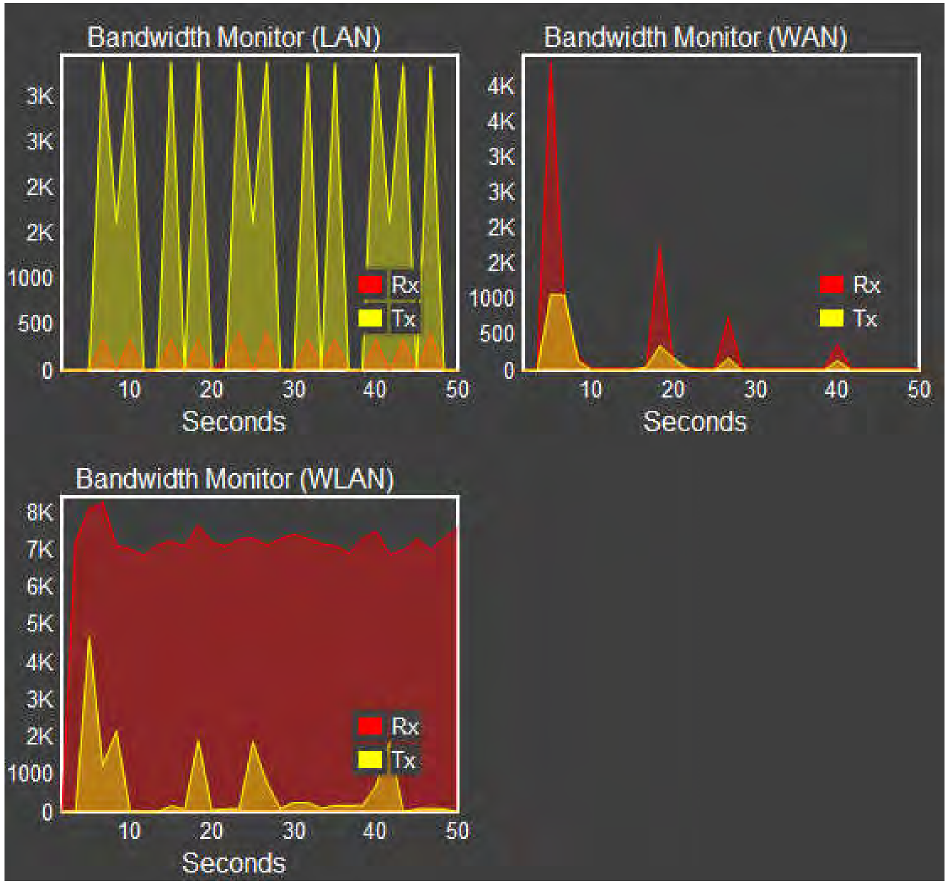
Records the system log of the router. The log displays any event that occurred after your router starts up. Click **Save** if you wish to save the log in a local file for further analysis. Click **Clear** if you wish to erase the current log. Click **Refresh** to get the most updated information. If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



```
day  1 03:31:49 [SYSTEM]: WLAN, start LLTD
day  1 03:31:49 [SYSTEM]: WLAN, LLTD Stopping
day  1 03:31:48 [SYSTEM]: UPnP, Start
day  1 03:31:45 [SYSTEM]: UPnP, Stopping
day  1 03:31:44 [SYSTEM]: NET, start IPv6 Firewall
day  1 03:31:44 [SYSTEM]: NET, stop IPv6 Firewall
day  1 03:31:43 [SYSTEM]: NET, start Firewall
day  1 03:31:43 [SYSTEM]: NET, start NAT
day  1 03:31:42 [SYSTEM]: NET, stop Firewall
day  1 03:31:42 [SYSTEM]: NET, stop NAT
day  1 03:31:42 [SYSTEM]: QoS, Stopping
day  1 03:31:42 [SYSTEM]: DHCP, start DHCP Server
day  1 03:31:42 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 03:31:42 [SYSTEM]: DNS, start DNS Proxy
day  1 03:31:41 [SYSTEM]: NET, start IPv6 Firewall
```

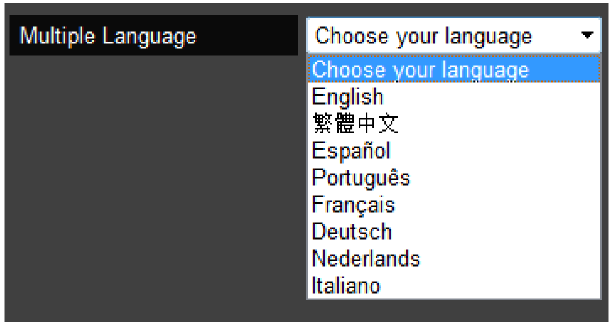
6.5. Monitor

Displays the bandwidth utilized on LAN, WAN and WLAN.



6.6. Language

ESR350H supports multiple languages. Please select your preferred language.



Multiple Language

Choose your language

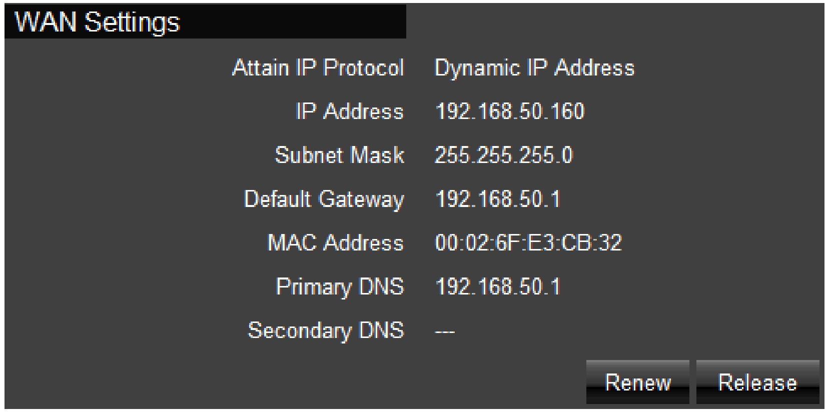
7. Internet

7.1. Status

Displays the Internet connection type and status

WAN Settings

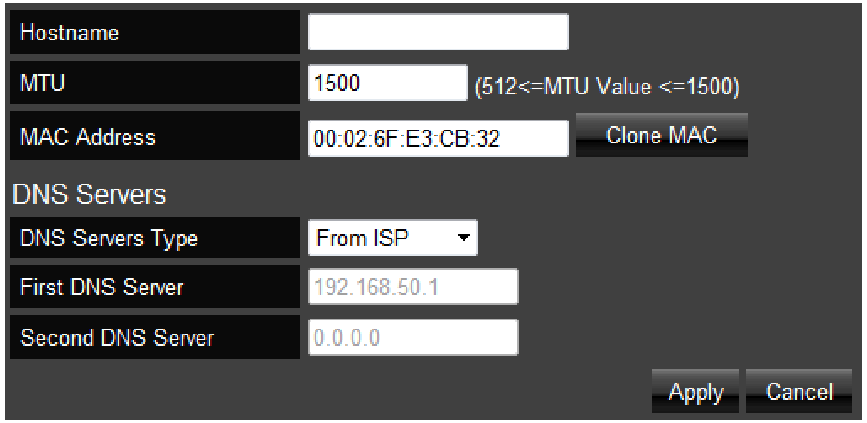
- **Attain IP Protocol**: Displays the IP Protocol currently used by the ESR350H. It can be Dynamic IP Address, Static IP, PPPoE, PPTP, L2TP.
- **IP Address**: Your router's WAN IP address
- **Subnet Mask**: Your router's WAN Subnet mask
- **Default Gateway**: Your ISP's Gateway IP address
- **MAC Address**: 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



WAN Settings

Attain IP Protocol	Dynamic IP Address
IP Address	192.168.50.160
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
MAC Address	00:02:6F:E3:CB:32
Primary DNS	192.168.50.1
Secondary DNS	---

7.2. Dynamic IP



Hostname		
MTU	1500	(512<=MTU Value <=1500)
MAC Address	00:02:6F:E3:CB:32	Clone MAC

DNS Servers

DNS Servers Type	From ISP
First DNS Server	192.168.50.1
Second DNS Server	0.0.0.0

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.

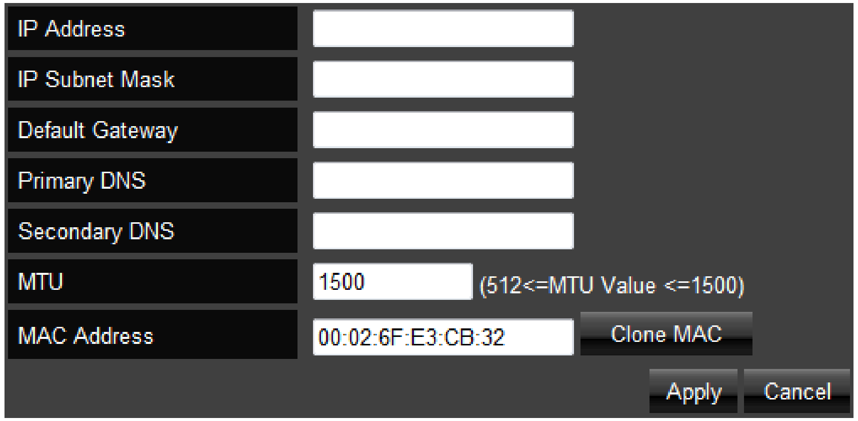
Click **Apply** to enable your settings.

7.3. 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.

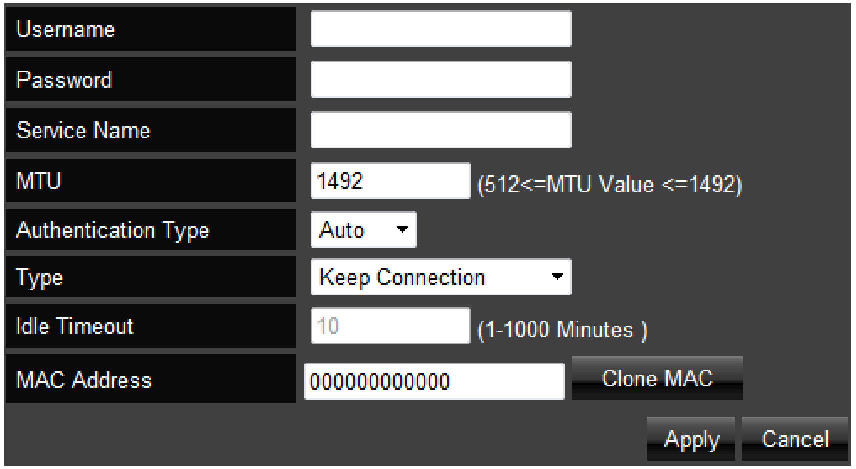
MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 1200 and 1500.

Click **Apply** to enable your settings.



IP Address	
IP Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
MTU	1500 (512<=MTU Value <=1500)
MAC Address	00:02:6F:E3:CB:32

7.4. PPPoE (Point-to-Point Protocol over Ethernet)



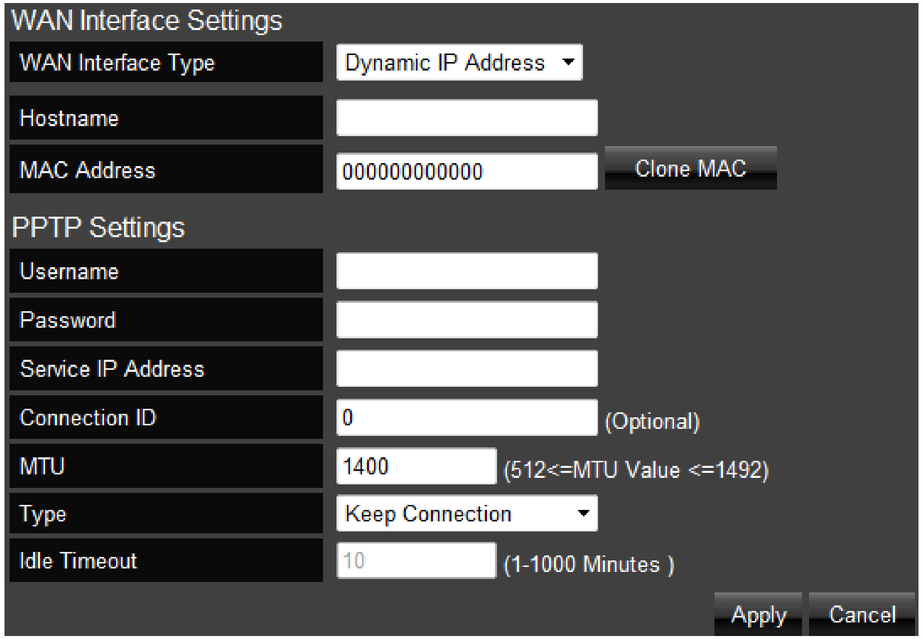
Username	
Password	
Service Name	
MTU	1492 (512<=MTU Value <=1492)
Authentication Type	Auto
Type	Keep Connection
Idle Timeout	10 (1-1000 Minutes)
MAC Address	000000000000 Clone MAC

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.

- **Username**: 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.

7.5. PPTP



WAN Interface Settings

WAN Interface Type	Dynamic IP Address	
Hostname		
MAC Address	000000000000	Clone MAC

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)

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.

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.

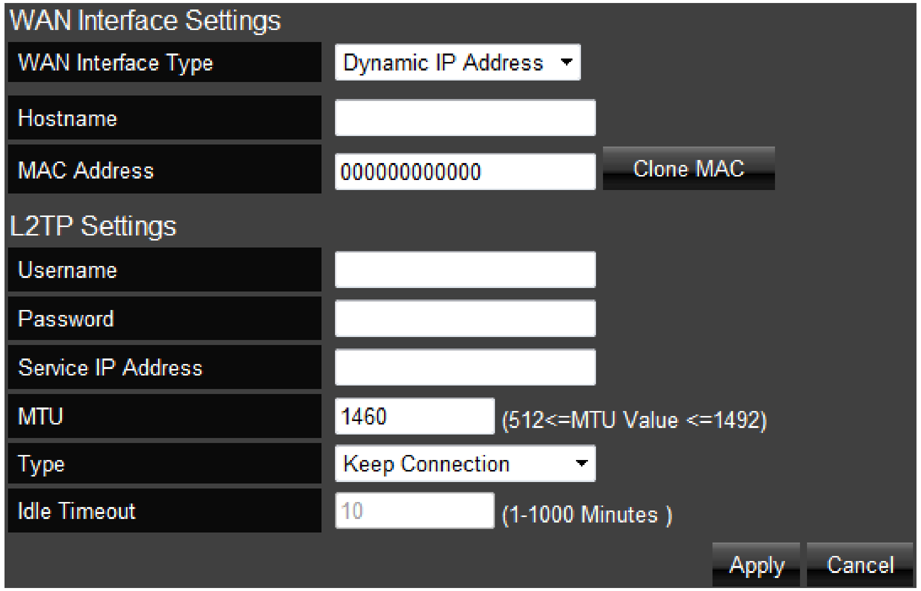
Type: Connection type, you can select Keep Connection, Automatic Connection, or Manual Connection.

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

Click **Apply** to enable your settings.

7.6. 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.



WAN Interface Settings

WAN Interface Type	Dynamic IP Address ▾	
Hostname		
MAC Address	000000000000	Clone MAC

L2TP Settings

Username		
Password		
Service IP Address		
MTU	1460	(512<=MTU Value <=1492)
Type	Keep Connection ▾	
Idle Timeout	10	(1-1000 Minutes)

Apply Cancel

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

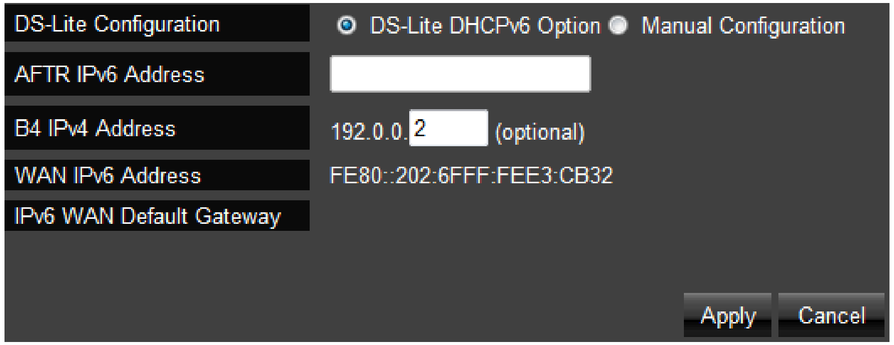
MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. The factory default MTU size of L2TP is 1460. If you wish to manually change the MTU size, set it between 1200 and 1492.

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.

Click **Apply** to enable your settings.

7.7. DS-Lite



DS-Lite Configuration: ● DS-Lite DHCPv6 Option ○ Manual Configuration

AFTR IPv6 Address:

B4 IPv4 Address: 192.0.0. 2 (optional)

WAN IPv6 Address: FE80::202:6FFF:FEE3:CB32

IPv6 WAN Default Gateway:

Dual-Stack Lite, or DS-Lite, allows ISPs to stop IPv4 addresses from reaching a customer's network devices and only use IPv6.

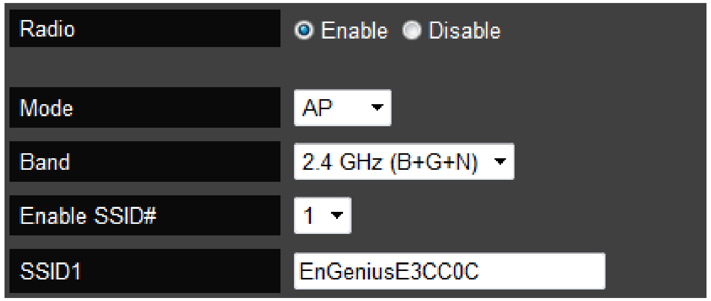
- **DS-Lite Configuration**: Select DS-Lite DHCPv6 Option or Manual Configuration.
- **AFTR IPv6 Address**: Enter the AFTR (Address Family Transition Router) IPv6 address.
- **B4 IPv4 Address**: Enter an Optional B4 IPv4 address.
- **WAN IPv6 Address**: Display the WAN IPv6 address.
- **IPv6 WAN Default Gateway**: Display the IPv6 WAN default gateway address.

Click **Apply** to enable your settings.

8. Wireless LAN

8.1. 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.



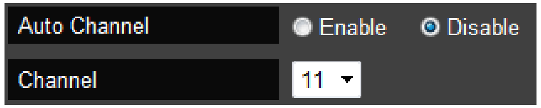
Radio	● Enable ○ Disable
Mode	AP
Band	2.4 GHz (B+G+N)
Enable SSID#	1
SSID1	EnGeniusE3CC0C

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 **ESR350H** 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).

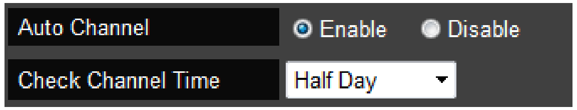


Auto Channel	○ Enable ● Disable
Channel	11

Enable SSID#: Set the number of Wireless Groups. Up to 4 can be set.

SSID[#]: The Name of the wireless network.

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.



Auto Channel	● Enable ○ Disable
Check Channel Time	Half Day

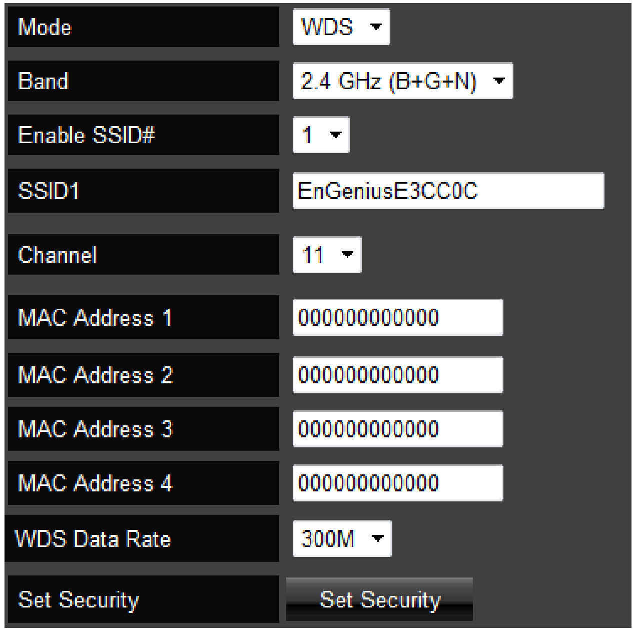
Check Channel Time: If Auto Channel is enabled, please select time period you wish the system check the appropriate channel for your router.

Wireless Distribution System Mode

Configure the router's wireless settings in WDS mode.

- **Channel**: Select a channel to assign to the wireless network.
- **MAC Address [#]**: Enter the MAC address(es) for the wireless access point(s) that are part of the WDS.
- **WDS Data Rate**: Select the data rate for the WDS.
- **Set Security**: Click **Set Security** to display the WDS security settings screen and setup the WDS security.

Click **Apply** to save the settings or **Cancel** to discard changes.

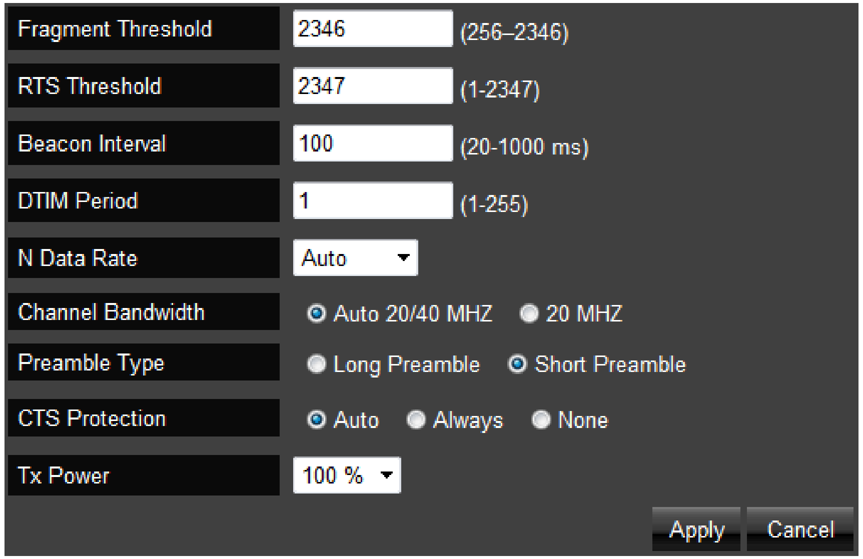


Mode	WDS
Band	2.4 GHz (B+G+N)
Enable SSID#	1
SSID1	EnGeniusE3CC0C
Channel	11
MAC Address 1	000000000000
MAC Address 2	000000000000
MAC Address 3	000000000000
MAC Address 4	000000000000
WDS Data Rate	300M
Set Security	Set Security

8.2. Advanced

To change more advanced wireless features of the **ESR350H**, select the **Advanced** option of the Wireless section.

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



Fragment Threshold	2346	(256–2346)
RTS Threshold	2347	(1-2347)
Beacon Interval	100	(20-1000 ms)
DTIM Period	1	(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	
Tx Power	100 %	

- **Fragment Threshold**: This specifies the maximum size of a packet during data transmission. A value too low could lead to low performance.
- **RTS Threshold**: If the packet size is smaller than the RTS threshold, the **ESR350H** will not use RTS/CTS to send the data packet.
- **Beacon Interval**: This is the amount of time that the ESR350H will resynchronize the network.
- **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.
- **N Data Rate**: This is the rate in which the **ESR350H** will transmit data packets to Wireless N compatible devices.
- **Channel Bandwidth**: The factory default enables Auto 20/40MHz to optimize the best performance by auto selecting channel bandwidth.
- **Preamble Type**: Select either Long Preamble (better LAN compatibility) or Short Preamble (better wireless performance).
- **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 **ESR350H**.
- **Tx Power**: Select the wireless signal strength level. Valid values are between 10% and 100%.

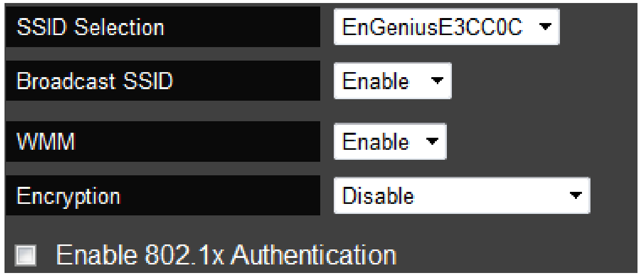
Click **Apply** to save your settings.

8.3. Security

To change the wireless security of the **ESR350H**, 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.

- **SSID Selection**: Choose the wireless network group to change the wireless security settings for.
- **Broadcast SSID**: Choose whether or not you want the Wireless Group to be visible to other members.
- **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.
- **Encryption**: Encrypt your router with passwords in different security level.



SSID Selection	EnGeniusE3CC0C
Broadcast SSID	Enable
WMM	Enable
Encryption	Disable

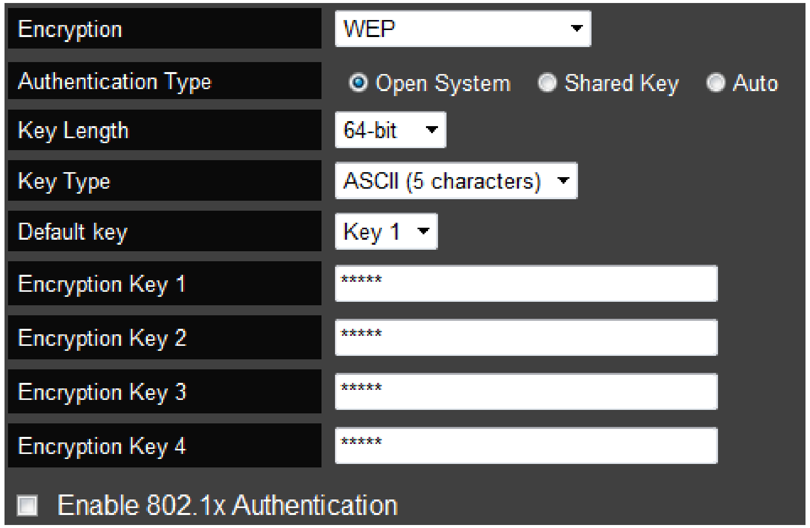
□ Enable 802.1x Authentication

Wired Equivalent Privacy (WEP)

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

- **Authentication Type**: You can select between Open System (wireless stations can associate with this **ESR350H** wirelessly without WEP encryption) or Shared Key (devices must provide the corresponding WEP key [up to 4] when trying to connect to the **ESR350H** wirelessly).
- **Key Length**: You can select between 64-bit encryption or 128-encryption keys.
- **Key Type**: You can set the characters used for the WEP Key (ASCII or Hexadecimal).
- **Encryption Key [#]**: The encryption keys used to encrypt the data packets during data transmission.

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



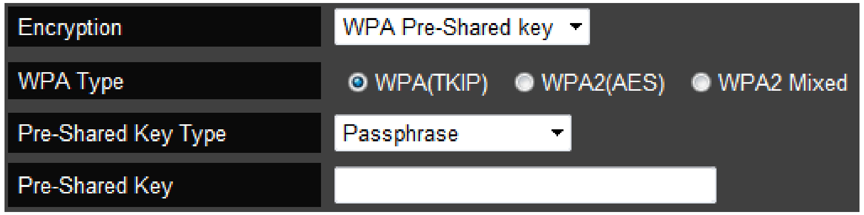
Encryption	WEP
Authentication Type	● Open System ○ Shared Key ○ Auto
Key Length	64-bit
Key Type	ASCII (5 characters)
Default key	Key 1
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****

□ Enable 802.1x Authentication

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

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

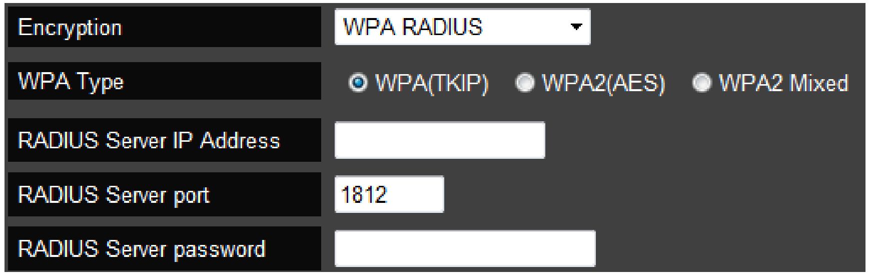
- **WPA Type:** You can select between WPA (TKIP) (Temporal Key Integrity Protocol; a 128-bit key is user per packet and is generates a new key for each packet sent), WPA2(AES) (Advanced Encryption Standard; government standard packet encryption and stronger than TKIP), or WPA2 Mixed.
- **Pre-Shared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



Encryption	WPA Pre-Shared key
WPA Type	◉ WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
Pre-Shared Key Type	Passphrase
Pre-Shared Key	

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 **ESR350H**.



Encryption	WPA RADIUS
WPA Type	◉ WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
RADIUS Server IP Address	
RADIUS Server port	1812
RADIUS Server password	

Note: 802.11n does not allow WEP/WPA-PSK TKIP/WPA-PSK2 TKIP security mode. The connection mode will drop from 802.11n to 802.11g.

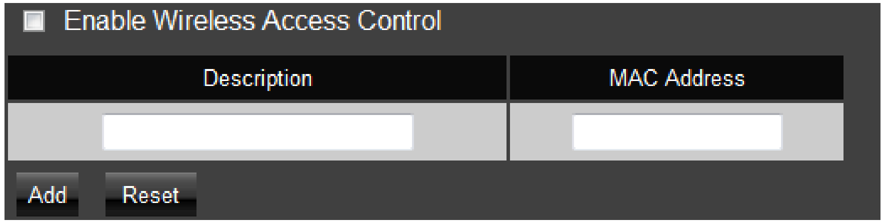
8.4. Filter

When Enable Wireless Access Control selected, only wireless clients with MAC addresses listed in the table are allowed to connect to the wireless network.

Enable Wireless Access Control

- **Description**: Enter a description of the device allowed to connect to the network.
- **MAC Address**: Enter the MAC address of the wireless device.

Click **Add** to append a new device to the list or **Reset** to discard changes.



MAC Address Filtering Table

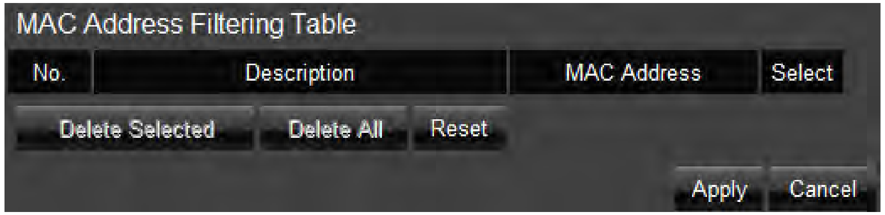
- **No.**: The sequence number of the device.
- **Description**: The description of the device.
- **MAC Address**: The MAC address of the device.
- **Select**: Indicates the device(s) that can have actions performed on them.

Click **Delete Selected** to remove selected devices from the list.

Click **Delete All** to remove all devices form the list.

Click **Reset** the discard changes.

Click **Apply** to save the settings or **Cancel** to discard changes.

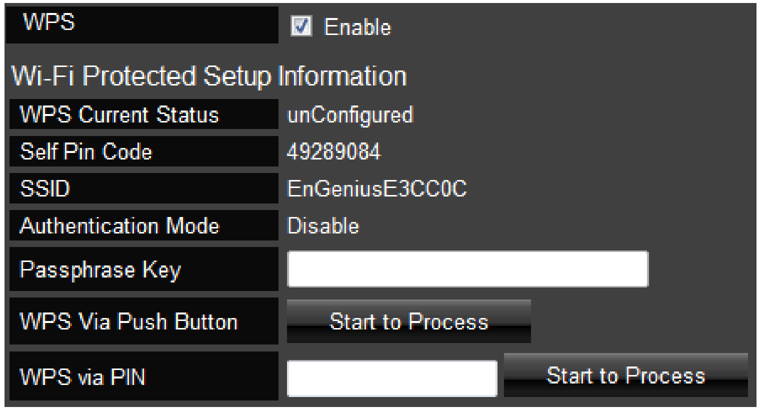


8.5. WPS

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 **ESR350H**. This can automate connection between the device and the **ESR350H** by use of a button or a PIN.

- **WPS**: Check the box if you want to enable WPS.
- **WPS Current Status**: A notification if the wireless security is configured or not configured.
- **Self Pin Code**: This is the Wireless PIN of this **ESR350H**.
- **SSID**: This is the wireless network name you are currently configuring.
- **Authentication Mode**: The current security settings for the corresponding SSID.
- **Passphrase Key**: The randomly generated key created by the **ESR350H** during WPS.
- **WPS via Push Button**: Start the WPS process via a button.
- **WPS via PIN**: Start the WPS process by entering the PIN of the wireless device.



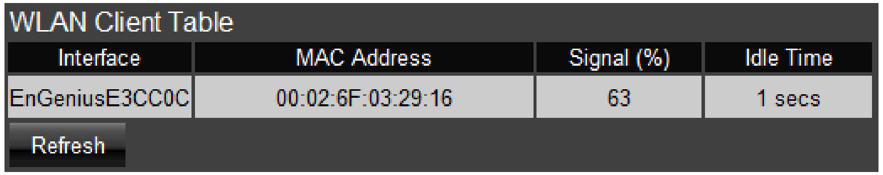
WPS	☑ Enable

Wi-Fi Protected Setup Information

WPS Current Status	unConfigured
Self Pin Code	49289084
SSID	EnGeniusE3CC0C
Authentication Mode	Disable
Passphrase Key	
WPS Via Push Button	Start to Process
WPS via PIN	Start to Process

8.6. Client List

To view the wireless devices currently connected to the **ESR350H**, select the **Client List** option in the Wireless section.



WLAN Client Table

Interface	MAC Address	Signal (%)	Idle Time
EnGeniusE3CC0C	00:02:6F:03:29:16	63	1 secs

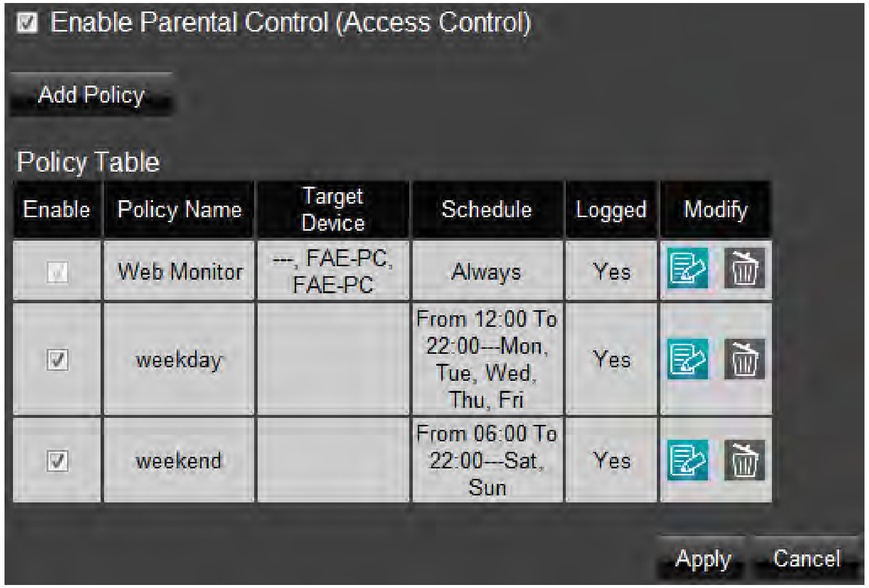
9. Parental Control

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.

9.1. 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 Parental Control (Access Control)

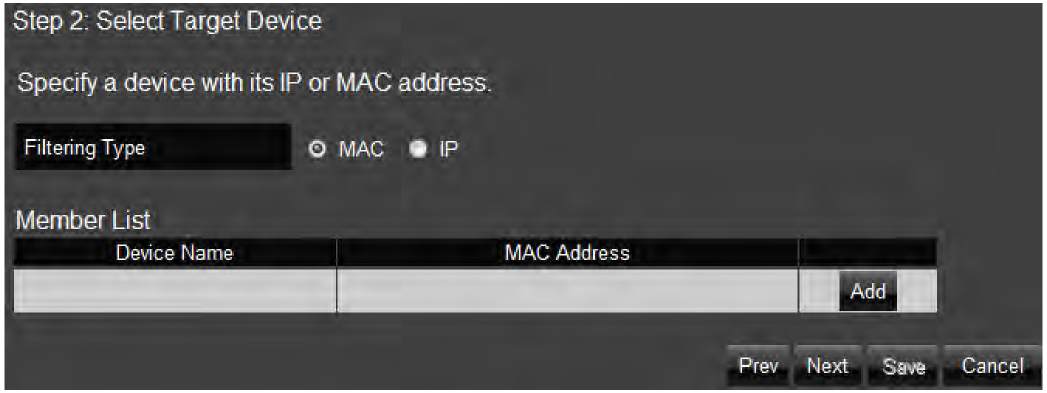
Policy Table

Enable	Policy Name	Target Device	Schedule	Logged	Modify
☐	Web Monitor	---, FAE-PC, FAE-PC	Always	Yes	✎ 🗑
☑	weekday		From 12:00 To 22:00---Mon, Tue, Wed, Thu, Fri	Yes	✎ 🗑
☑	weekend		From 06:00 To 22:00---Sat, Sun	Yes	✎ 🗑

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

Name the Policy. Click **Next.**

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



Step 2: Select Target Device

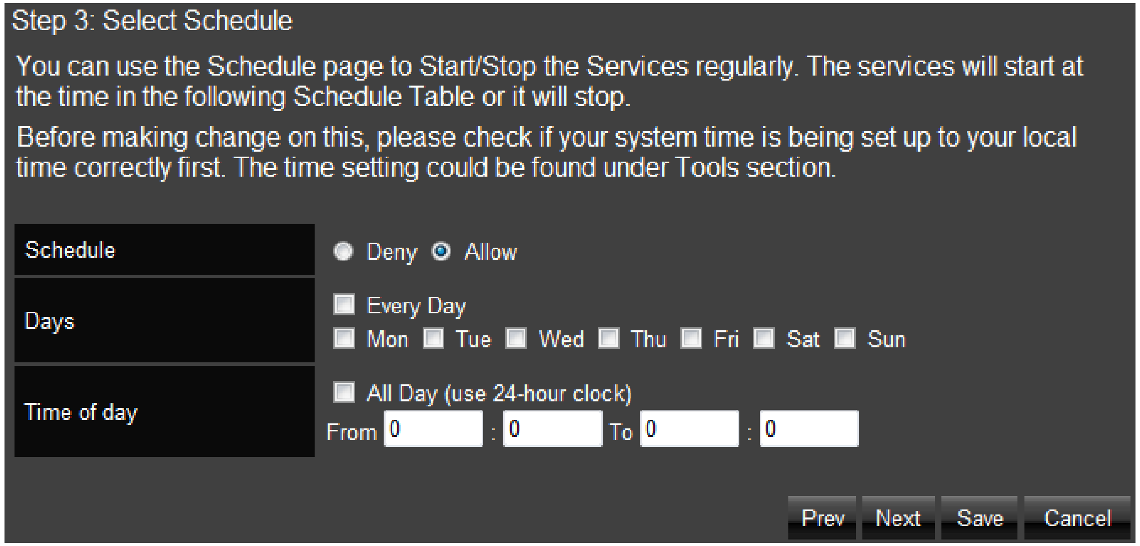
Specify a device with its IP or MAC address.

Filtering Type ● MAC ○ IP

Member List

Device Name	MAC Address	
		Add

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



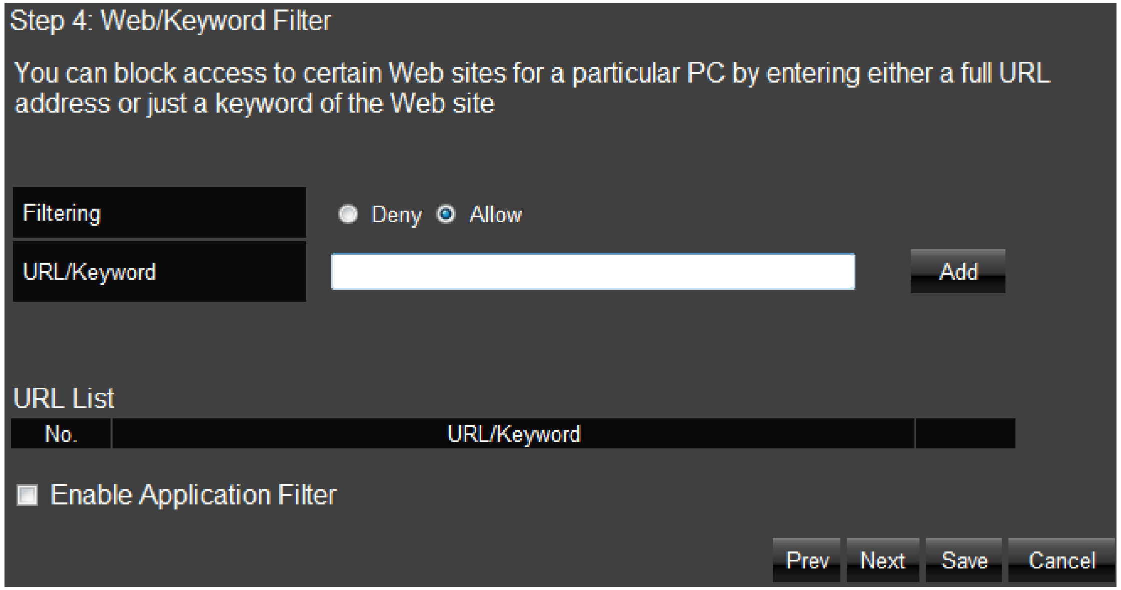
Step 3: Select Schedule

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.

Before making change on this, please check if your system time is being set up to your local time correctly first. The time setting could be found under Tools section.

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

3. 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

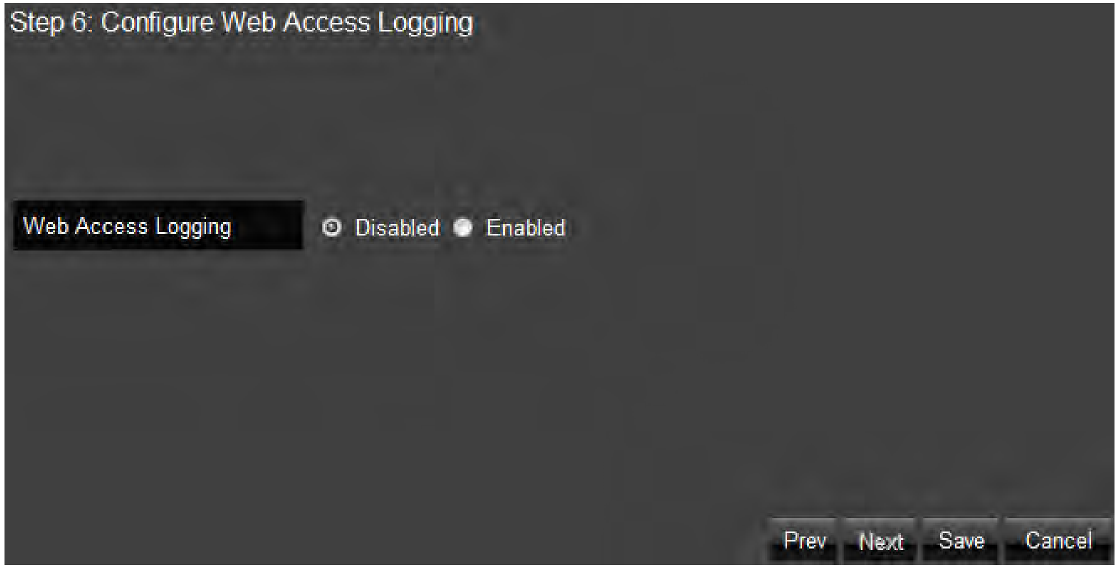
URL/Keyword

URL List

No.	URL/Keyword	

□ Enable Application Filter

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

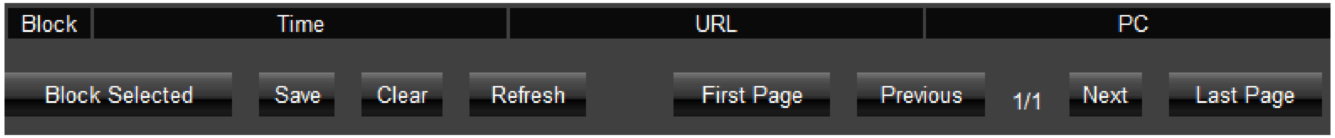


Step 6: Configure Web Access Logging

Web Access Logging ● Disabled ○ Enabled

9.2. 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.



Block	Time	URL	PC

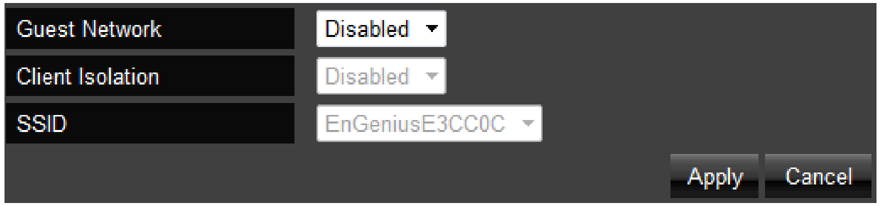
10. Guest Network

The Guest Network function enables you to offer Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.

The Guest Network is controlled by the Wireless SSID function. When the Guest Network function is enabled, the Guest SSID can only get the internet connection from WAN, but can not reach the client from the LAN port.

10.1. Enabling Guest Network

- **Guest Network**: Enable or Disable the Guest Network function
- **Client Isolation**: Guest clients are isolated and can not communicate with each other.
- **SSID**: Choose a SSID for the Guest Network used. The SSID can be defined from the Wireless setting page.



Guest Network: Disabled
Client Isolation: Disabled
SSID: EnGeniusE3CC0C

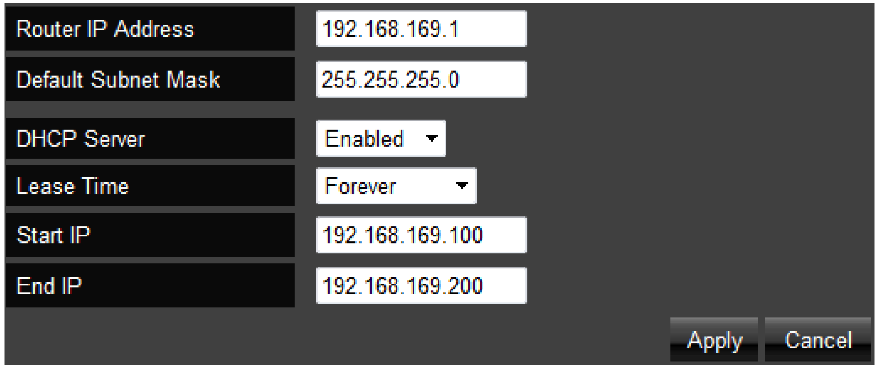
Click **Apply** to save the settings or **Cancel** to discard changes.

10.2. DHCP Server Setting

DHCP server automatically assigns IP address to computers on your Guest network.

- **Router IP Address**: Define the router IP address for the Guest network.
- **Default Subnet Mask**: Define the Subnet Mask IP address for the Guest network.
- **DHCP Server**: To enable or disable the Guest network DHCP server.
- **Lease Time**: To define the Guest Network DHCP server lease time.
- **Start IP**: To define the Guest network DHCP server start IP.
- **End IP**: To define the Guest network DHCP server end IP.

Click **Apply** to save the settings or **Cancel** to discard changes.



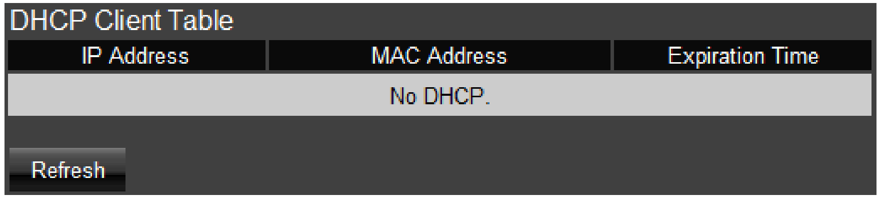
Router IP Address	192.168.169.1
Default Subnet Mask	255.255.255.0
DHCP Server	Enabled
Lease Time	Forever
Start IP	192.168.169.100
End IP	192.168.169.200

10.3. DHCP Client Table

Displays all the connected DHCP clients whose IP addresses are assigned by the DHCP Server in your Guest network.

DHCP Client Table: View the guest network client list.

Click **Refresh** to refresh the view of the list.



DHCP Client Table

IP Address	MAC Address	Expiration Time
	No DHCP.	

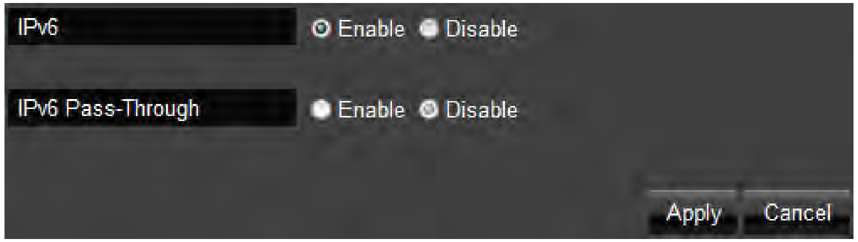
11.IPv6

There are several connection types to choose from: Auto Detection, Static IPv6, Auto configuration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 Tunnel, 6to4, and Link-local. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

11.1. Basic

- **IPv6**: Enable or disable IPv6 feature.
- **IPv6 Pass-Through**: Enable or disable IPv6 Pass-Through feature.

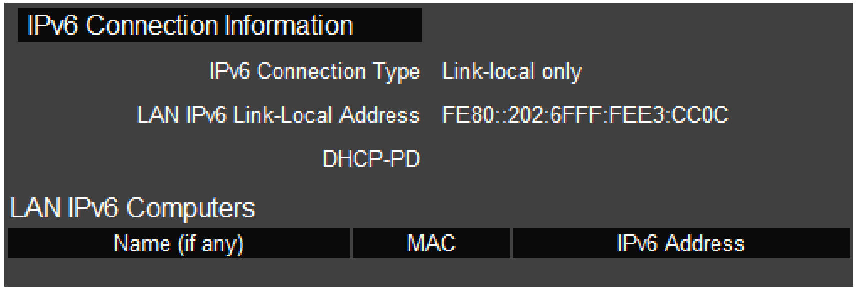


IPv6 ● Enable ○ Disable

IPv6 Pass-Through ○ Enable ● Disable

11.2. Status

- **IPv6 Connection Information**: Shows the IPv6 connection type, the LAN IPv6 link-local address and the DHCP-PD.
- **LAN IPv6 Computers Table**: Shows a list of network computers and their IPv6 connection information.



IPv6 Connection Information

IPv6 Connection Type Link-local only

LAN IPv6 Link-Local Address FE80::202:6FFF:FEE3:CC0C

DHCP-PD

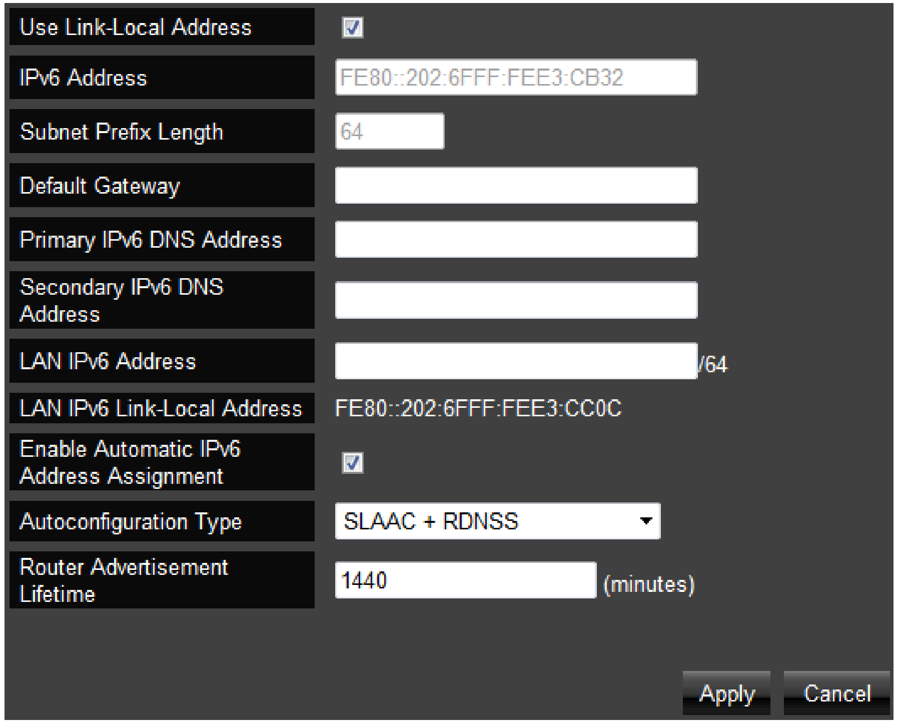
LAN IPv6 Computers

Name (if any)	MAC	IPv6 Address

11.3. Static IPv6

- **Use Link-Local Address**: Enable or disable LAN link-local address.
- **IPv6 Address**: Enter the LAN (local) IPv6 address for the router.
- **Subnet Prefix Length**: Enter the subnet prefix length.
- **Default Gateway**: Enter the default gateway.
- **Primary IPv6 DNS Address**: Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address**: Enter the secondary IPv6 DNS address.
- **LAN IPv6 Address**: Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address**: Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment**: Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type**: Select the autoconfiguration type. (Default: SLAAC +RDNSS).
- **Router Advertisement Lifetime**: Enter the IPv6 Address Lifetime (in minutes).

Click **Apply** to save the settings or **Cancel** to discard changes.

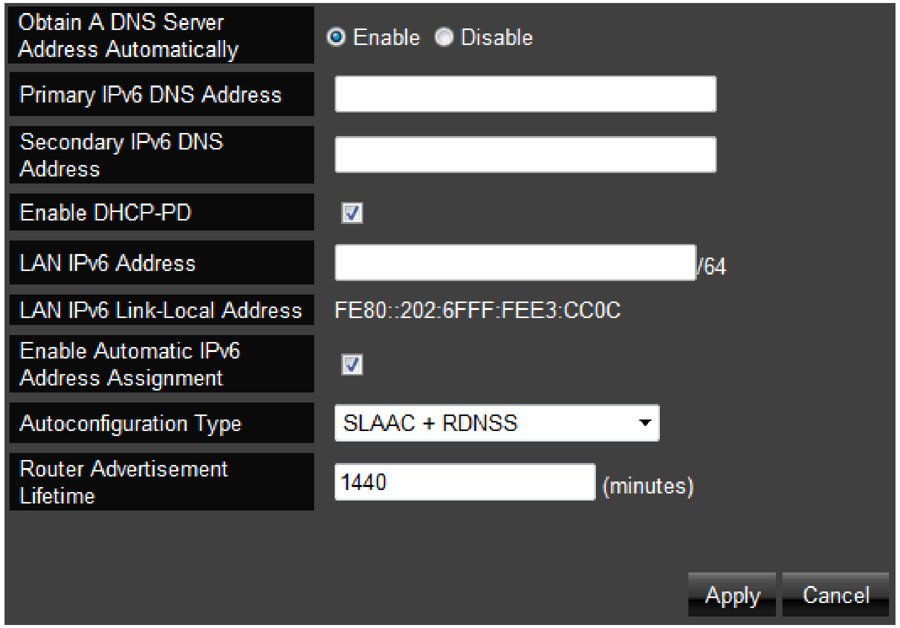


Use Link-Local Address	☑
IPv6 Address	FE80::202:6FFF:FEE3:CB32
Subnet Prefix Length	64
Default Gateway	
Primary IPv6 DNS Address	
Secondary IPv6 DNS Address	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	FE80::202:6FFF:FEE3:CC0C
Enable Automatic IPv6 Address Assignment	☑
Autoconfiguration Type	SLAAC + RDNSS
Router Advertisement Lifetime	1440 (minutes)

11.4. Auto Configuration

- **Obtain A DNS Server Address Automatically**: Enable or disable obtaining a DNS server automatically.
- **Primary IPv6 DNS Address**: Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address**: Enter the secondary IPv6 DNS address.
- **Enable DHCP-PD**: Enable or disable DHCP-prefix delegation (PD).
- **LAN IPv6 Address**: Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address**: Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment**: Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type**: Select the autoconfiguration type. (Default: SLAAC +RDNSS)
- **Router Advertisement Lifetime**: Enter the IPv6 Address Lifetime (in minutes).

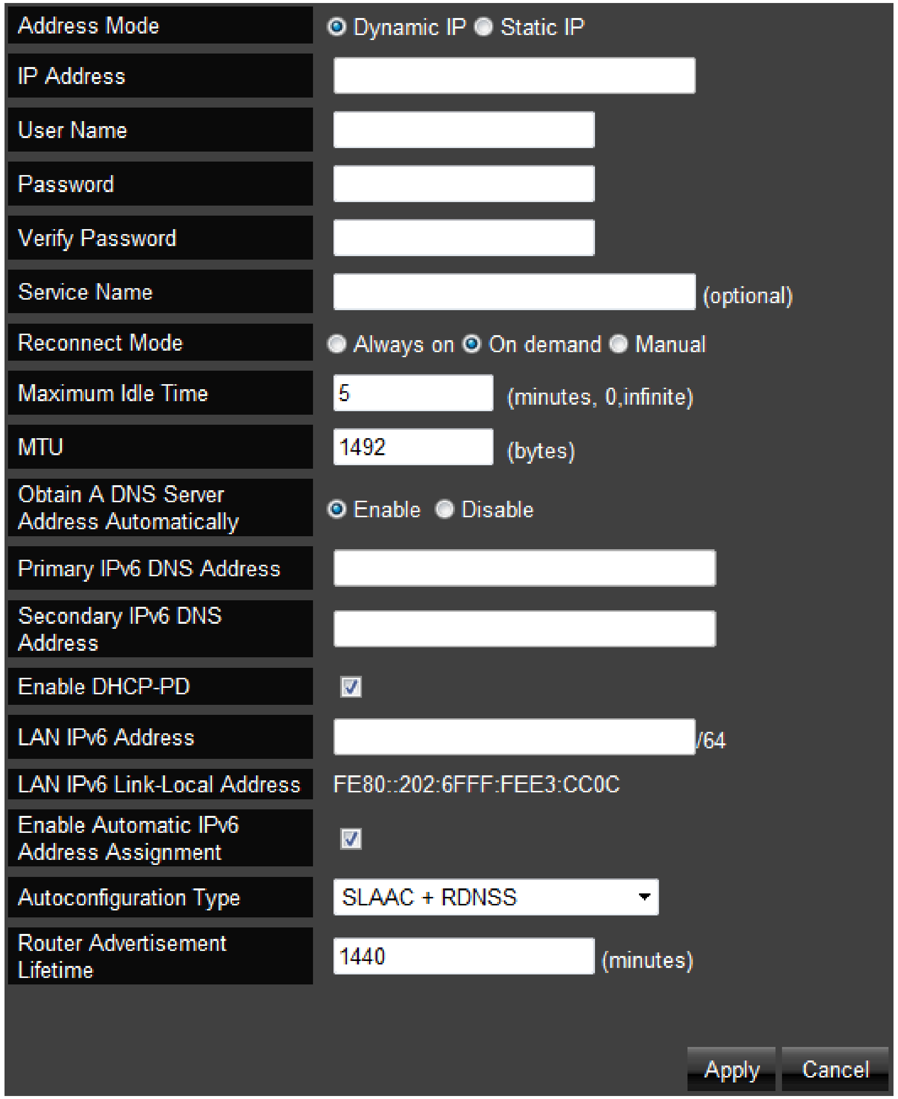
Click **Apply** to save the settings or **Cancel** to discard changes.



Obtain A DNS Server Address Automatically	● Enable ○ Disable
Primary IPv6 DNS Address	
Secondary IPv6 DNS Address	
Enable DHCP-PD	☑
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	FE80::202:6FFF:FEE3:CC0C
Enable Automatic IPv6 Address Assignment	☑
Autoconfiguration Type	SLAAC + RDNSS
Router Advertisement Lifetime	1440 (minutes)

11.5. PPPoE

- **Address Mode**: Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.
- **IP Address**: Enter the IP address (Static PPPoE only).
- **User Name**: Enter your PPPoE user name.
- **Password**: Enter your PPPoE password.
- **Verify Password**: Retype the your PPPoE password.
- **Service Name**: Enter the ISP Service Name (optional).
- **Reconnect Mode**: Select either Always-on, On-Demand, or Manual.
- **Maximum Idle Time**: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
- **MTU**: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.
- **Obtain A DNS Server Address Automatically**: Enable or disable obtaining a DNS server automatically.
- **Primary IPv6 DNS Address**: Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address**: Enter the secondary IPv6 DNS address.
- **Enable DHCP-PD**: Enable or disable DHCP-prefix delegation (PD).
- **LAN IPv6 Address**: Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address**: Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment**: Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type**: SelectEnter the autoconfiguration type. (Default: SLAAC +RDNSS)
- **Router Advertisement Lifetime**: Enter the IPv6 Address Lifetime (in minutes).



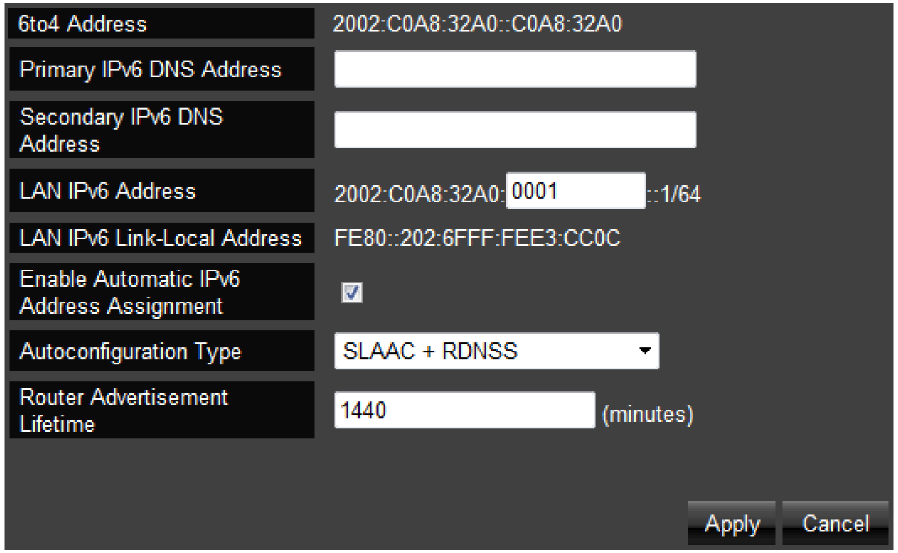
Address Mode	● Dynamic IP ○ Static IP
IP Address	
User Name	
Password	
Verify Password	
Service Name	(optional)
Reconnect Mode	○ Always on ● On demand ○ Manual
Maximum Idle Time	5 (minutes, 0,infinite)
MTU	1492 (bytes)
Obtain A DNS Server Address Automatically	● Enable ○ Disable
Primary IPv6 DNS Address	
Secondary IPv6 DNS Address	
Enable DHCP-PD	☑
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	FE80::202:6FFF:FEE3:CC0C
Enable Automatic IPv6 Address Assignment	☑
Autoconfiguration Type	SLAAC + RDNSS
Router Advertisement Lifetime	1440 (minutes)

Click **Apply** to save the settings or **Cancel** to discard changes.

11.6. 6to4

- **6to4 Address**: Enter the 6to4 IP address.
- **Primary IPv6 DNS Address**: Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address**: Enter the secondary IPv6 DNS address.
- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address**: Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment**: Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type**: Select the autoconfiguration type. (Default: SLAAC +RDNSS)
- **Router Advertisement Lifetime**: Enter the IPv6 Address Lifetime (in minutes).

Click **Apply** to save the settings or **Cancel** to discard changes.

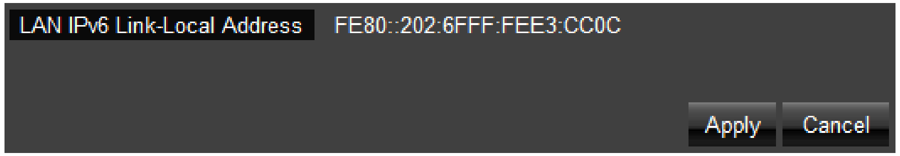


6to4 Address	2002:C0A8:32A0::C0A8:32A0
Primary IPv6 DNS Address	
Secondary IPv6 DNS Address	
LAN IPv6 Address	2002:C0A8:32A0: 0001 ::1/64
LAN IPv6 Link-Local Address	FE80::202:6FFF:FEE3:CC0C
Enable Automatic IPv6 Address Assignment	☑
Autoconfiguration Type	SLAAC + RDNSS
Router Advertisement Lifetime	1440 (minutes)

11.7. Link Local

- **LAN IPv6 Link-Local Address**: Enter the LAN IPv6 link-local address.

Click **Apply** to save the settings or **Cancel** to discard changes.



LAN IPv6 Link-Local Address FE80::202:6FFF:FEE3:CC0C

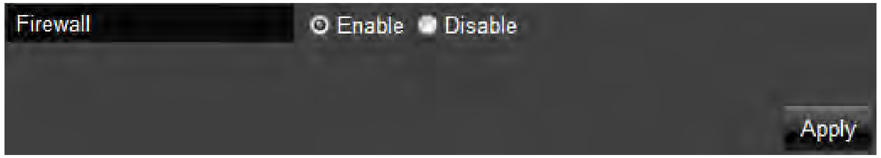
12. Firewall

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

12.1. Basic

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

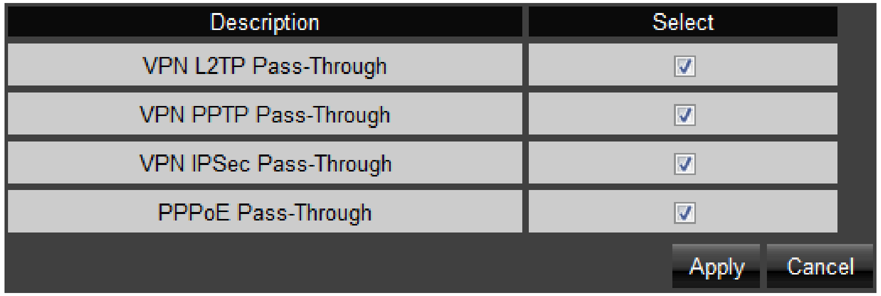
In the **Basic** option, select whether or not you wan to Enable or Disable the firewall settings of the **ESR350H**.



Firewall ● Enable ○ Disable

12.2. 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, VPN IPSec Passthrough and PPPoE Passthrough are enabled by factory default.



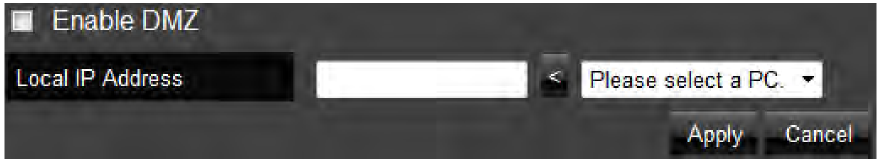
Description	Select
VPN L2TP Pass-Through	☑
VPN PPTP Pass-Through	☑
VPN IPSec Pass-Through	☑
PPPoE Pass-Through	☑

12.3. 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**.

- **Enable DMZ**: Click Enable DMZ to activate DMZ functionality.
- **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.


☐ Enable DMZ
Local IP Address

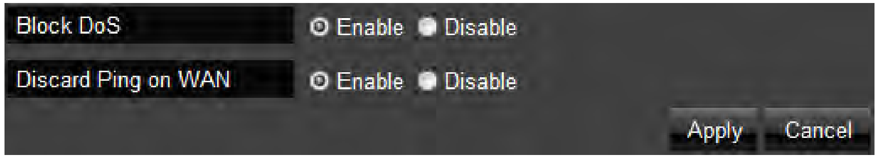
Click **Apply** to save the settings or **Cancel** to discard changes.

12.4. 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.

- **Block DoS**: Enable or disable blocking DoS attacks.
- **Discard Ping on WAN**: ICMP (ping) packages are blocked while Block DoS is enabled. Enable Discard Ping on WAN if the WAN port is required.



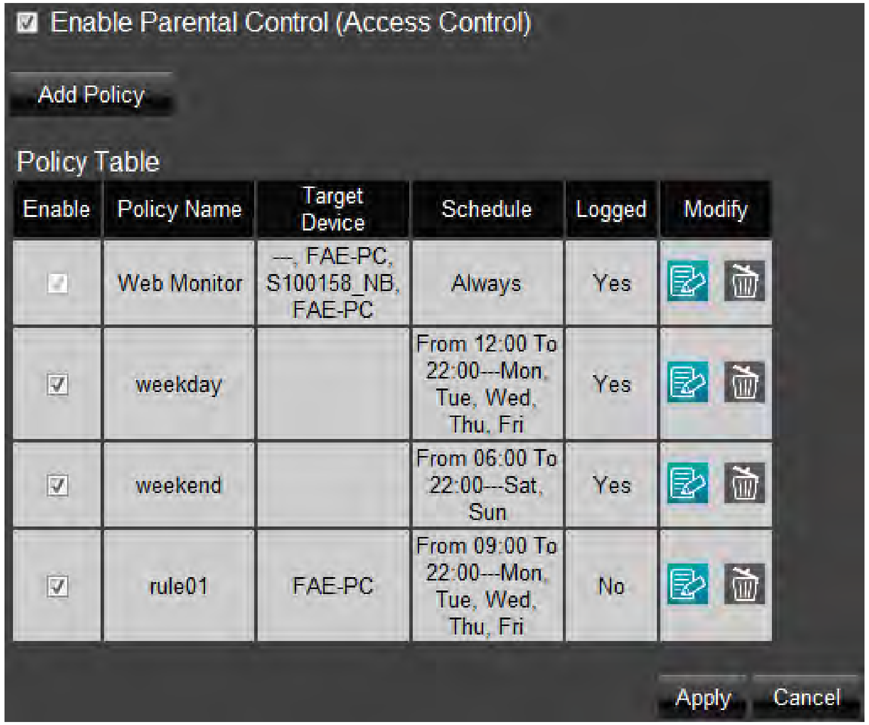
Block DoS ◉ Enable ○ Disable

Discard Ping on WAN ◉ Enable ○ Disable

Click **Apply** to save the settings or **Cancel** to discard changes.

12.5. 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.



☑ Enable Parental Control (Access Control)

Policy Table

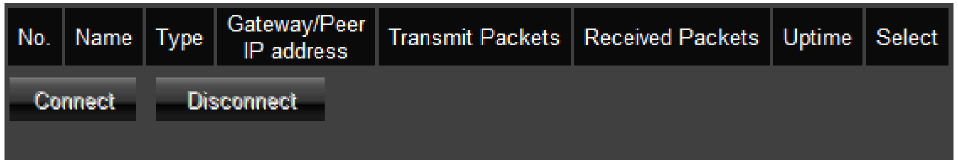
Enable	Policy Name	Target Device	Schedule	Logged	Modify
☑	Web Monitor	---, FAE-PC, S100158_NB, FAE-PC	Always	Yes	✎ 🗑
☑	weekday		From 12:00 To 22:00---Mon, Tue, Wed, Thu, Fri	Yes	✎ 🗑
☑	weekend		From 06:00 To 22:00---Sat, Sun	Yes	✎ 🗑
☑	rule01	FAE-PC	From 09:00 To 22:00---Mon, Tue, Wed, Thu, Fri	No	✎ 🗑

13. VPN (Virtual Private Network)

13.1. 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 ESR350H 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 **ESR350H**, 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.

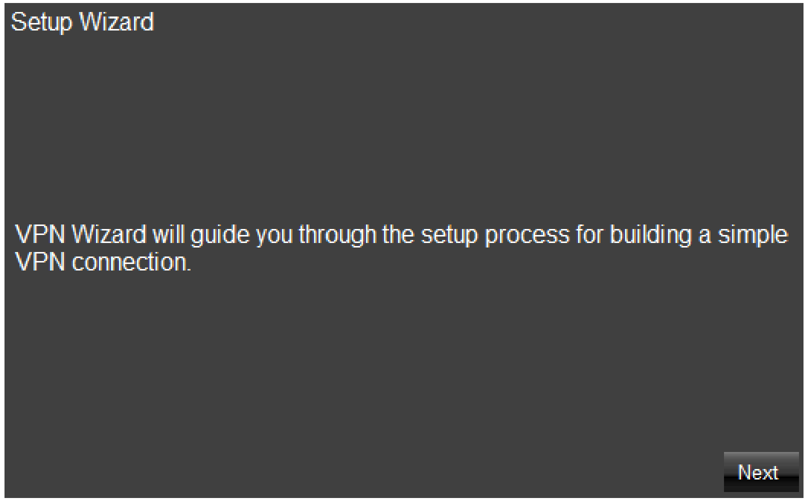


No.	Name	Type	Gateway/Peer IP address	Transmit Packets	Received Packets	Uptime	Select

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.

13.2. VPN Wizard

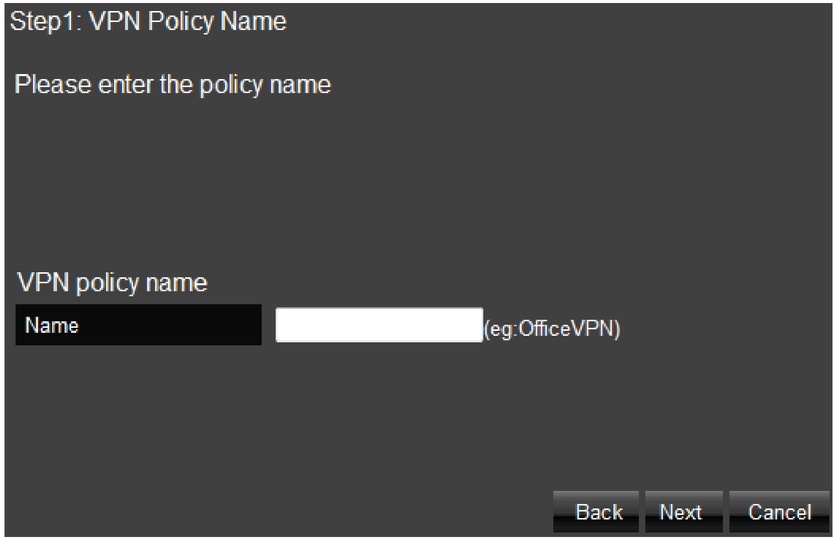
Click **Next** to start VPN Wizard



Setup Wizard

VPN Wizard will guide you through the setup process for building a simple VPN connection.

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



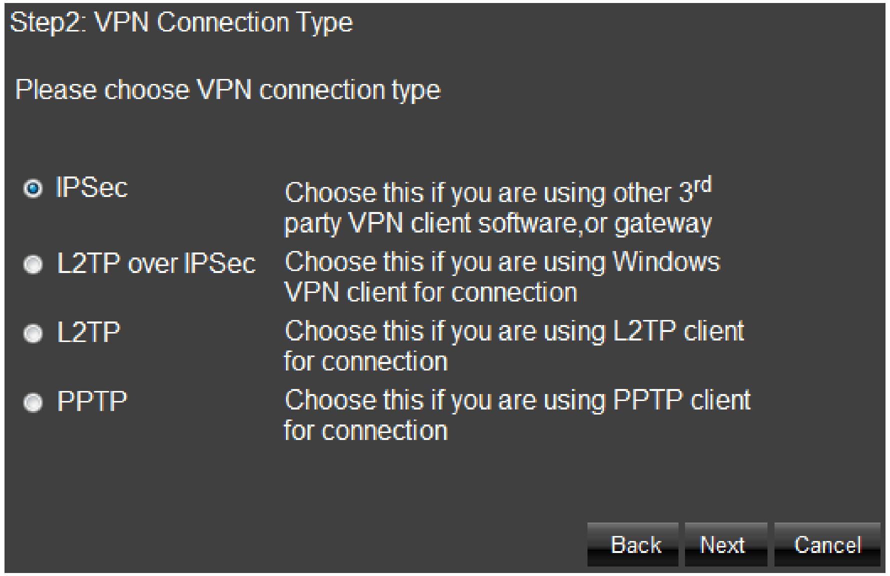
Step1: VPN Policy Name

Please enter the policy name

VPN policy name

Name (eg:OfficeVPN)

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



Step2: VPN Connection Type

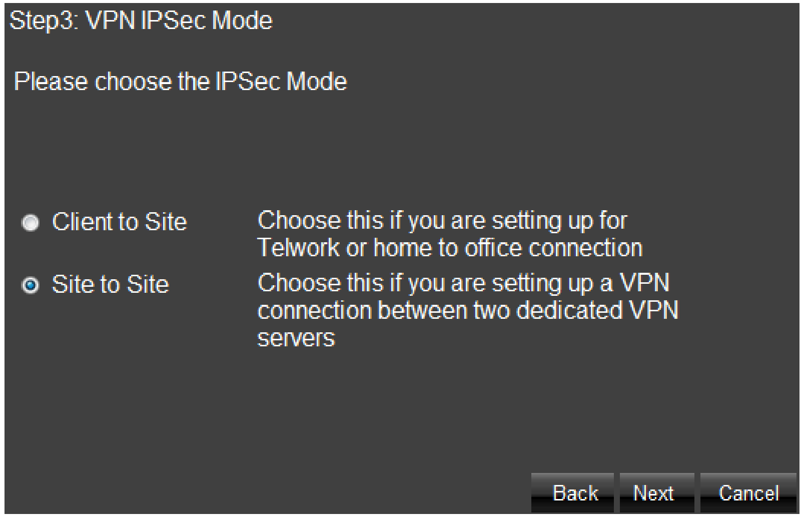
Please choose VPN connection type

- ● IPSec — Choose this if you are using other 3rd party VPN client software,or gateway
- ○ L2TP over IPSec — Choose this if you are using Windows VPN client for connection
- ○ L2TP — Choose this if you are using L2TP client for connection
- ○ PPTP — Choose this if you are using PPTP client for connection

IPSec Setting

You can select **Client to Site** or **Site to Site** in this page then click **Next** to next page.

Note. If you select **Client to Site**, you will pass next step.



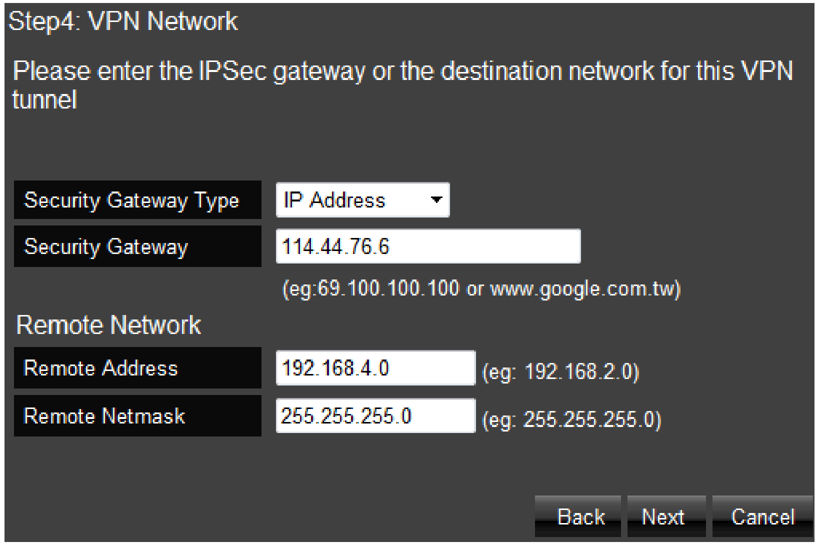
Step3: VPN IPSec Mode

Please choose the IPSec Mode

○ Client to Site — Choose this if you are setting up for Telwork or home to office connection

● Site to Site — Choose this if you are setting up a VPN connection between two dedicated VPN servers

Enter the **Security Gateway** and **Remote Network**. Then click **Next** to next page.



Step4: VPN Network

Please enter the IPSec gateway or the destination network for this VPN tunnel

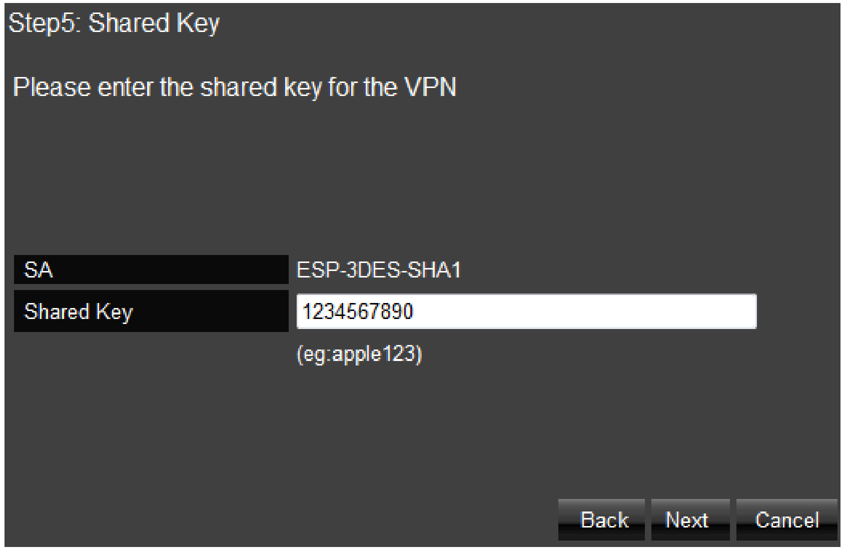
Security Gateway Type	IP Address
Security Gateway	114.44.76.6

(eg:69.100.100.100 or www.google.com.tw)

Remote Network

Remote Address	192.168.4.0	(eg: 192.168.2.0)
Remote Netmask	255.255.255.0	(eg: 255.255.255.0)

Enter the **Shared Key** for the VPN connection. Then click **Next** to next page.

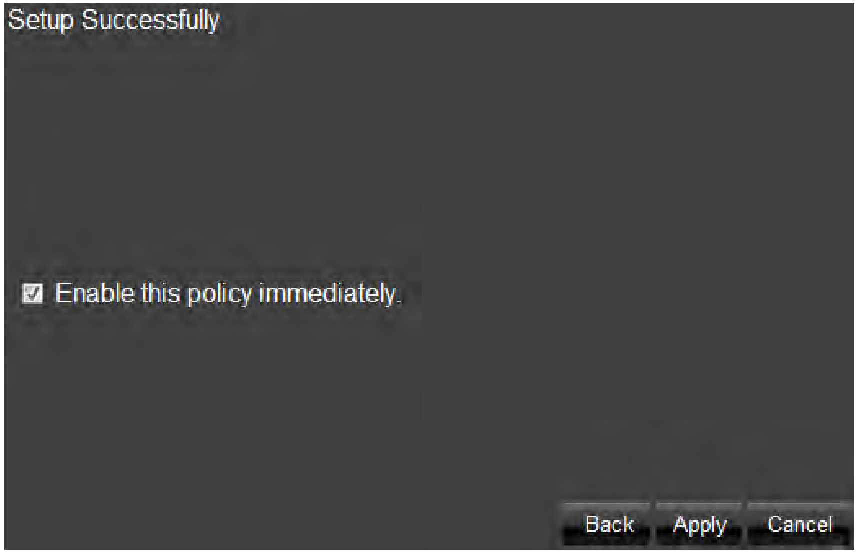


Step5: Shared Key

Please enter the shared key for the VPN

SA	ESP-3DES-SHA1
Shared Key	1234567890 (eg:apple123)

Setup successfully, enable this policy immediately. If you don’t want enable this policy, you can un-tick the box. Then click **Apply** button to apply the settings.

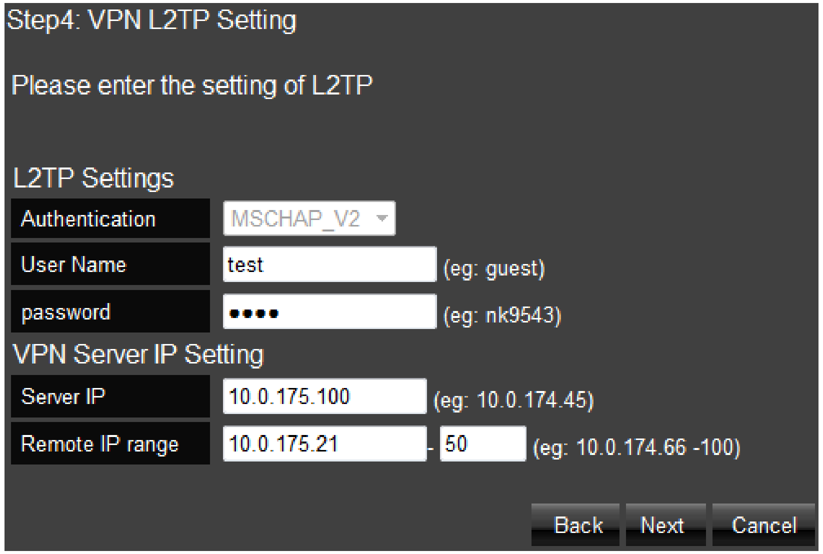


Setup Successfully

☑ Enable this policy immediately.

L2TP over IPSec Setting

Enter the **Username**, **Password** and **VPN Server IP setting**. Then click **Next** to next page.



Step4: VPN L2TP Setting

Please enter the setting of L2TP

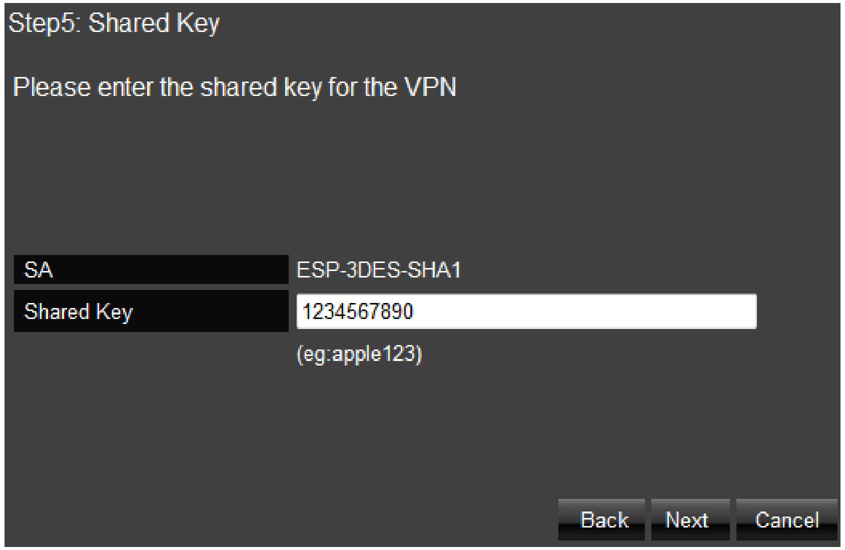
L2TP Settings

Authentication	MSCHAP_V2	
User Name	test	(eg: guest)
password	••••	(eg: nk9543)

VPN Server IP Setting

Server IP	10.0.175.100	(eg: 10.0.174.45)
Remote IP range	10.0.175.21 - 50	(eg: 10.0.174.66 -100)

Enter the **Shared Key** for the VPN connection. Then click **Next** to next page.

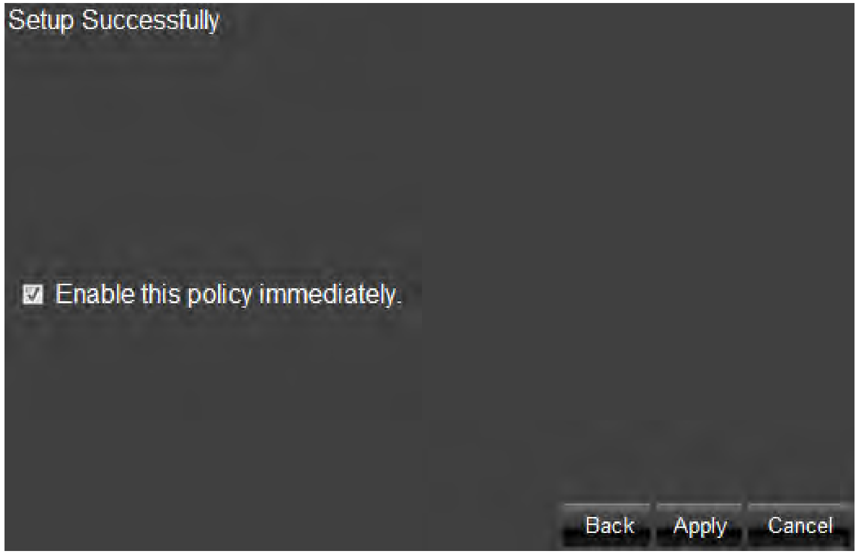


Step5: Shared Key

Please enter the shared key for the VPN

SA	ESP-3DES-SHA1
Shared Key	1234567890 (eg:apple123)

Setup successfully, enable this policy immediately. If you don't want enable this policy, you can un-tick the box. Then click **Apply** to apply the settings.



Setup Successfully

☑ Enable this policy immediately.

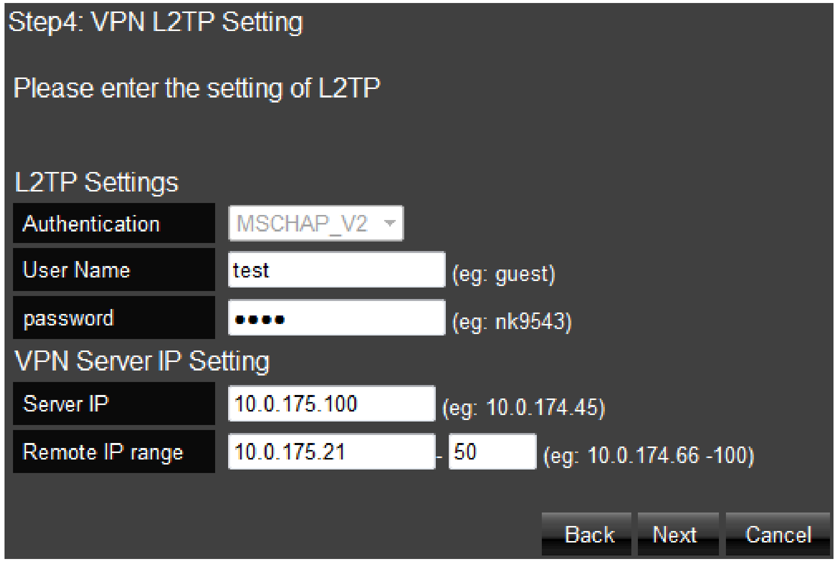
L2TP Settings

- **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 ESR350H 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

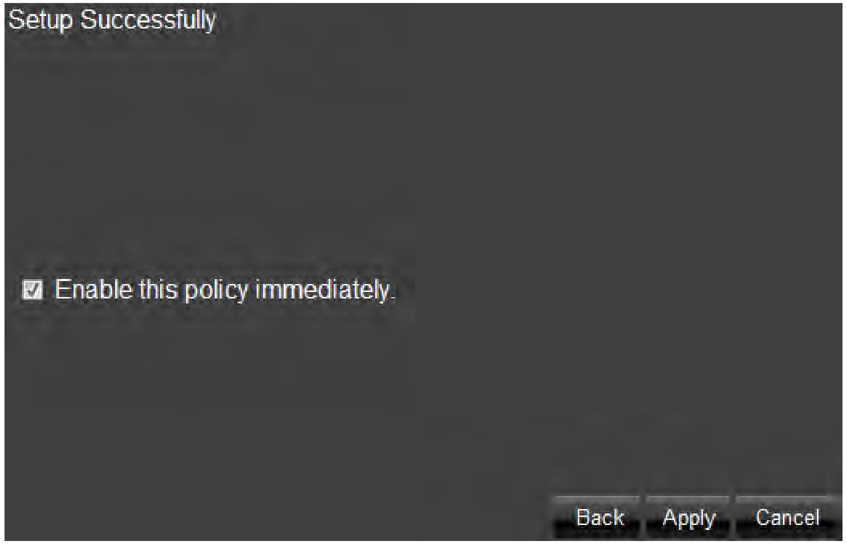
L2TP Settings

Authentication	MSCHAP_V2	
User Name	test	(eg: guest)
password	••••	(eg: nk9543)

VPN Server IP Setting

Server IP	10.0.175.100	(eg: 10.0.174.45)
Remote IP range	10.0.175.21 - 50	(eg: 10.0.174.66 -100)

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.



Setup Successfully

☑ Enable this policy immediately.

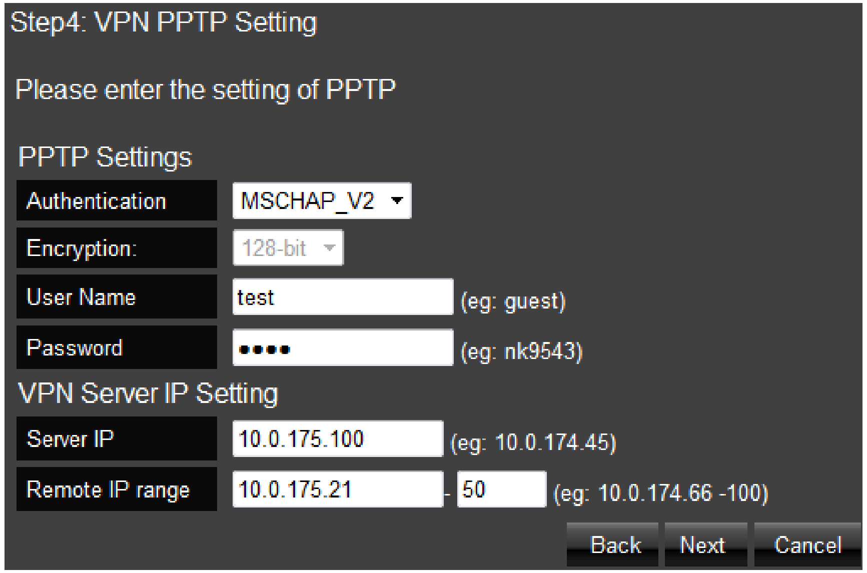
PPTP Setting

- **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 ESR350H 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

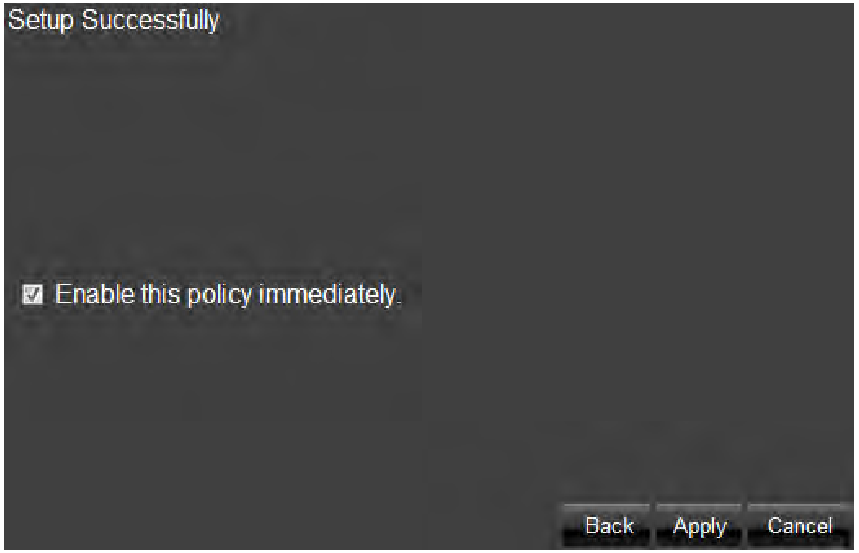
PPTP Settings

Authentication	MSCHAP_V2	
Encryption:	128-bit	
User Name	test	(eg: guest)
Password	••••	(eg: nk9543)

VPN Server IP Setting

Server IP	10.0.175.100	(eg: 10.0.174.45)
Remote IP range	10.0.175.21 - 50	(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.



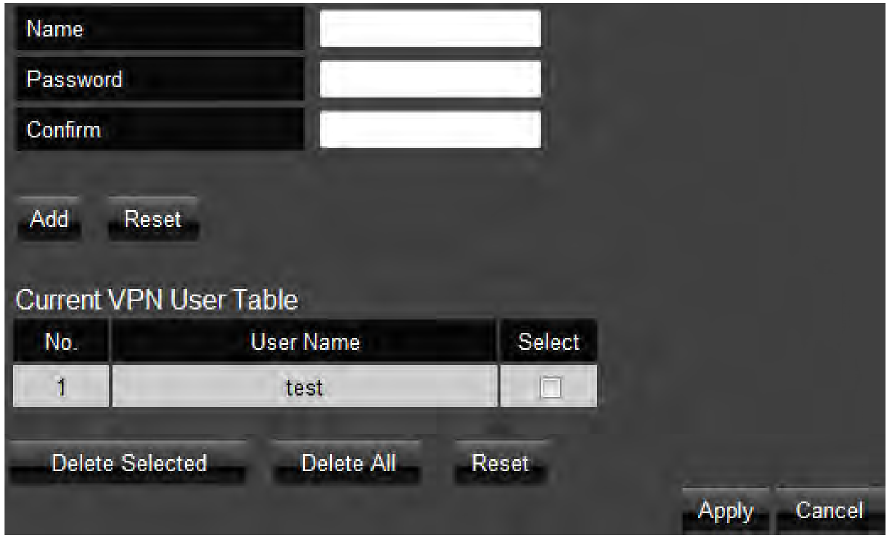
Setup Successfully

☑ Enable this policy immediately.

13.3. 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**.



Name	
Password	
Confirm	

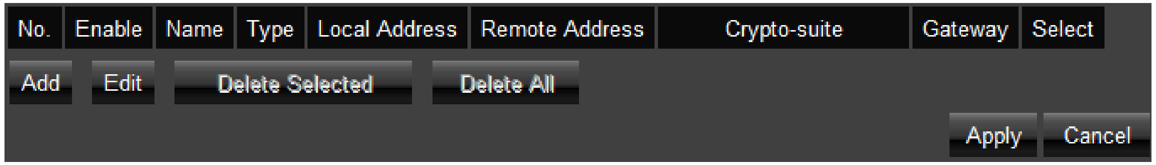
Current VPN User Table

No.	User Name	Select
1	test	□

13.4. Profile Setting

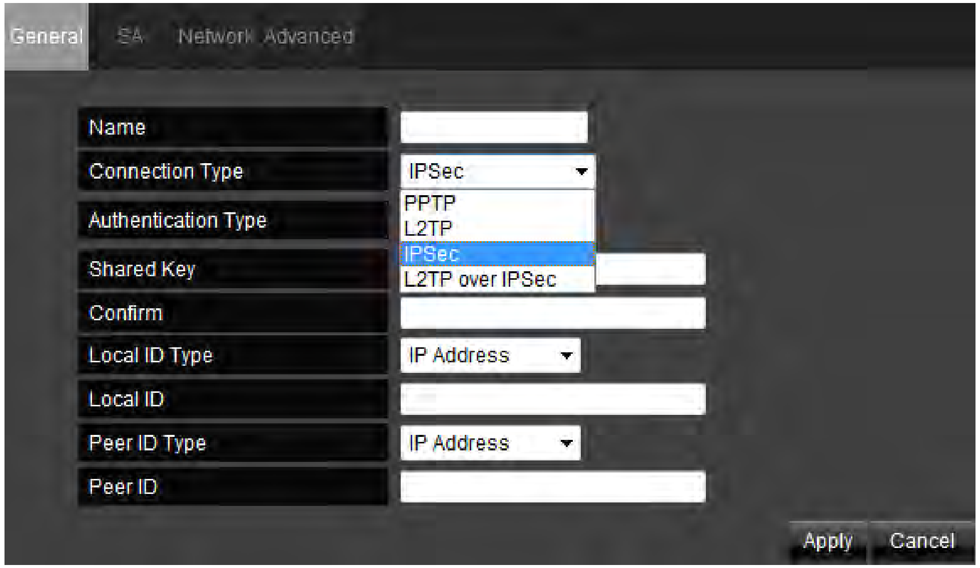
If you wish to manually setup a VPN tunnel, you can go to **Profile Setting** in the VPN section. Before getting started, please select **User Setting** to create the user profile ahead of time.

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



No.	Enable	Name	Type	Local Address	Remote Address	Crypto-suite	Gateway	Select

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

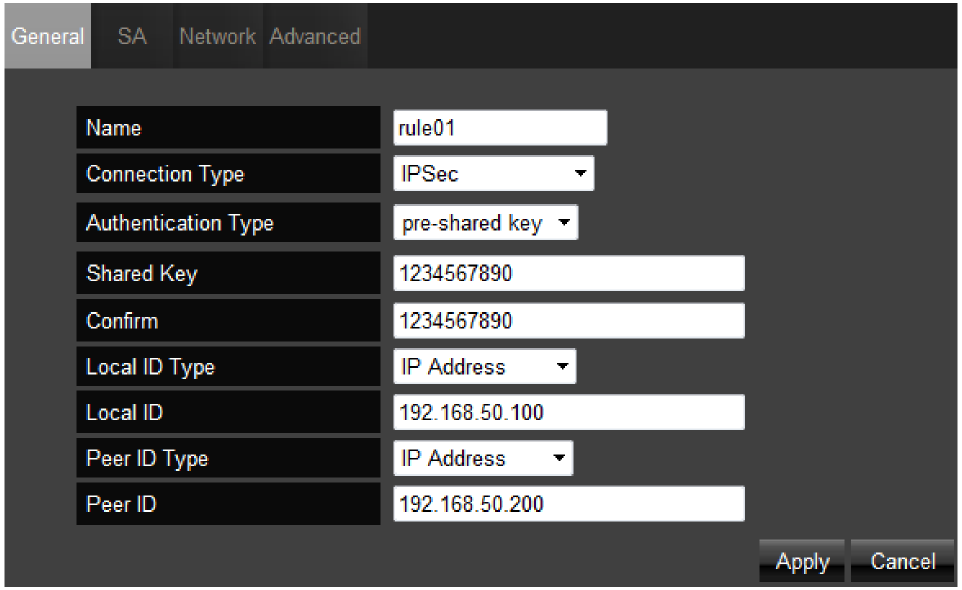


Name	
Connection Type	IPSec
Authentication Type	
Shared Key	
Confirm	
Local ID Type	IP Address
Local ID	
Peer ID Type	IP Address
Peer ID	

IPSec profile setting

General

- **Name**: Enter a name for your VPN policy.
- **Connection Type**: Supports **PPTP**, **L2TP**, **IPSec** and **L2TP over IPSec** methods to establish VPN connection.
- **Authentication Type**: Supports pre-shared key method for authentication.
- **Shared Key**: Enter the Shared Key in box.
- **Confirm**: Enter your Shared Key again for verification.
- **Local ID Type**: Supports IP Address, Domain Name, Email Address methods for Local ID Type.
- **Local ID**: Enter an ID to identify and authenticate the local VPN endpoint.
- **Peer ID Type**: Supports IP Address, Domain Name, Email Address methods for Peer ID Type.
- **Peer ID**: Enter an ID to identify and authenticate the remote VPN endpoint.

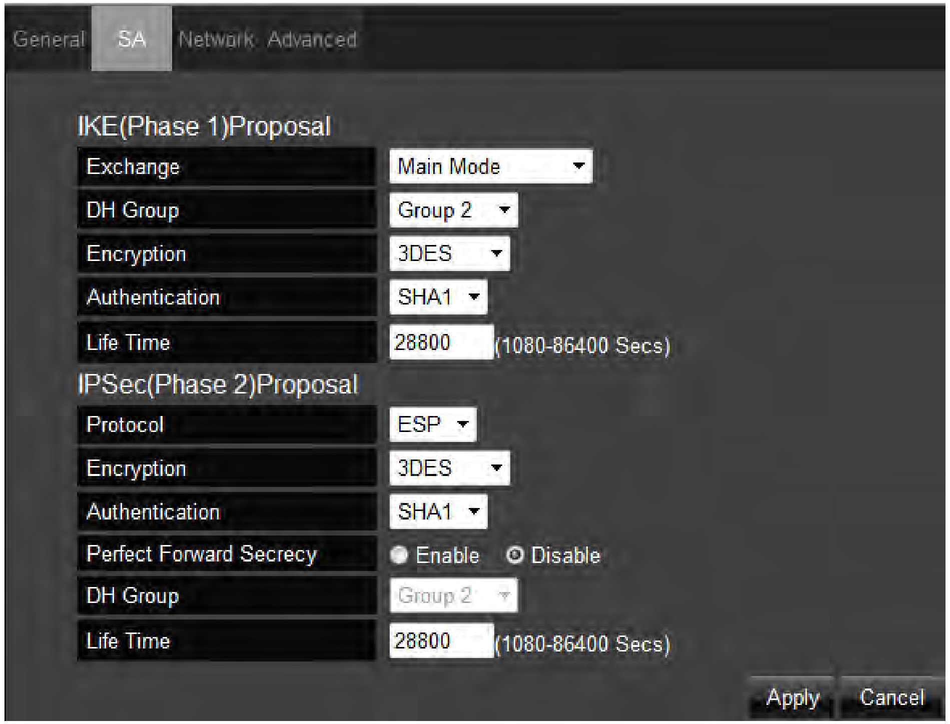


Name	rule01
Connection Type	IPSec
Authentication Type	pre-shared key
Shared Key	1234567890
Confirm	1234567890
Local ID Type	IP Address
Local ID	192.168.50.100
Peer ID Type	IP Address
Peer ID	192.168.50.200

SA (Security Association)

IKE (Phase 1) Proposal

- **Exchange**: Select **Main Mode** or **Aggressive Mode** for IKE Phase 1 negotiation.
  - **Main Mode**: Select this option to configure the standard negotiation parameters for IKE Phase 1 of the VPN Tunnel. (Recommended Setting)
  - **Aggressive Mode**: Select this option to configure IKE Phase 1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended - Less Secure)
- **DH Group**: Select a DH Group from the drop-down menu (**Group 1**, **Group 2**, **Group 5** and **Group 14**). As the DH Group number increases, the higher the level of encryption implemented for IKE Phase 1.
- **Encryption**: Supports **DES**, **3DES**, **AES128**, **AES192**, **AES256** encryption methods for traffic through the VPN.
- **Authentication**: Supports **SHA1**, **MD5** methods for authentication.
- **Life Time**: Enter the number of seconds for the IKE Lifetime. The period of time to pass before establishing a new IKE security association (SA) with the remote endpoint. The default value is 28800.



IKE(Phase 1)Proposal

Exchange	Main Mode
DH Group	Group 2
Encryption	3DES
Authentication	SHA1
Life Time	28800 (1080-86400 Secs)

IPSec(Phase 2)Proposal

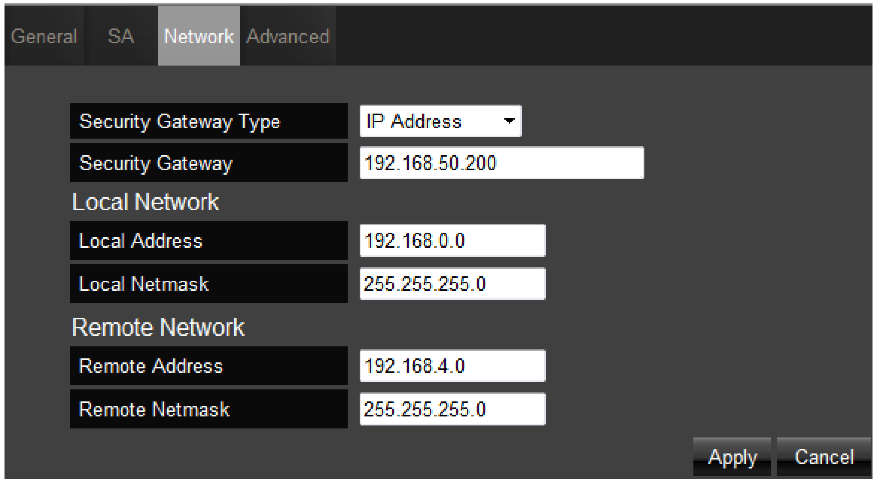
Protocol	ESP
Encryption	3DES
Authentication	SHA1
Perfect Forward Secrecy	○ Enable ● Disable
DH Group	Group 2
Life Time	28800 (1080-86400 Secs)

IPSec (Phase 2) Proposal

- **Protocol**: Select ESP (Encapsulating Security Payload) or AH (Authentication Header) for traffic through the VPN.
  - **AH (Authentication Header)** to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replay attacks.
  - **ESP (Encapsulating Security Payload)** to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.
- **Encryption**: Supports **DES**, **3DES**, **AES128**, **AES192**, **AES256** encryption methods for traffic through the VPN.
- **Authentication**: Supports **SHA1**, **MD5** methods for authentication.

- **Perfect Forward Secrecy**: Select Enable or Disable to enable or disable PFS (Perfect Forward Secrecy). PFS is an additional security protocol.
- **DH Group**: Select a PFS DH Group from the drop-down menu (**Group 1**, **Group 2**, **Group 5**, **Group 14**). As the DH Group number increases, the higher the level of encryption implemented for PFS.
- **Life Time**: Enter the number of seconds for the IPSec Lifetime. The period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 28800.

Network



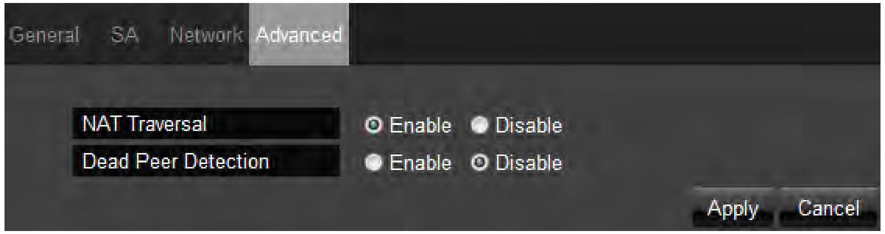
Security Gateway Type: IP Address
Security Gateway: 192.168.50.200

Local Network
Local Address: 192.168.0.0
Local Netmask: 255.255.255.0

Remote Network
Remote Address: 192.168.4.0
Remote Netmask: 255.255.255.0

- **Security Gateway Type**: Security Gateway Type supports IP Address and Domain Name. Select one of them.
- **Security Gateway**: The IP address or domain name of the VPN server.
- **Local Network**: Enter the local (LAN) subnet and mask. (ex. 192.168.0.0/255.255.255.0)
- **Remote Network**: Enter the remote subnet and mask. (ex. 192.168.9.0/255.255.255.0)

Advanced



NAT Traversal: ● Enable ○ Disable
Dead Peer Detection: ○ Enable ● Disable

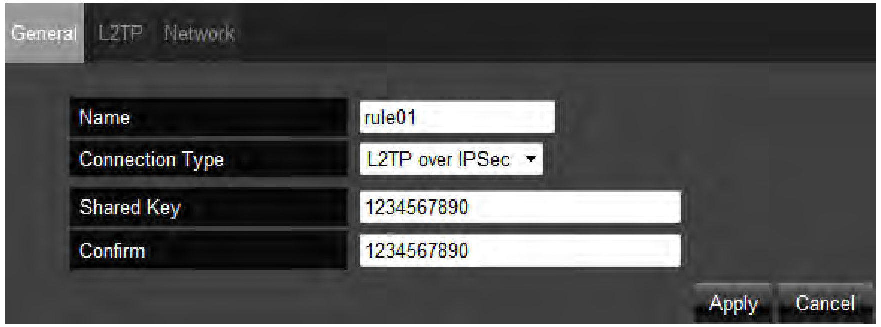
- **NAT Traversal**: Enabling NAT Traversal allow IPSec traffic from this endpoint to traverse through the translation process during NAT. The remote VPN endpoint must also support this feature and it must be enabled to function properly over the VPN.
- **Dead Peer Detection**: Enable DPD (Dead Peer Detection) to delete the VPN tunnel if there is no traffic detected. The VPN will re-establish once traffic is again sent through the tunnel.

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

L2TP over IPSec profile setting

General

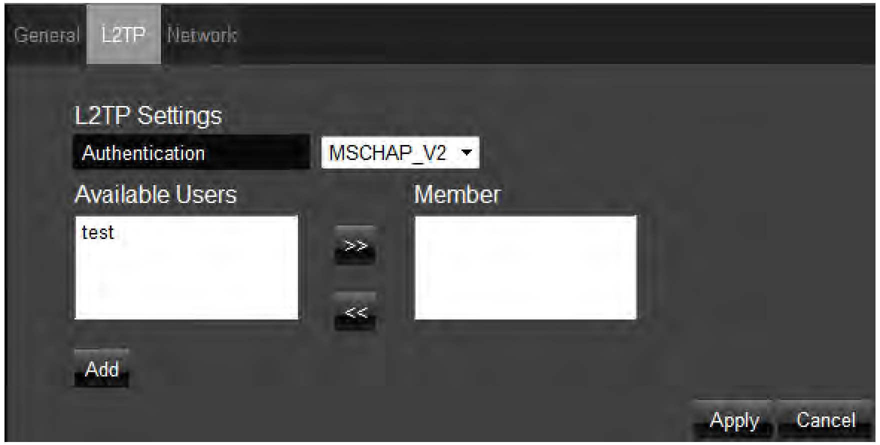
- **Name**: Enter a name for your VPN policy.
- **Connection Type**: Supports **PPTP**, **L2TP**, **IPSec** and **L2TP over IPSec** methods to establish VPN connection.
- **Shared Key**: Enter the Shared Key in box.
- **Confirm**: Enter your Shared Key again for verification.



Name	rule01
Connection Type	L2TP over IPSec
Shared Key	1234567890
Confirm	1234567890

L2TP

- **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 L2TP 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**.



L2TP Settings

Authentication	MSCHAP_V2

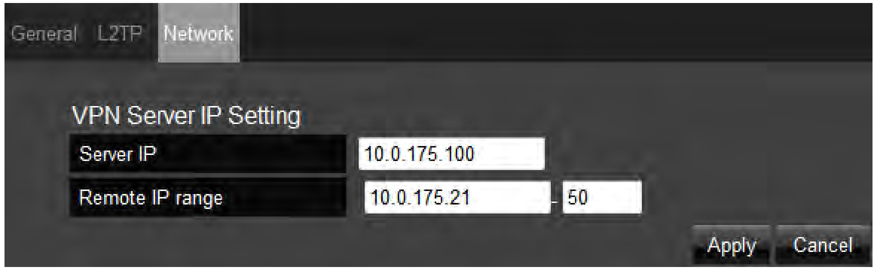
Available Users: test

Member:

Network

- **Server IP**: Enter an IP address which is different from your router's LAN IP address.
- **Remote IP Range**: Enter an IP range under the same subnet of the above Server IP.

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



VPN Server IP Setting

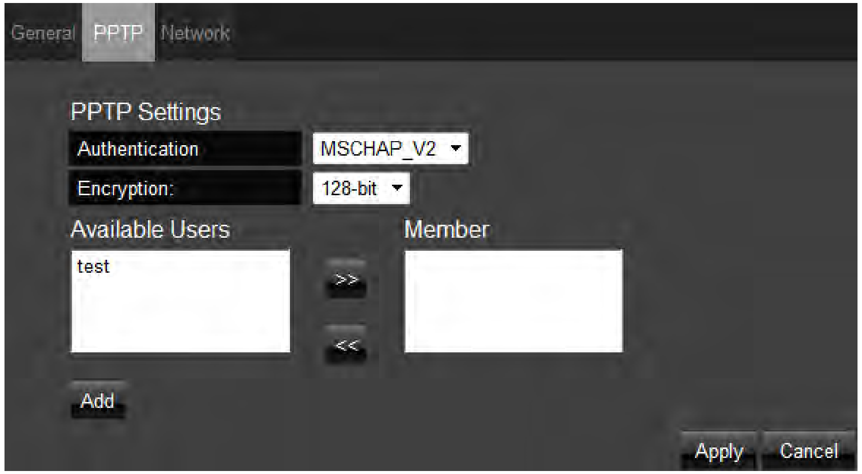
Server IP	10.0.175.100
Remote IP range	10.0.175.21 - 50

PPTP profile setting

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

PPTP

- **Authentication**: There are three authentication algorithms. Please select **CHAP**, **PAP**, or **MSCHAP_V2**.
- **Encryption**: Supports **No**, **40-bit** or **128-bit** encryption lengths for traffic through the VPN.
- **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**.



PPTP Settings

Authentication: MSCHAP_V2

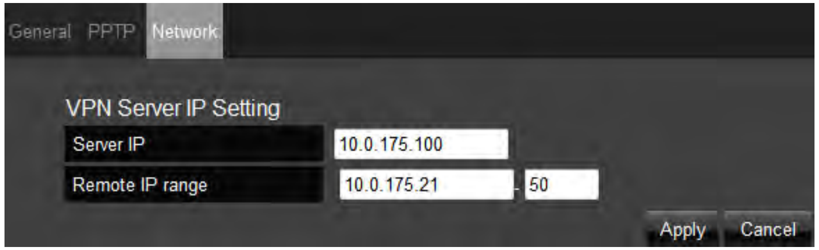
Encryption: 128-bit

Available Users: test

Member

Network

- **Server IP**: Enter an IP address which is different from your router's LAN IP address.
- **Remote IP Range**: Enter an IP range under the same subnet of the above Server IP.



VPN Server IP Setting

Server IP: 10.0.175.100

Remote IP range: 10.0.175.21 - 50

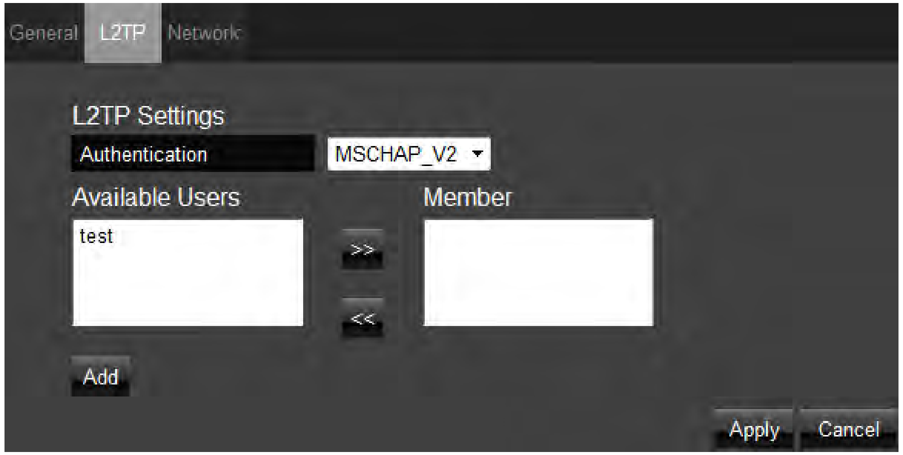
Click **Apply** to save the PPTP VPN profile setting.

L2TP profile setting

If you select L2TP as VPN Connection Type, go to **L2TP** tab.

L2TP

- **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 L2TP 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**.



L2TP Settings

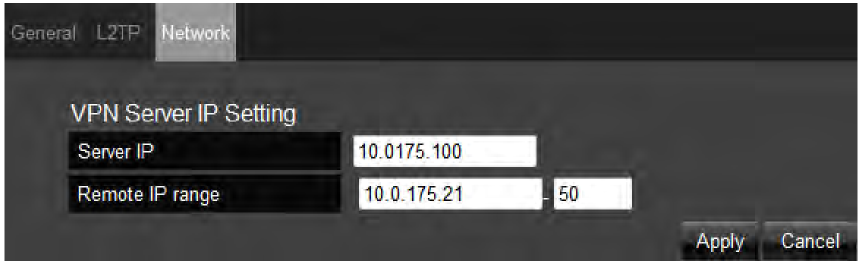
Authentication: MSCHAP_V2

Available Users: test

Member:

Network

- **Server IP**: Enter an IP address which is different from your router's LAN IP address.
- **Remote IP Range**: Enter an IP range under the same subnet of the above Server IP.



VPN Server IP Setting

Server IP: 10.0175.100

Remote IP range: 10.0.175.21 - 50

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

14. Advanced

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

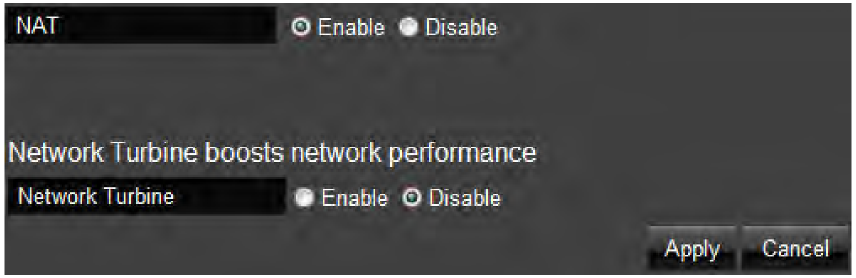
14.1. NAT (Network Address Translation)

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.

- **NAT**: Enable or Disable the NAT.
- **Network Turbine**: Enable or Disable the network turbine.

Note: The network turbine is designed to improve the router's performance. There is about 20~30% improvement when the network turbine is enabled.

Note: The network turbine may cause problems with the Internet connection. Disable the network turbine function if you experience connection issues.



NAT ◉ Enable ○ Disable

Network Turbine boosts network performance

Network Turbine ○ Enable ◉ Disable

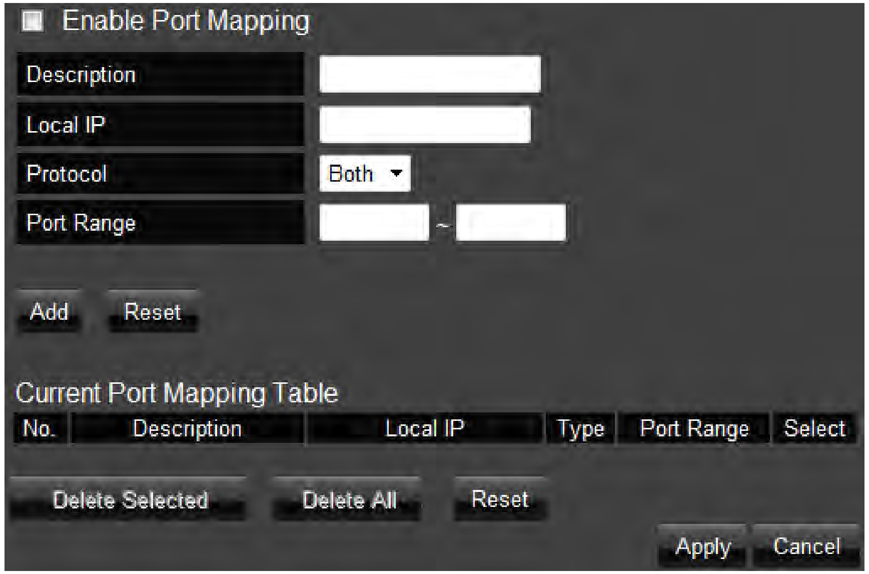
Click **Apply** to save the settings or **Cancel** to discard changes.

14.2. 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.

- **Enable Port Mapping**: Mark the checkbox to Enable Port Mapping.
- **Description**: Enter the description on why the ports will be mapped.
- **Local IP**: The local IP address of the server behind the NAT firewall.
- **Protocol**: Select whether TCP, UDP, or Both ports will be mapped.
- **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.



☐ Enable Port Mapping

Description	
Local IP	
Protocol	Both
Port Range	~

Current Port Mapping Table

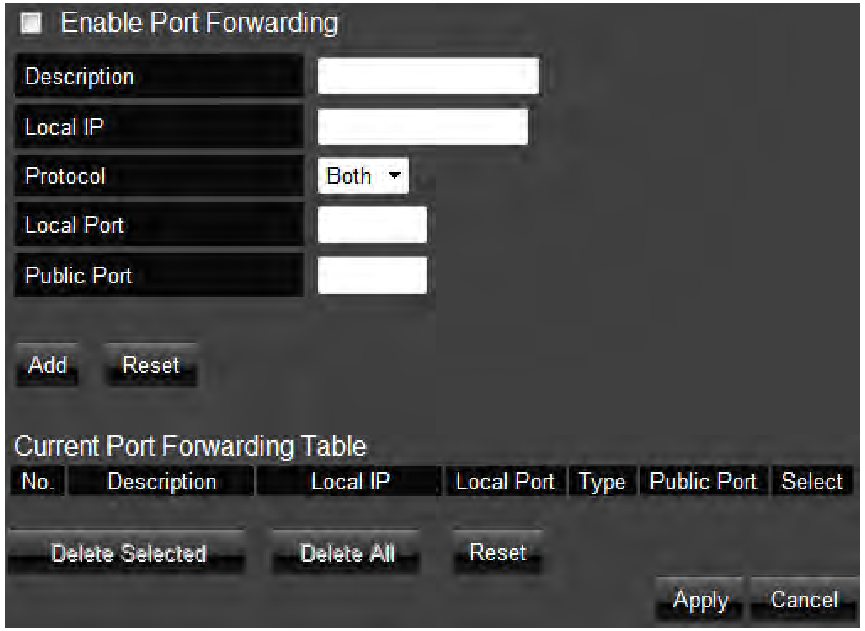
No.	Description	Local IP	Type	Port Range	Select

14.3. 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.
- **Description**: Enter the description on why the ports will be forwarded.
- **Local IP**: Enter the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.
- **Protocol**: Select whether TCP, UDP, or Both ports will be forwarded.
- **Local Port**: This is the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.
- **Public Port**: Port number will be changed to Local Port when the packet enters your LAN Network.

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



□ Enable Port Forwarding

Description	
Local IP	
Protocol	Both
Local Port	
Public Port	

Current Port Forwarding Table

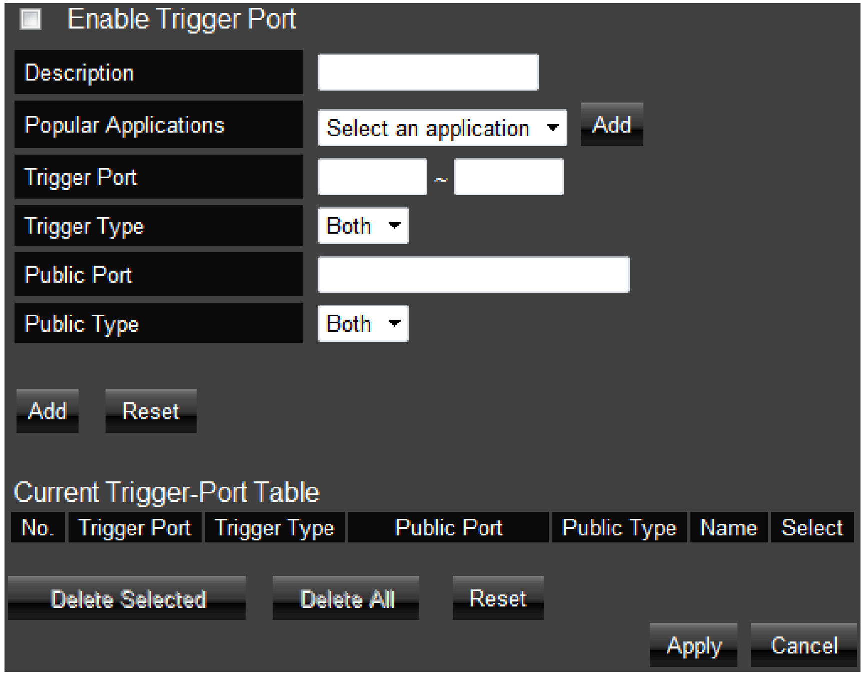
No.	Description	Local IP	Local Port	Type	Public Port	Select

14.4. 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.

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



□ Enable Trigger Port

Description	
Popular Applications	Select an application ▾
Trigger Port	~
Trigger Type	Both ▾
Public Port	
Public Type	Both ▾

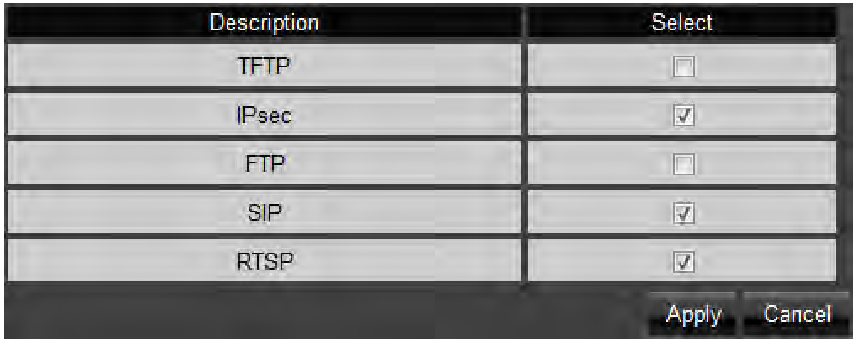
Current Trigger-Port Table

No.	Trigger Port	Trigger Type	Public Port	Public Type	Name	Select

14.5. 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.

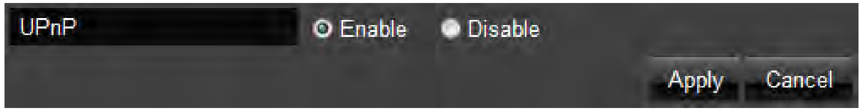
Select the listed applications that need **ALG** support and then the router will authorize them to pass through the NAT gateway. Then click Apply.



Description	Select
TFTP	□
IPsec	☑
FTP	□
SIP	☑
RTSP	☑

14.6. UPnP (Universal Plug and Play)

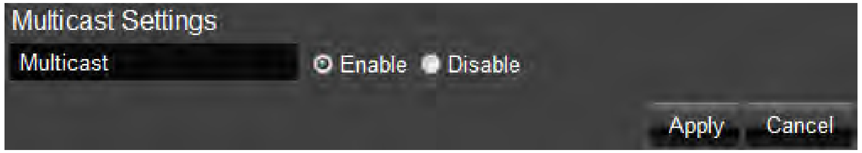
UPnP helps Internet devices, such as gaming and videoconferencing to access the network and connect to other registered UPnP devices.



UPnP ◉ Enable ○ Disable

14.7. IGMP (Internet Group Multicast Protocol)

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



Multicast Settings

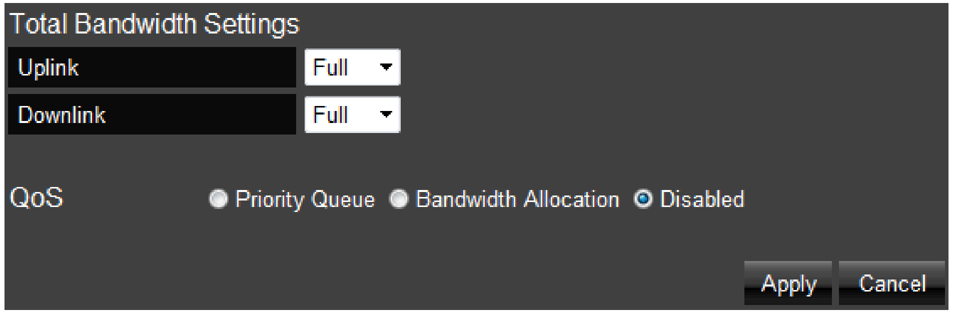
Multicast ● Enable ○ Disable

14.8. QoS (Quality of Service)

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.

<u>Total Bandwidth Settings</u>

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.



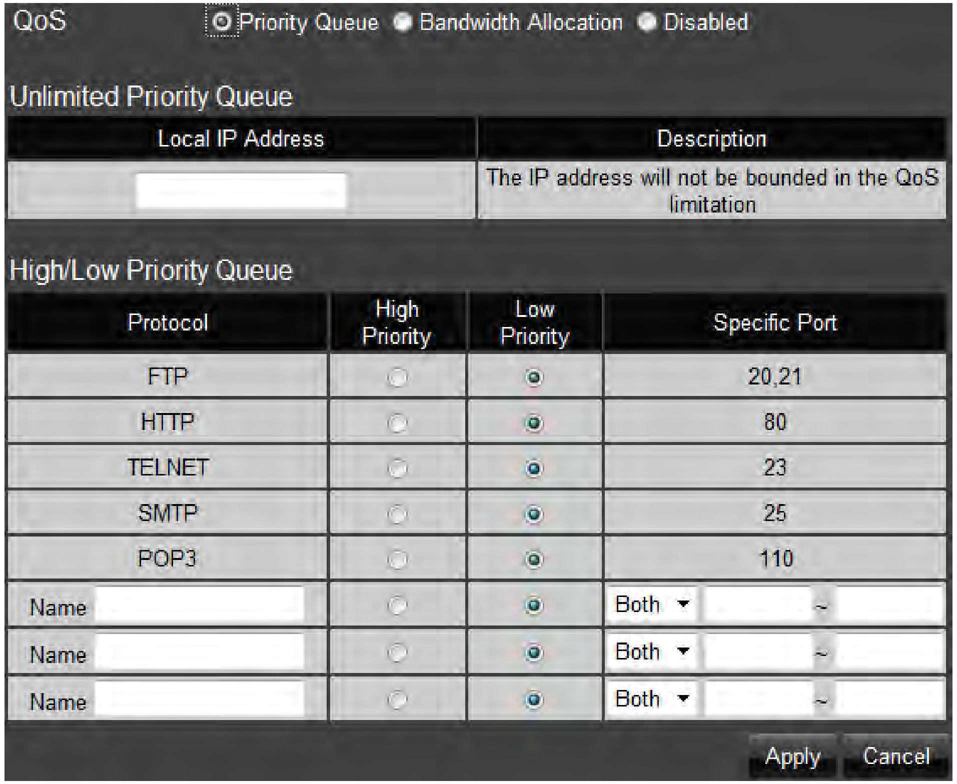
Total Bandwidth Settings

Uplink	Full
Downlink	Full

QoS ○ Priority Queue ○ Bandwidth Allocation ● Disabled

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.



QoS ● Priority Queue ○ Bandwidth Allocation ○ Disabled

Unlimited Priority Queue

Local IP Address	Description
	The IP address will not be bounded in the QoS limitation

High/Low Priority Queue

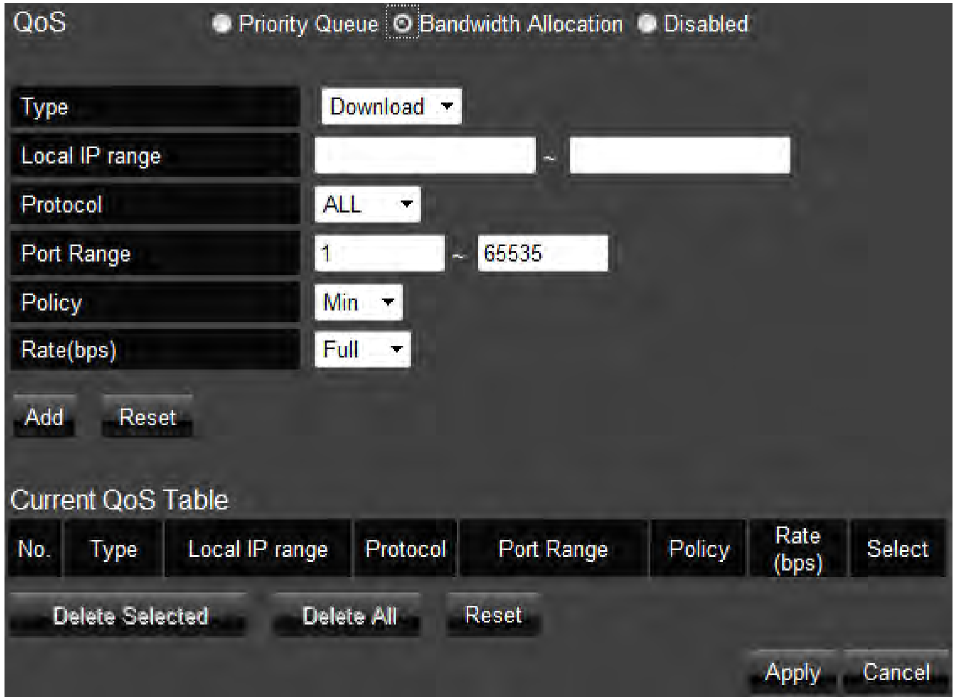
Protocol	High Priority	Low Priority	Specific Port
FTP	○	●	20,21
HTTP	○	●	80
TELNET	○	●	23
SMTP	○	●	25
POP3	○	●	110
Name	○	●	Both ~
Name	○	●	Both ~
Name	○	●	Both ~

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.



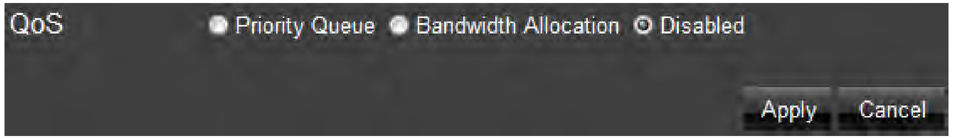
QoS ○ Priority Queue ● Bandwidth Allocation ○ Disabled

Type	Download ▾
Local IP range	~
Protocol	ALL ▾
Port Range	1 ~ 65535
Policy	Min ▾
Rate(bps)	Full ▾

Current QoS Table

No.	Type	Local IP range	Protocol	Port Range	Policy	Rate (bps)	Select

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



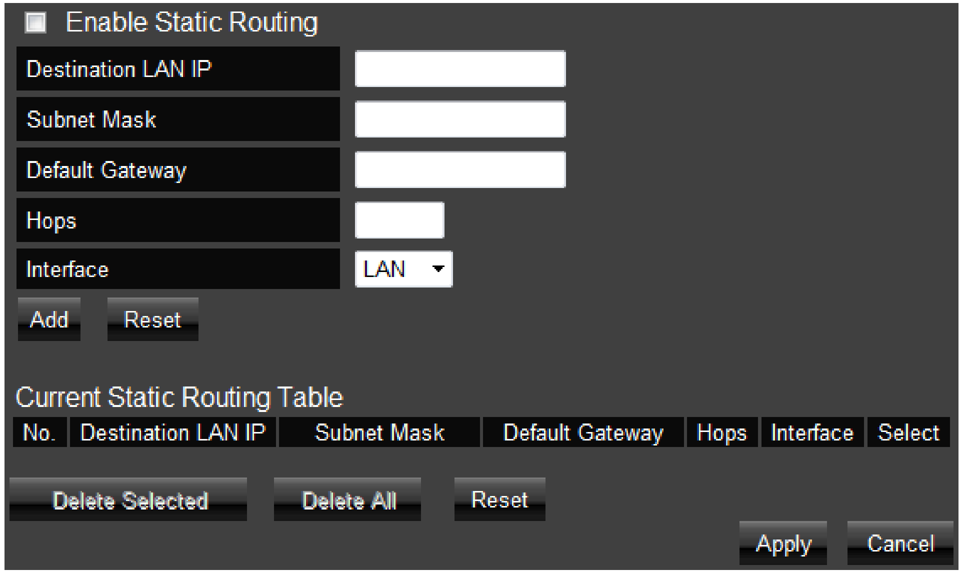
QoS ○ Priority Queue ○ Bandwidth Allocation ● Disabled

Click **Apply** to save your settings.

14.9. Routing

Typically you do not need to setup static routing since the ESR350H 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.

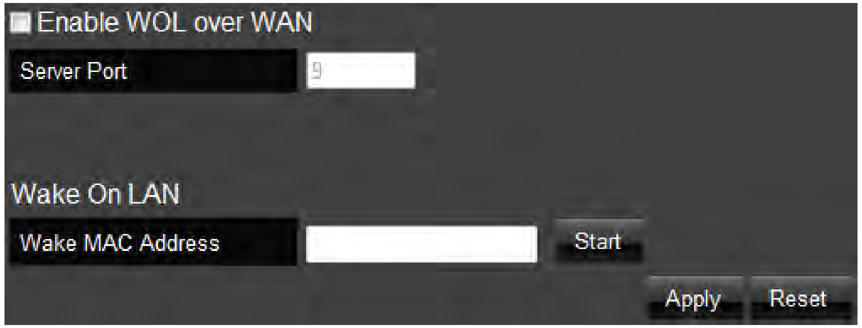
- **Enable Static Routing**: Mark the checkbox to Enable Static Routing.
- **Destination LAN IP**: Enter the static IP Address of the remote network to which you want to setup a static route.
- **Subnet Mask**: Enter the Subnet Mask of the remote network to which you want to setup a static route.
- **Default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



Click **Apply** to save the settings or **Cancel** to discard changes.

14.10. 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.



☐ Enable WOL over WAN

Server Port: 9

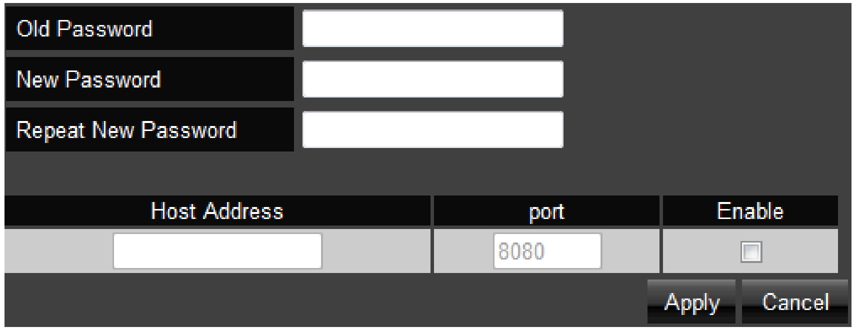
Wake On LAN

Wake MAC Address:

15. Tools

15.1. 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. The password can contain 0 to 12 alphanumeric characters and is case sensitive. You can also allow only one computer to edit the settings on the **ESR350H** by supplying its static IP address.



Old Password	
New Password	
Repeat New Password	

Host Address	port	Enable
	8080	□

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.

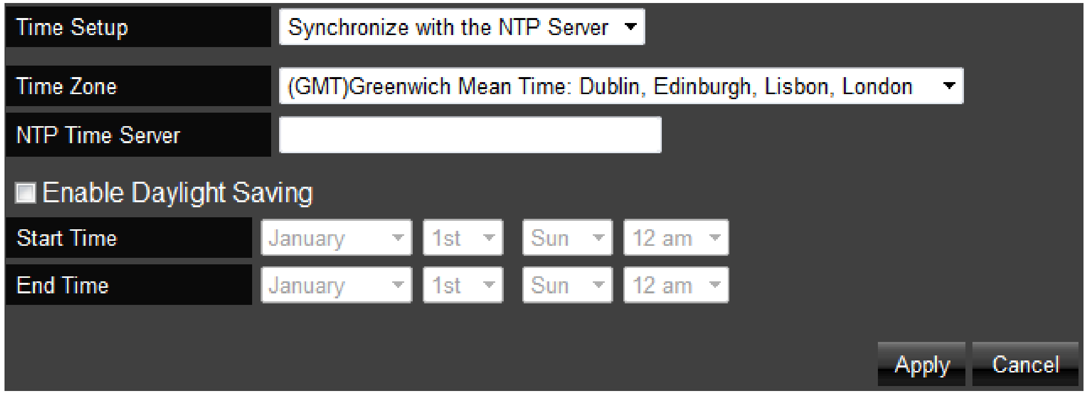
Port: Enter the port number for remote accessing management web interface.
The default Port for remote management is 8080.

Click **Apply** to save the settings.

To access the settings of the ESR350H remotely, enter the router's WAN IP address and port number of the ESR350H. 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.

15.2. Time

In the **Time** option of the Tools section, you can change the current time on the **ESR350H**. Enter the web address of the Network Time Protocol you want to have the **ESR350H** to match time with or have it synchronize with the PC accessing the **ESR350H**. You can also enable Daylight Saving.



Time Setup	Synchronize with the NTP Server
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
NTP Time Server	

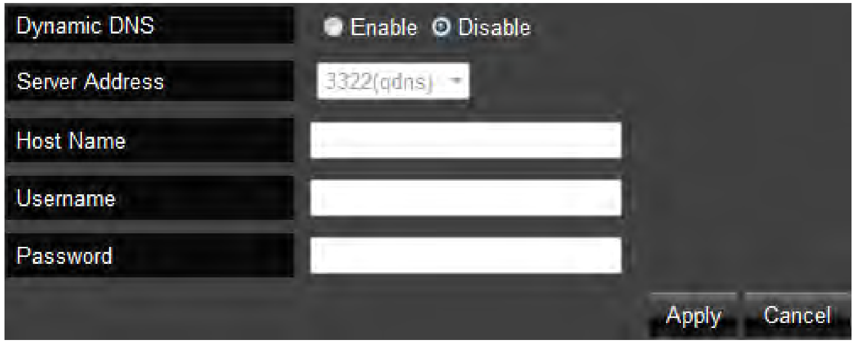
☐ Enable Daylight Saving

Start Time	January	1st	Sun	12 am
End Time	January	1st	Sun	12 am

15.3. 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.

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



Dynamic DNS ○ Enable ● Disable

Server Address 3322(qdns)

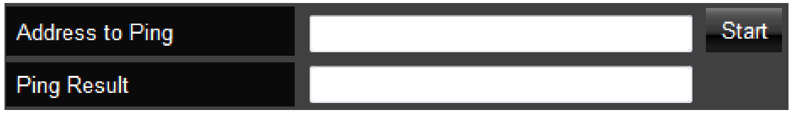
Host Name

Username

Password

15.4. Diagnosis

The diagnosis feature allows the administrator to verify that another device is available on the network and is accepting request packets. If the ping result returns **alive**, it means a device is on line. This feature does not work if the target device is behind a firewall or has security software installed.



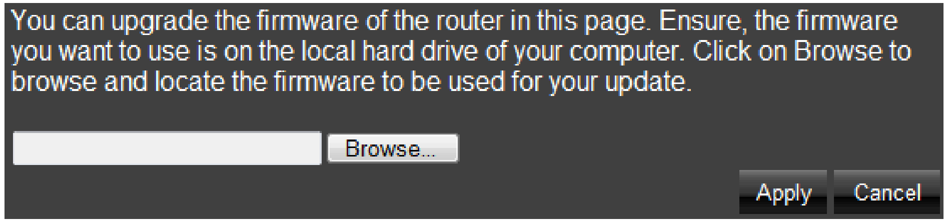
Address to Ping	
Ping Result	

15.5. Firmware

In the **Firmware** option of the Tools section, you can update the firmware of the **ESR350H**. 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 **ESR350H** will restart when completed.

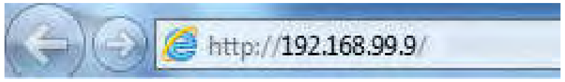


You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.

Emergency Upgrade

If your firmware upgrade failed, you may enter the Emergency Upgrade WEB page.

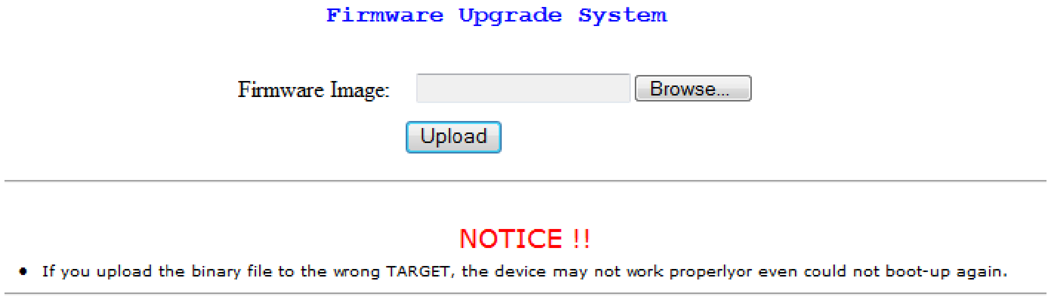
1. Enter IP address: **192.168.99.9** and enter Emergency Upgrade WEB page.



http://192.168.99.9/

Note: You have to configure PC/Notebook IP address to 192.168.99.8 manually.

2. Click the **Browse** button and navigate to the location of the upgrade file and then click **Upload**.



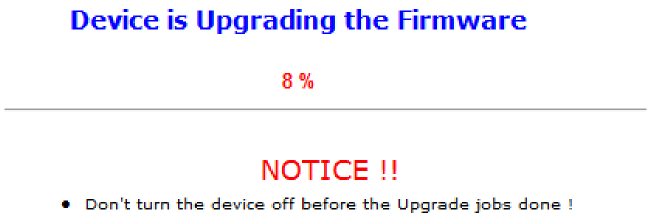
Firmware Upgrade System

Firmware Image:

NOTICE !!

- If you upload the binary file to the wrong TARGET, the device may not work properlyor even could not boot-up again.

3. Wait for firmware upgrade and reboot the device.



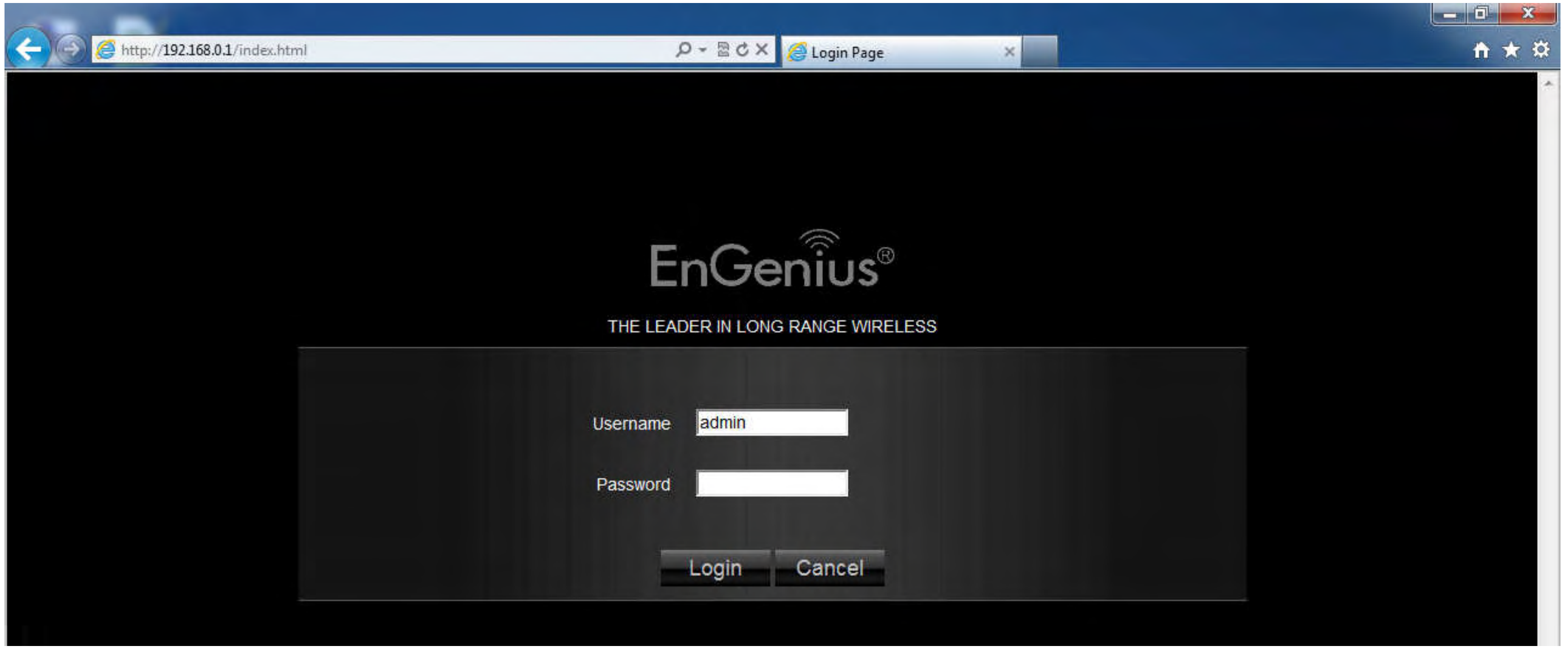
Device is Upgrading the Firmware

8 %

NOTICE !!

- Don't turn the device off before the Upgrade jobs done !

4. You can access the device again.



http://192.168.0.1/index.html

Login Page

THE LEADER IN LONG RANGE WIRELESS

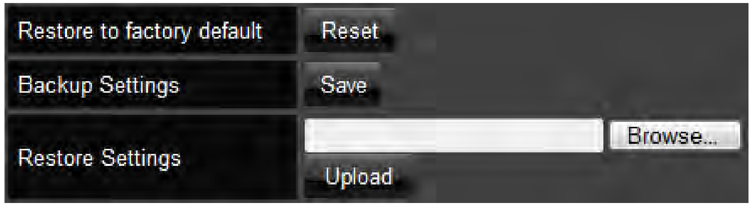
Username: admin

Password:

15.6. Back-Up

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

1. Restore the **ESR350H** to factory defaults.
2. Save the current configuartion on the **ESR350H** to a .dlf file.
3. Restore saved settings by:
   a. Select **Browse**.
   b. Browse location for the file with the saved settings of the **ESR350H**.
   c. Select **Upload**.



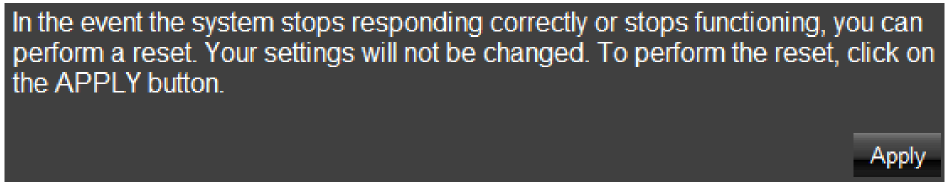
Restore to factory default — Reset

Backup Settings — Save

Restore Settings — Browse... Upload

15.7. Reset

In the **Reset** option of the Tools section, you can manually restart the **ESR350H**.



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.

Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

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.

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

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.

French translation:

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.

French translation:

NOTE IMPORTANTE:
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.