EnGenius®

Wireless Gigabit VPN Router

EVR100

Wireless Gigabit VPN Router

V1.0

Revision History

Version	Date	Notes
1.0	2011/01/11	First Release

1. Introduction

1.1. Package Contents

- EnGenius WIRELESS GIGABIT VPN ROUTER
- AC Adapter
- RJ-45 Ethernet LAN Cable
- CD-ROM with User Manual and Setup Wizard
- Quick Guide

1.2. System Requirements

- RJ-45 Ethernet Based Internet (ADSL or Cable Modem)
- Computer with Wireless Network function
- Windows, Mac OS or Linux based operating systems
- Internet Explorer or Firefox or Safari Web-Browser Software

1.3.Introduction

EVR100 is a 2T2R Wireless 11N Gigabit VPN Router that delivers up to 6x faster speeds and 3x extended coverage than 802.11g devices. EVR100 supports home network with superior throughput and performance and unparalleled wireless range. With easy to use on the WPS function, it helps users to connect to wireless device with just one push button.

There's also a built-in 4-port full-duplex 10/100/1000 Fast Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network shares a high-speed cable or DSL Internet connection.

1.4. LED Overview

LED Lights	Icon	Description
Wireless LAN	📡	Color – Blue Lights when Wireless signal is activated. Blinks when Wireless data transfer.
Internet	W	Color – Blue Blinks when WPS handshake is initialized.
LAN	🖥	Color – Blue Lights when wired network device is connected to RJ-45 port. Blinks when data transfer occurs on RJ-45 port.
Power	⏻	Color – Orange Lights when device is powered ON. Blinks device is Reset.

2. Before you Begin

This section will guide you through the installation process. Placement of the EVR100 is very important to avoid poor signal reception and performance. Avoid placing the device in enclosed spaces such as a closet, cabinet or wardrobe.

2.1. Considerations for Wireless Installation

The operating distance of all wireless devices cannot be pre-determined due to a number of unknown obstacles in the environment that the device is deployed. These could be the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through. Here are some key guidelines to ensure that you have the optimal wireless range.

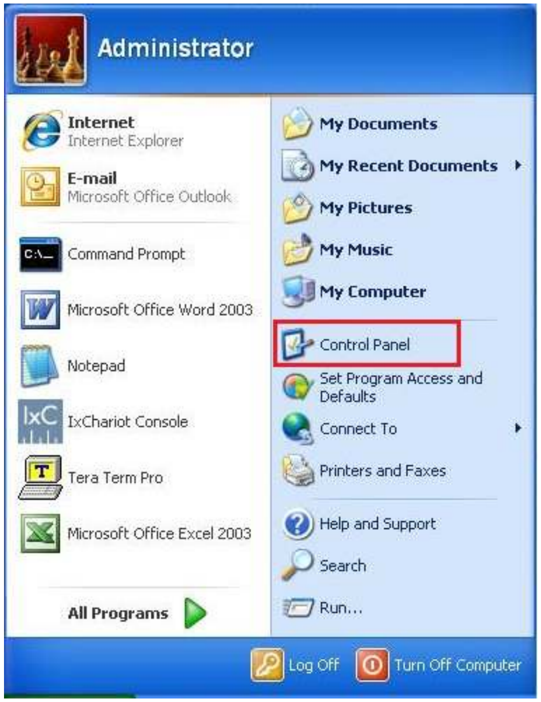
1. Keep the number of walls and ceilings between the EnGenius access point and other network devices to a minimum. Each wall or ceiling can reduce the signal strength, the degradation depends on the building’s material.

2. Building materials makes a difference. A solid metal door or aluminum stubs may have a significant negative effect on range. Locate your wireless devices carefully so the signal can pass through a drywall or open doorways. Materials such as glass, steel, metal, concrete, water (fish tanks), mirrors, file cabinets and brick will also degrade your wireless signal.

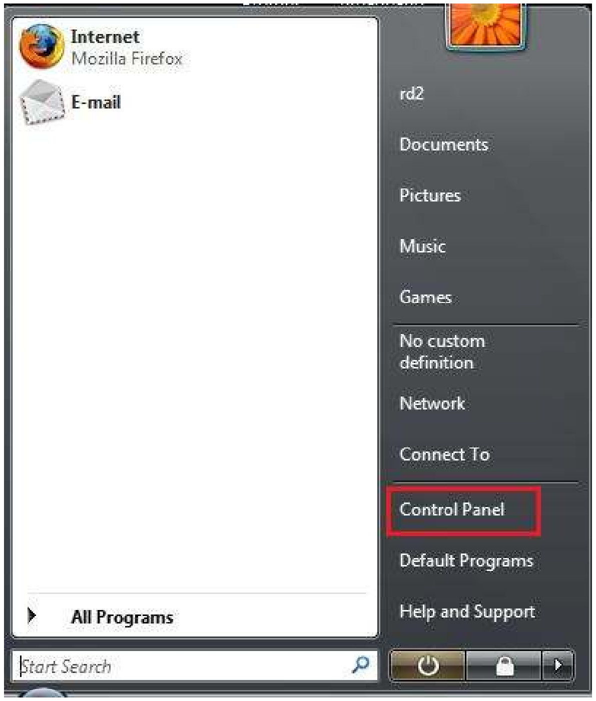
3. Interferences can also come from your other electrical devices or appliances that generate RF noise. The most usual types are microwaves, or cordless phones.

2.2. Computer Settings (Windows XP/Windows Vista/Windows 7)

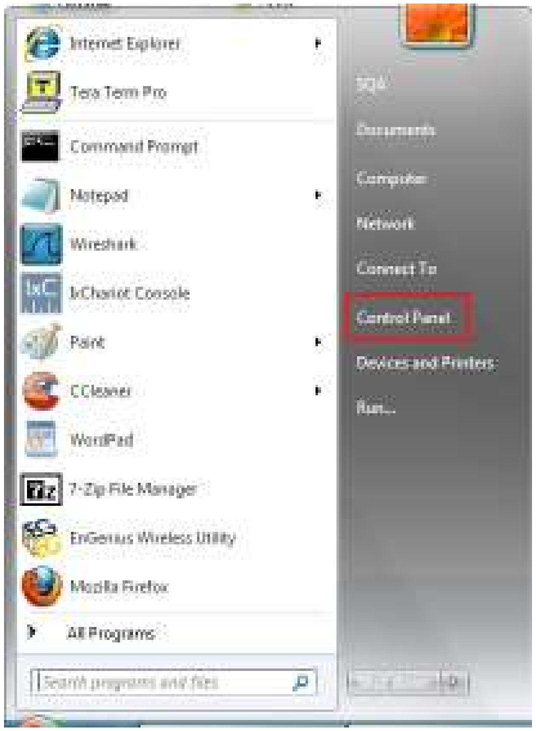
- Click Start button and open Control Panel.



Windows XP

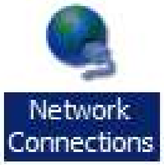


Windows Vista

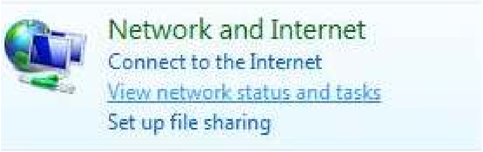


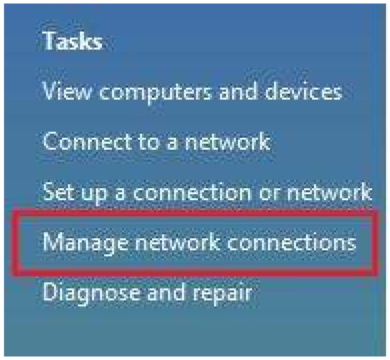
Windows 7

- Windows XP, click [Network Connection]

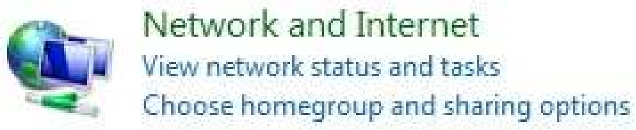


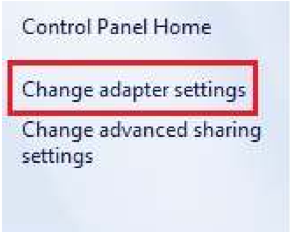
- Windows Vista, click [View Network Status and Tasks] then [Manage Network Connections]



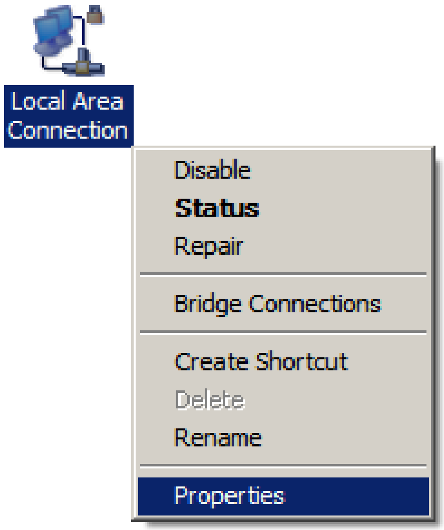

Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair

- Windows 7, click [View Network Status and Tasks] then [Change adapter settings]

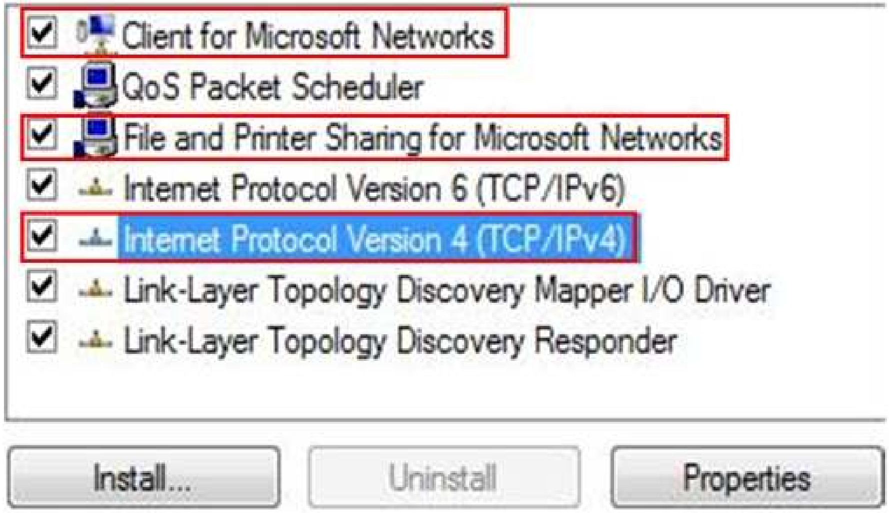

Network and Internet
View network status and tasks
Choose homegroup and sharing options



- Right click on [Local Area Connection] and select [Properties].

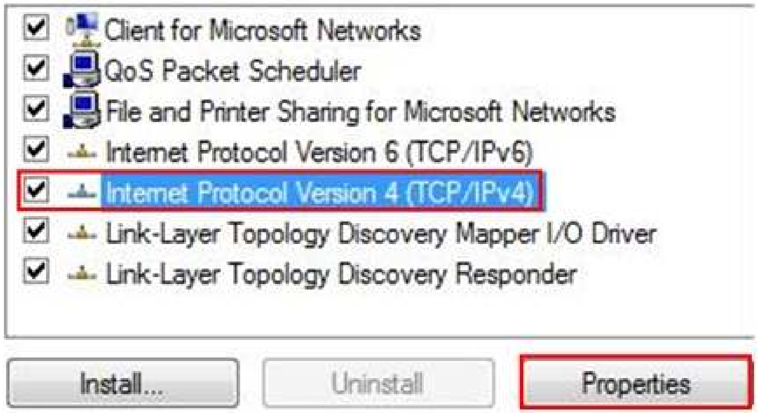


- Check “Client for Microsoft Networks”, “File and Printer Sharing for Microsoft Networks”, and “Internet Protocol (TCP/IP) is ticked. If not, please install them.



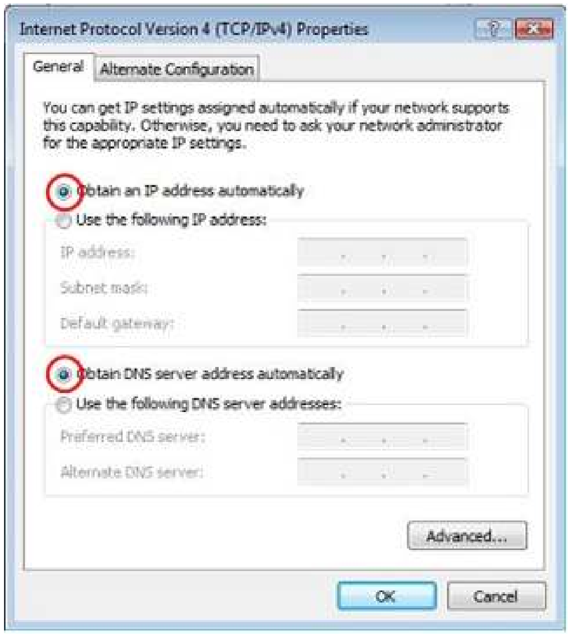
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

- Select "Internet Protocol (TCP/IP)" and click [Properties]



☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

- Select "Obtain an IP Address automatically" and "Obtain DNS server address automatically" then click [OK].



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

2.3. Hardware Installation

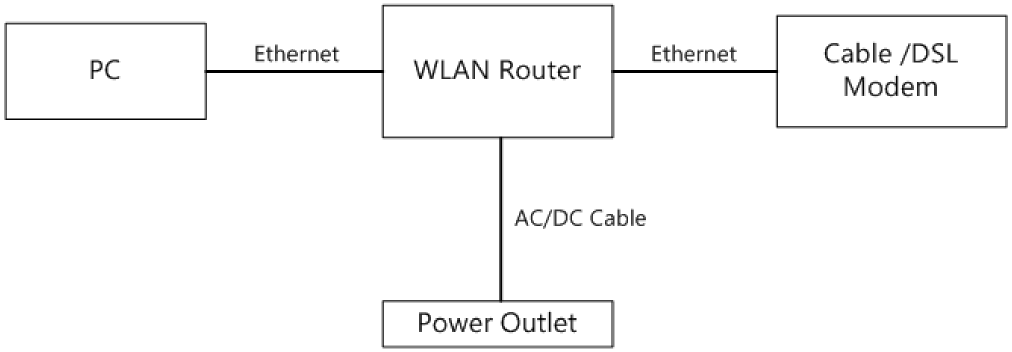
1. Place the unit in an appropriate location after conducting a site survey.

2. Plug one end of the Ethernet cable into the LAN port of the device and another end into your PC/Notebook.

3. Plug one end of another Ethernet cable to WAN port of the device and the other end into you cable/DSL modem (Internet)

4. Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

This diagram depicts the hardware configuration



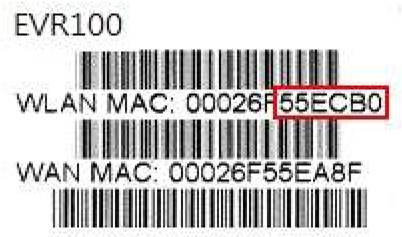
3. Configuring your Router

This section will show you how to configure the device using the web-based configuration interface.

Please use your wireless network adapter to connect the WIRELESS ROUTER.

Default Settings

IP Address	192.168.0.1
Username / Password	admin / admin
Wireless Mode	Enable
Wireless SSID	EnGenius*xxxxxx*
Wireless Security	None



EVR100

WLAN MAC: 00026F55ECB0

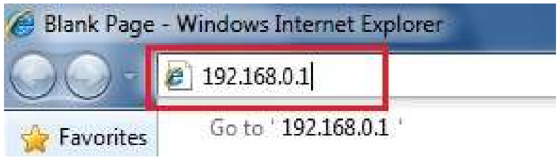
WAN MAC: 00026F55EA8F

Note: *xxxxxx* represented in the wireless SSID above is the last 6 characters of your device MAC Address. This can be found on the device body label and is unique for each device.

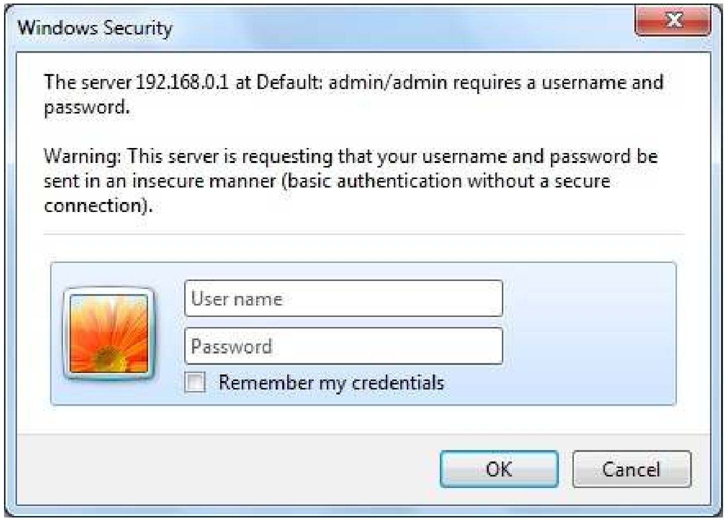
4. Setup Wizard

1. Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address http://192.168.0.1

   Note: If you have changed the default LAN IP Address of the WIRELESS ROUTER, ensure you enter the correct IP Address.



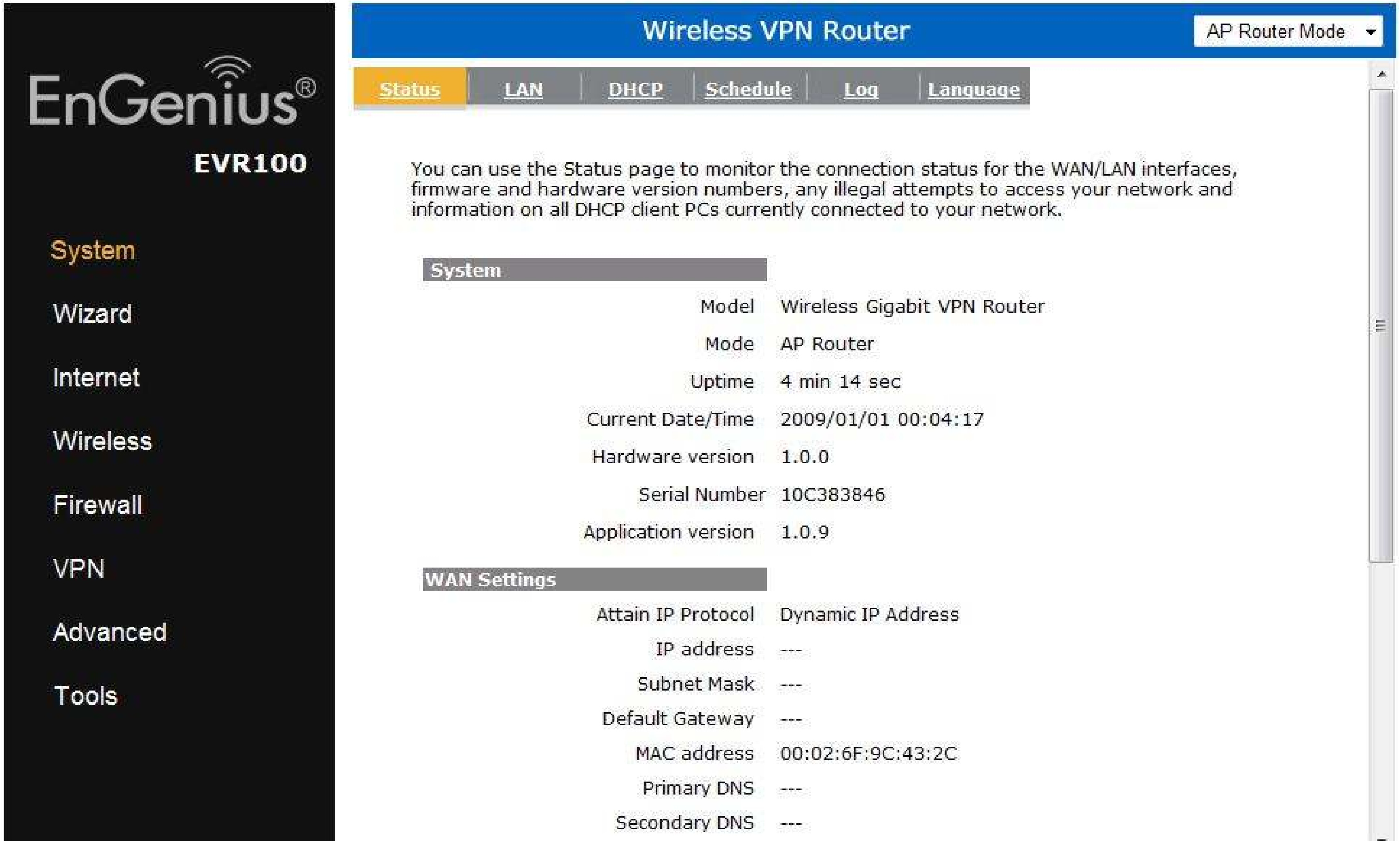
2. The default username and password are **admin**. Once you have entered the correct username and password, click the **OK** button to open the web-base configuration page.



The server 192.168.0.1 at Default: admin/admin requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

3. You will see the following webpage if login successfully.

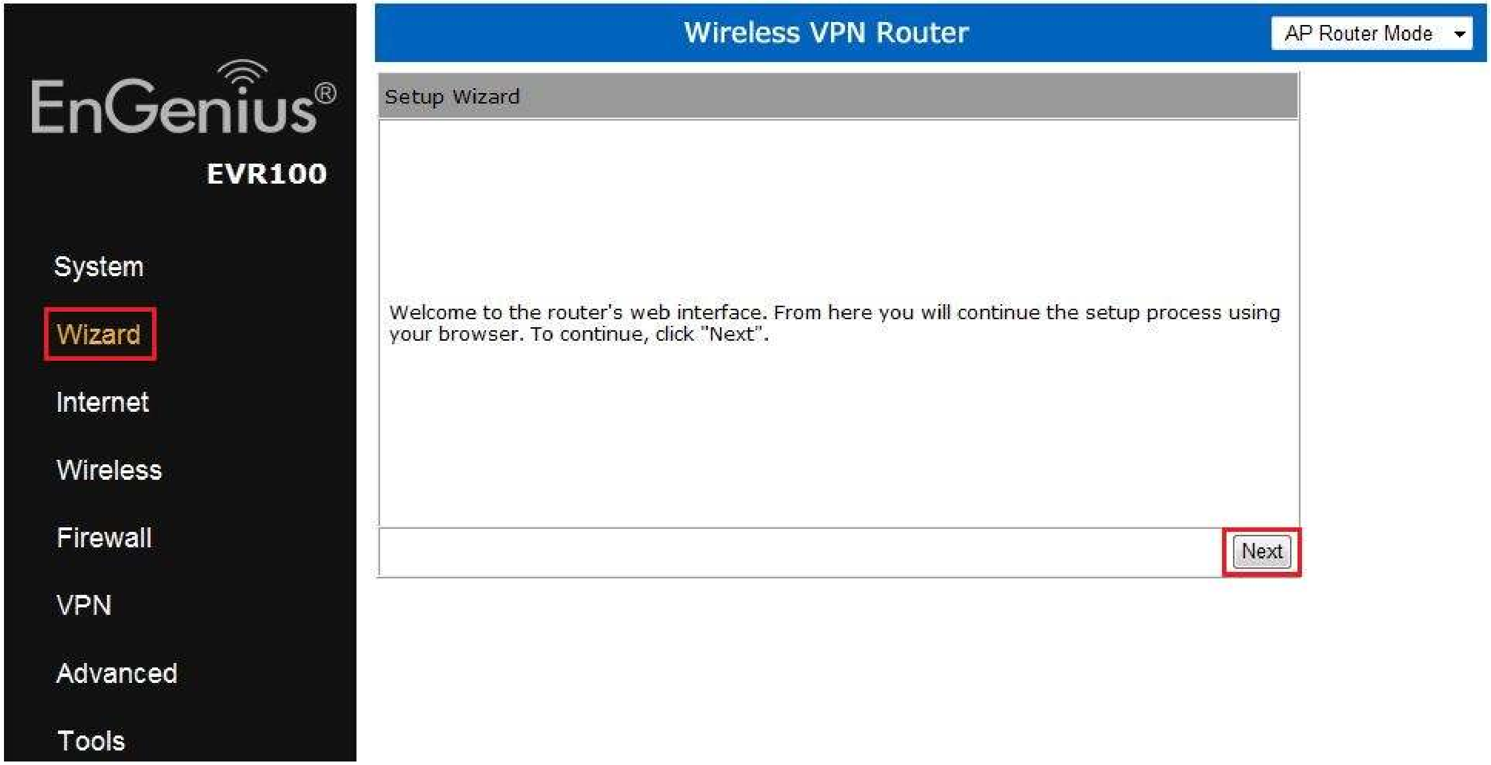


You can use the Status page to monitor the connection status for the WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network and information on all DHCP client PCs currently connected to your network.

System	
Model	Wireless Gigabit VPN Router
Mode	AP Router
Uptime	4 min 14 sec
Current Date/Time	2009/01/01 00:04:17
Hardware version	1.0.0
Serial Number	10C383846
Application version	1.0.9

WAN Settings	
Attain IP Protocol	Dynamic IP Address
IP address	---
Subnet Mask	---
Default Gateway	---
MAC address	00:02:6F:9C:43:2C
Primary DNS	---
Secondary DNS	---

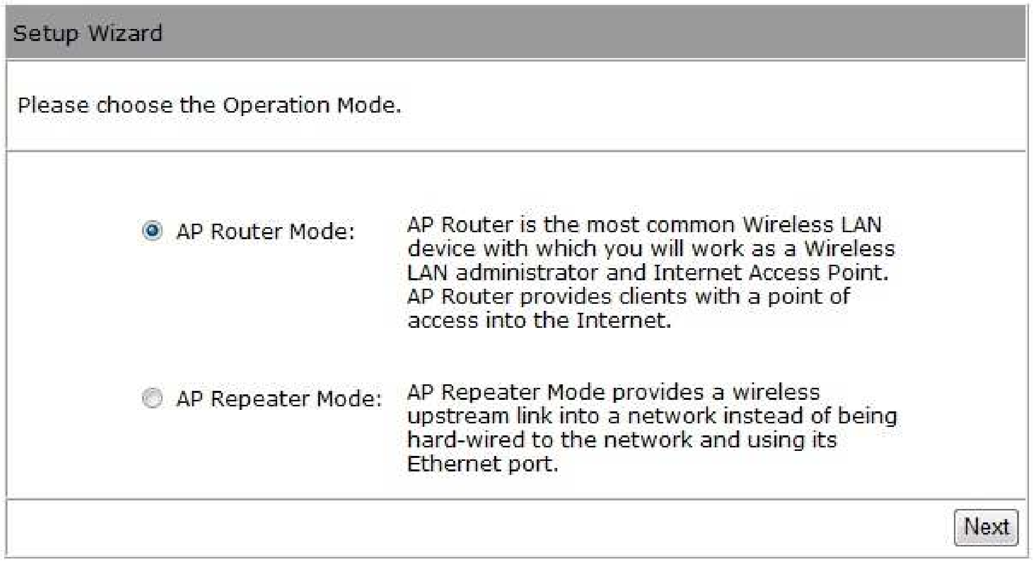
4. Click **Wizard** to enter the Setup Wizard.
   Then click **Next** to begin the wizard.



Welcome to the router's web interface. From here you will continue the setup process using your browser. To continue, click "Next".

5. Select the Operation Mode.

Please ensure you have the proper cables connected as described in the Hardware Installation section.



Setup Wizard

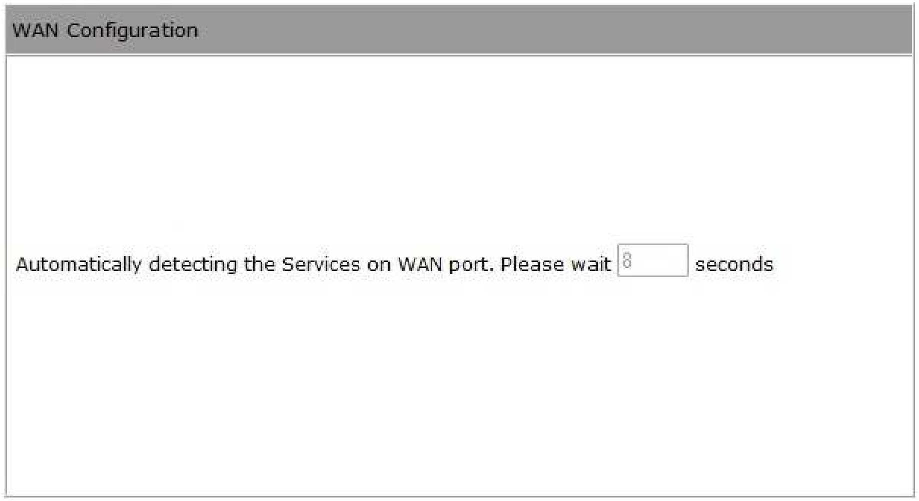
Please choose the Operation Mode.

● AP Router Mode: AP Router is the most common Wireless LAN device with which you will work as a Wireless LAN administrator and Internet Access Point. AP Router provides clients with a point of access into the Internet.

○ AP Repeater Mode: AP Repeater Mode provides a wireless upstream link into a network instead of being hard-wired to the network and using its Ethernet port.

AP Router Mode

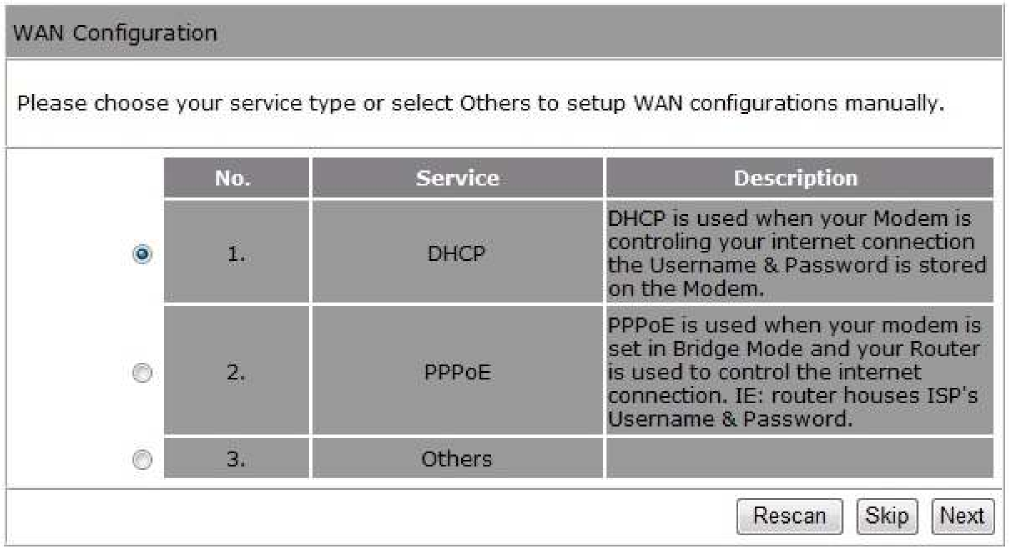
a) The device will search for the correct Internet settings automatically.



WAN Configuration

Automatically detecting the Services on WAN port. Please wait 8 seconds

b) The most appropriate WAN type will be determined and selected automatically. If it is incorrect, please select **Others** to set up the WAN settings manually.

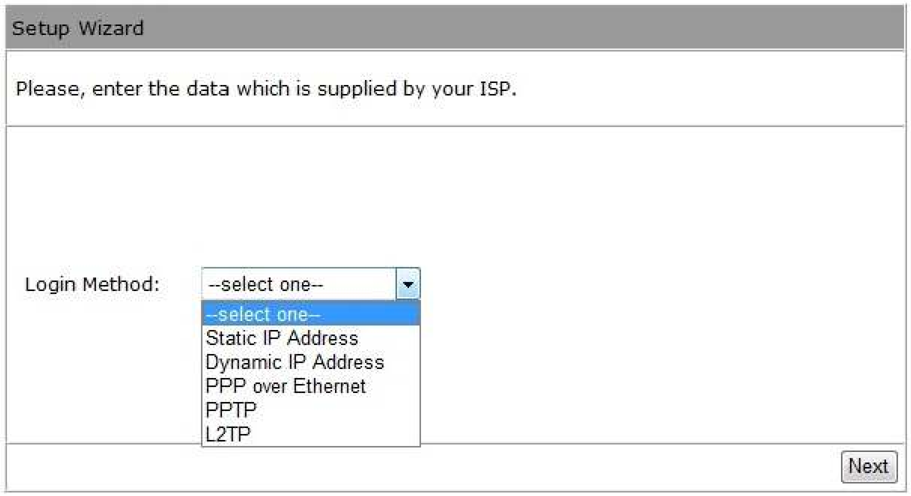


WAN Configuration

Please choose your service type or select Others to setup WAN configurations manually.

	No.	Service	Description
●	1.	DHCP	DHCP is used when your Modem is controling your internet connection the Username & Password is stored on the Modem.
○	2.	PPPoE	PPPoE is used when your modem is set in Bridge Mode and your Router is used to control the internet connection. IE: router houses ISP's Username & Password.
○	3.	Others	

c) There are many WAN service types available. Please obtain the correct settings from your Internet Service Provider (ISP).

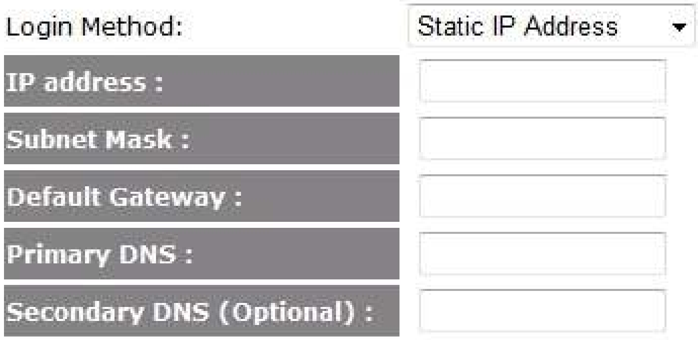

Setup Wizard

Please, enter the data which is supplied by your ISP.

Login Method: --select one--

Static IP Address

If your ISP Provider has assigned you a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.


Login Method: Static IP Address

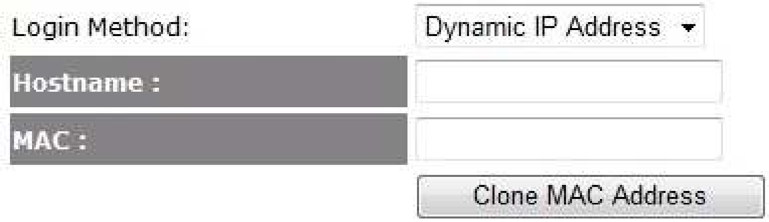
IP address :	
Subnet Mask :	
Default Gateway :	
Primary DNS :	
Secondary DNS (Optional) :	

Dynamic IP Address

The IP Address is allocated automatically. However some ISP's will also recognize the MAC address and will reject connections if the MAC address does not match.

If your ISP has recorded the MAC address of your computer's Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC Address** button.

This will replace the AP Router MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.

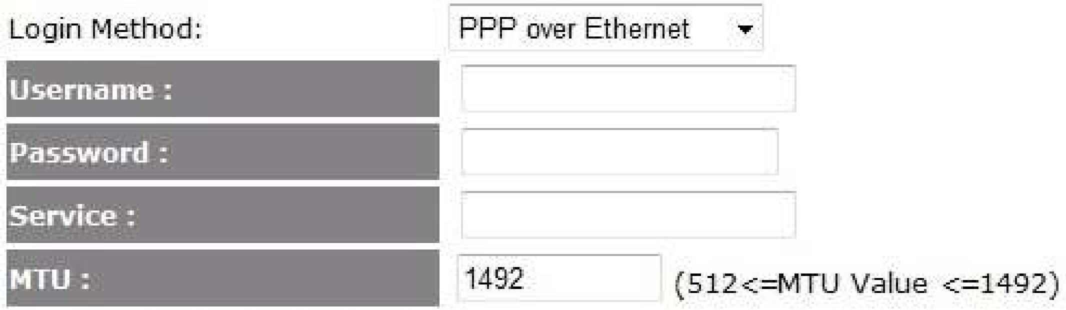


Login Method: Dynamic IP Address

Dynamic IP Address	
Hostname	This is optional. Only required if specified by ISP
MAC	The MAC Address that is used to connect to the ISP.

PPP over Ethernet

ISP requires an account username and password.

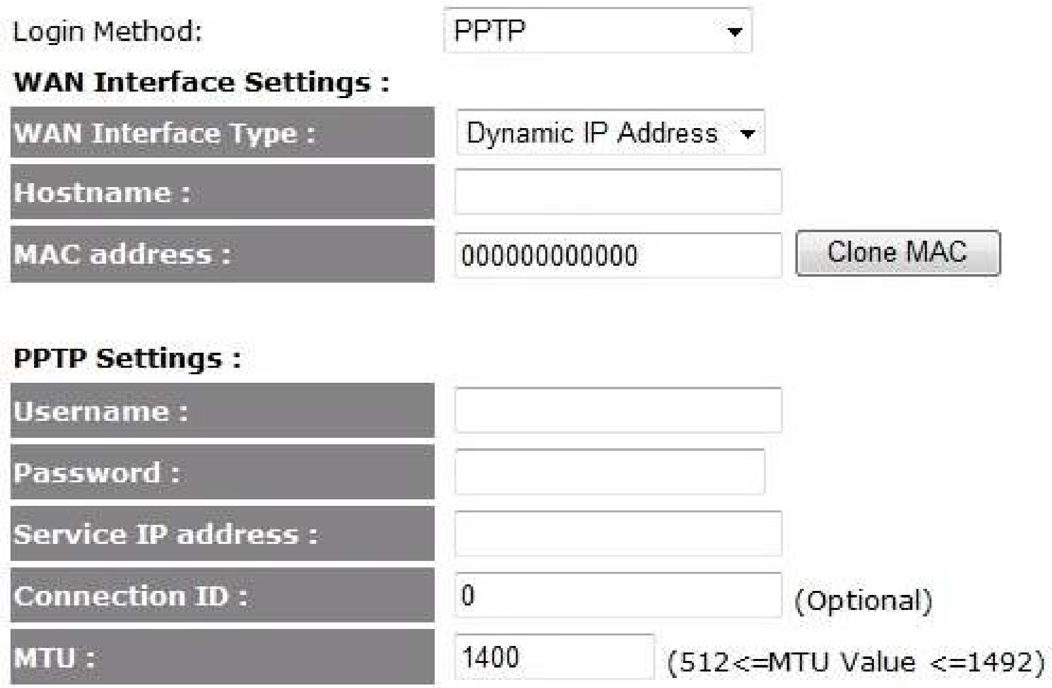


Login Method:	PPP over Ethernet
Username :	
Password :	
Service :	
MTU :	1492 (512<=MTU Value <=1492)

PPP over Ethernet	
Username	Username assigned to you by the ISP
Password	Password for this username.
Service	You can assign a name for this service. (Optional)
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by some ISPs.



Login Method: PPTP

WAN Interface Settings :

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

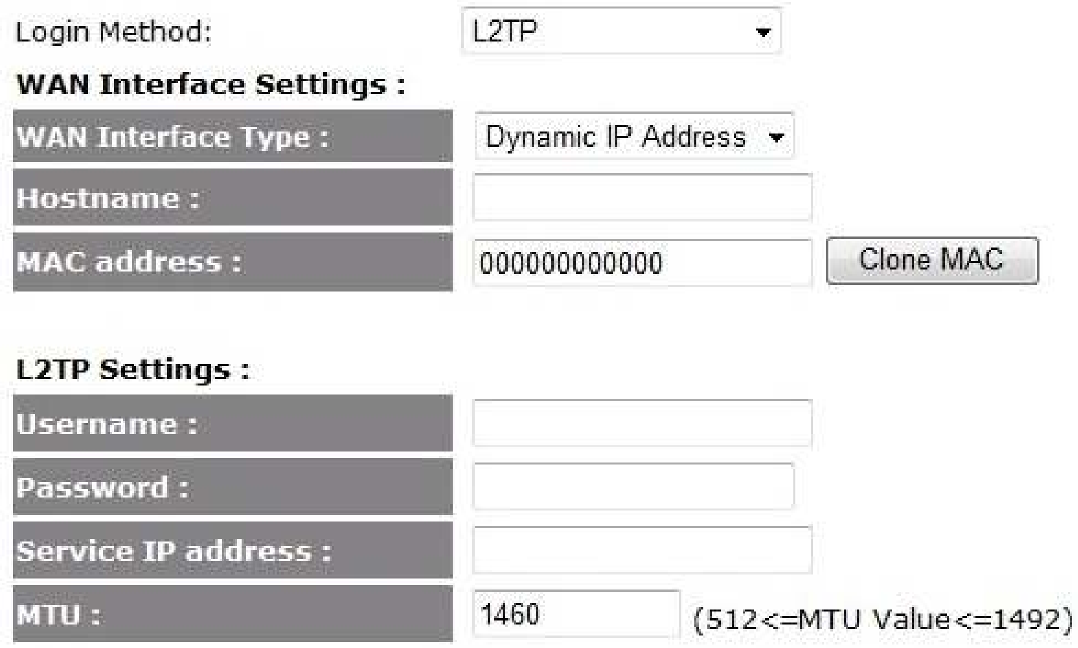
PPTP Settings :

Username :		
Password :		
Service IP address :		
Connection ID :	0	(Optional)
MTU :	1400	(512<=MTU Value <=1492)

PPTP WAN Interface Settings	
WAN Interface Type	Select whether the ISP is set to Static IP or Dynamic IP address.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC address that is used to connect to the ISP.
PPTP Settings	
Login	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
Connection ID	This is optional. Only required if specified by ISP
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.

Layer-2 Tunneling Protocol (L2TP)

L2TP is used by some ISPs.



Login Method:	L2TP ▾	

WAN Interface Settings :

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

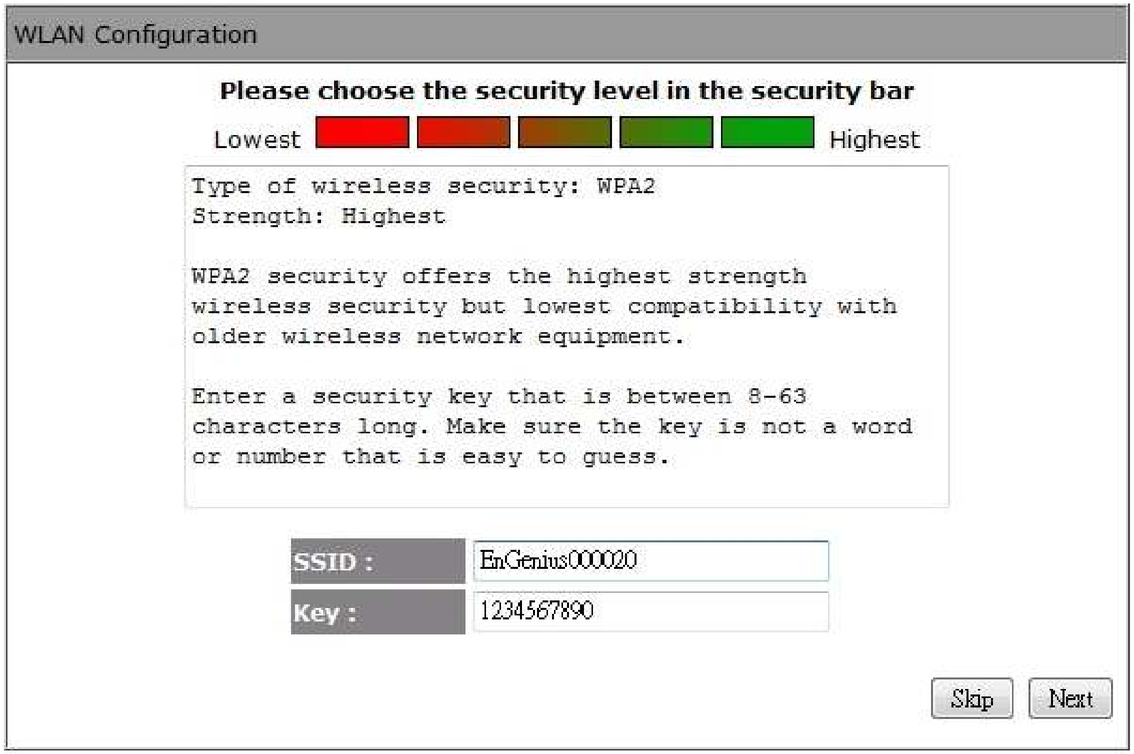
L2TP Settings :

Username :		
Password :		
Service IP address :		
MTU :	1460	(512<=MTU Value<=1492)

L2TP WAN Interface Settings	
WAN Interface Type	Select whether the ISP is set to Static IP or Dynamic IP address.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC address that is used to connect to the ISP.
L2TP Settings	
Login	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.

d) Setup the level of wireless security to be used.
EnGenius recommends the **Highest** level of security to be used.

Note: 802.11n wireless speeds may not be achievable if the security level is setting the Lowest or Low.



WLAN Configuration

Please choose the security level in the security bar

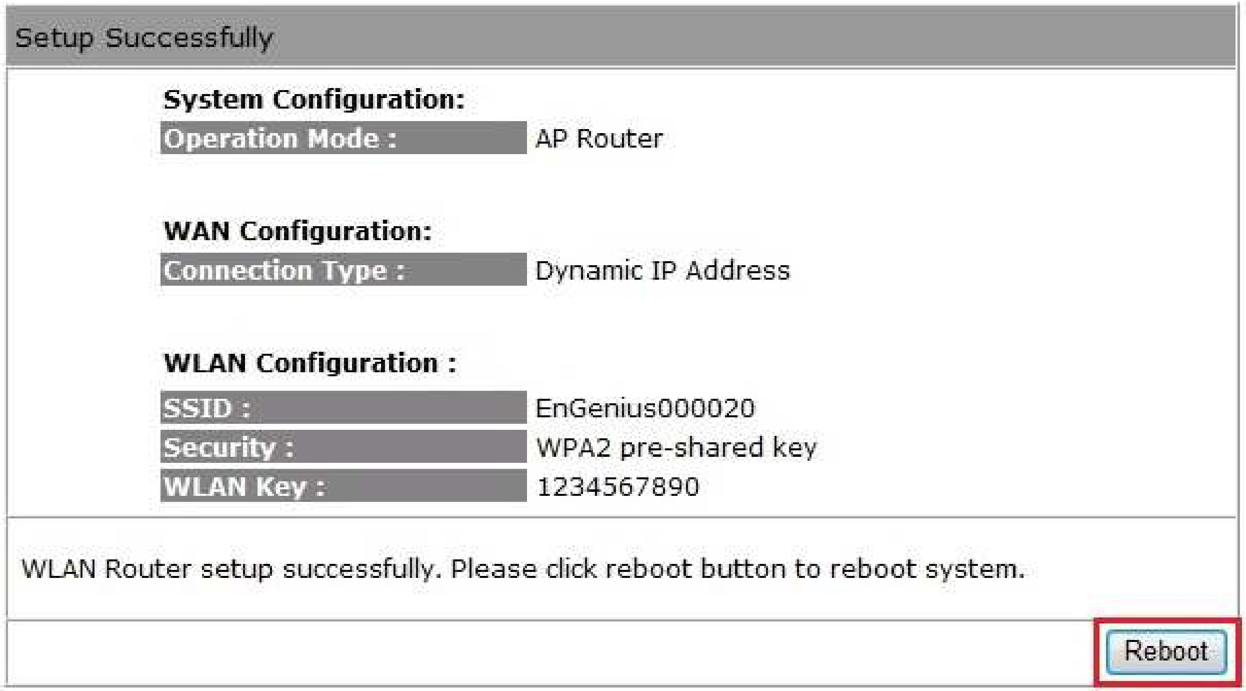
Lowest 🟥 🟥 🟫 🟩 🟩 Highest

```
Type of wireless security: WPA2
Strength: Highest

WPA2 security offers the highest strength
wireless security but lowest compatibility with
older wireless network equipment.

Enter a security key that is between 8-63
characters long. Make sure the key is not a word
or number that is easy to guess.
```

SSID :	EnGenius000020
Key :	1234567890

SSID	Enter the name of your wireless network.
Key	Enter the security key for your wireless network.

e) Check the settings are correct, and then click **Reboot** to apply the settings.



Setup Successfully

System Configuration:

Operation Mode :	AP Router

WAN Configuration:

Connection Type :	Dynamic IP Address

WLAN Configuration :

SSID :	EnGenius000020
Security :	WPA2 pre-shared key
WLAN Key :	1234567890

WLAN Router setup successfully. Please click reboot button to reboot system.

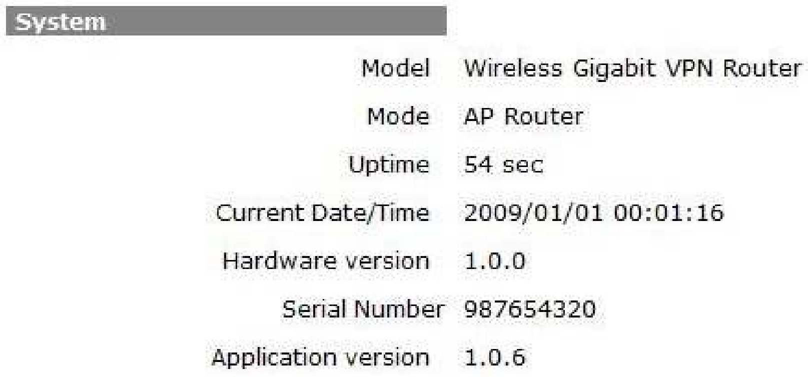
5. VPN Wizard

Using VPN Wizard, you can establish VPN connection easily. Please refer to 11.3.

6. System

6.1. Status

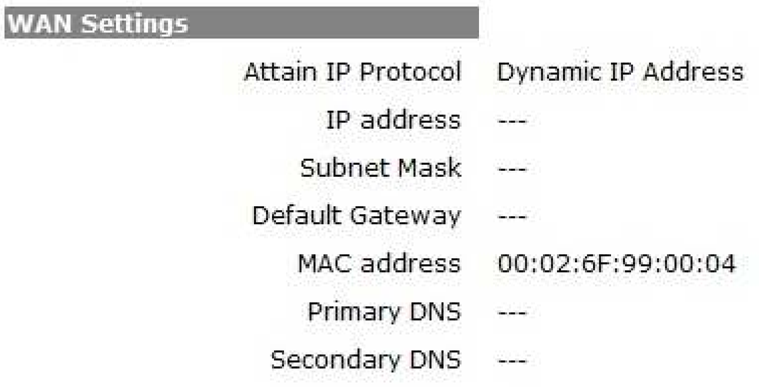
This page will display status of the device.



System

Model	Wireless Gigabit VPN Router
Mode	AP Router
Uptime	54 sec
Current Date/Time	2009/01/01 00:01:16
Hardware version	1.0.0
Serial Number	987654320
Application version	1.0.6

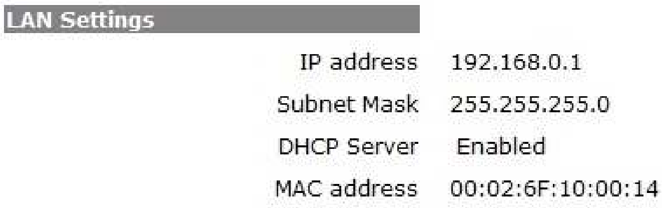
Status	
Model	Description of this device.
Mode	The device is currently in which mode.
Uptime	The duration about the device has been operating without powering down or reboot.
Current Date/Time	The device’s system time. If this is incorrect, please set the time in the Tools / Time page.
Hardware version and Serial Number	Hardware information for this device.
Application version	Firmware information for this device.



WAN Settings

Attain IP Protocol	Dynamic IP Address
IP address	---
Subnet Mask	---
Default Gateway	---
MAC address	00:02:6F:99:00:04
Primary DNS	---
Secondary DNS	---

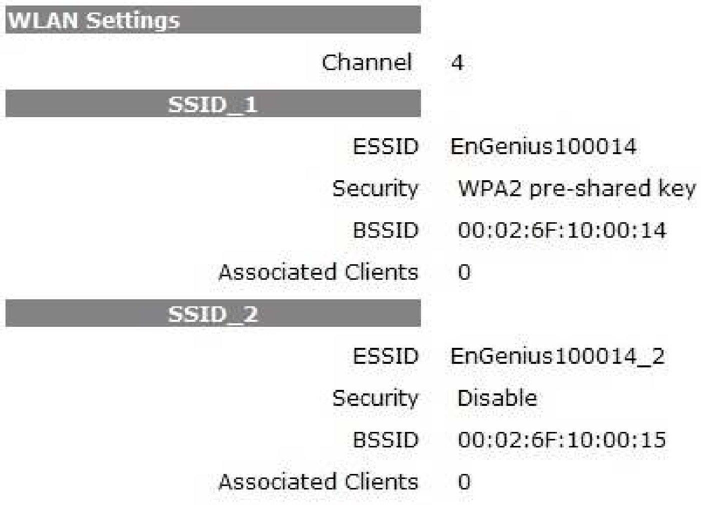
WAN Settings	
Attain IP Protocol	Method used to connect to the Internet
IP address	The WAN IP Address of the device.
Subnet Mask	The WAN Subnet Mask of the device.
MAC address	The MAC address of the device’s WAN Interface.
Primary and Secondary DNS	Primary and Secondary DNS servers assigned to the WAN connection.



LAN Settings

IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC address	00:02:6F:10:00:14

LAN Settings	
IP address	The LAN IP Address of the device.
Subnet Mask	The LAN Subnet Mask of the device.
DHCP Server	Whether the DHCP server is Enabled or Disabled.
MAC address	The MAC address of the device's LAN Interface.



WLAN Settings

Channel 4

SSID_1

ESSID EnGenius100014

Security WPA2 pre-shared key

BSSID 00:02:6F:10:00:14

Associated Clients 0

SSID_2

ESSID EnGenius100014_2

Security Disable

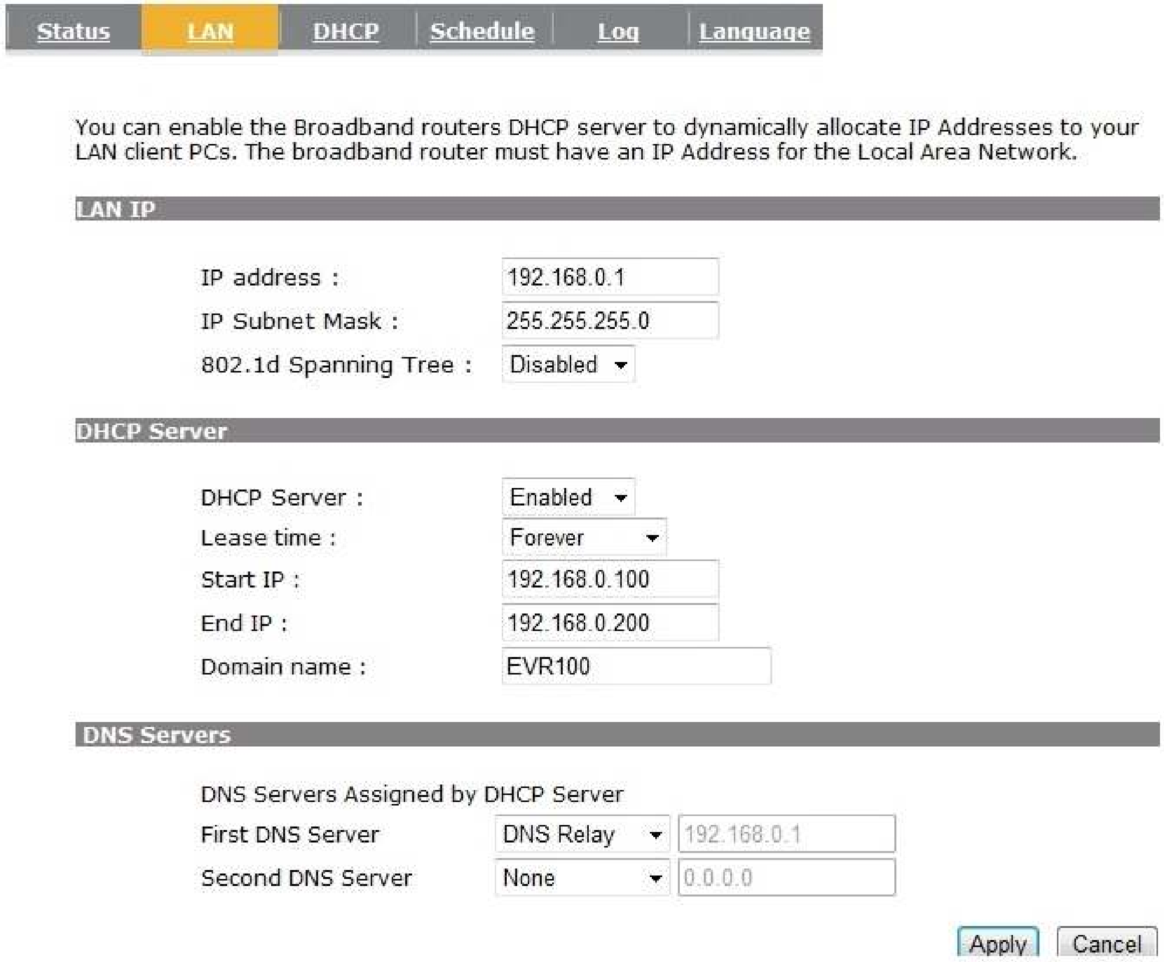
BSSID 00:02:6F:10:00:15

Associated Clients 0

WLAN Settings	
Channel	The wireless channel in use.
ESSID	The SSID (Network Name) of the wireless network. (up to 4 SSIDs are supported)
Security	Wireless encryption is enabled for this SSID.
BSSID	The MAC address of this SSID.
Associated Clients	The number of wireless clients connected to this SSID.

6.2. LAN

This page allows you to modify the device's LAN settings.



You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP

IP address :	192.168.0.1
IP Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disabled

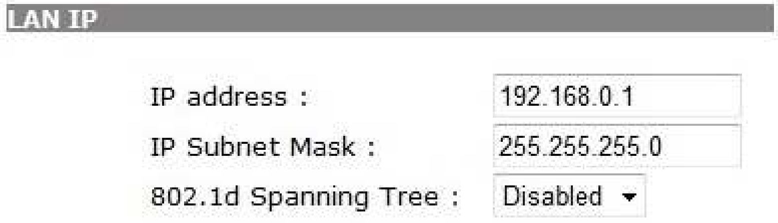
DHCP Server

DHCP Server :	Enabled
Lease time :	Forever
Start IP :	192.168.0.100
End IP :	192.168.0.200
Domain name :	EVR100

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



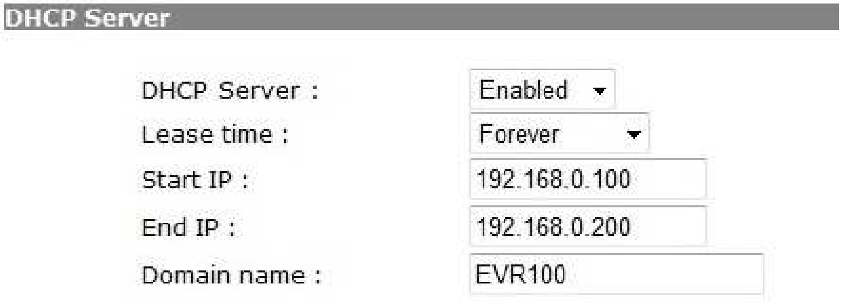
LAN IP

IP address : 192.168.0.1

IP Subnet Mask : 255.255.255.0

802.1d Spanning Tree : Disabled

LAN IP	
IP address	The LAN IP Address of this device.
IP Subnet Mask	The LAN Subnet Mask of this device.
802.1d Spanning Tree	When Enabled, the Spanning Tree protocol will prevent network loops in your LAN network.



DHCP Server

DHCP Server : Enabled

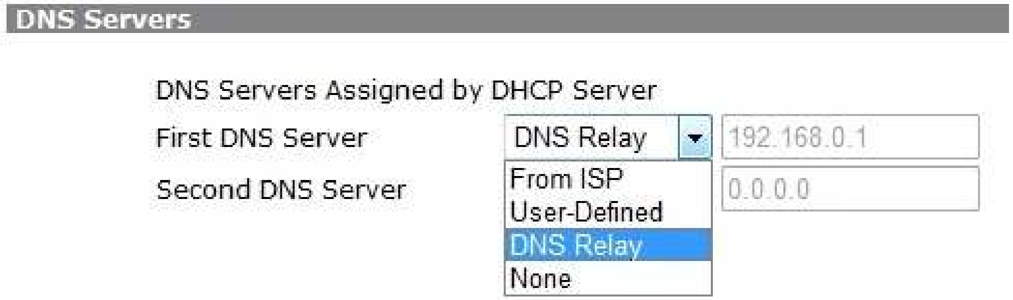
Lease time : Forever

Start IP : 192.168.0.100

End IP : 192.168.0.200

Domain name : EVR100

DHCP Server	
DHCP Server	The DHCP Server automatically allocates IP addresses to your LAN device.
Lease Time	The duration of the DHCP server allocates each IP address to a LAN device.
Start / End IP	The range of IP addresses of the DHCP server will allocate to LAN device.
Domain name	The domain name for this LAN network.



DNS Servers

DNS Servers Assigned by DHCP Server

First DNS Server DNS Relay 192.168.0.1

Second DNS Server 0.0.0.0

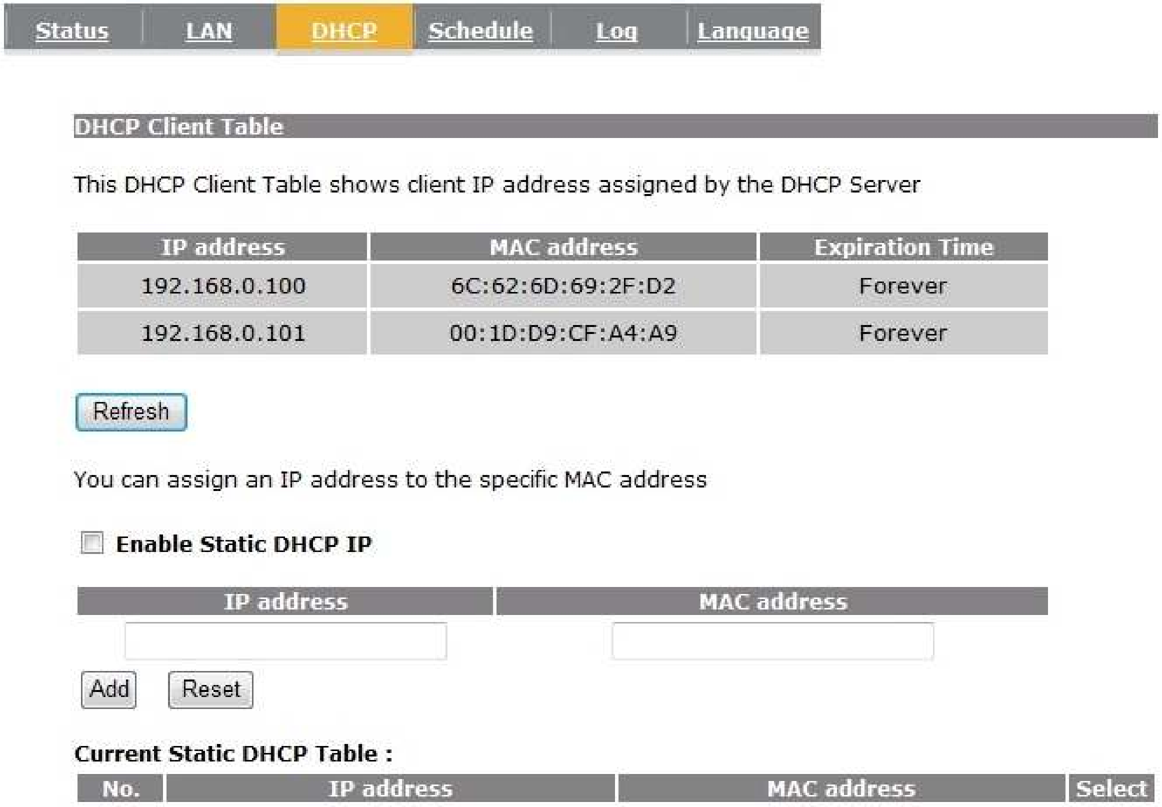
Two DNS servers can be assigned for use by your LAN device.

There are four modes available.

DNS Servers	
From ISP	The DNS server IP address is assigned from your ISP.
User-Defined	The DNS server IP address is assigned manually.
DNS Relay	LAN clients are assigned the device's IP address as the DNS server. DNS requests are relayed to the ISP's DNS server.

6.3. DHCP

This page shows the status of the DHCP server and also allows you to control how the IP addresses are allocated.



DHCP Client Table

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.0.100	6C:62:6D:69:2F:D2	Forever
192.168.0.101	00:1D:D9:CF:A4:A9	Forever

You can assign an IP address to the specific MAC address

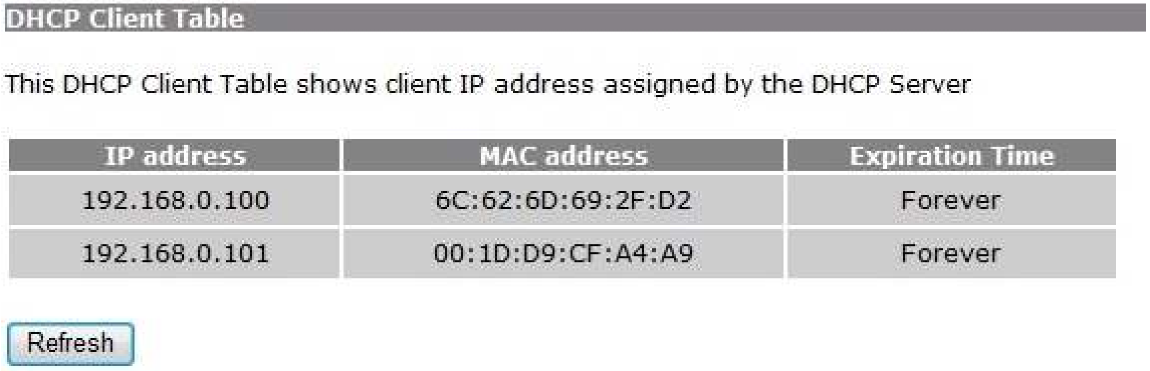
□ Enable Static DHCP IP

IP address	MAC address

Current Static DHCP Table :

No.	IP address	MAC address	Select

The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server



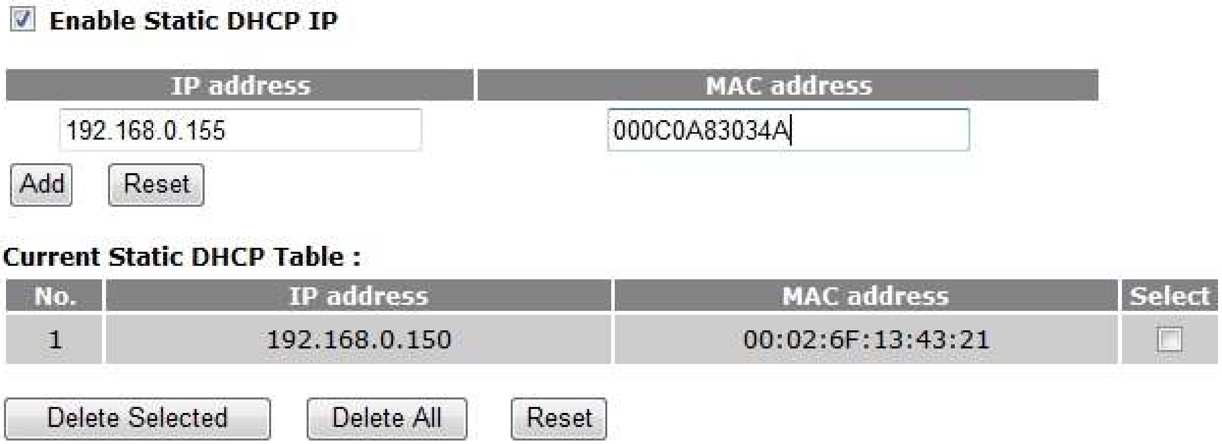
DHCP Client Table

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.0.100	6C:62:6D:69:2F:D2	Forever
192.168.0.101	00:1D:D9:CF:A4:A9	Forever

.

DHCP Client Table	
IP address	The LAN IP address of the client.
MAC address	The MAC address of the client's LAN interface.
Expiration Time	The time that the allocated IP address will expire.
Refresh	Click this button to update the DHCP Client Table.



☑ Enable Static DHCP IP

IP address	MAC address
192.168.0.155	000C0A83034A

Current Static DHCP Table :

No.	IP address	MAC address	Select
1	192.168.0.150	00:02:6F:13:43:21	□

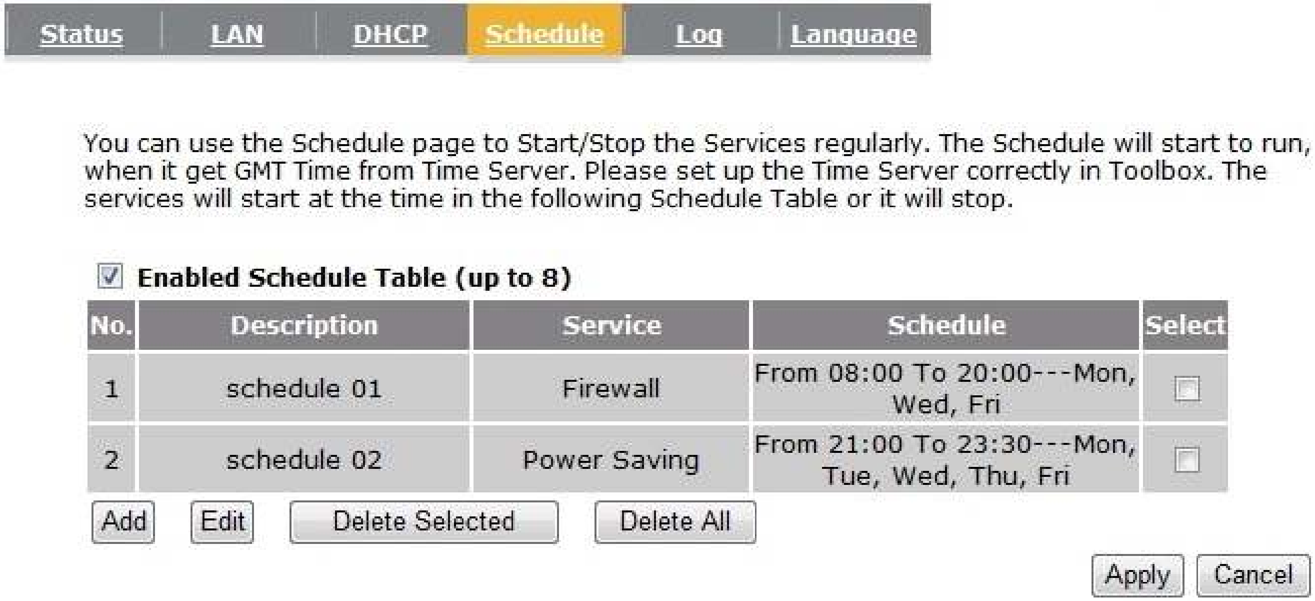
You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

6.4. Schedule

This page allows you to setup the schedule times that the Firewall and Power Saving features will be activated / deactivated.

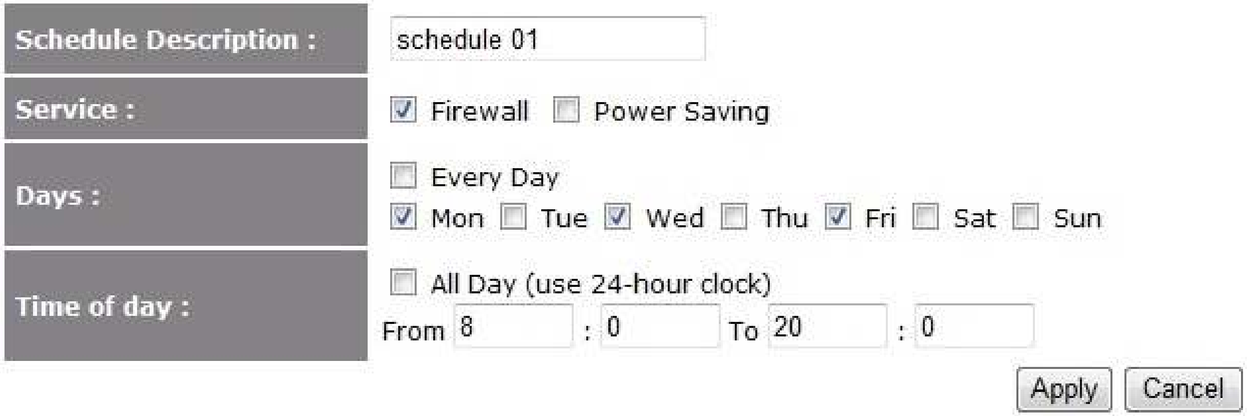
Click **Add** to create a Schedule entry.



You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

☑ **Enabled Schedule Table (up to 8)**

No.	Description	Service	Schedule	Select
1	schedule 01	Firewall	From 08:00 To 20:00---Mon, Wed, Fri	□
2	schedule 02	Power Saving	From 21:00 To 23:30---Mon, Tue, Wed, Thu, Fri	□

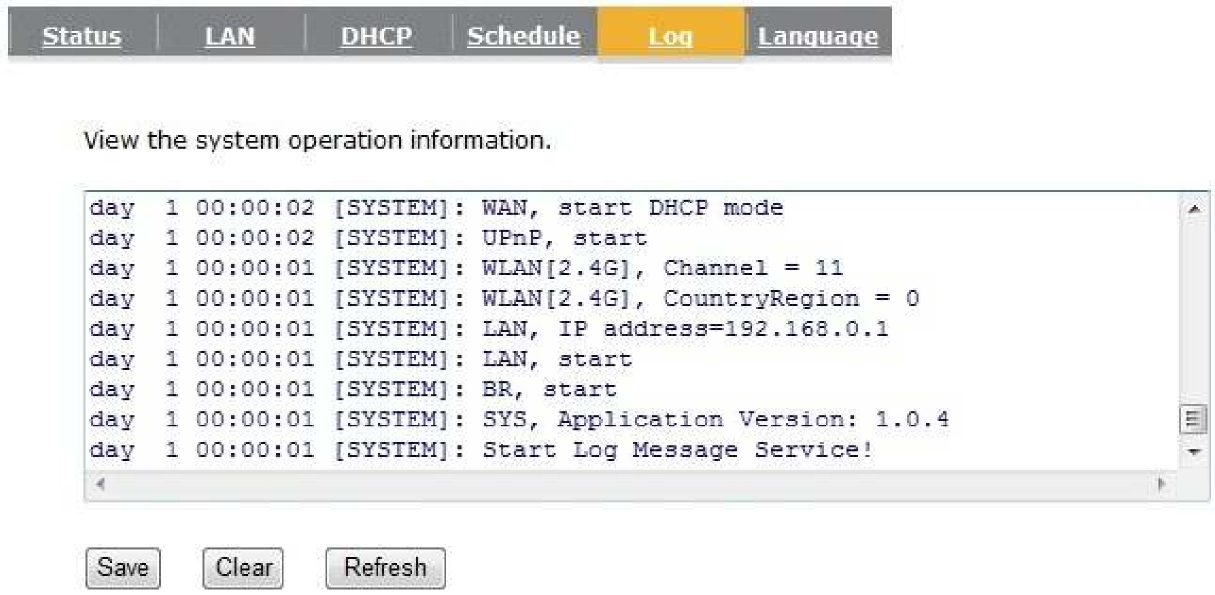


Schedule Description :	schedule 01
Service :	☑ Firewall ☐ Power Saving
Days :	☐ Every Day ☑ Mon ☐ Tue ☑ Wed ☐ Thu ☑ Fri ☐ Sat ☐ Sun
Time of day :	☐ All Day (use 24-hour clock) From 8 : 0 To 20 : 0

Schedule	
Schedule Description	Assign a name to the schedule.
Service	The service provides for the schedule.
Days	Define the Days to activate or deactivate the schedule.
Time of day	Define the Time of day to activate or deactivated the schedule. Please use 24-hour clock format.

6.5. Log

This page displays the system log of the device. When powered down or rebooted, the log will be cleared.



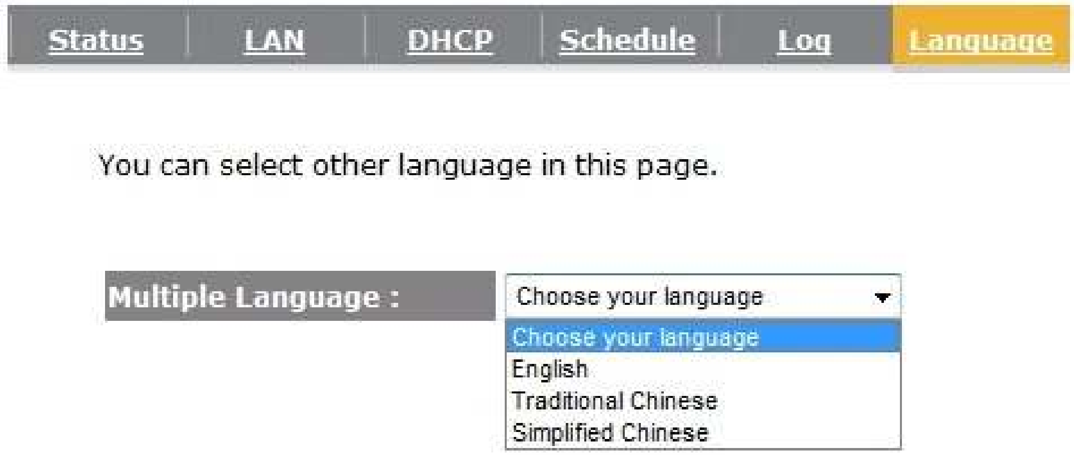
View the system operation information.

```
day  1 00:00:02 [SYSTEM]: WAN, start DHCP mode
day  1 00:00:02 [SYSTEM]: UPnP, start
day  1 00:00:01 [SYSTEM]: WLAN[2.4G], Channel = 11
day  1 00:00:01 [SYSTEM]: WLAN[2.4G], CountryRegion = 0
day  1 00:00:01 [SYSTEM]: LAN, IP address=192.168.0.1
day  1 00:00:01 [SYSTEM]: LAN, start
day  1 00:00:01 [SYSTEM]: BR, start
day  1 00:00:01 [SYSTEM]: SYS, Application Version: 1.0.4
day  1 00:00:01 [SYSTEM]: Start Log Message Service!
```

Log	
Save	Save the log to a file.
Clear	Clear the log.
Refresh	Update the log.

6.6. Language

This page allows you to change the Language of the User Interface.



You can select other language in this page.

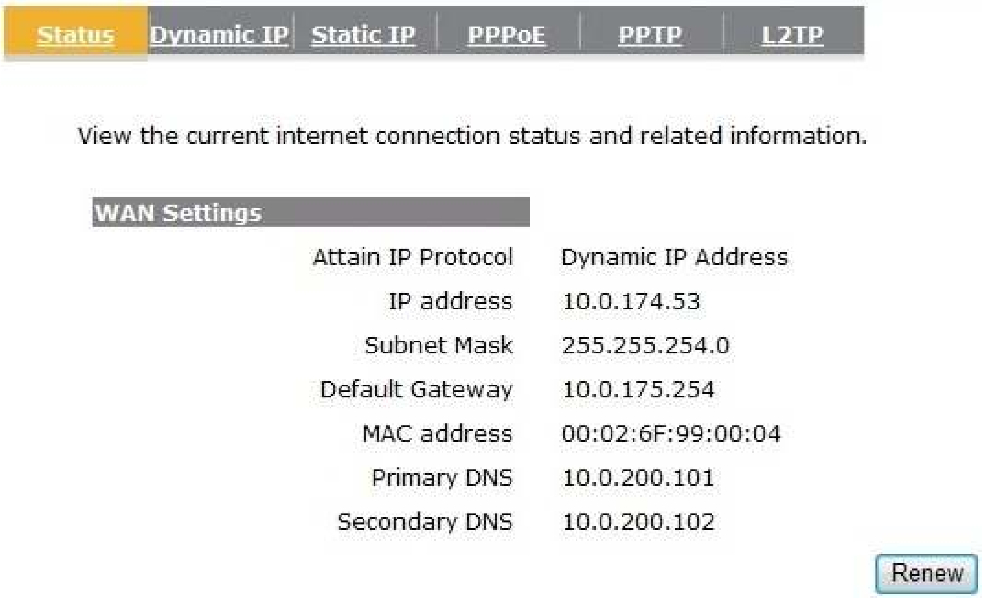
Multiple Language : Choose your language

7. Internet

The Internet section allows you to manually set the WAN type connection and its related settings.

7.1. Status

This page shows the current status of the device's WAN connection.



View the current internet connection status and related information.

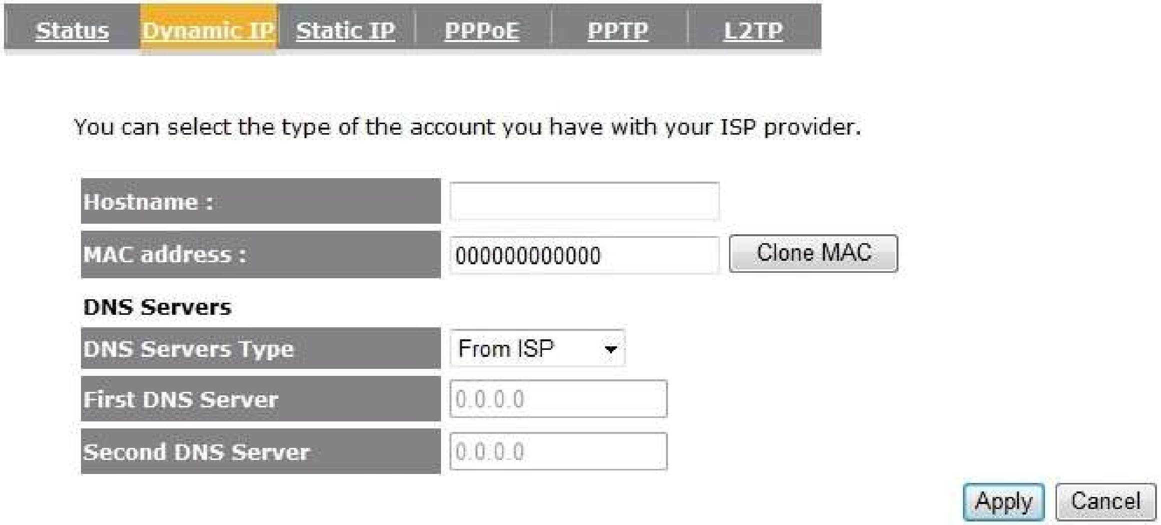
WAN Settings	
Attain IP Protocol	Dynamic IP Address
IP address	10.0.174.53
Subnet Mask	255.255.254.0
Default Gateway	10.0.175.254
MAC address	00:02:6F:99:00:04
Primary DNS	10.0.200.101
Secondary DNS	10.0.200.102

7.2. Dynamic IP Address

The IP Address is allocated automatically. However some ISP’s will also recognize the MAC address and will reject connections if the MAC address does not match.

If your ISP has recorded the MAC address of your computer’s Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC** button.

This will replace the AP Router MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.



You can select the type of the account you have with your ISP provider.

Hostname :	
MAC address :	000000000000

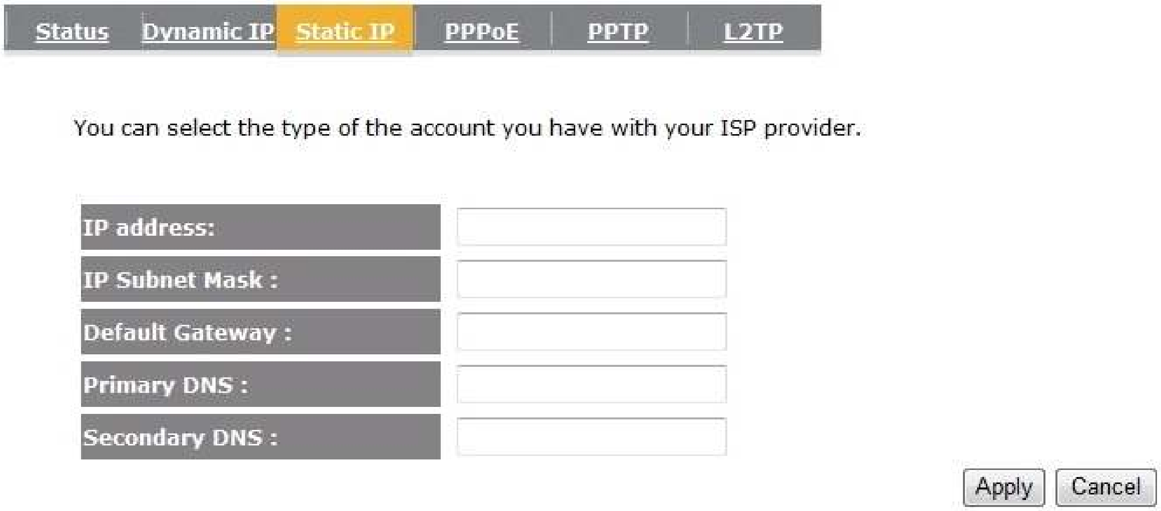
DNS Servers

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

Dynamic IP Address	
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
DNS Servers	
Two DNS servers can be assigned for use by your LAN devices. There are two modes available.	
From ISP	LAN devices are assigned the DNS server IP address of your ISP.
User-Defined	Set the DNS server IP address manually.

7.3. Static IP Address

If your ISP Provider has assigned you a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.



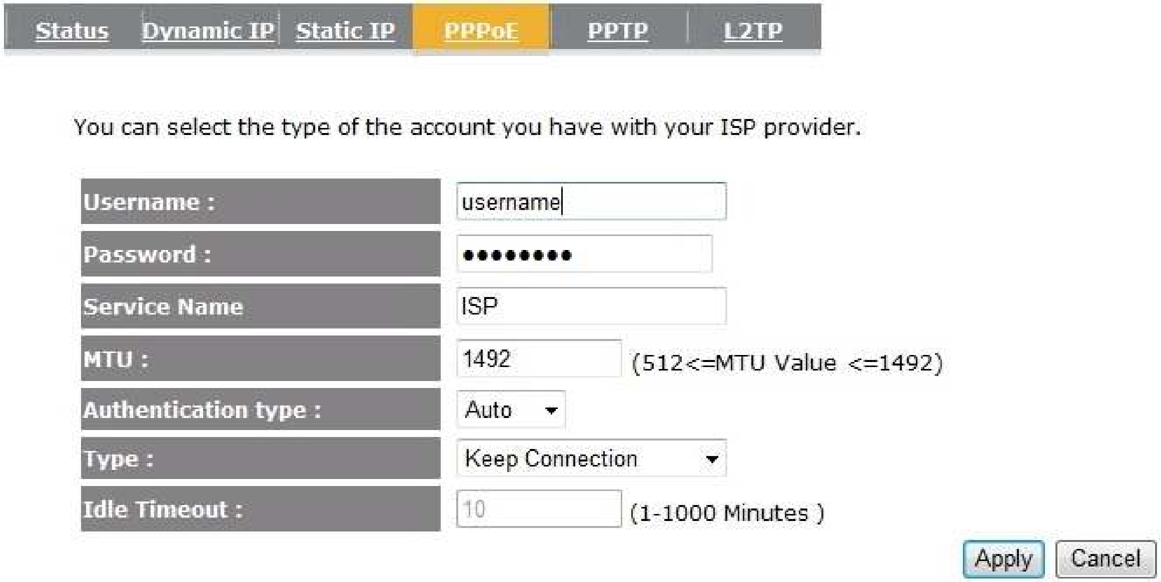
You can select the type of the account you have with your ISP provider.

IP address:	
IP Subnet Mask :	
Default Gateway :	
Primary DNS :	
Secondary DNS :	

Static IP Address	
IP address	Assign an IP address Manually.
IP Subnet Mask	Specify an IP address's subnet mask.
Default Gateway	Specify the gateway of your network.
Primary DNS	Specify the primary DNS server's IP address.
Secondary DNS	Specify the second DNS server's IP address.

7.4. PPP over Ethernet

ISP requires an account username and password.



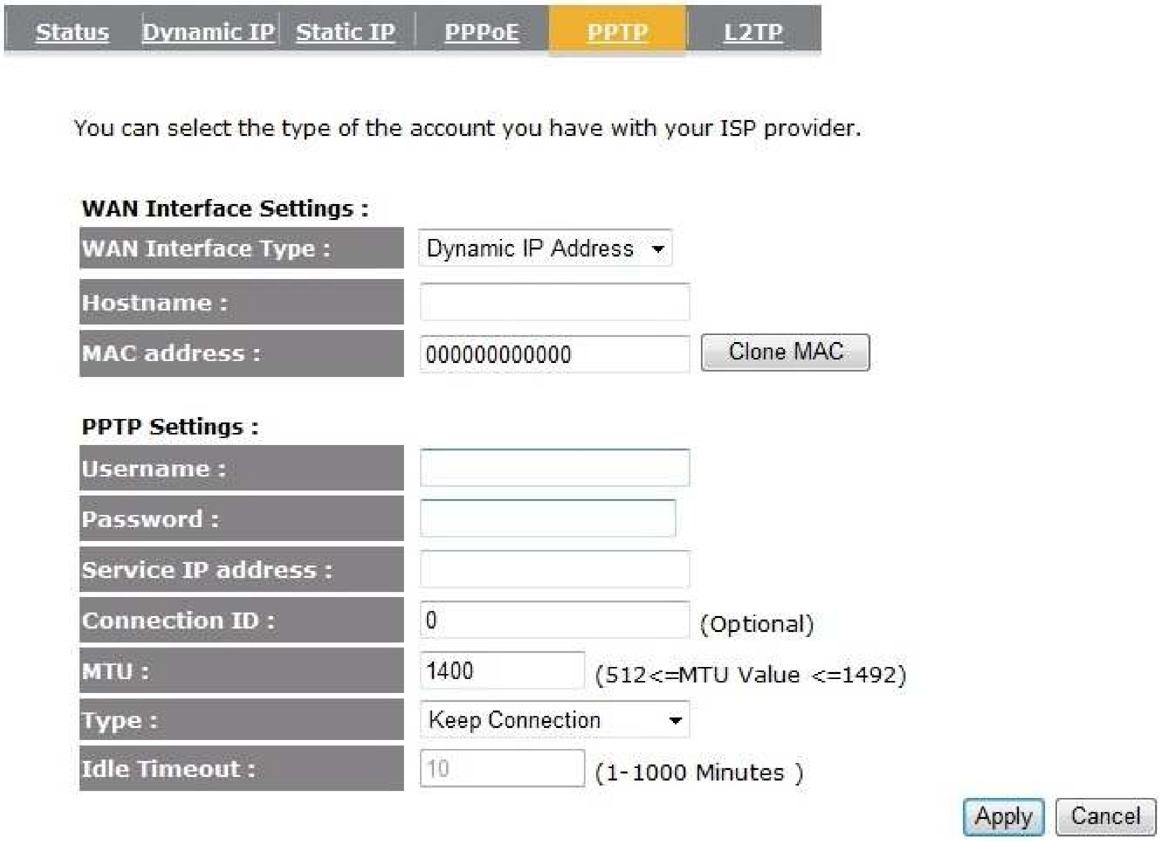
You can select the type of the account you have with your ISP provider.

Username :	username
Password :	●●●●●●●●●
Service Name	ISP
MTU :	1492 (512<=MTU Value <=1492)
Authentication type :	Auto
Type :	Keep Connection
Idle Timeout :	10 (1-1000 Minutes)

PPP over Ethernet (PPPoE)	
Username	Username assigned to you by the ISP
Password	Password for this username.
Service	You can assign a name for this service. (Optional)
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Authentication type	Select whether the ISP uses PAP or CHAP methods for authentication. Select **Auto** if unsure.
Type	You can choose the method that the router maintains connection with the ISP. **Keep Connection:** The device will maintain a constant connection with the ISP. **Automatic Connection:** The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. **Manual Connection:** The user will need to manually connect to the ISP by clicking the **Connect** button.
Idle Timeout:	When the connection type is **Automatic Connection**, when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

7.5. Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by some ISPs.



You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :	Dynamic IP Address
Hostname :	
MAC address :	000000000000

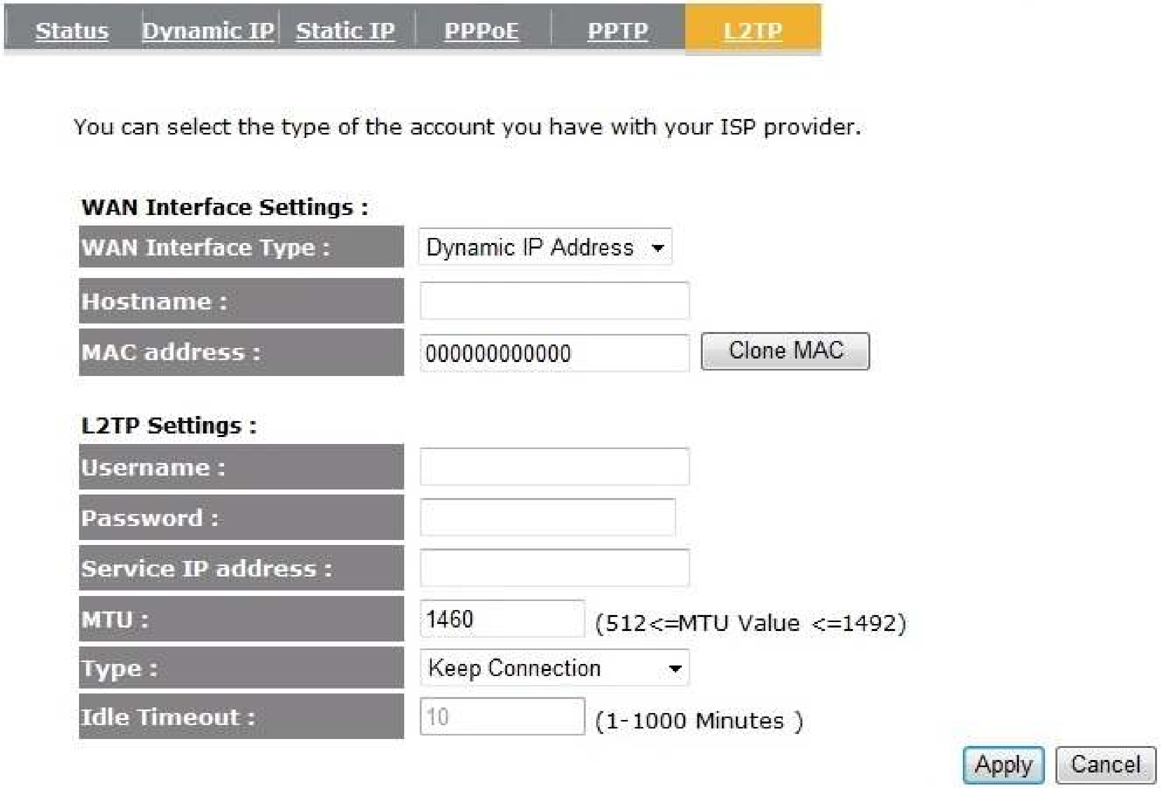
PPTP Settings :

Username :	
Password :	
Service IP address :	
Connection ID :	0 (Optional)
MTU :	1400 (512<=MTU Value <=1492)
Type :	Keep Connection
Idle Timeout :	10 (1-1000 Minutes)

Point-to-Point Tunneling Protocol (PPTP)	
WAN Interface Type	Select whether the ISP is set to Static IP or will allocate Dynamic IP address.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
Username	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the PPTP server.
Connection ID	This is optional. Only required if specified by ISP
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Type	You can choose the method that the router maintains connection with the ISP. **Keep Connection:** The device will maintain a constant connection with the ISP. **Automatic Connection:** The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. **Manual Connection:** The user will need to manually connect to the ISP by clicking the **Connect** button.
Idle Timeout:	When the connection type is **Automatic Connection**, when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

7.6. Layer-2 Tunneling Protocol (L2TP)

L2TP is used by some ISPs.



You can select the type of the account you have with your ISP provider.

WAN Interface Settings :

WAN Interface Type :	Dynamic IP Address
Hostname :	
MAC address :	000000000000

L2TP Settings :

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

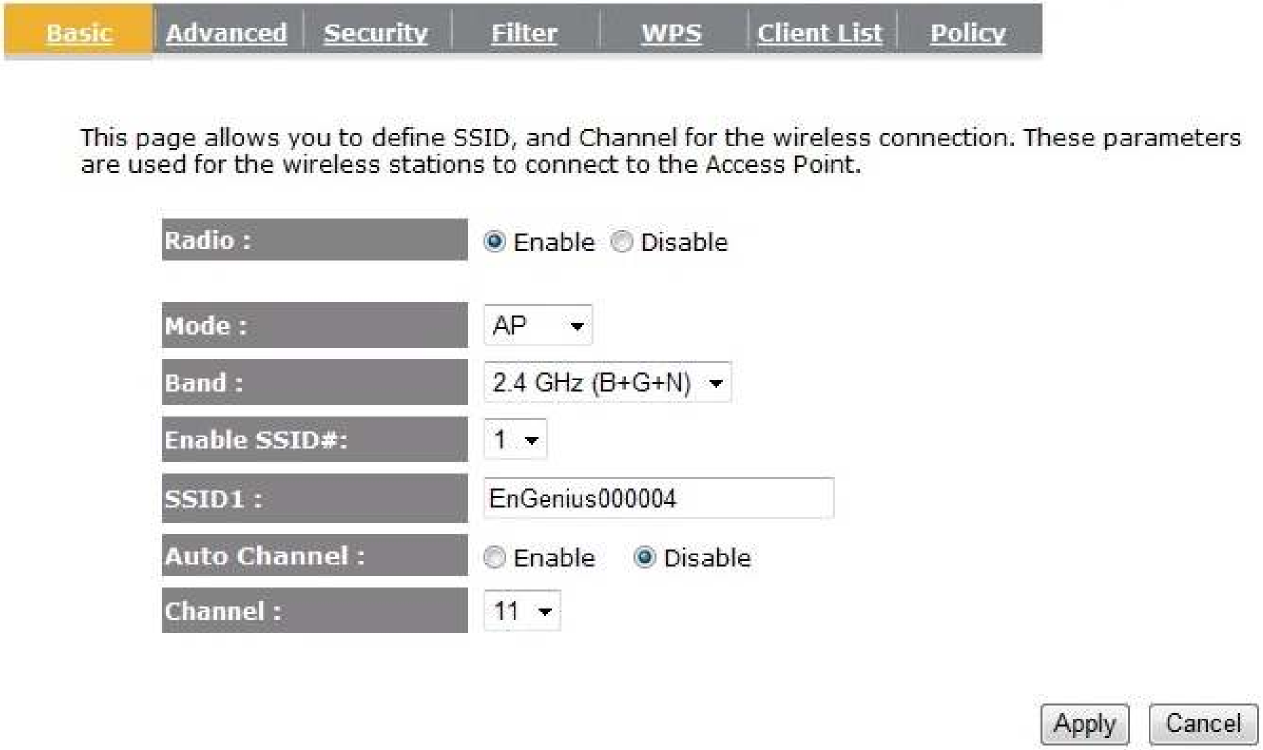
Layer-2 Tunneling Protocol (L2TP)	
WAN Interface Type	Select whether the ISP is set to Static IP or will allocate Dynamic IP address.
Hostname	This is optional. Only required if specified by ISP
MAC address	The MAC Address that is used to connect to the ISP.
Username	Username assigned to you by the ISP
Password	Password for this username.
Service IP Address	The IP Address of the L2TP server.
MTU	The maximum size of packets. Do not change unless mentioned by the ISP.
Type	You can choose the method that the router maintains connection with the ISP. **Keep Connection:** The device will maintain a constant connection with the ISP. **Automatic Connection:** The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. **Manual Connection:** The user will need to manually connect to the ISP by clicking the **Connect** button.
Idle Timeout:	When the connection type is **Automatic Connection**, when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

8. Wireless

The Wireless section allows you to configure the Wireless settings.

8.1. Basic

This page shows the current status of the device’s Wireless settings.



This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Radio :	● Enable ○ Disable
Mode :	AP
Band :	2.4 GHz (B+G+N)
Enable SSID#:	1
SSID1 :	EnGenius000004
Auto Channel :	○ Enable ● Disable
Channel :	11

Basic	
Radio	Enable or Disable the device’s wireless signal.
Mode	Select between Access Point or Wireless Distribution System (WDS) modes.
Band	Select the types of wireless clients that the device will accept. **eg: 2.4 GHz (B+G+N)** Only 802.11b and 11g clients will be allowed.
Enable SSID#	Select the number of SSID’s (Wireless Network names) you would like. You can create up to 4 separate wireless networks.
SSID#	Enter the name of your wireless network. You can use up to 32 characters.
Auto Channel	When enabled, the device will scan the wireless signals around your area and select the channel with the least interference.
Channel	Manually select which channel the wireless signal will use.
Check Channel Time	When Auto Channel is Enabled, you can specify the period of the device will scan the wireless signals around your area.

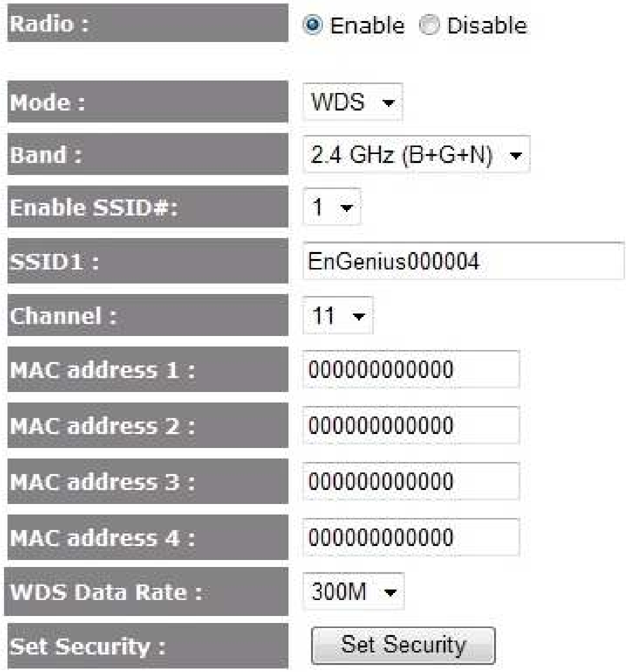
Wireless Distribution System (WDS)

Using WDS to connect Access Point wirelessly, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note that compatibility between different brands and models is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note that all Access Points in the WDS network needs to use the same Channel and Security settings.

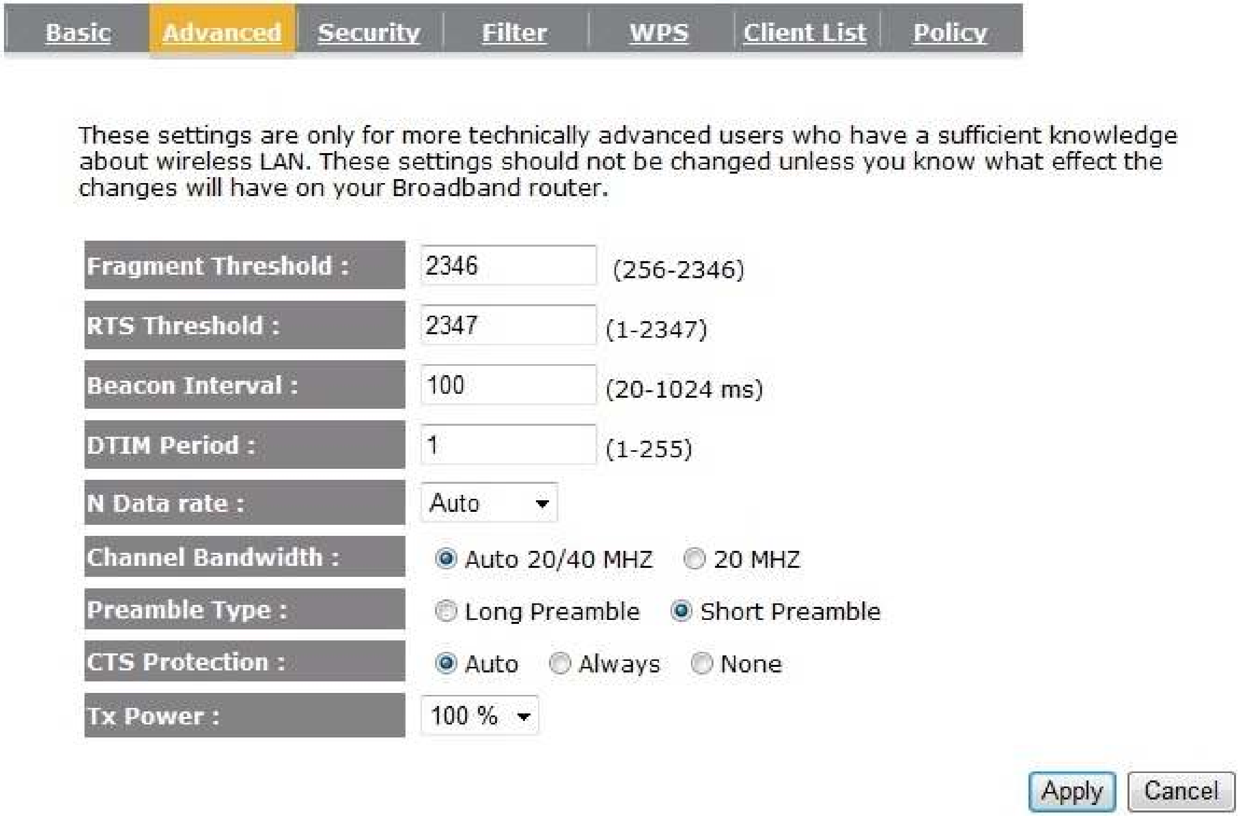
To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four access points.



Radio :	● Enable ○ Disable
Mode :	WDS
Band :	2.4 GHz (B+G+N)
Enable SSID#:	1
SSID1 :	EnGenius000004
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

This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.



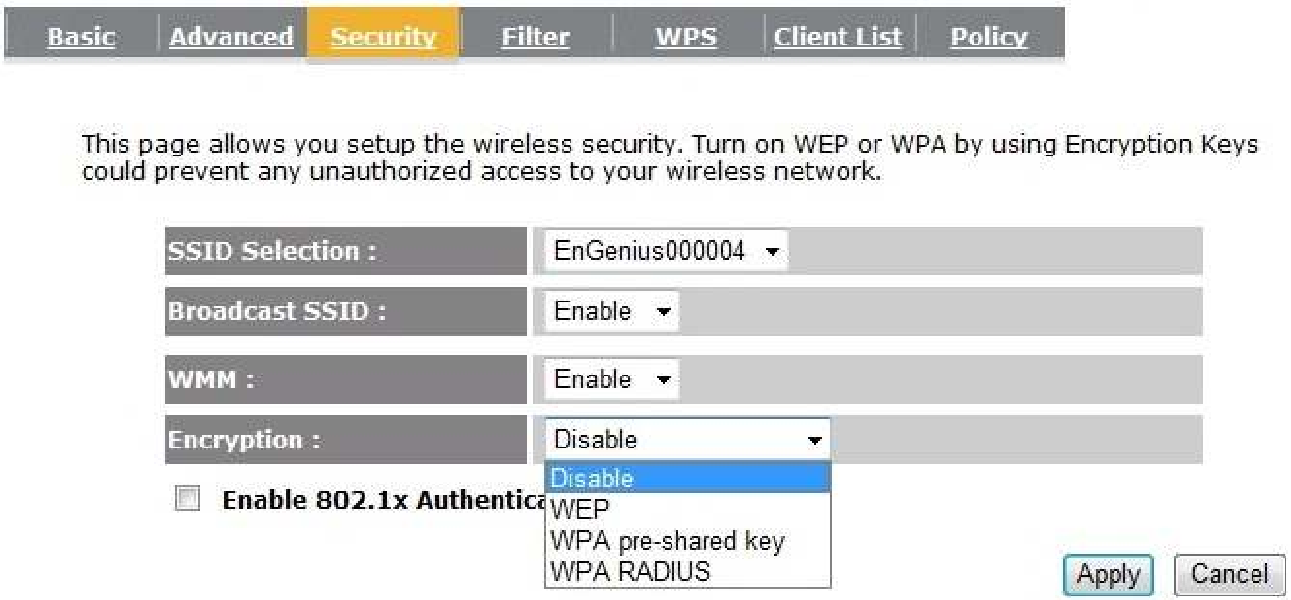
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold :	2346	(256-2346)
RTS Threshold :	2347	(1-2347)
Beacon Interval :	100	(20-1024 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 %	

Advanced	
Fragment Threshold	Specifies the size of the packet per fragment. This function can reduce the chance of packet collision. However when this value is set too low, there will be increased overheads resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, then the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.
Beacon Interval	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.
DTIM Period	A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multi-casted data.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20 or 40Mhz. To achieve 11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, so it decreases compatibility but increases performance.
CTS Protection	When Enabled, the performance is slightly lower however the chances of packet collision is greatly reduced.
Tx Power	Set the power output of the wireless signal.

8.3. Security

This page allows you to set the wireless security settings.



This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Selection : EnGenius000004

Broadcast SSID : Enable

WMM : Enable

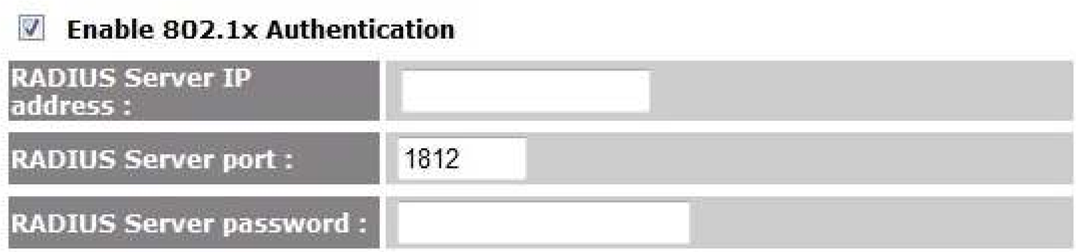
Encryption : Disable

□ Enable 802.1x Authentica

Security	
SSID Selection	Select the SSID that the security settings will apply to.
Broadcast SSID	If Disabled, then the device will not be broadcasting the SSID. Therefore it will be invisible to wireless clients.
WMM	Wi-Fi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background. Note that in certain situations, WMM needs to be enabled to achieve 11n transfer speeds.

Encryption	The encryption method to be applied. You can choose from WEP, WPA pre-shared key or WPA RADIUS. • **Disabled** - no data encryption is used. • **WEP** - data is encrypted using the WEP standard. • **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP. • **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. • **WPA-RADIUS** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. If this option is selected: • This Access Point must have a "client login" on the Radius Server. • Each user must have a "user login" on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

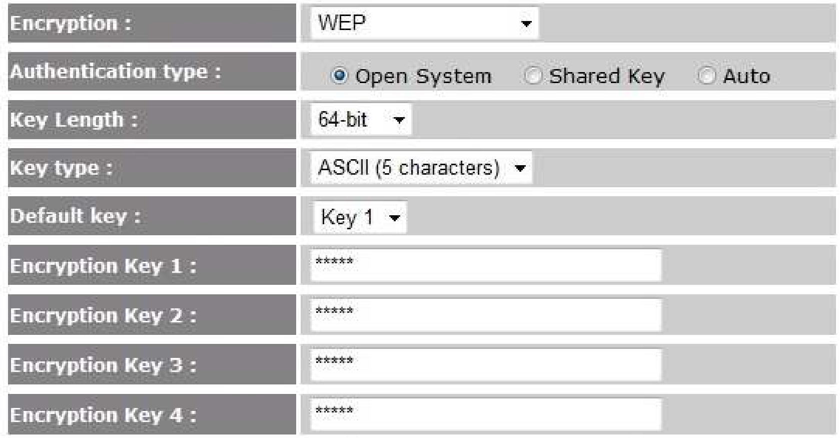


☑ Enable 802.1x Authentication

RADIUS Server IP address :	
RADIUS Server port :	1812
RADIUS Server password :	

802.1x Authentication	
RADIUS Server IP Address	The IP Address of the RADIUS Server
RADIUS Server port	The port number of the RADIUS Server.
RADIUS Server password	The RADIUS Server's password.

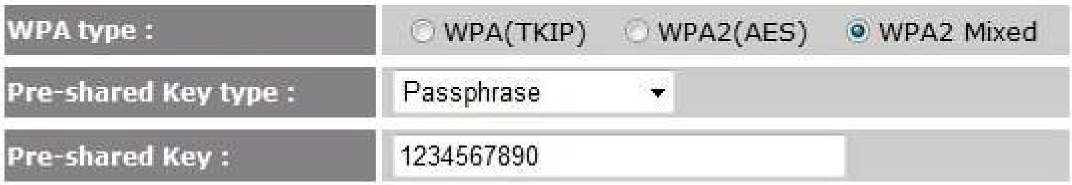
WEP Encryption:



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 :	*****

WEP Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
Key type	**ASCII**: regular text (recommended) **HEX**: for advanced users
Key Length	Select the desired option, and ensure the wireless clients use the same setting. • **64 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **128 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**.
Encryption Key #	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

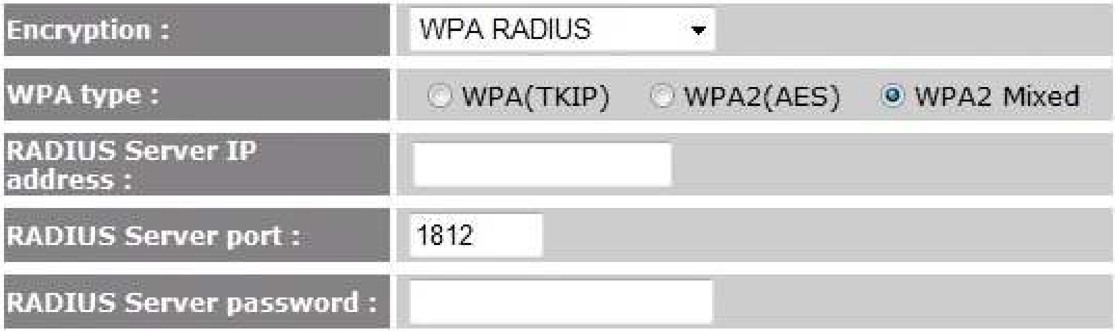
WPA Pre-Shared Key Encryption:



WPA type :	○ WPA(TKIP) ○ WPA2(AES) ● WPA2 Mixed
Pre-shared Key type :	Passphrase ▾
Pre-shared Key :	1234567890

WPA Pre-Shared Key Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
WPA type	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
Pre-shared Key Type	Select whether you would like to enter the Key in HEX or Passphrase format.
Pre-shared Key	Wireless clients must use the same key to associate the device. If using passphrase format, the Key must be from 8 to 63 characters in length.

WPA RADIUS Encryption:

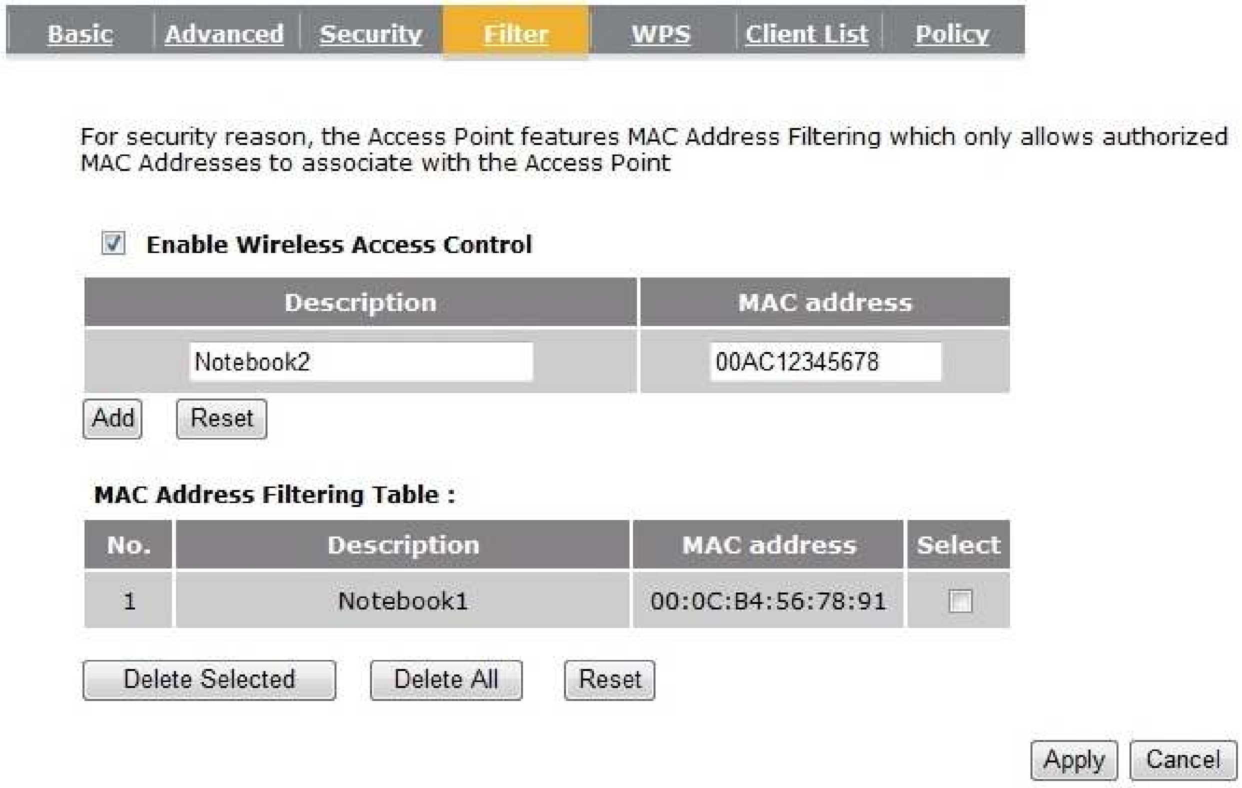


Encryption :	WPA RADIUS ▾
WPA type :	○ WPA(TKIP) ○ WPA2(AES) ● WPA2 Mixed
RADIUS Server IP address :	
RADIUS Server port :	1812
RADIUS Server password :	

WPA RADIUS Encryption	
WPA type	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
RADIUS Server IP address	Enter the IP address of the RADIUS Server
RADIUS Server Port	Enter the port number used for connections to the RADIUS server.
RADIUS Server password	Enter the password required to connect to the RADIUS server.

8.4. Filter

This page allows you to create filters to control which wireless clients can connect to this device by only allowing the MAC addresses entered into the Filtering Table.



For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point

☑ Enable Wireless Access Control

Description	MAC address
Notebook2	00AC12345678

MAC Address Filtering Table :

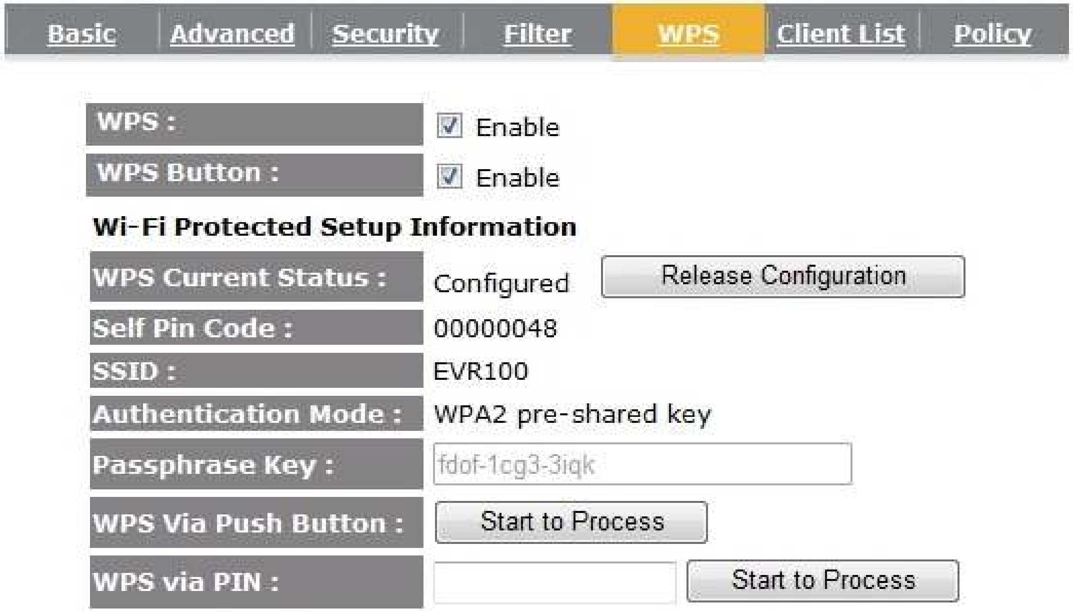
No.	Description	MAC address	Select
1	Notebook1	00:0C:B4:56:78:91	□

Wireless Filter	
Enable Wireless Access Control	Tick the box to Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description	Enter a name or description for this entry.
MAC address	Enter the MAC address of the wireless client that you wish to allow connection.
Add	Click this button to add the entry.
Reset	Click this button if you have made a mistake and want to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed access to the wireless network.	
Delete Selected	Delete the selected entries.
Delete All	Delete all entries
Reset	Un-tick all selected entries.

8.5. Wi-Fi Protected Setup (WPS)

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.



WPS :	☑ Enable
WPS Button :	☑ Enable

Wi-Fi Protected Setup Information

WPS Current Status :	Configured
Self Pin Code :	00000048
SSID :	EVR100
Authentication Mode :	WPA2 pre-shared key
Passphrase Key :	fdof-1cg3-3iqk
WPS Via Push Button :	
WPS via PIN :	

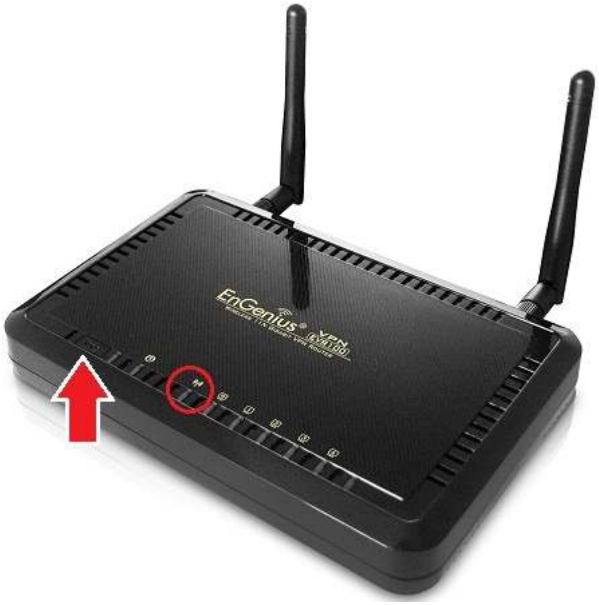
Wi-Fi Protected Setup (WPS)	
WPS	Tick to Enable the WPS feature.
WPS Button	Tick to Enable the WPS push button.
Wi-Fi Protected Setup Information	
WPS Current Status	Shows whether the WPS function is **Configured** or **Un-configured**. Configured means that WPS has been used to authorize connection between the device and wireless clients.
SSID	The SSID (wireless network name) used when connecting using WPS.
Authentication Mode	Shows the encryption method used by the WPS process.
Passphrase Key	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.
WPS Via Push Button	Click this button to initialize WPS feature using the push button method.
WPS Via PIN	Enter the PIN code of the wireless device and click this button to initialize WPS feature using the PIN method.

Initializing WPS Feature

There are two methods to initialize the WPS feature: Push Button and Pin code methods.

1. WPS Push Button Method

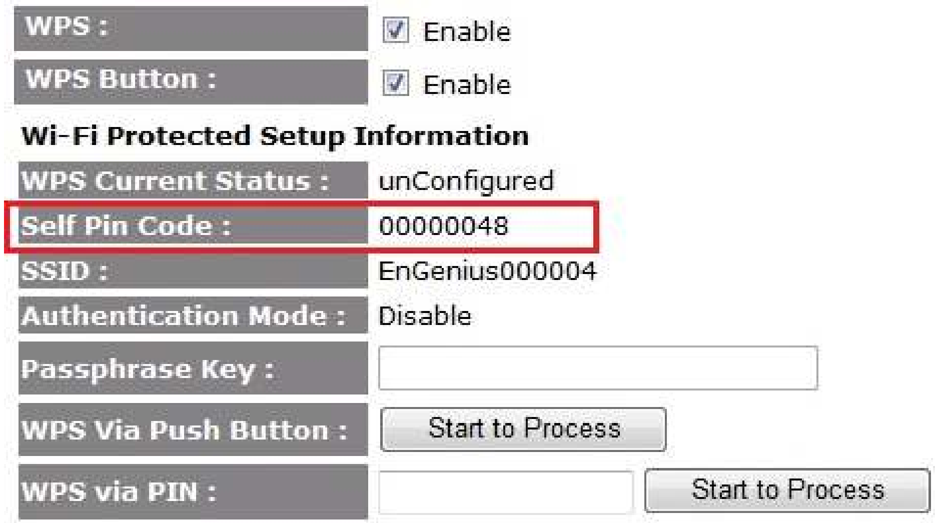
Push the WPS button on the WIRELESS ROUTER device. The Wireless LED light will start to flash to indicate that the WPS process is ready.



While the Wireless LED is flashing on the WIRELESS ROUTER, press the WPS button on your wireless client. This could either be a physical hardware button, or a software button in the utility.

2. Pin Code Method

Note the Pin code of your WIRELESS ROUTER device.



WPS :	☑ Enable
WPS Button :	☑ Enable

Wi-Fi Protected Setup Information

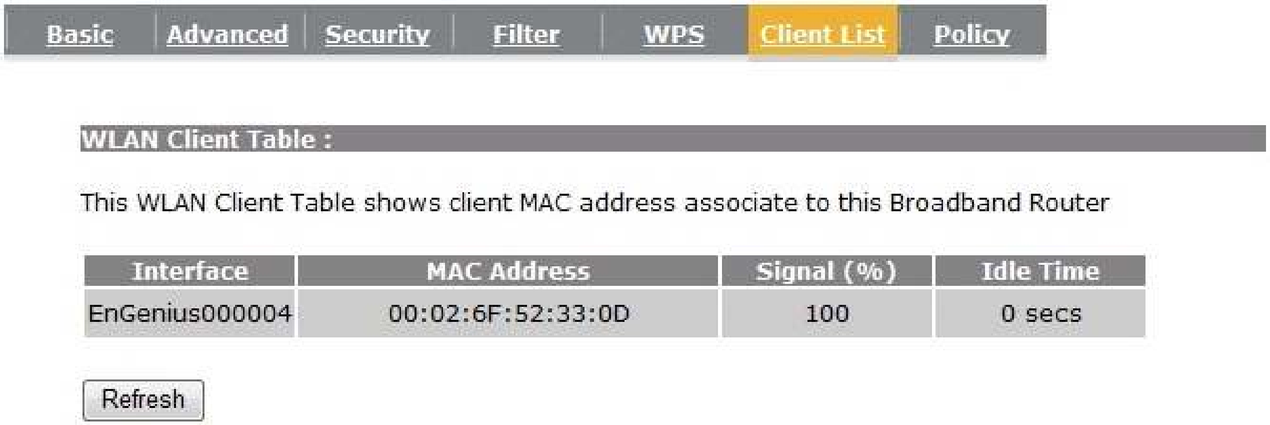
WPS Current Status :	unConfigured
Self Pin Code :	00000048
SSID :	EnGenius000004
Authentication Mode :	Disable
Passphrase Key :	
WPS Via Push Button :	Start to Process
WPS via PIN :	Start to Process

Please use this Pin code to initialize the WPS process from the wireless client configuration utility.

This process will be different for each brand or model. Please consult the user manual of the wireless client for more information.

8.6. Client List

This page shows the wireless clients that are connected to the WIRELESS ROUTER device.



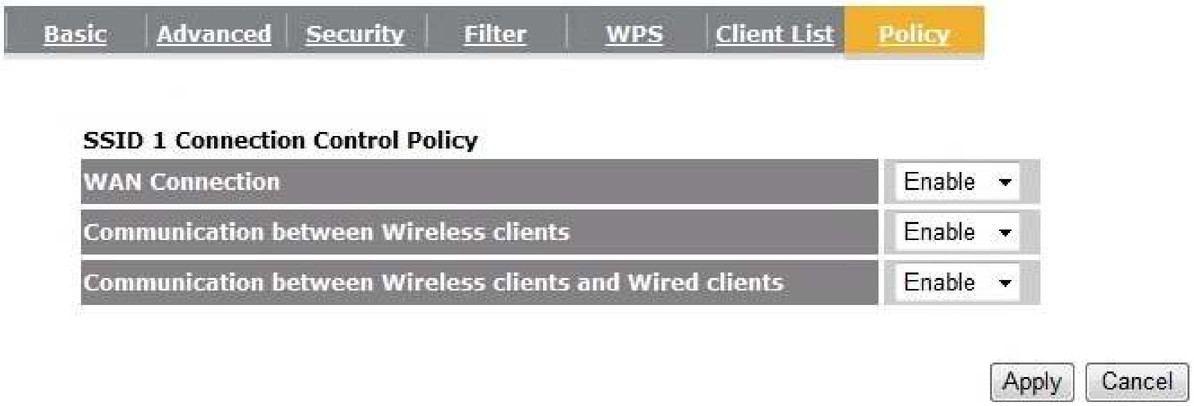
WLAN Client Table :

This WLAN Client Table shows client MAC address associate to this Broadband Router

Interface	MAC Address	Signal (%)	Idle Time
EnGenius000004	00:02:6F:52:33:0D	100	0 secs

8.7. Policy

This page allows you to configure the access policies for each SSID (wireless network).



SSID 1 Connection Control Policy

WAN Connection	Enable
Communication between Wireless clients	Enable
Communication between Wireless clients and Wired clients	Enable

Policy	
WAN Connection	Allow wireless clients on this SSID to access the WAN port which typically is an Internet connection.
Communication between Wireless clients	Whether each wireless client can communicate with each other in this SSID. When Disabled, the wireless clients will be isolated from each other.
Communication between Wireless clients and Wired clients	Whether wireless clients on this SSID can communicate with computers attached to the wired LAN port.

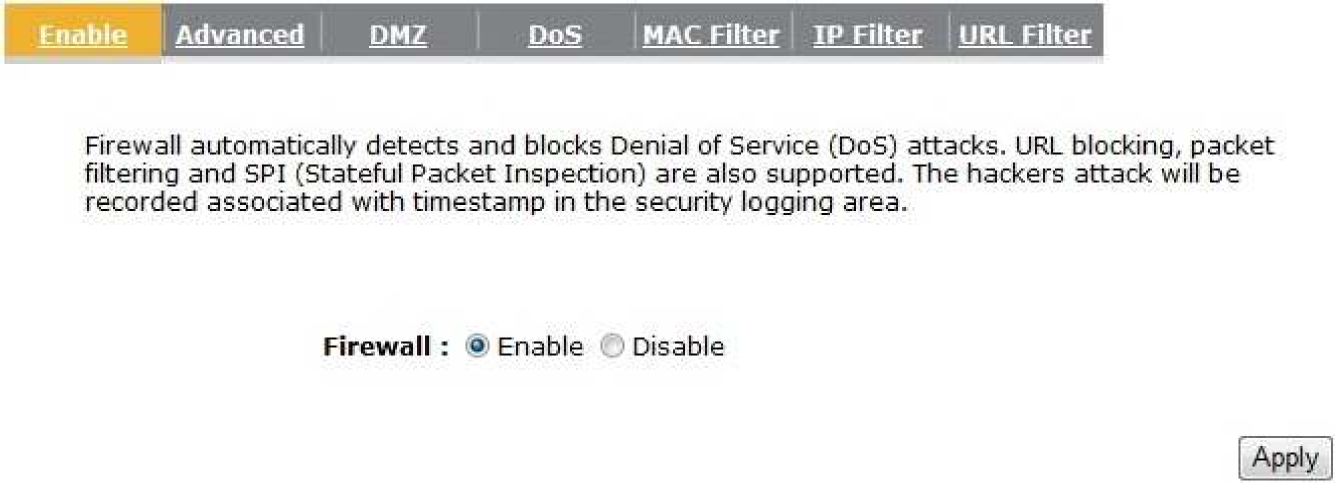
9. Firewall

The Firewall section allows you to set the access control and Firewall settings.

9.1. Enable

This page allows you to Enable / Disable the Firewall features.

If Enabled Firewall service, the Denial of Service (DoS) and SPI (Stateful Packet Inspection) features will also be enabled.

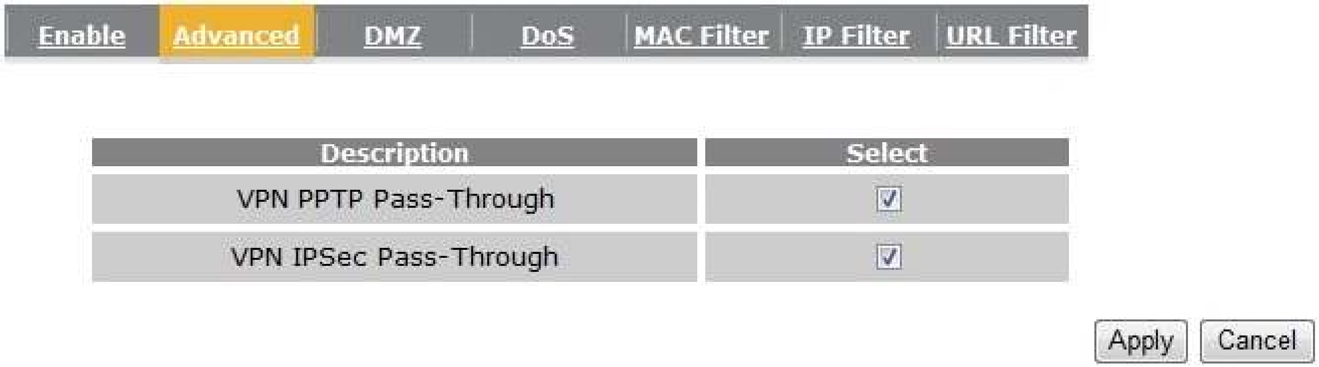


Firewall automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hackers attack will be recorded associated with timestamp in the security logging area.

Firewall : ● Enable ○ Disable

9.2. Advanced

You can choose whether to allow VPN (Virtual Private Network) packets to pass through the Firewall.



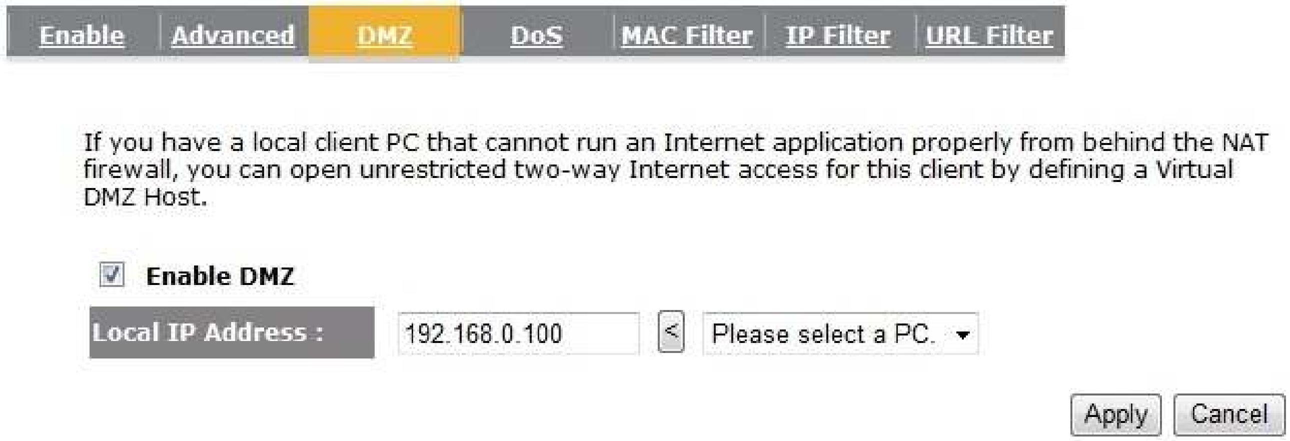
Description	Select
VPN PPTP Pass-Through	☑
VPN IPSec Pass-Through	☑

9.3. DMZ

If enabled this feature, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the server.
- The “DMZ PC” will receive all Unknown connections and data.
- If the DMZ feature is enabled, please enter the IP address of the PC to be used as the “DMZ PC”

Note: The “DMZ PC” is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.



If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

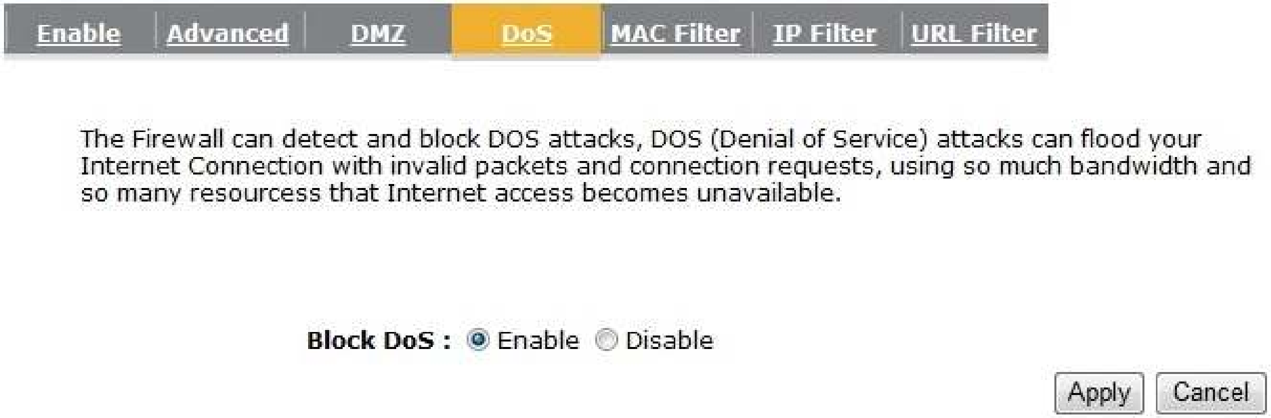
☑ Enable DMZ

Local IP Address : 192.168.0.100 < Please select a PC.

9.4. Denial of Service (DoS)

Denial of Service (Denial of Service) is a type of Internet attack that sends a high amount of data to you with the intent to overload your Internet connection.

Enable the DoS firewall feature to automatically detect and block these DoS attacks.

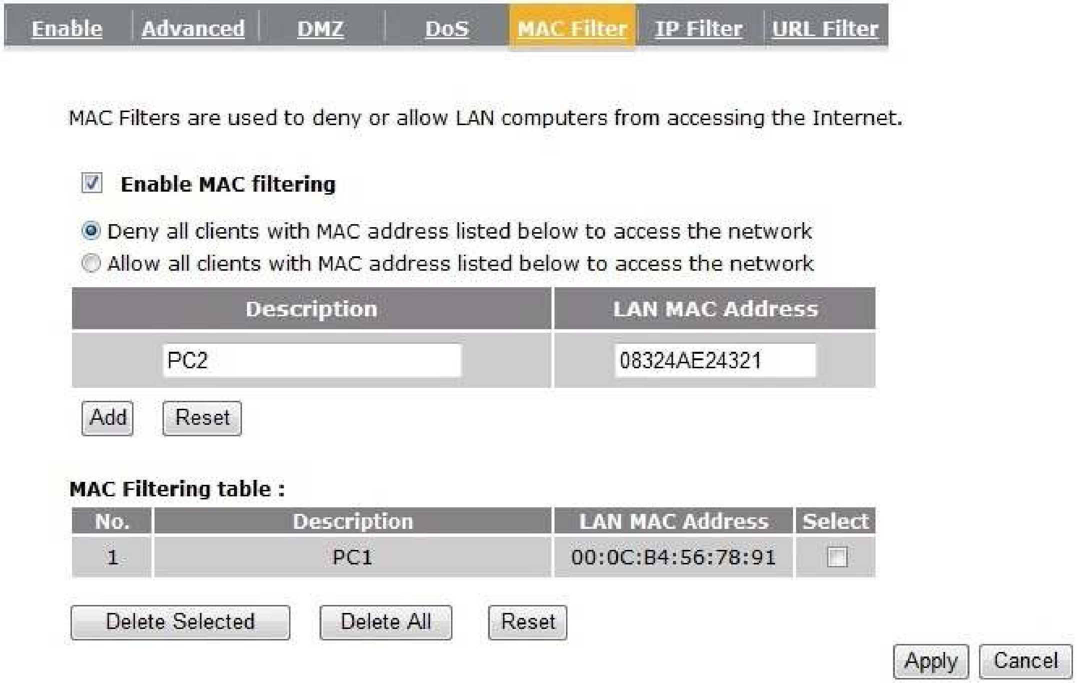


The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resourcess that Internet access becomes unavailable.

Block DoS : ● Enable ○ Disable

9.5. MAC Filter

You can choose whether to Deny or only Allow those computers listed in the MAC Filtering table to access the Internet.



MAC Filters are used to deny or allow LAN computers from accessing the Internet.

☑ Enable MAC filtering

● Deny all clients with MAC address listed below to access the network
○ Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address
PC2	08324AE24321

MAC Filtering table :

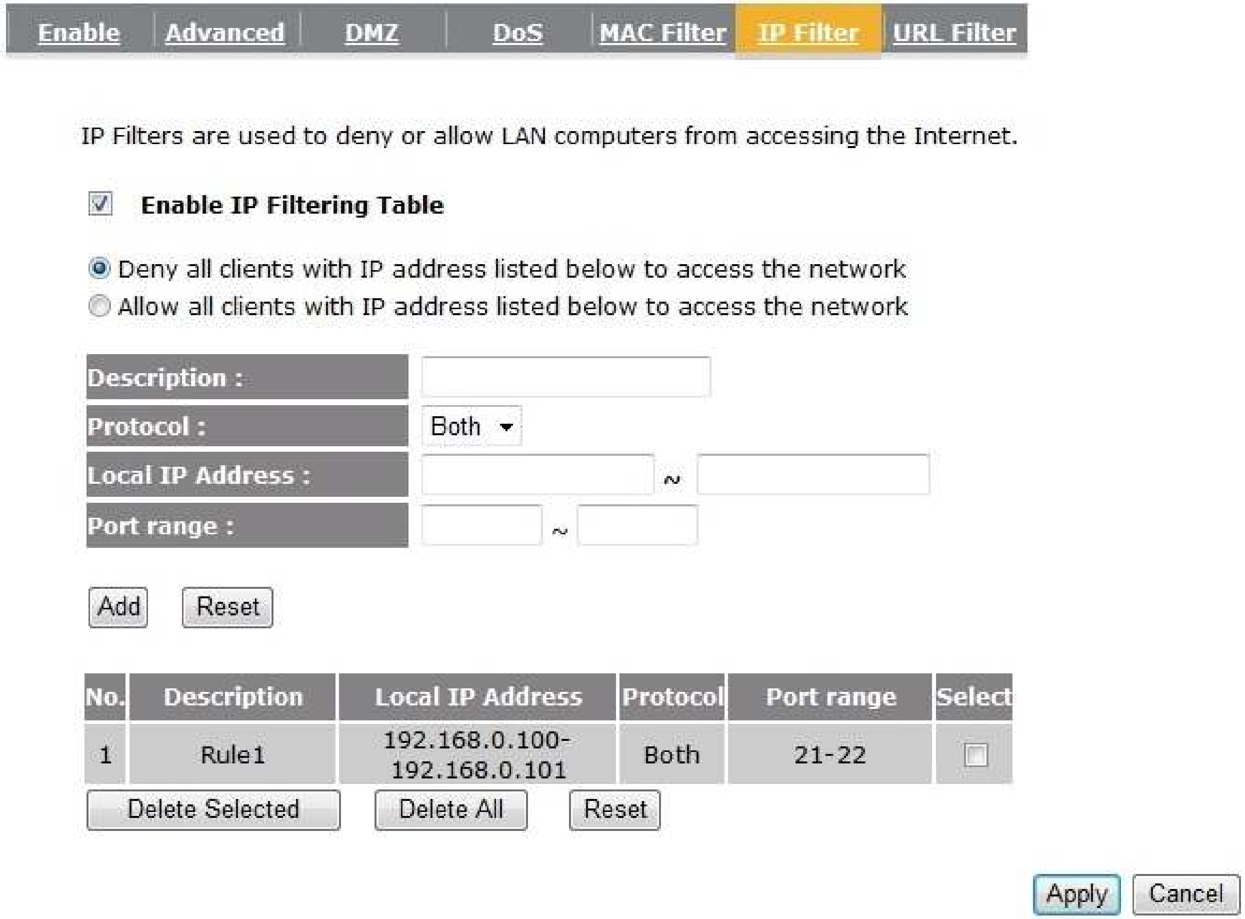
No.	Description	LAN MAC Address	Select
1	PC1	00:0C:B4:56:78:91	□

MAC Filter	
Enable MAC filtering	Tick this box to Enable the MAC filtering feature.
Deny all clients with MAC addresses listed below to access the network	When selected, the computers listed in the MAC Filtering table will be **Denied** access to the Internet.
Allow all clients with MAC addresses listed below to access the network	When selected, only the computers listed in the MAC Filtering table will be **Allowed** access to the Internet.

9.6.IP Filter

You can choose whether to Deny or only Allow, computer with those IP Addresses from accessing certain Ports.

This can be used to control which Internet applications the computers can access.
You may need to have certain knowledge of what Internet ports the applications use.



IP Filters are used to deny or allow LAN computers from accessing the Internet.

☑ **Enable IP Filtering Table**

● Deny all clients with IP address listed below to access the network
○ Allow all clients with IP address listed below to access the network

Description :	
Protocol :	Both
Local IP Address :	~
Port range :	~

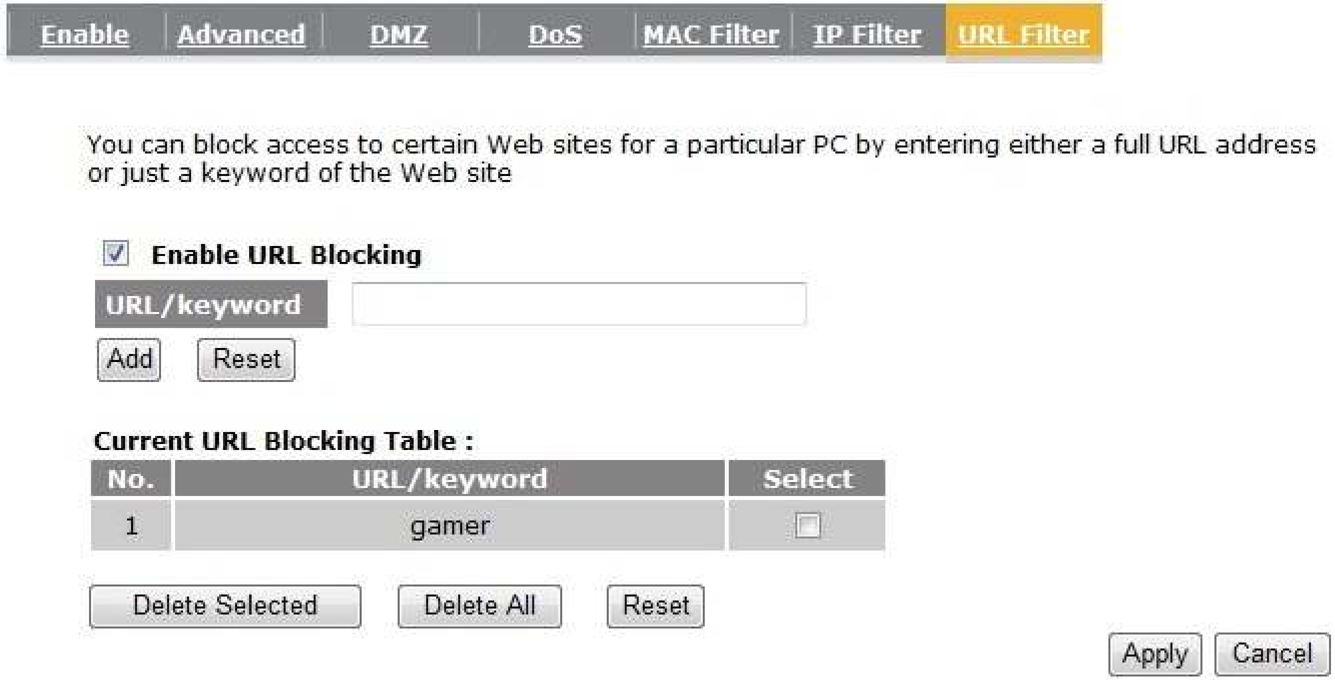
No.	Description	Local IP Address	Protocol	Port range	Select
1	Rule1	192.168.0.100- 192.168.0.101	Both	21-22	□

IP Filter	
Enable IP filtering	Tick this box to Enable the IP filtering feature.
Deny all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified will be **Denied** access to the indicated Internet ports.
Allow all clients with IP addresses listed below to access the network	When selected, the computers with IP addresses specified will be **Allowed** access only to the indicated Internet ports.

9.7.URL Filter

You can deny access to certain websites by blocking keywords in the URL web address.

For example, “gamer” has been added to the URL Blocking Table. Any web address that includes “gamer” will be blocked.



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

☑ Enable URL Blocking

URL/keyword	

Current URL Blocking Table :

No.	URL/keyword	Select
1	gamer	□

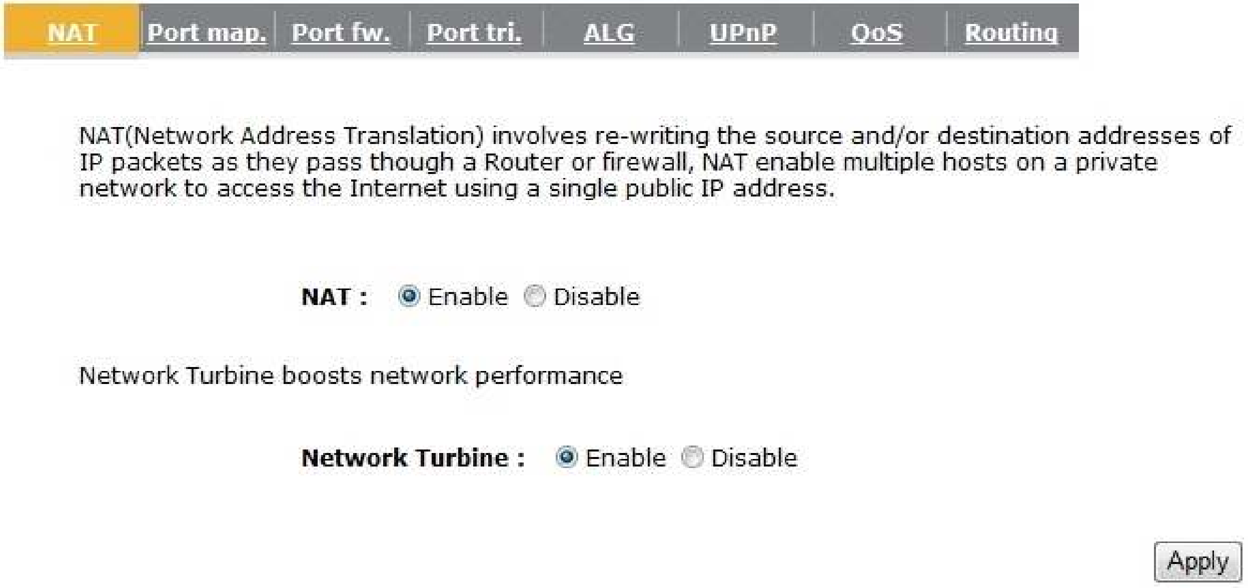
10. Advanced

The Advanced section allows you to configure the **Advanced** settings of the router.

10.1. Network Address Translation (NAT)

This page allows you to Enable / Disable the Network Address Translation (NAT) and Network Turbine features. The NAT is required to share one Internet account with multiple LAN users. Enabling Network Turbine will speed up your NAT throughput.

It also is required for certain Firewall features to work properly.



NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass though a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT : ● Enable ○ Disable

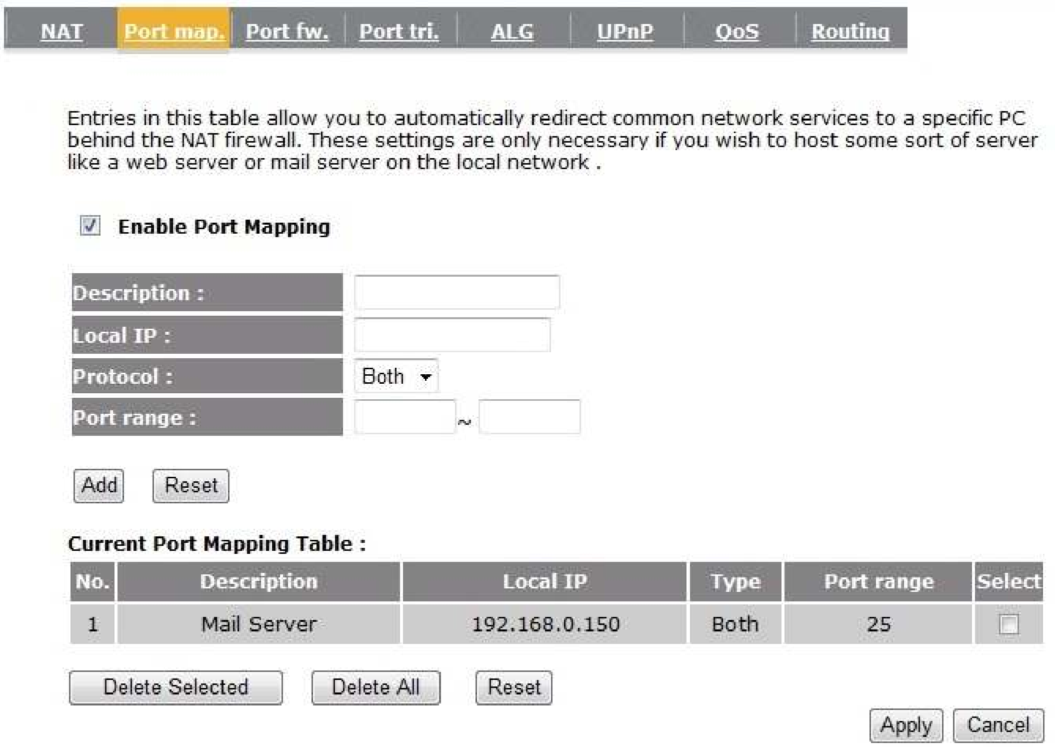
Network Turbine boosts network performance

Network Turbine : ● Enable ○ Disable

10.2. Port Mapping

Port Mapping allows you to redirect a particular range of ports to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a Mail Server that requires ports 25.
When there is a connection from the Internet on those ports, it will be redirected to the Mail Server at IP address 192.168.0.150.



Entries in this table allow you to automatically redirect common network services to a specific PC behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the local network .

☑ Enable Port Mapping

Description :	
Local IP :	
Protocol :	Both
Port range :	~

Current Port Mapping Table :

No.	Description	Local IP	Type	Port range	Select
1	Mail Server	192.168.0.150	Both	25	□

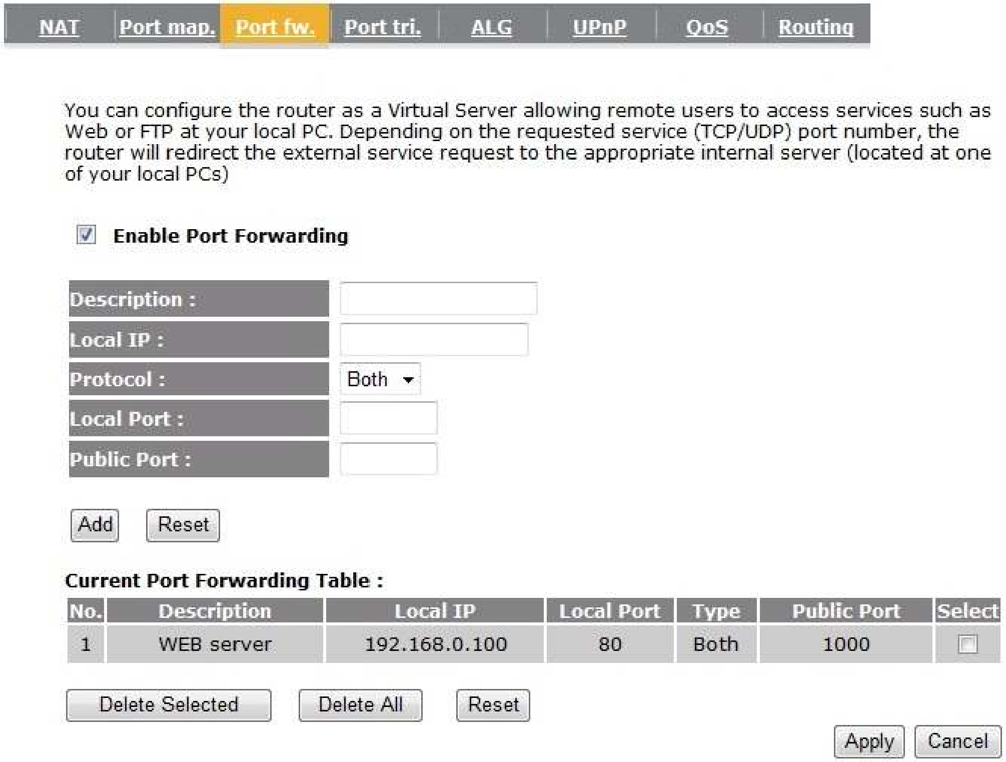
Port Mapping	
Enable Port Mapping	Tick this box to Enable the Port Mapping feature.
Description	Enter a name or description to help you identify this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to either TCP, UDP or Both types of packet transmissions.
Port range	The range of ports that this feature will be applied to.

10.3. Port Forwarding

Port Forwarding allows you to redirect a particular public port to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a WEB Server running on port 80 on the LAN. For security reasons, the Administrator would like to provide this server to Internet connection on port 1000.

Therefore then there is a connection from the Internet on port 1000, it will be forwarded to the computer with the IP address 192.168.0.100 and changed to port 80.



You can configure the router as a Virtual Server allowing remote users to access services such as Web or FTP at your local PC. Depending on the requested service (TCP/UDP) port number, the router will redirect the external service request to the appropriate internal server (located at one of your local PCs)

☑ Enable Port Forwarding

Description :	
Local IP :	
Protocol :	Both
Local Port :	
Public Port :	

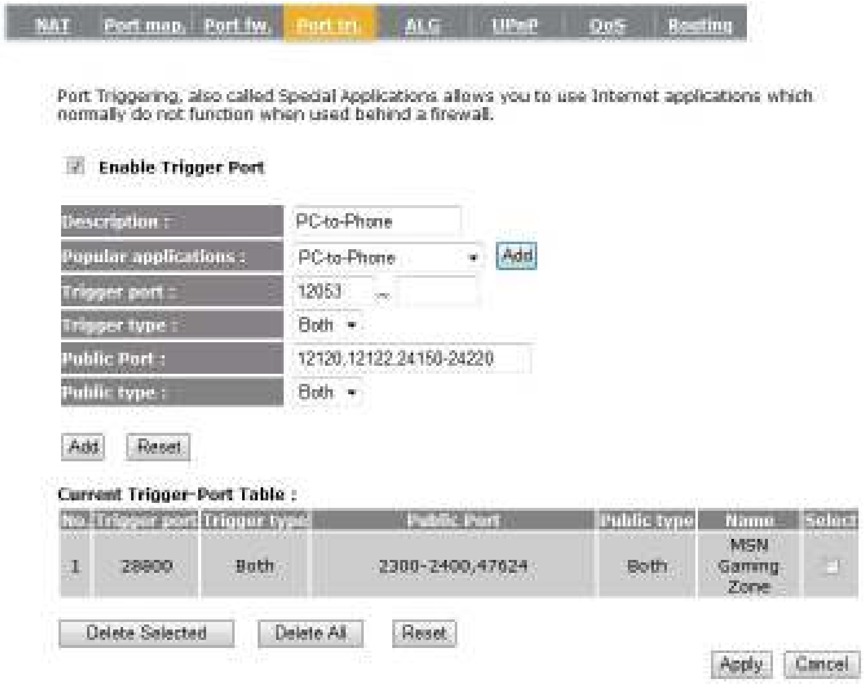
Current Port Forwarding Table :

No.	Description	Local IP	Local Port	Type	Public Port	Select
1	WEB server	192.168.0.100	80	Both	1000	□

Port Forwarding	
Enable Port Forwarding	Tick this box to Enable the Port Forwarding feature.
Description	Enter a name or description to help you identify this entry.
Local IP	The local IP address of the computer the server is hosted on.
Protocol	Select to apply the feature to either TCP, UDP or Both types of packet transmissions.
Local Port	The port that the server is running on the local computer.
Public Port	When a connection from the Internet is on this port, then it will be forwarded to the indicated local IP address.

10.4. Port Trigger

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Trigger will be required for these applications to work.



Port Triggering, also called Special Applications allows you to use Internet applications which normally do not function when used behind a firewall.

☑ Enable Trigger Port

Description :	PC-to-Phone
Popular applications :	PC-to-Phone [Add]
Trigger port :	12053 ~
Trigger type :	Both
Public Port :	12120,12122,24150-24220
Public type :	Both

[Add] [Reset]

Current Trigger-Port Table :

No.	Trigger port	Trigger type	Public Port	Public type	Name	Select
1	28800	Both	2300-2400,47624	Both	MSN Gaming Zone	□

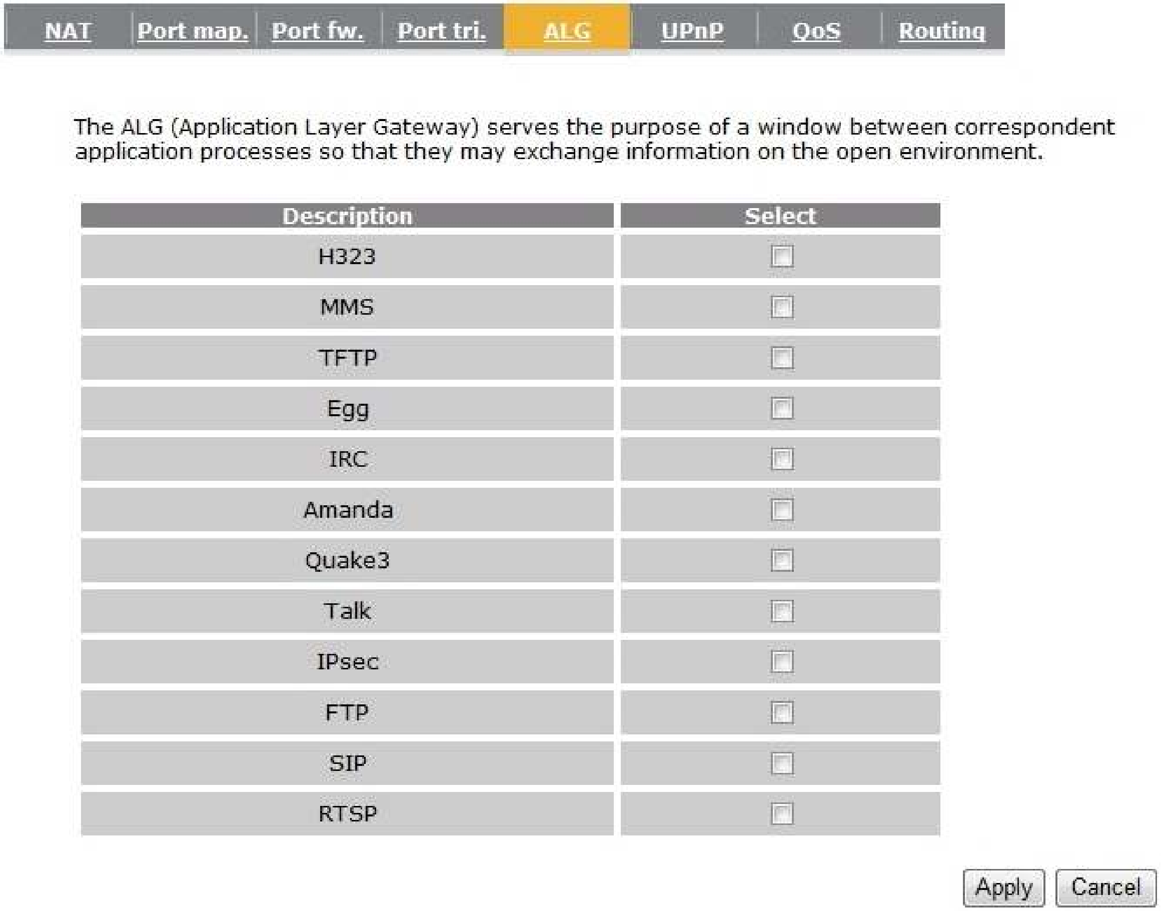
[Delete Selected] [Delete All] [Reset]

[Apply] [Cancel]

Port Trigger	
Enable Port Forwarding	Tick this box to Enable the Port Trigger feature.
Popular applications	This is a list of some common applications with preset settings. Select the application and click **Add** to automatically enter the settings.
Trigger port	This is the outgoing (outbound) port numbers for this application.
Trigger type	Select whether the application uses TCP, UDP or Both types of protocols for outbound transmissions.
Public Port	These are the inbound (incoming) ports for this application.
Public type	Select whether the application uses TCP, UDP or Both types of protocols for inbound transmissions.

10.5. Application Layer Gateway (ALG)

Certain applications may require the use of ALG feature to function correctly. If you use any of the applications listed, please tick and select it to enable this feature.

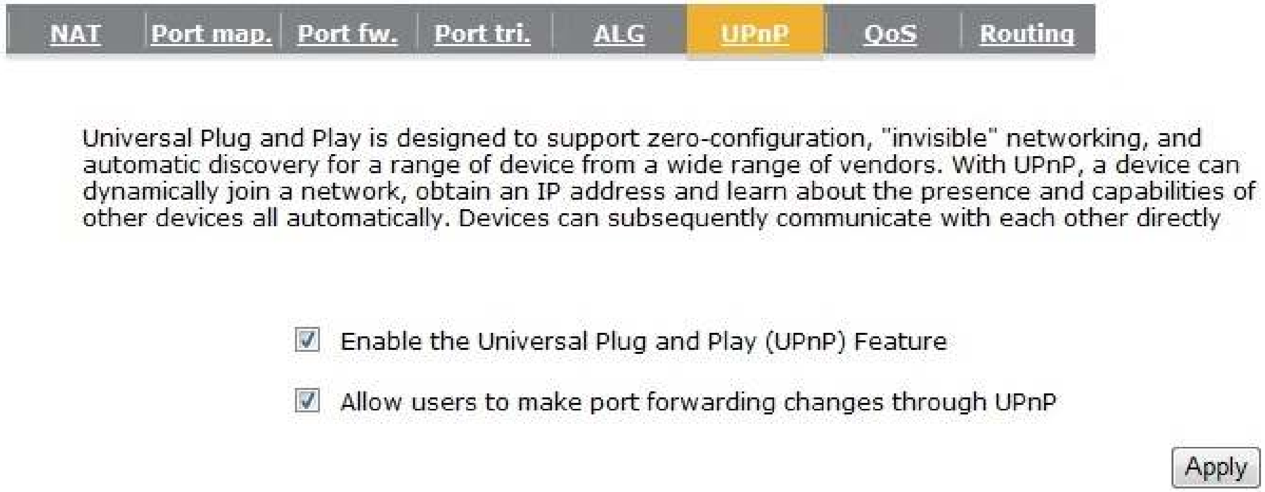


The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

Description	Select
H323	☐
MMS	☐
TFTP	☐
Egg	☐
IRC	☐
Amanda	☐
Quake3	☐
Talk	☐
IPsec	☐
FTP	☐
SIP	☐
RTSP	☐

10.6. Universal Plug and Play (UPnP)

The UPnP function allows automatic discovery and configuration of UPnP enabled devices on your network. It also provides automatic port forwarding for supported applications to seamlessly bypass the Firewall.



Universal Plug and Play is designed to support zero-configuration, "invisible" networking, and automatic discovery for a range of device from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address and learn about the presence and capabilities of other devices all automatically. Devices can subsequently communicate with each other directly

☑ Enable the Universal Plug and Play (UPnP) Feature

☑ Allow users to make port forwarding changes through UPnP

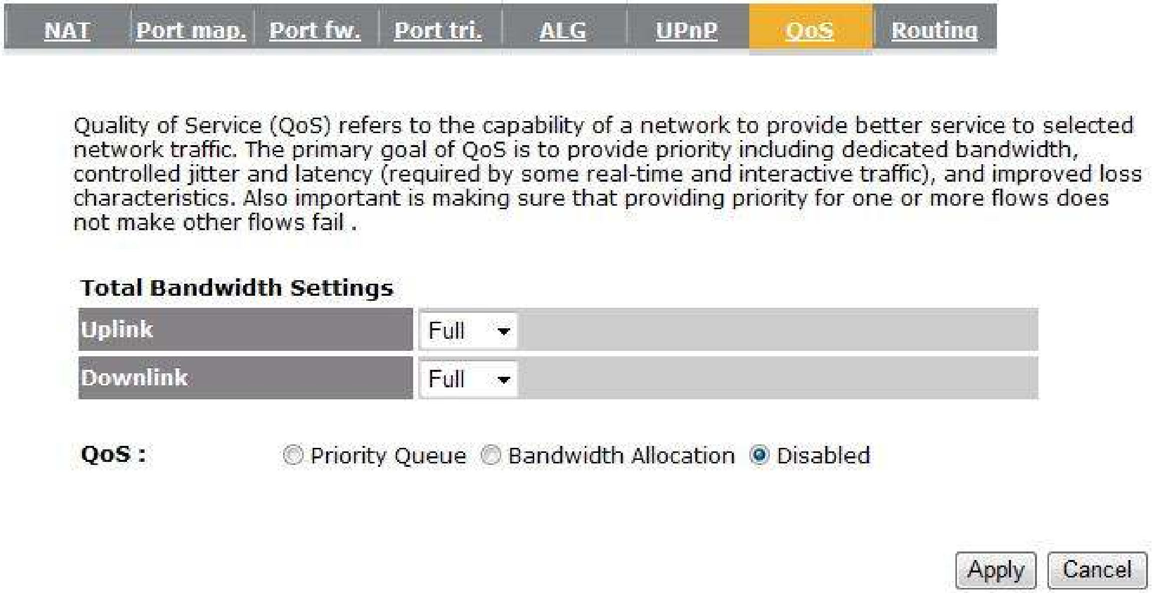
Universal Plug and Play (UPnP)	
Enable the UPnP Feature	Tick this box to Enable the UPnP feature to allow supported devices to be visible on the network.
Allow users to make port forwarding changes through UPnP	Tick this box to allow applications to automatically set their port forwarding rules to bypass the firewall without any user set up.

10.7. Quality of Service (QoS)

QoS allows you to control the priority that the data is transmitted over the Internet, or to reserve a specific amount of Internet bandwidth. This is to ensure that applications get enough Internet bandwidth for a pleasant user experience.

If not, then the performance and user experience of time sensitive transmissions such as voice and video could be very poor.

In order for this feature to function properly, the user should first set the Uplink and Downlink bandwidth provided by your Internet Service Provider.



Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail .

Total Bandwidth Settings

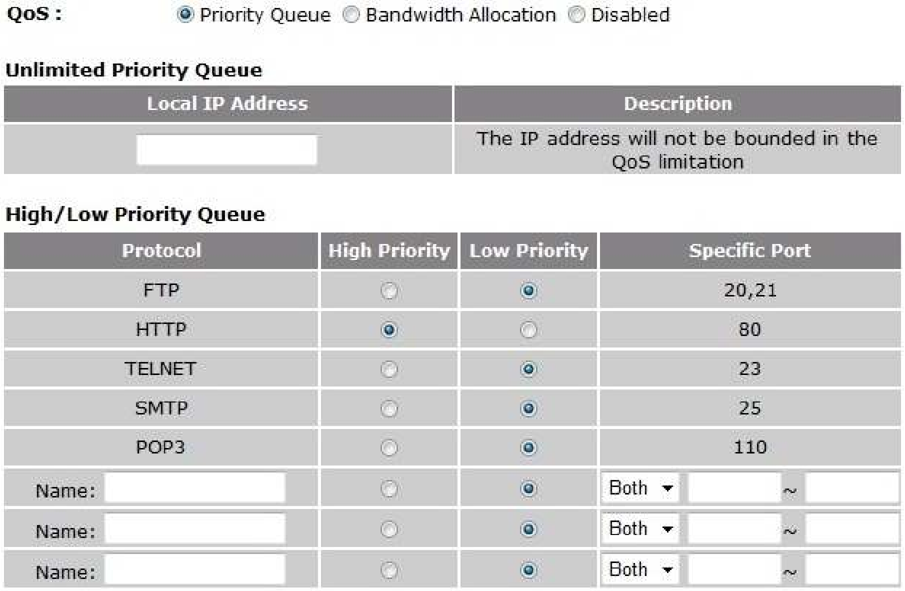
Uplink	Full
Downlink	Full

QoS : ○ Priority Queue ○ Bandwidth Allocation ● Disabled

Total Bandwidth Settings	
Uplink	Set the Uplink bandwidth provided by your Internet Service Provider.
Downlink	Set the Downlink bandwidth provided by your Internet Service Provider.
Priority Queue	Sets the QoS method to Priority Queue.
Bandwidth Allocation	Sets the QoS method to Bandwidth Allocation.
Disabled	Disables the QoS feature.

Priority Queue Method

Bandwidth priority is set to either High or Low. The transmissions in the High queue will be processed first.



QoS : ● Priority Queue ○ Bandwidth Allocation ○ Disabled

Unlimited Priority Queue

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

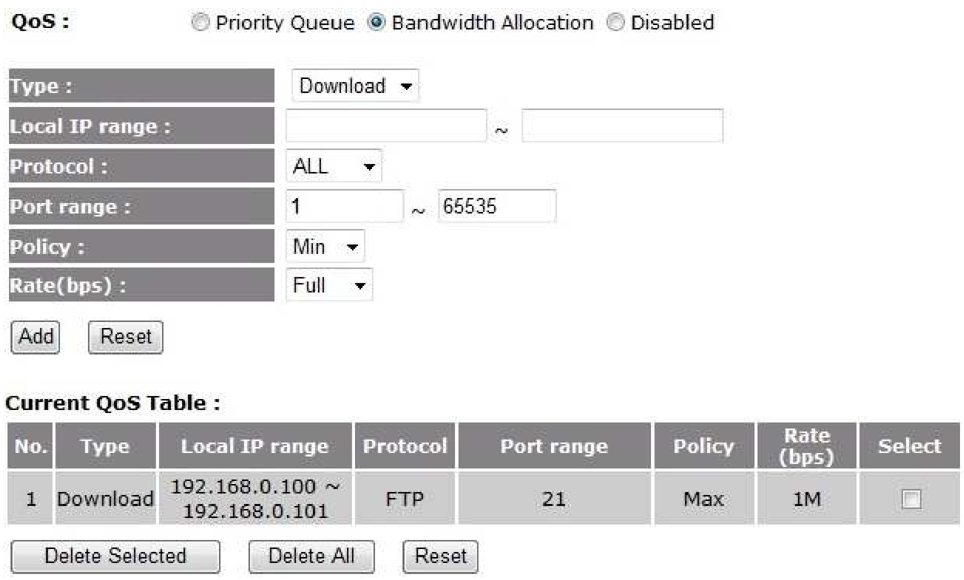
High/Low Priority Queue

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

Unlimited Priority Queue	
Local IP Address	The computer with this IP Address will not be bound by the QoS rules.
High / Low Priority Queue	
Protocol	The type of network protocol.
High / Low Priority	Sets the protocol to High or Low priority.
Specific Port	Each protocol uses a specific port range. Please specify the ports used by this protocol.

Bandwidth Allocation Method

You can set the **maximum** amount of bandwidth a certain protocol will use at one time. Or you can set a **minimum** amount of bandwidth that will be guaranteed to a certain protocol.



QoS : ○ Priority Queue ● Bandwidth Allocation ○ Disabled

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

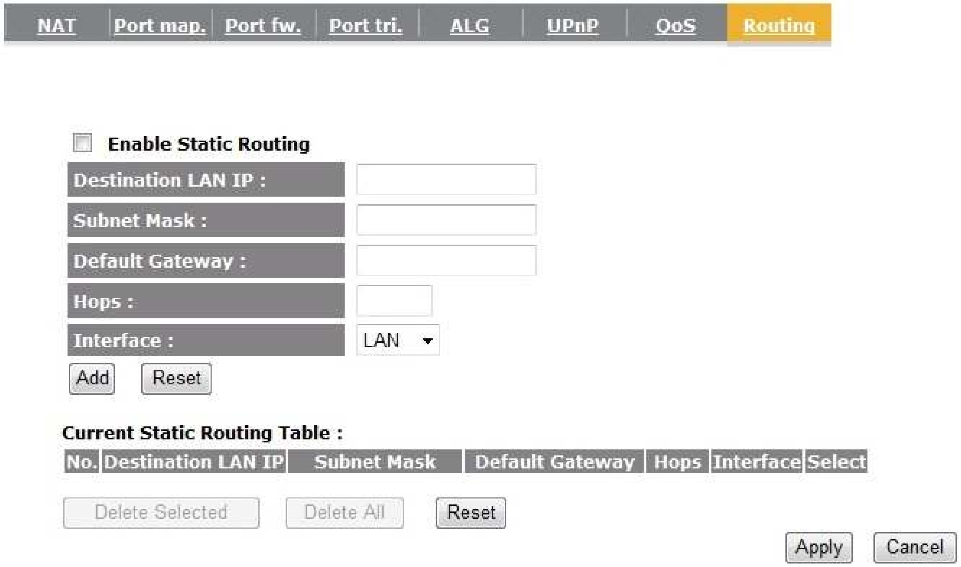
Current QoS Table :

No.	Type	Local IP range	Protocol	Port range	Policy	Rate (bps)	Select
1	Download	192.168.0.100 ~ 192.168.0.101	FTP	21	Max	1M	□

Bandwidth Allocation	
Type	Set whether the QoS rules apply to transmission that are Download, Upload or Both directions.
Local IP range	Enter the IP address range of the computers that you would like the QoS rules to apply to.
Protocol	Select from this list of protocols to automatic set the related port numbers.
Port range	Each protocol uses a specific port range. Please specify the ports used by this protocol..
Policy	Choose whether this rule is to set a limit on the **Maximum** amount of bandwidth allocated to this protocol, or to set the guaranteed M**inimum** amount of bandwidth for this protocol.

10.8. Routing

If your WIRELESS ROUTER device is connected a network with different subnets, then this feature will allow the different subnets to communicate with each other.



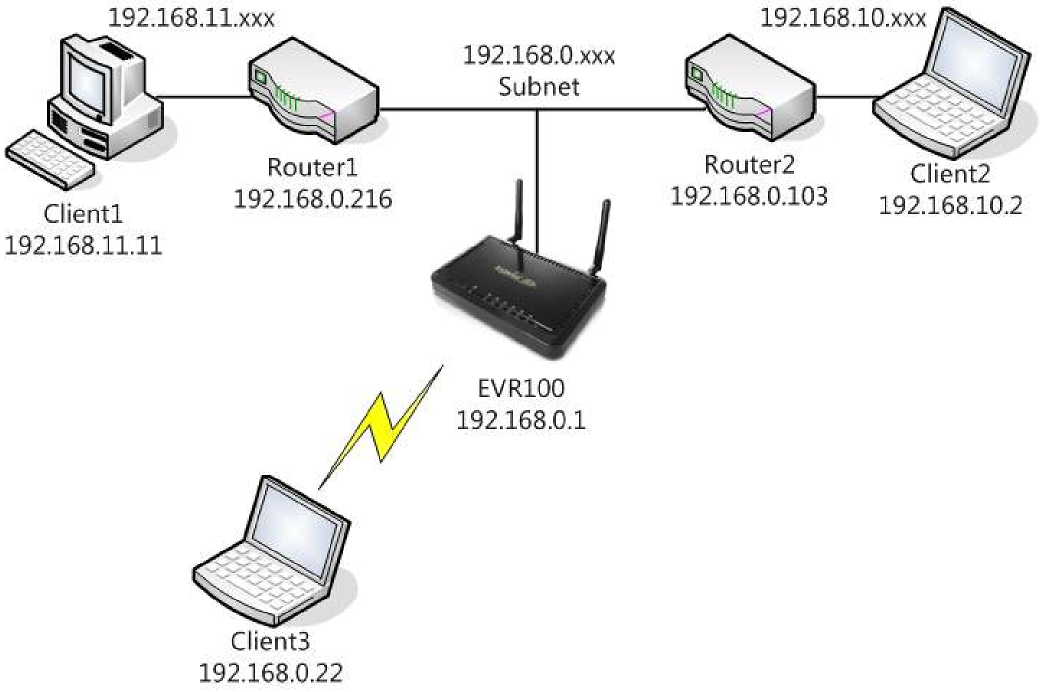
□ Enable Static Routing

Destination LAN IP :	
Subnet Mask :	
Default Gateway :	
Hops :	
Interface :	LAN

Current Static Routing Table :

No.	Destination LAN IP	Subnet Mask	Default Gateway	Hops	Interface	Select

Static Routing	
Enable Static Routing	Tick this box to Enable the Static Router feature.
Destination LAN IP	Enter the IP address of the destination LAN.
Subnet Mask	Enter the Subnet Mask of the destination LAN IP address
Default Gateway	Enter the IP address of the Default Gateway for this destination IP and Subnet.
Hops	Specify the maximum number of Hops in the static routing rule.
Interface	Select whether the routing applies to LAN or WAN interfaces.



Destination	Subnet Mask	Gateway	Hop	Interface
192.168.11.0	255.255.255.0	192.168.0.216	1	LAN
192.168.10.0	255.255.255.0	192.168.0.103	1	LAN

So if, for example, Client3 wants to send an IP data packet to 192.168.10.2 (Client 2), it would use the above table to determine that it had to go via 192.168.0.103 (Router 2)

And if it sends Packets to 192.168.11.11 (Client 1) will go via 192.168.0.216 (Router 1).

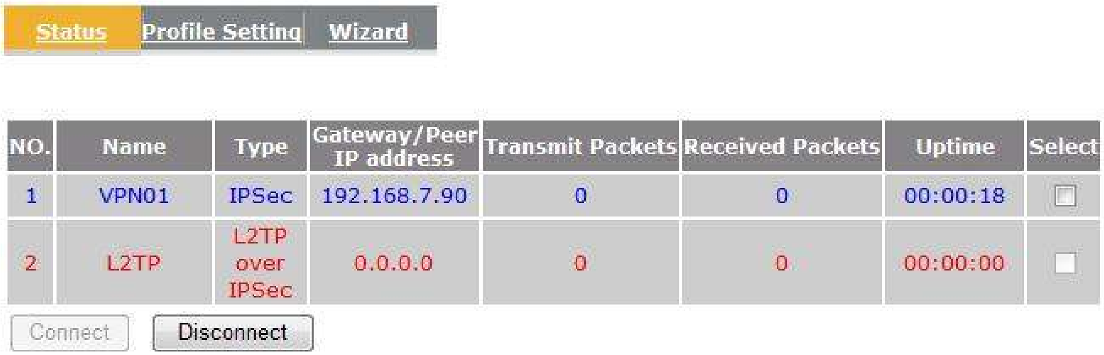
11. VPN

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

EVR100 supports IPSec (Site to Site, Remote to Site) and L2TP over IPSec methods to establish VPN connections and the maximum VPN session number is up to 5.

11.1. Status

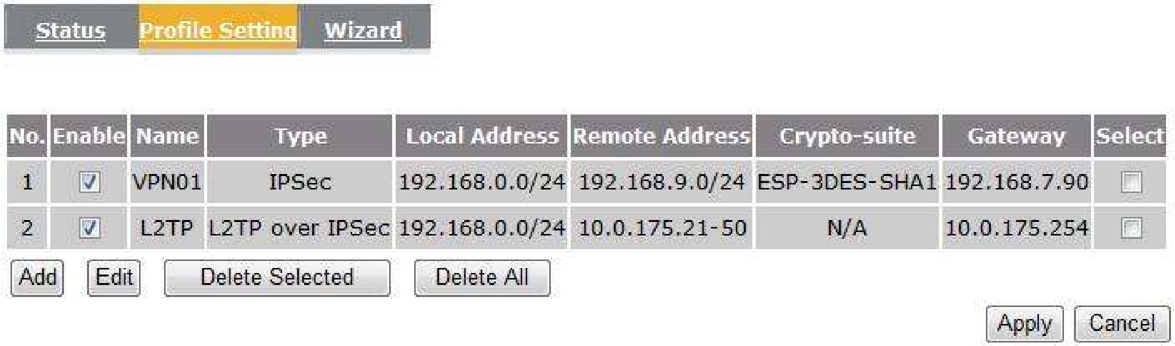
This page displays the connect status of VPN connection. You can select one of them to connect or disconnect the VPN connection. Note. If connection type is remote dial-in (Client to Site or L2TP over IPSec), you can’t disconnect this session manually.



NO.	Name	Type	Gateway/Peer IP address	Transmit Packets	Received Packets	Uptime	Select
1	VPN01	IPSec	192.168.7.90	0	0	00:00:18	☐
2	L2TP	L2TP over IPSec	0.0.0.0	0	0	00:00:00	☐

11.2. Profile Setting

This page allows you to **Enable**, **Add**, **Edit** and **Delete** VPN profiles.



No.	Enable	Name	Type	Local Address	Remote Address	Crypto-suite	Gateway	Select
1	☑	VPN01	IPSec	192.168.0.0/24	192.168.9.0/24	ESP-3DES-SHA1	192.168.7.90	□
2	☑	L2TP	L2TP over IPSec	192.168.0.0/24	10.0.175.21-50	N/A	10.0.175.254	□

Profile Setting	
Enable	Tick the box to Enable the VPN profile.
Add	Click this button to add the entry.
Edit	Select one profile and click this button to edit the entry.
Delete Selected	Delete the selected entries.
Delete All	Delete all entries

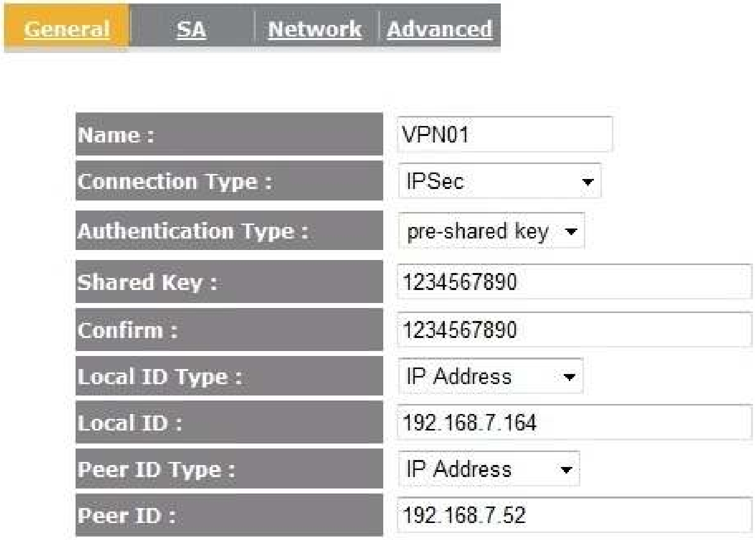
10.1.1. IPSec

IPSec (Internet Protocol Security) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

General

The page allows you to configure the general VPN settings.



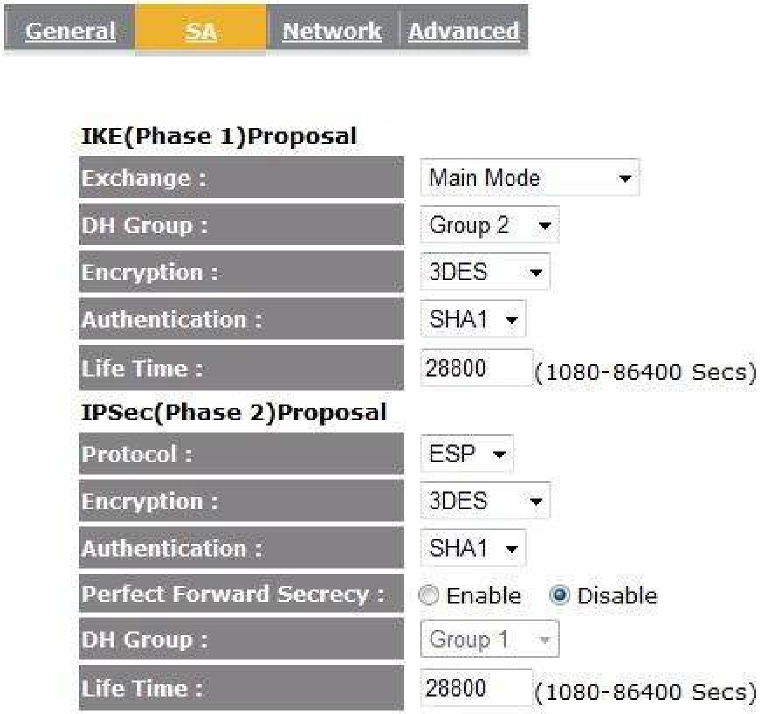
Name :	VPN01
Connection Type :	IPSec
Authentication Type :	pre-shared key
Shared Key :	1234567890
Confirm :	1234567890
Local ID Type :	IP Address
Local ID :	192.168.7.164
Peer ID Type :	IP Address
Peer ID :	192.168.7.52

General	
Name	Enter a name for your VPN policy.
Connection Type	Supports **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.

SA (Security Association)

A Security Association (SA) is the establishment of shared security attributes between two network entities to support secure communication. An SA may include attributes such as: cryptographic algorithm and mode; traffic encryption key; and parameters for the network data to be passed over the connection. Establishment of an SA is described in RFC 2408, the Internet Security Association and Key Management Protocol.

This page allows you to configure SA.



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

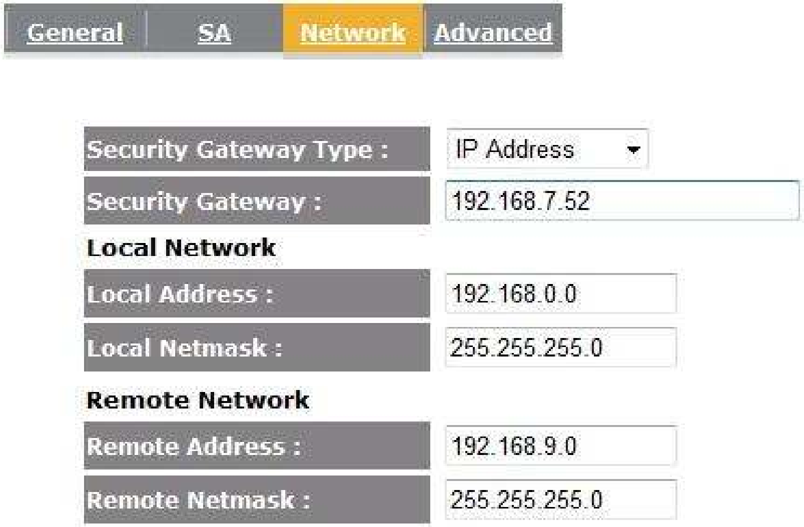
Protocol :	ESP
Encryption :	3DES
Authentication :	SHA1
Perfect Forward Secrecy :	○ Enable ● Disable
DH Group :	Group 1
Life Time :	28800 (1080-86400 Secs)

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**, **Group2**, **Group5** and **Group14**). As the DH Group number increases, the higher the level of encryption implemented for IKE Phase 1.

Encryption	EVR100 supports **DES**, **3DES**, **AES128**, **AES192**, **AES256** encryption methods for traffic through the VPN.
Authentication	EVR100 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.
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	EVR100 supports **DES**, **3DES**, **AES128**, **AES192**, **AES256** encryption methods for traffic through the VPN.
Authentication	EVR100 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**, **Group2**, **Group5**, **Group14**). 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

This page allows you to configure the VPN server and local/remote subnet.



Security Gateway Type : IP Address

Security Gateway : 192.168.7.52

Local Network

Local Address : 192.168.0.0

Local Netmask : 255.255.255.0

Remote Network

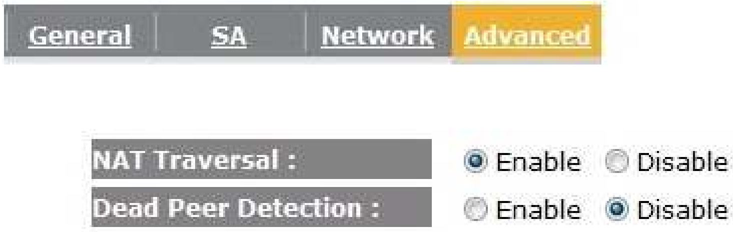
Remote Address : 192.168.9.0

Remote Netmask : 255.255.255.0

Network	
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

This page allows you to configure advanced VPN settings.



NAT Traversal : ● Enable ○ Disable

Dead Peer Detection : ○ Enable ● Disable

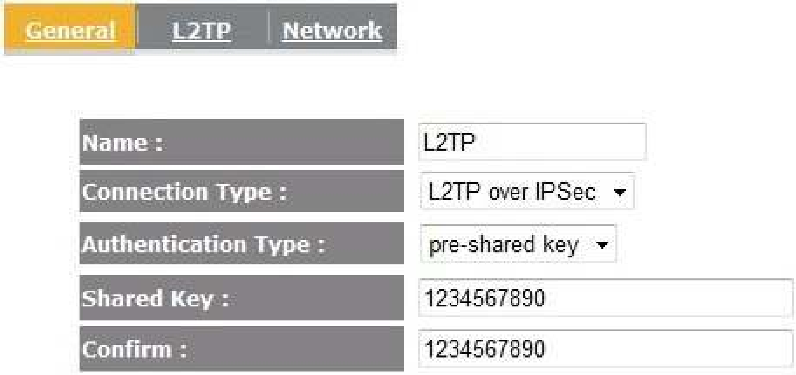
Advanced	
NAT Traversal	Enabling **NAT Traversal** allow IPSec traffic from this endpoint to traverse through the translation process during NAT. The remote VPN endpoint must also support this feature and it must be enabled to function properly over the VPN.
Dead Peer Detection	Enable **DPD (Dead Peer 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.

10.1.2. L2TP over IPSec

L2TP over IPSec VPNs enable a business to transport data over the Internet, while still maintaining a high level of security to protect data. You can use this type of secure connection for small or remote office clients that need access to the corporate network. You can also use L2TP over IPSec VPNs for routers at remote sites by using the local ISP and creating a demand-dial connection into corporate headquarters.

General

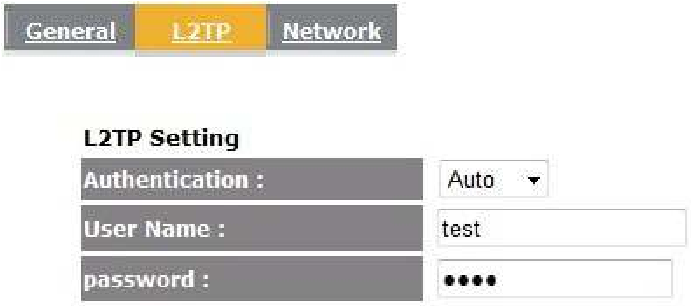
The page allows you to configure the general VPN settings.



Name :	L2TP
Connection Type :	L2TP over IPSec
Authentication Type :	pre-shared key
Shared Key :	1234567890
Confirm :	1234567890

General	
Name	Enter a name for your VPN policy.
Connection Type	EVR100 supports **IPSec** and **L2TP over IPSec** methods to establish VPN connection.
Authentication Type	EVR100 supports **pre-shared key** method for authentication.
Shared Key	Enter the Shared Key in box.
Confirm	Enter your Shared Key again for verification.

L2TP

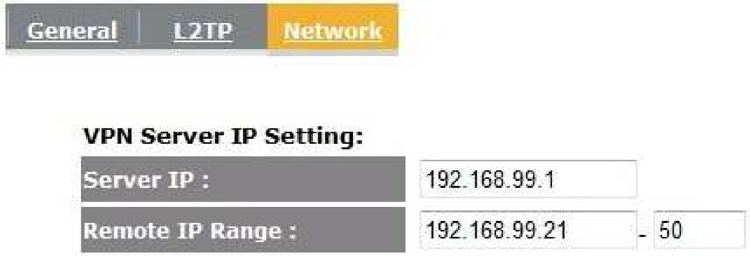


L2TP Setting

Authentication :	Auto
User Name :	test
password :	••••

L2TP Setting	
Authentication	Select the desired authentication protocol (PAP, CHAP, Auto). Select **Auto** by default.
User Name	Enter the username for authentication.
Password	Enter the password for authentication.

Network



VPN Server IP Setting:

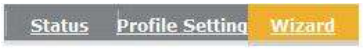
Server IP : 192.168.99.1

Remote IP Range : 192.168.99.21 - 50

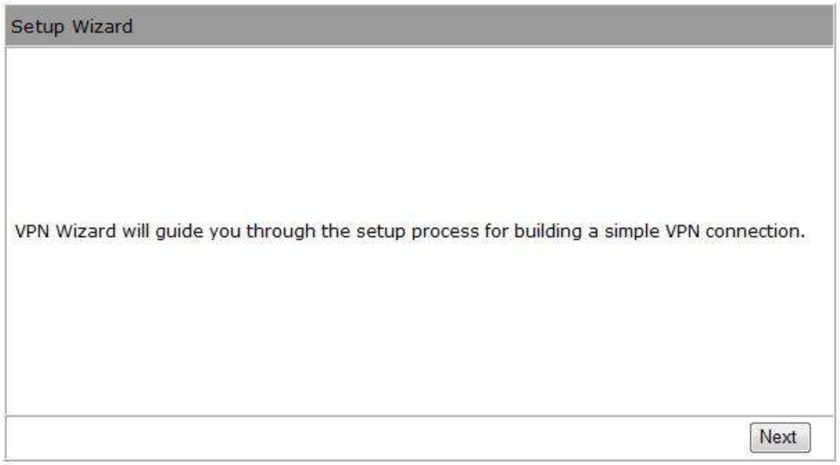
Network	
Server IP	Enter the VPN Server IP address.
Remote IP Range	Assign a range of IP addresses. The assigned IP range should be on the same IP network but not the in the same range as your DHCP IP range.

11.3. Wizard

You can use Wizard to create a VPN profile easily.

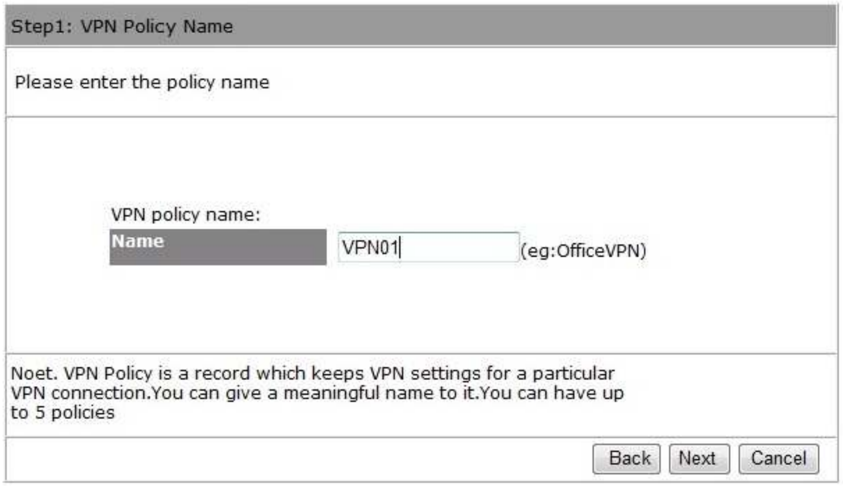


1. Click **Next** button to begin the wizard.


Setup Wizard

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

2. Enter the VPN policy name then click **Next** button to next page.


Step1: VPN Policy Name

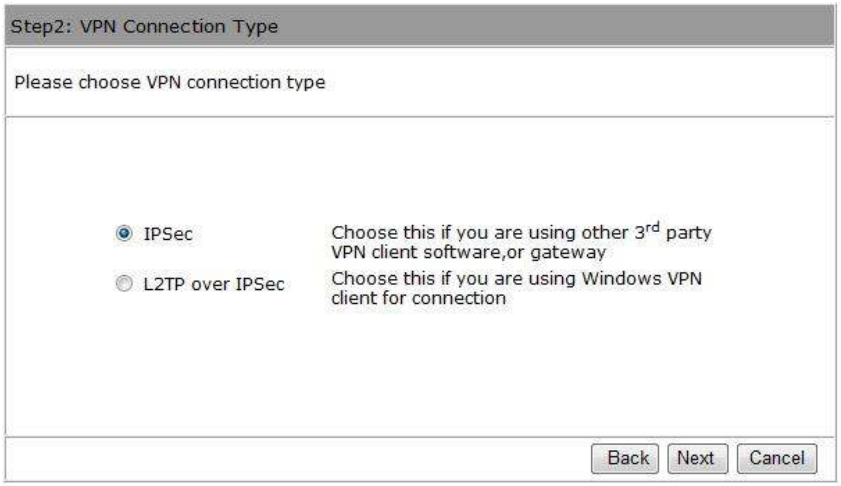
Please enter the policy name

VPN policy name:

Name: VPN01 (eg:OfficeVPN)

Noet. VPN Policy is a record which keeps VPN settings for a particular VPN connection.You can give a meaningful name to it.You can have up to 5 policies

3. You can select [IPSec] or [L2TP over IPSec] in this page then click **Next** button to next page. If you select [IPSec] then go to step 3.1. If you select [L2TP over IPSec] then go to step 3.2.



Step2: VPN Connection Type

Please choose VPN connection type

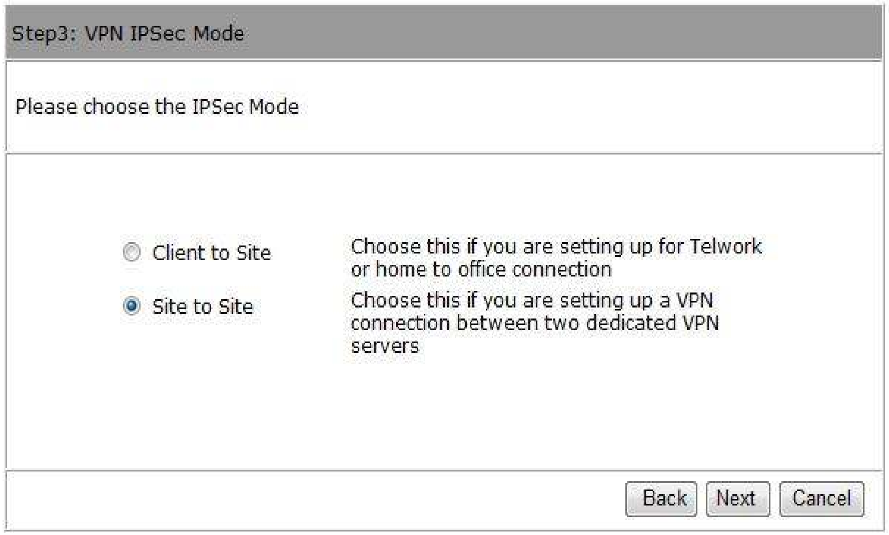
● IPSec — Choose this if you are using other 3rd party VPN client software,or gateway

○ L2TP over IPSec — Choose this if you are using Windows VPN client for connection

3.1 IPSec

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

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



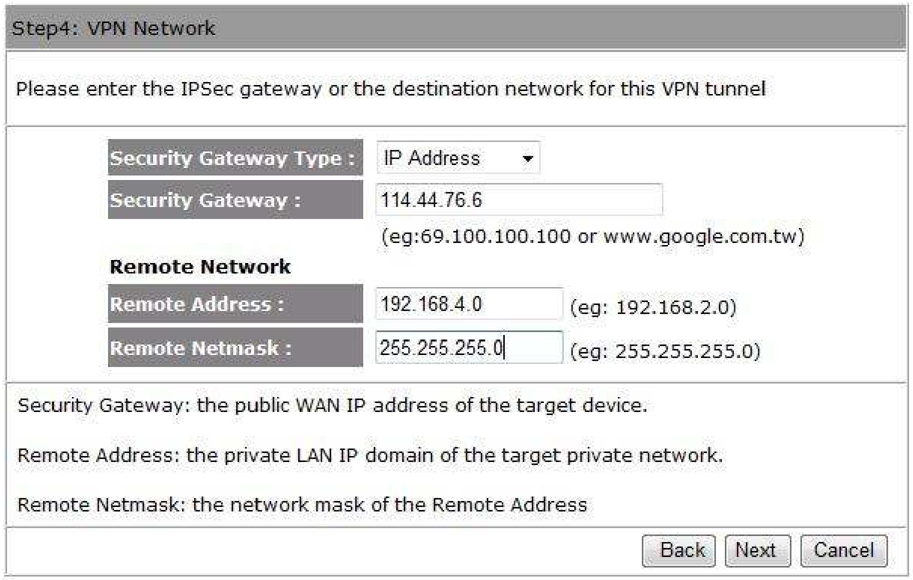
Step3: VPN IPSec Mode

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** button 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)

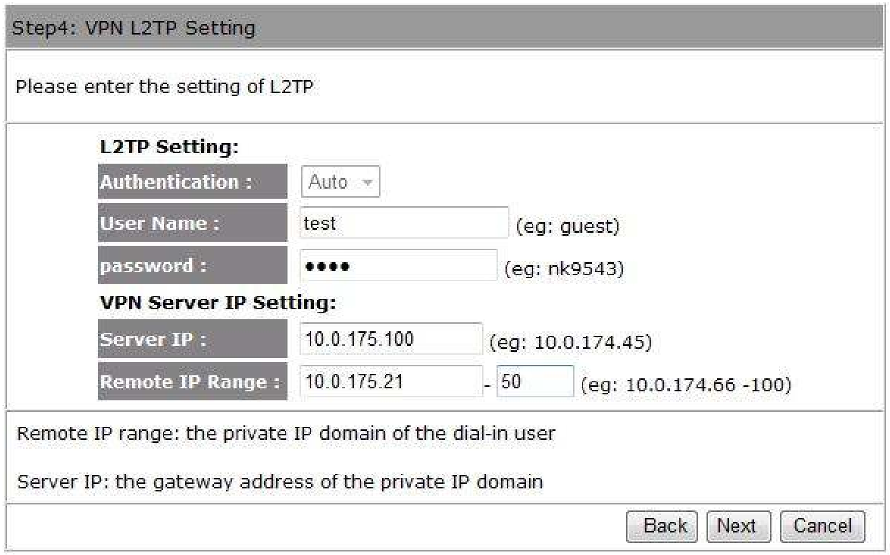
Security Gateway: the public WAN IP address of the target device.

Remote Address: the private LAN IP domain of the target private network.

Remote Netmask: the network mask of the Remote Address

3.2 L2TP over IPSec

Enter the username, password and VPN server IP setting. Then click **Next** button to next page.



Step4: VPN L2TP Setting

Please enter the setting of L2TP

L2TP Setting:

Authentication : Auto

User Name : test (eg: guest)

password : •••• (eg: nk9543)

VPN Server IP Setting:

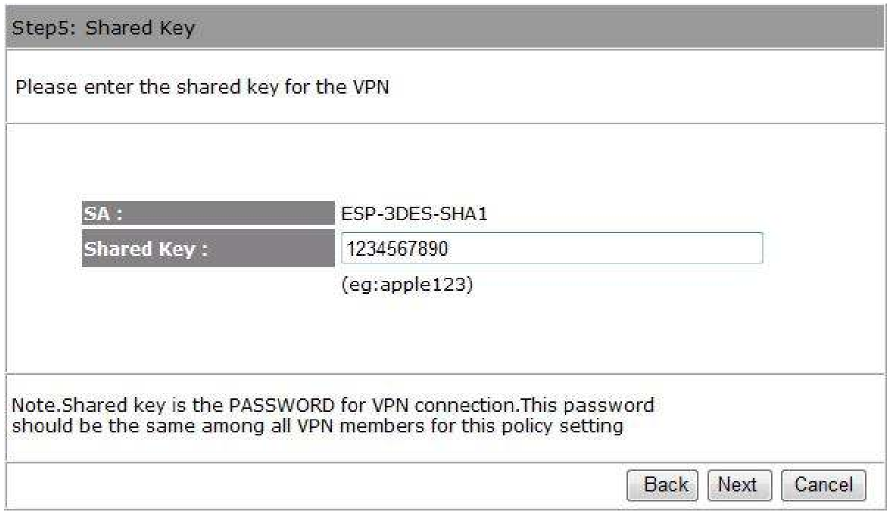
Server IP : 10.0.175.100 (eg: 10.0.174.45)

Remote IP Range : 10.0.175.21 - 50 (eg: 10.0.174.66 -100)

Remote IP range: the private IP domain of the dial-in user

Server IP: the gateway address of the private IP domain

4. Enter the shared key for the VPN connection.



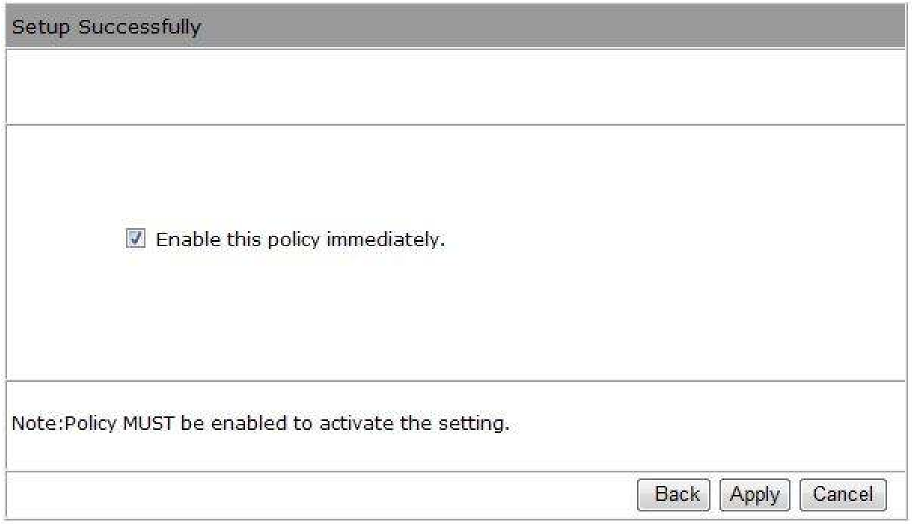
Step5: Shared Key

Please enter the shared key for the VPN

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

Note.Shared key is the PASSWORD for VPN connection.This password should be the same among all VPN members for this policy setting

5. 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.



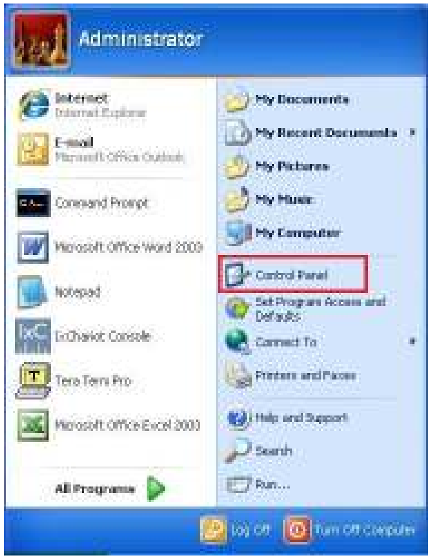
Setup Successfully

☑ Enable this policy immediately.

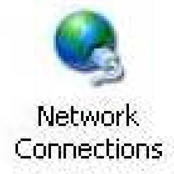
Note:Policy MUST be enabled to activate the setting.

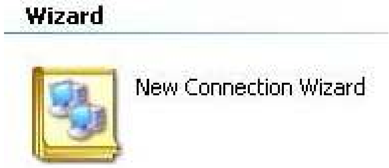
How to establish a L2TP over IPSec VPN connection on Windows XP

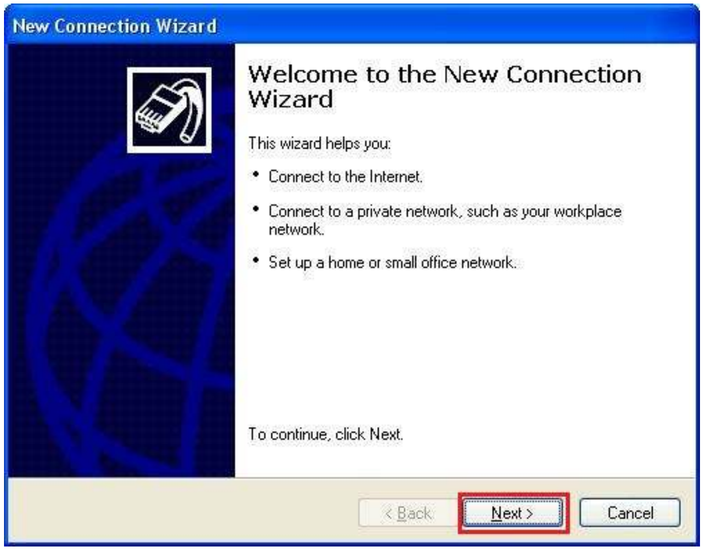
1. Click Start button and open Control Panel.



2. Click [Network Connections], double click [New Connection Wizard] then click **Next** button.







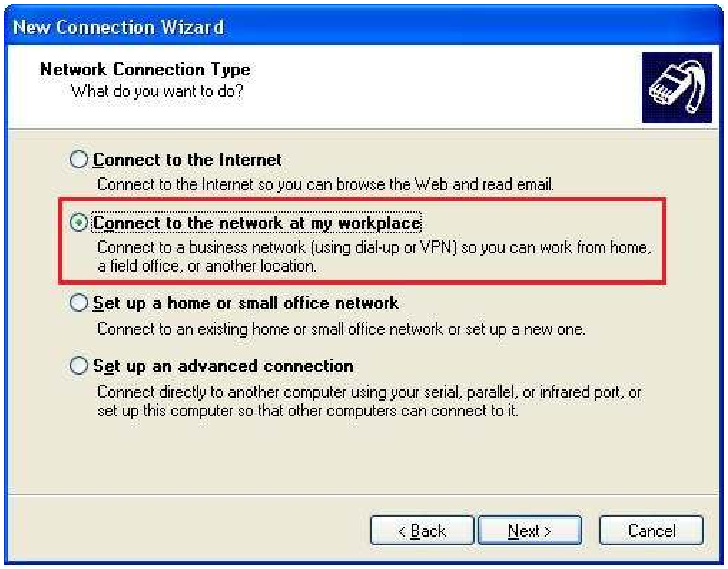
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

3. Select [Connect to the network at my workplace] then click **Next** button.



New Connection Wizard

Network Connection Type
What do you want to do?

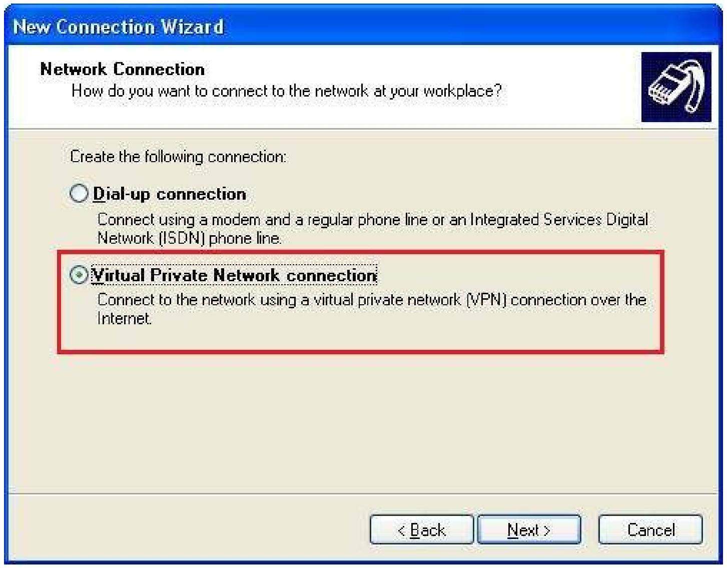
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

4. Select [Virtual Private Network connection] then click **Next** button.



New Connection Wizard

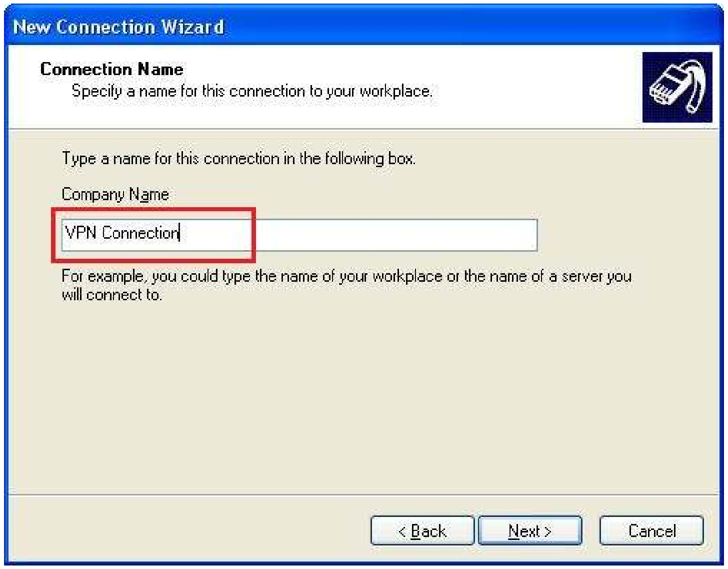
Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

5. Enter the [Company Name] then click Next button.



Connection Name

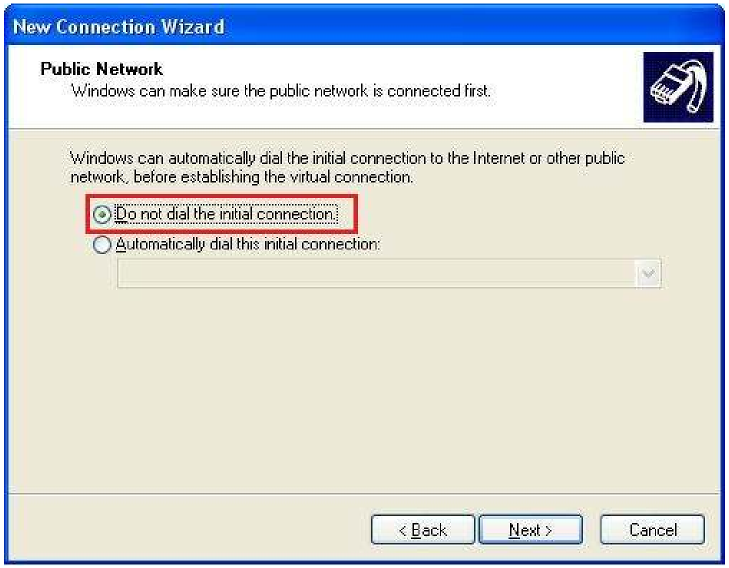
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name: VPN Connection

For example, you could type the name of your workplace or the name of a server you will connect to.

6. Select [Do not dial the initial connection] then click **Next** button.



Public Network

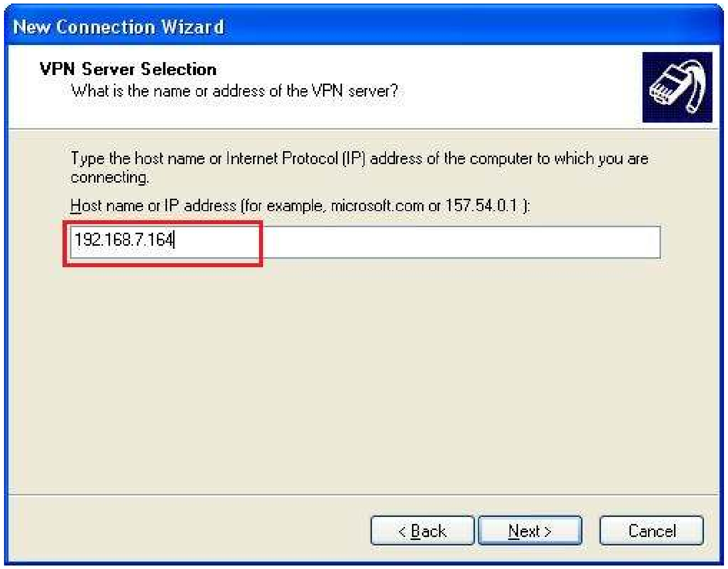
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

● Do not dial the initial connection.

○ Automatically dial this initial connection:

7. Enter the VPN server IP address then click **Next** button.



New Connection Wizard

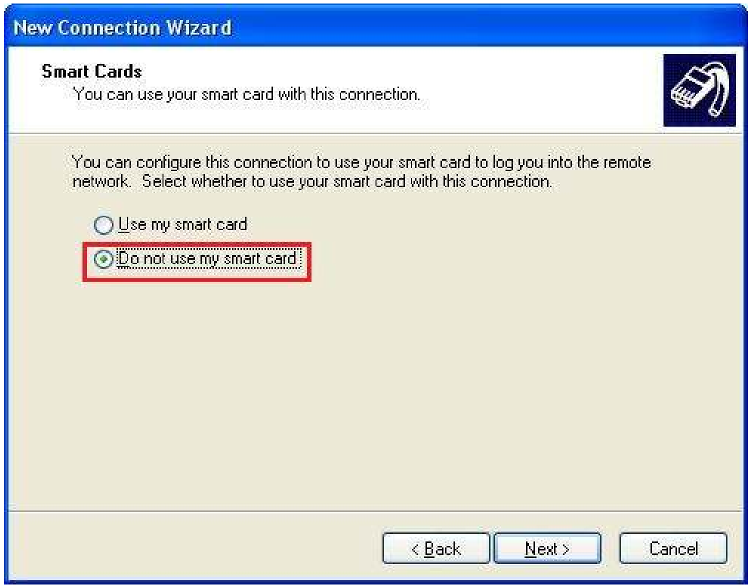
VPN Server Selection
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

192.168.7.164

8. Select [Do not use my smart card] then click **Next** button.



New Connection Wizard

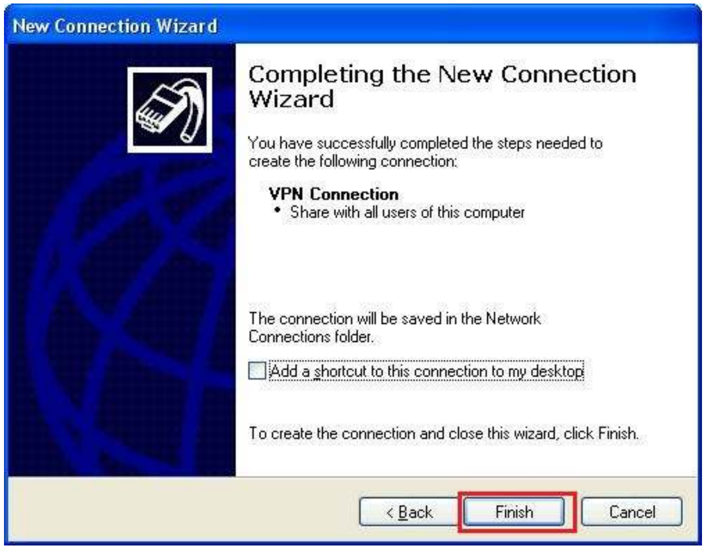
Smart Cards
You can use your smart card with this connection.

You can configure this connection to use your smart card to log you into the remote network. Select whether to use your smart card with this connection.

○ Use my smart card

● Do not use my smart card

9. Click **Finish** button to complete the wizard.



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

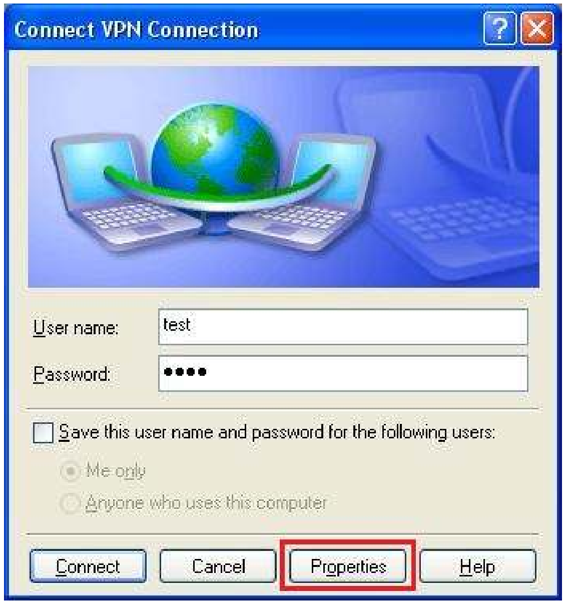
VPN Connection
- Share with all users of this computer

The connection will be saved in the Network Connections folder.

□ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

10. Click **Properities** button.



Connect VPN Connection

User name: test

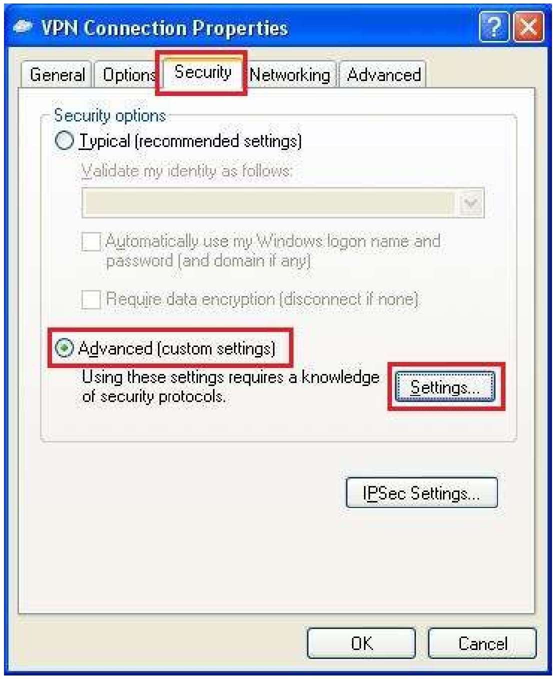
Password: ••••

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

11. In Security, select [Advanced (custom settings)] then click **Settings** button.



VPN Connection Properties

Security options

○ Typical (recommended settings)

Validate my identity as follows:

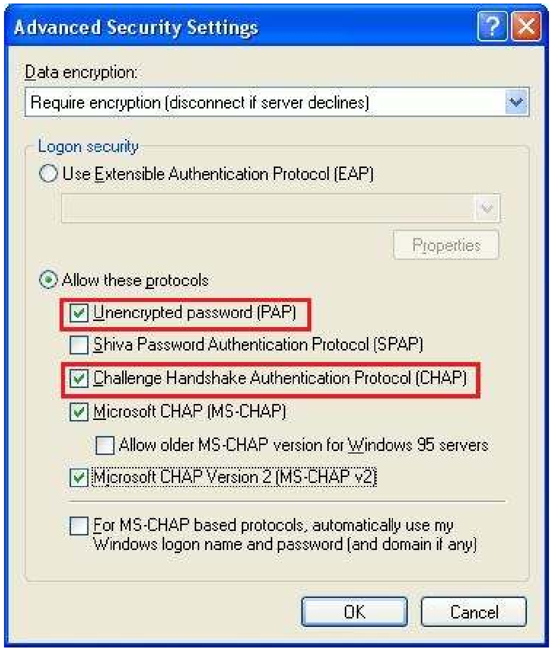
□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

12. Check [Unencrypted password (PAP)] and [Challenge Handshake Authentication Protocol (CHAP)] then click **OK** button.



Advanced Security Settings

Data encryption:

Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

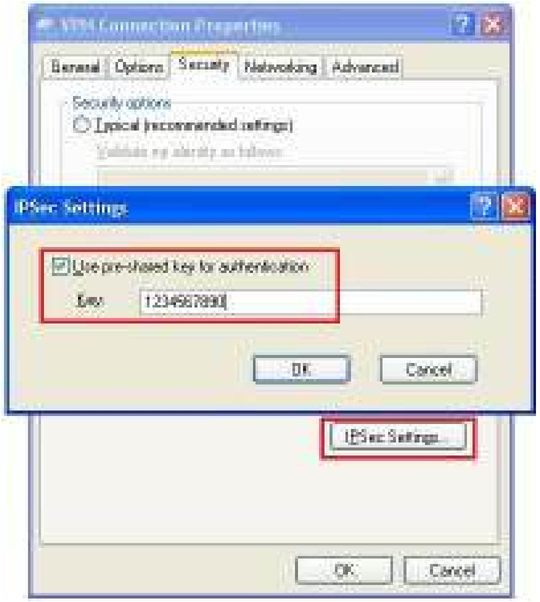
☑ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

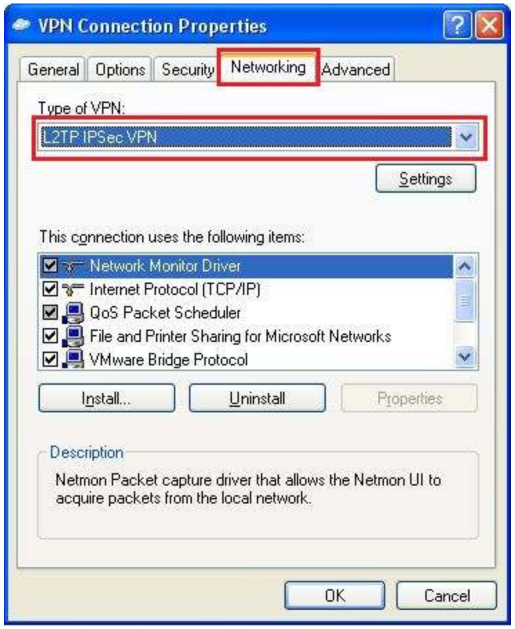
13. Click [IPSec Settings] then tick [Use pre-shared key for authentication], Enter the Key then click **OK** button.



☑ Use pre-shared key for authentication

Key: 1234567890

14. In Networking, select [L2TP IPSec VPN] then click **OK** button.



Type of VPN:

L2TP IPSec VPN

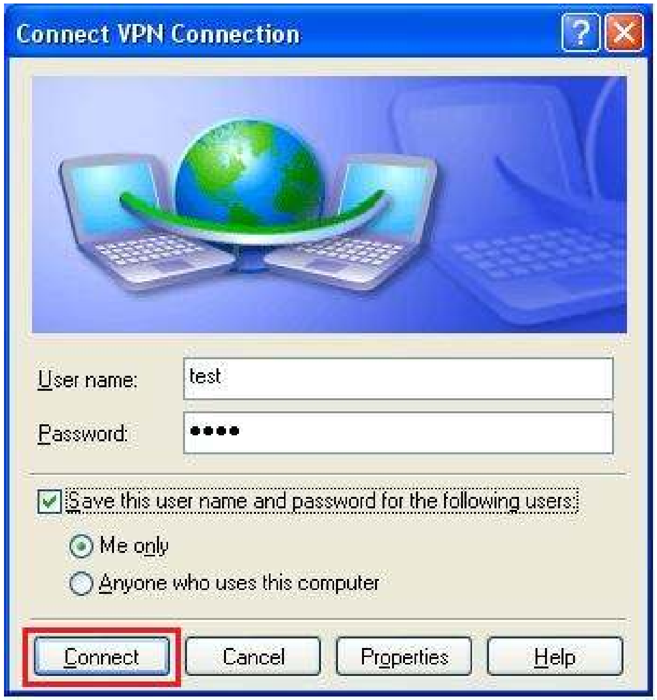
This connection uses the following items:

- ☑ Network Monitor Driver
- ☑ Internet Protocol (TCP/IP)
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ VMware Bridge Protocol

Description

Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network.

15. Click **Connect** button to connect VPN connection.



Connect VPN Connection

User name: test

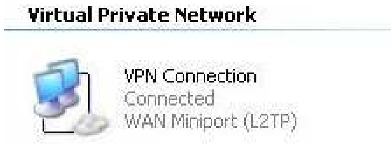
Password: ••••

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

16. You can see the VPN Connection has been established.

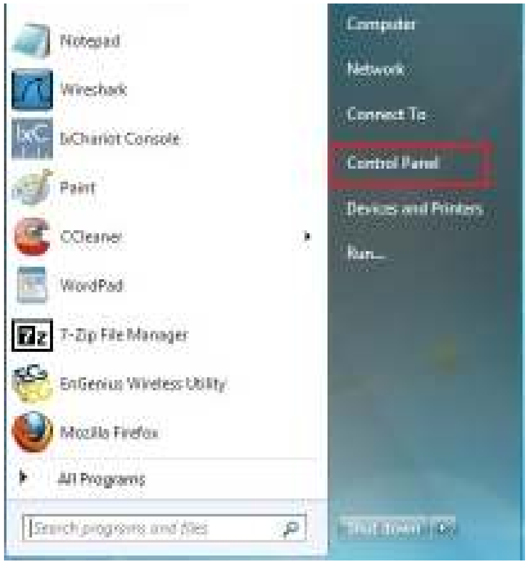


Virtual Private Network

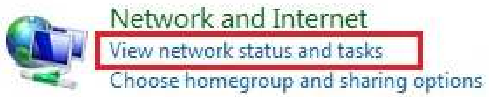
VPN Connection
Connected
WAN Miniport (L2TP)

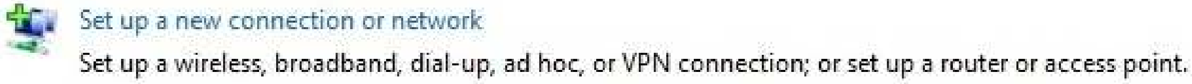
How to establish a L2TP over IPSec VPN connection in Windows 7

1. Click Start button and open Control Panel.



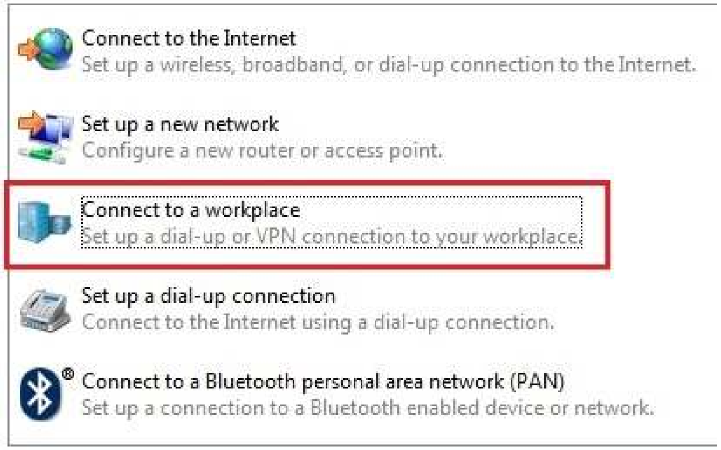
2. Click [View Network Status and Tasks] then [Set up a new connection or network]


Network and Internet
View network status and tasks
Choose homegroup and sharing options



Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

3. Click [Connect to a workplace] then [Use my Internet connection (VPN)]



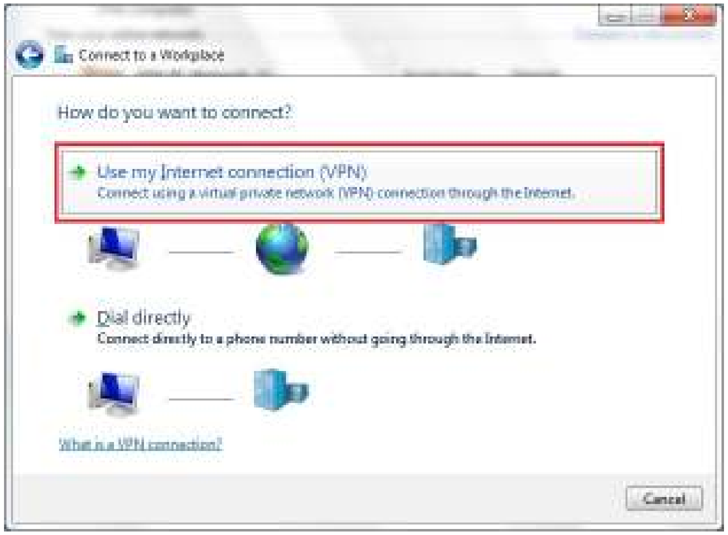
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

Connect to a Bluetooth personal area network (PAN)
Set up a connection to a Bluetooth enabled device or network.



Connect to a Workplace

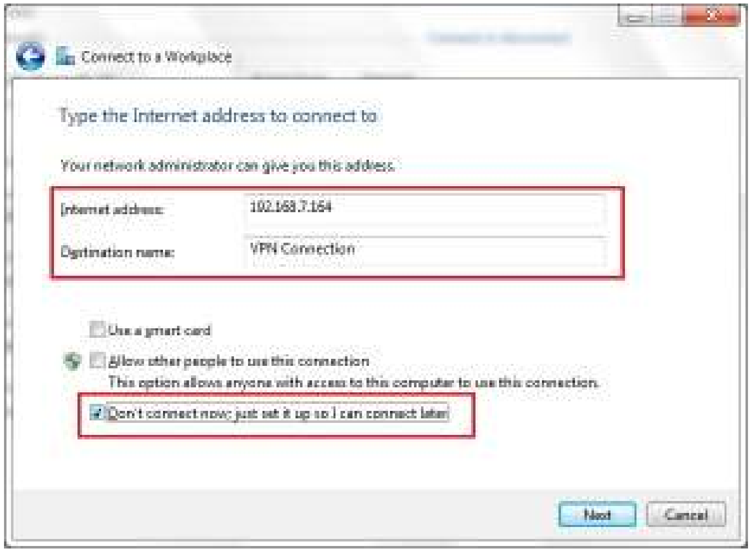
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

4. Enter the VPN server IP address: [*Internet address*], [*Destination name*] and tick [Don’t connect now; just set it up so I can connect later], then click the **Next** button.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

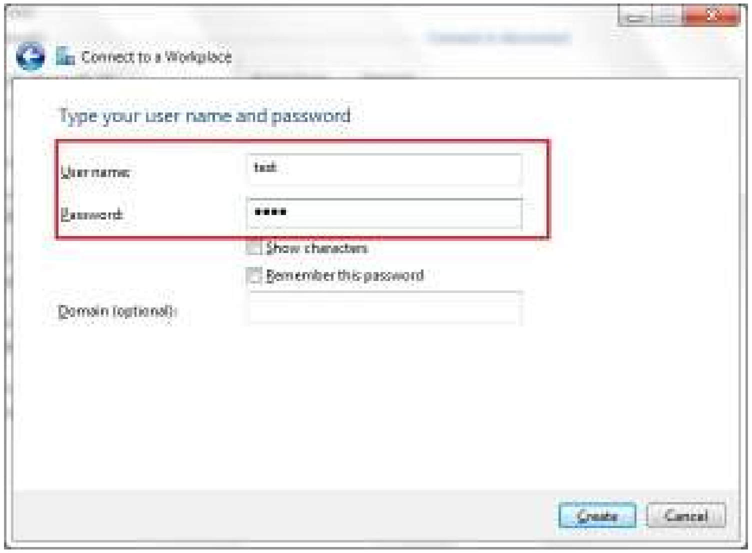
Internet address:	192.168.7.164
Destination name:	VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

5. Enter the correct *User name* and *Password* then click the **Create** button.



Type your user name and password

User name: test

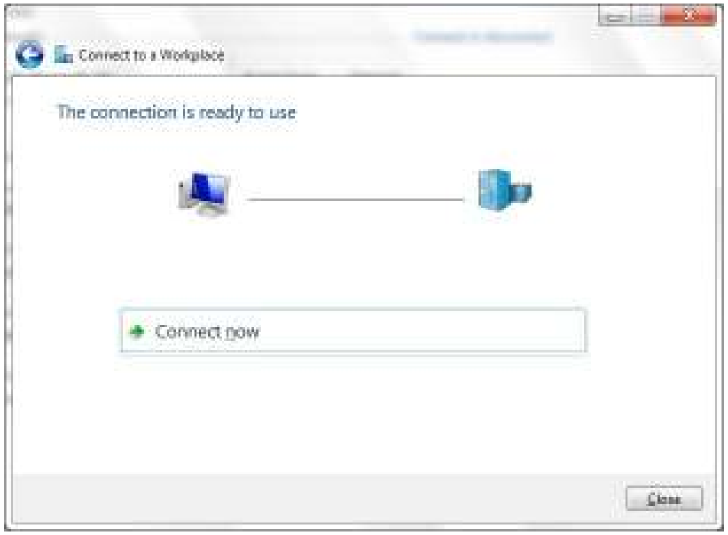
Password: ••••

□ Show characters

□ Remember this password

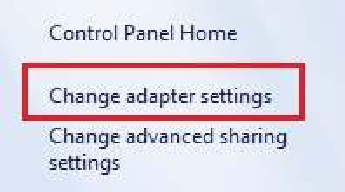
Domain (optional):

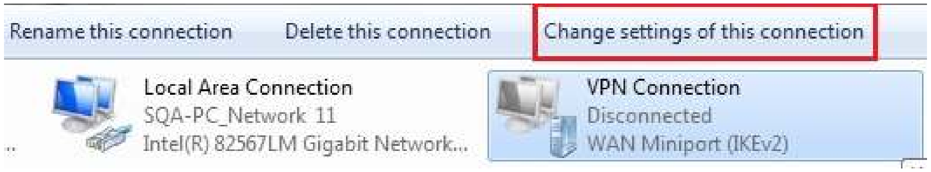
6. Click the **Close** button to close the VPN connection setting.



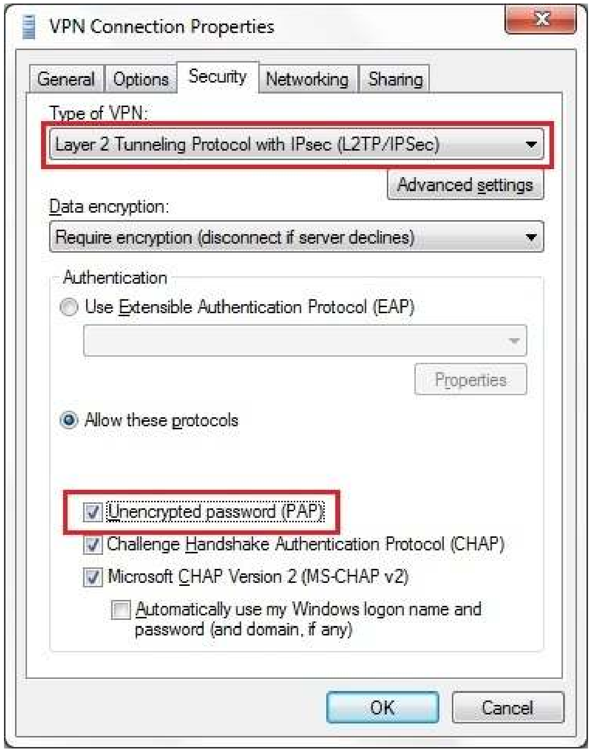
The connection is ready to use

7. Click [Change adapter settings] in Step 2, then select **VPN Connection** and click [Change settings of this connection]





8. Change Type of VPN to [Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)] and check [Unencrypted password (PAP)] in Security.



Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

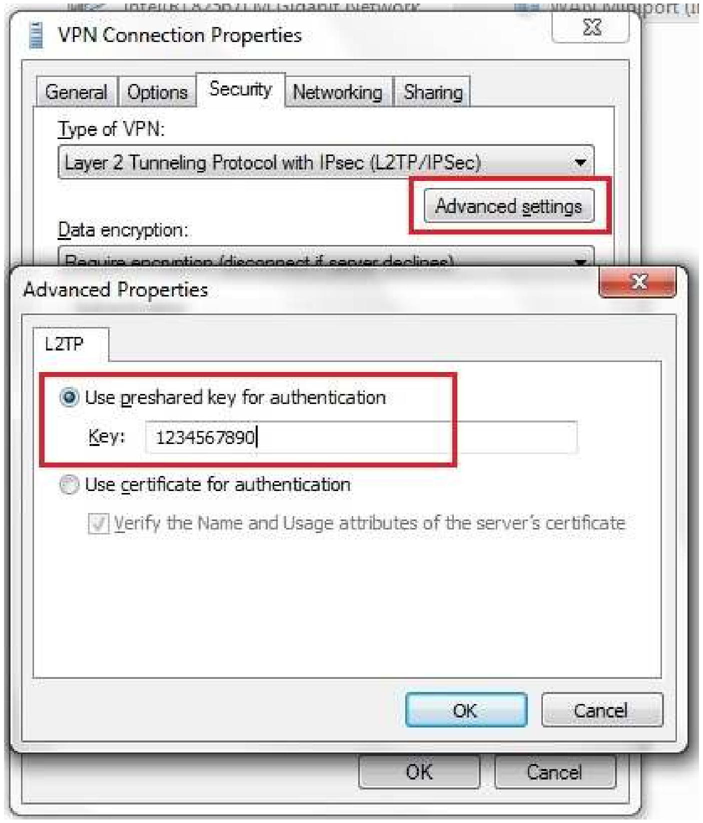
☑ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

9. Click the **Advanced settings** button and select [Use preshared key for authentication] and enter the correct key. Then click **OK** button.



VPN Connection Properties

Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption: Require encryption (disconnect if server declines)

Advanced Properties

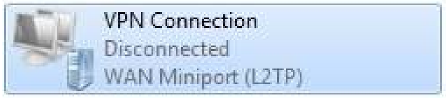
● Use preshared key for authentication

Key: 1234567890

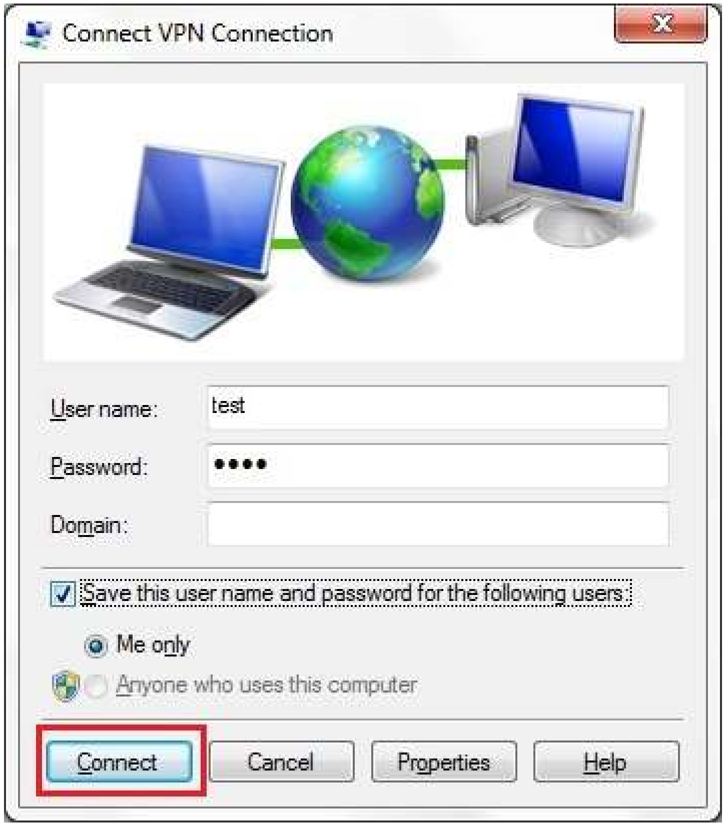
○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

10. Double click the **VPN Connection** then click the **Connect** button.



VPN Connection
Disconnected
WAN Miniport (L2TP)



Connect VPN Connection

User name: test

Password: ••••

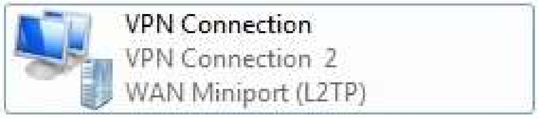
Domain:

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

11. You can see the VPN Connection has been established.



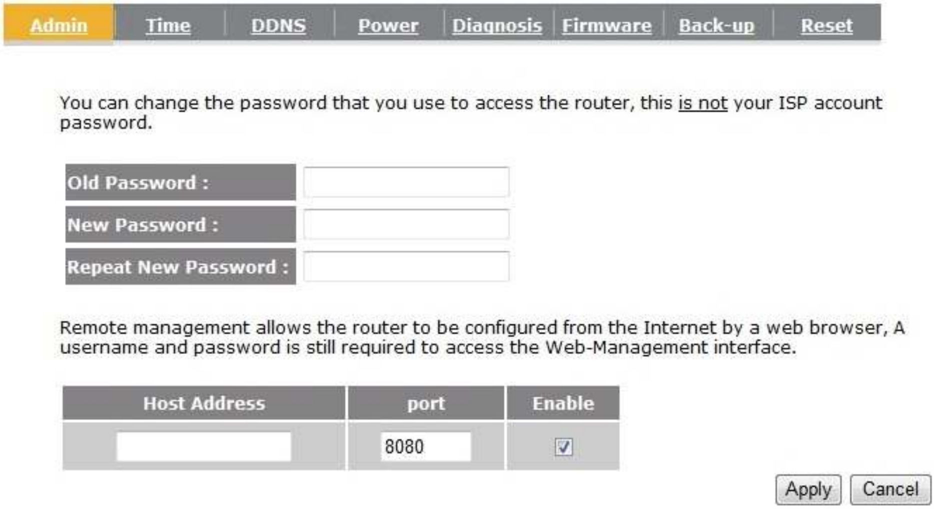
VPN Connection
VPN Connection 2
WAN Miniport (L2TP)

12. Tools

This section allows you to configure some device system settings.

12.1. Admin

This page allows you to change the system password and to configure remote management.



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

Old Password :	
New Password :	
Repeat New Password :	

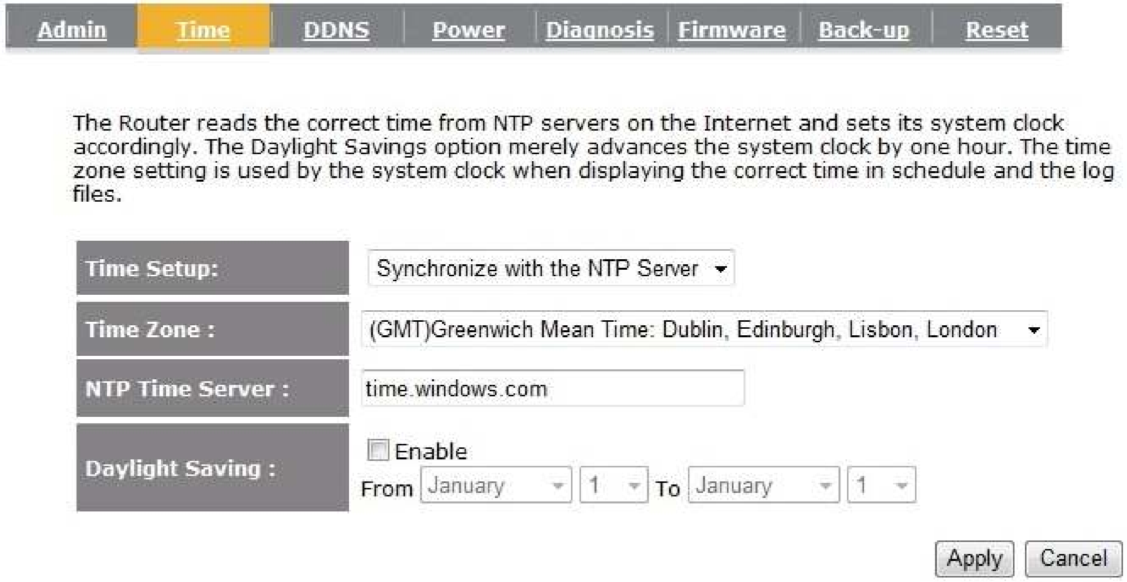
Remote management allows the router to be configured from the Internet by a web browser, A username and password is still required to access the Web-Management interface.

Host Address	port	Enable
	8080	☑

Change Password	
Old Password:	Enter the current password.
New Password:	Enter your new password.
Repeat New Password:	Enter your new password again for verification.
Remote Management	
Host Address:	You can only perform remote management from the specified IP address. Leave blank to allow any host to perform remote management.
Port:	Enter the port number you want to accept remote management connections.
Enable:	Tick to Enable the remote management feature.

12.2. Time

This page allows you to set the system time.



The Router reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

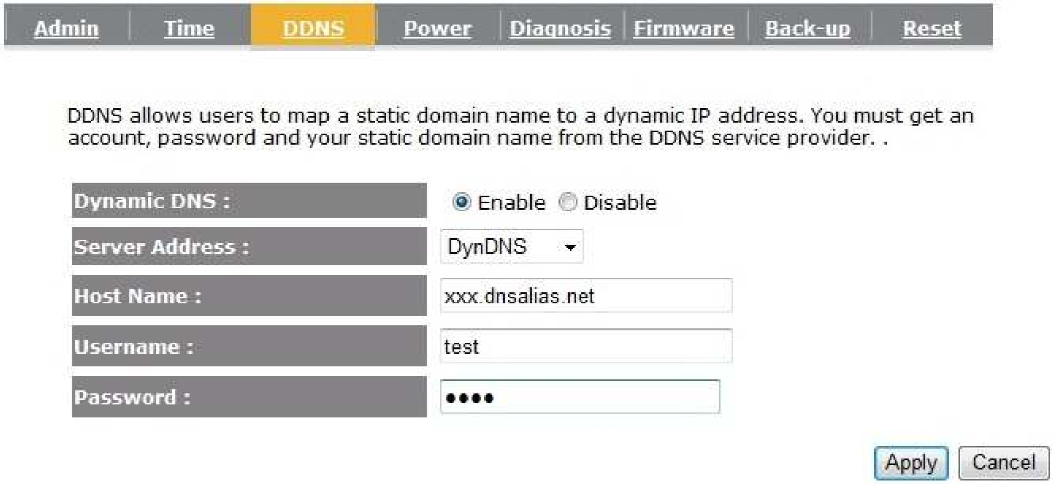
Time Setup:	Synchronize with the NTP Server
Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
NTP Time Server :	time.windows.com
Daylight Saving :	□ Enable From January 1 To January 1

Time	
Time Setup:	Select the method you want to set the time.
Time Zone:	Select the time zone for your current location.
NTP Time Server:	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
Daylight Savings:	Check whether daylight savings applies to your area.

12.3. Dynamic DNS (DDNS)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.



DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service provider. .

Dynamic DNS :	● Enable ○ Disable
Server Address :	DynDNS
Host Name :	xxx.dnsalias.net
Username :	test
Password :	••••

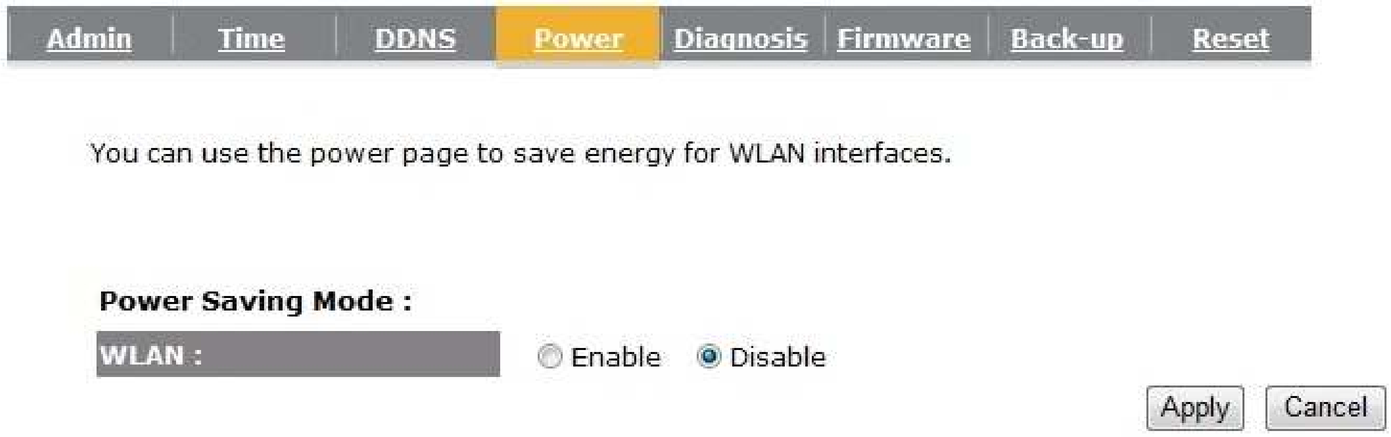
DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the EVR100's DDNS screen, and enable the DDNS feature.
4. The Wireless Router will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS	
Dynamic DNS	Tick this box to Enable the DDNS feature.
Server Address:	Select the list of Dynamic DNS homes you would like to use from this list.
Username / Password:	Enter the Username and Password of your DDNS account.

12.4. Power

This page allows you to Enable or Disable the wireless LAN power saving features.



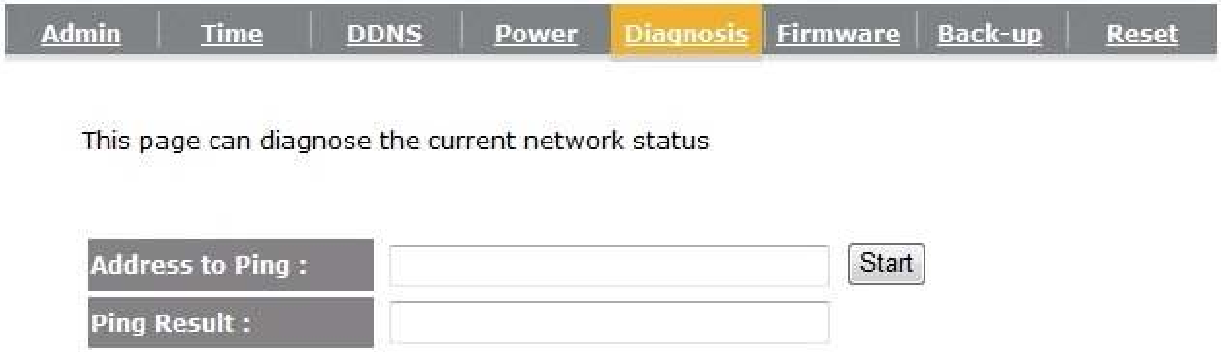
You can use the power page to save energy for WLAN interfaces.

Power Saving Mode :

WLAN : ○ Enable ● Disable

12.5. Diagnosis

This page allows you determine if the WIRELESS ROUTER device has an active Internet connection.



This page can diagnose the current network status

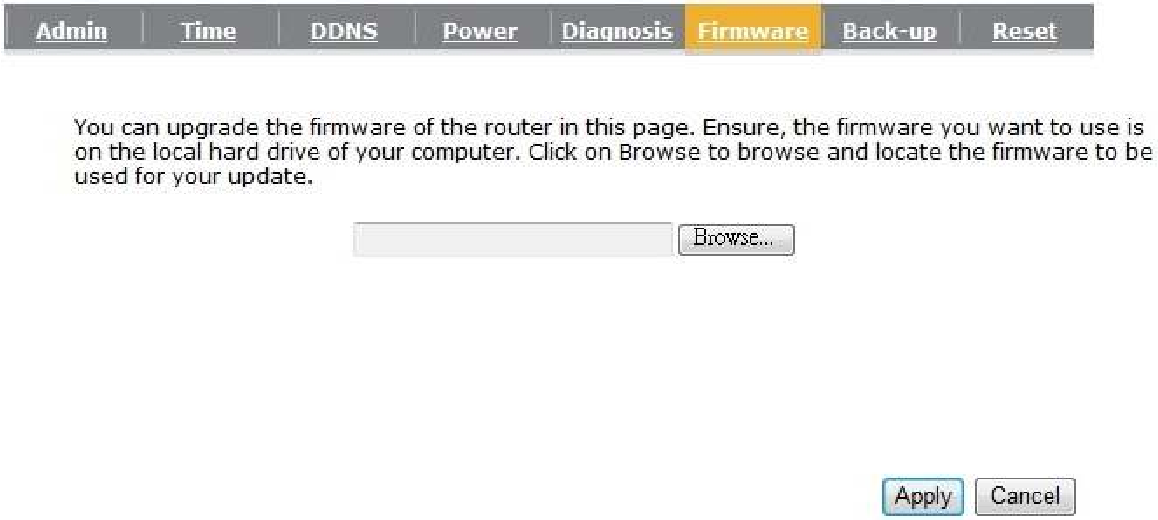
Address to Ping :

Ping Result :

Diagnosis	
Address to Ping:	Enter the IP address you like to see if a successful connection can be made.
Ping Result:	The results of the Ping test.

12.6. Firmware

The firmware (software) in the WIRELESS ROUTER device can be upgraded using your Web Browser.



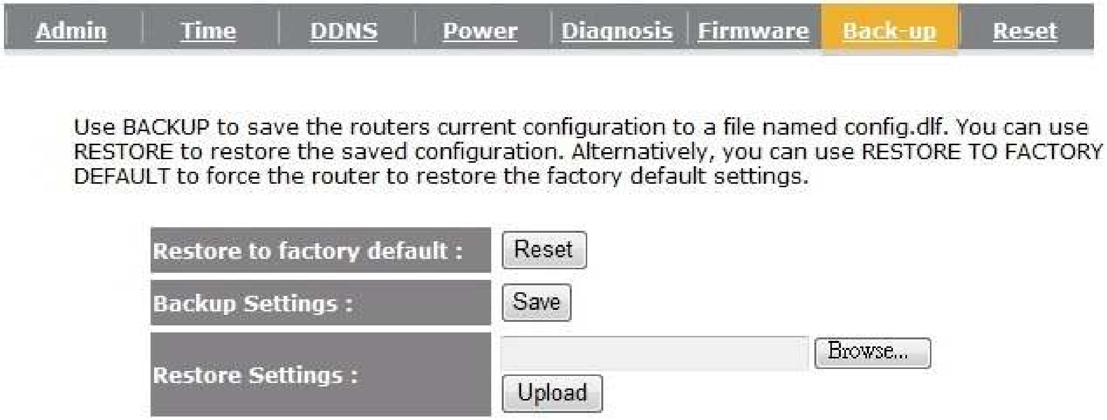
You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.

To perform the Firmware Upgrade:

1. Click the **Browse** button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the **Apply** button to commence the firmware upgrade.

Note: The Wireless Router is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Router will be lost.

12.7. Back-up



Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings.

Restore to factory default :

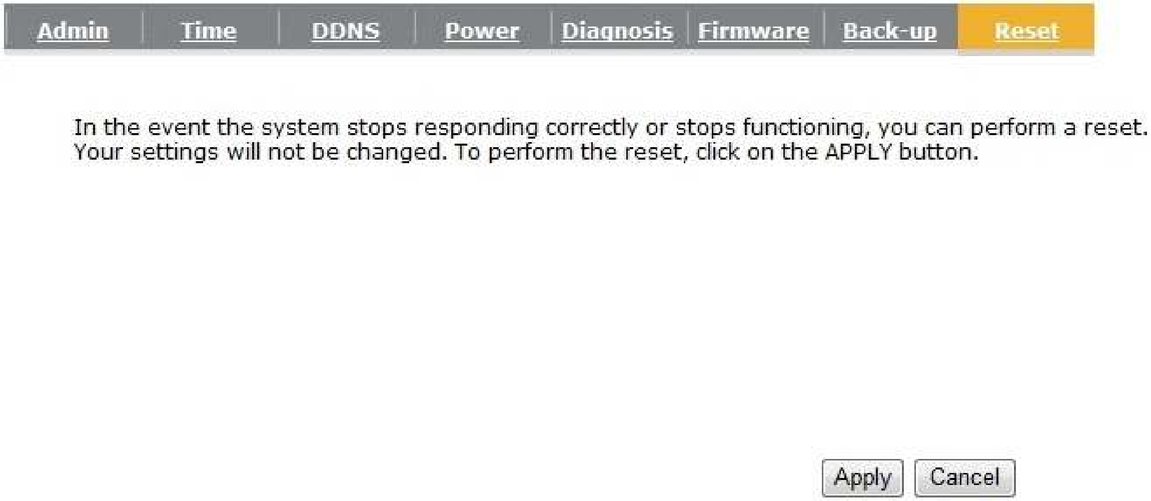
Backup Settings :

Restore Settings :

Back-up	
Restore to factory default:	Restores the device to factory default settings.
Backup Settings:	Save the current configuration settings to a file.
Restore Settings:	Restores a previously saved configuration file. Click **Browse** to select the file. Then **Upload** to load the settings.

12.8. Reset

In some circumstances it may be required to force the device to reboot.



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 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.

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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

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

Appendix B – IC Interference Statement

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.

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.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.