EnGenius®

Wireless-N Pocket AP/Router

ETR9350

Ultra Portable Pocket AP (Travel Router)

V1.0

1. Package Contents 5
2. System Requirements 5
3. Introduction 6
4. Features 7
5. Hardware Overview 8
6. Before you Begin 10
   6.1 Considerations for Wireless Installation 10
   6.2 AP Router / AP / Client Bridge Modes 11
   6.3 Check Network Settings (Windows XP/Vista) 12
7. Hardware Installation 15
8. Configuring Travel Router 17
   8.1 Setup Wizard 18
      8.1.1 AP Router Mode 22
      8.1.2 AP Mode 33
      8.1.3 Client Bridge Mode 35
   8.2 Web-Based Configuration 36
      8.2.1 System 36
      8.2.2 Internet 52
      8.2.3 Wireless 64
      8.2.4 Firewall 83

8.2.5 Advanced 90
8.2.6 Tools 101
8.3 AP and Client Bridge Modes 109
8.4 Client Bridge Mode 114
8.4.1 Wireless 114
Appendix A – FCC Interference Statement 117
Appendix B – IC Interference Statement 119

Revision History

Version	Date	Notes
1.0	October 21, 2009	Initial Release version

1. Package Contents

- EnGenius TRAVEL ROUTER Ultra Portable Pocket AP
- AC Power Cord
- RJ45 Ethernet LAN Cable
- CD-ROM with User Manual and Setup Utility
- QIG

2. System Requirements

- RJ45 Ethernet Based or 3G USB Internet Connection
- Computer with Wireless Network function
- Windows, MAC OS or Linux based operating systems
- Internet Explorer or Firefox or Safari Web-Browser Software

3. Introduction

TRAVEL ROUTER is the world's smallest 11n Wireless Router and Access Point with 3G connectivity that brings superior convenience for users who need to create a wireless network to share the Internet, documents or multimedia files quickly between computers at speeds of up to 300Mbps.

Also, you can leave the bulky power adapter behind as the power supply unit is embedded in the device, so it can be slipped into your pocket easily.

The TRAVEL ROUTER can be connected to the Internet through a DSL/Cable modem or 3G USB card at any available location. It can even share the connection in your hotel's room if a RJ45 network cable is used.

To ensure your data is secure, the TRAVEL ROUTER supports WiFi Protected Setup (WPS) for simple and easy setup of WPA2 encryption of the wireless signal.

4. Features

• WORLD'S SMALLEST AP

Superior design to bring you the world's smallest 11n AP Router for a true portable wireless solution.

• INTERNAL POWER

No need to bring bulky power adapters for improved space saving convenience.

• 3G MOBILE INTERNET SHARING

Attach a 3G USB adapter to wirelessly share your 3G Internet connection to multiple computers.

• 3 OPERATION MODES

AP Router, Access Point and Client Bridge modes for flexible usage in different scenarios.

• 802.11n COMPLIANT

Fully 802.11n standard compliant to bring you 6x faster and 3x farther wireless connections at speeds up to 300Mbps.

• WPS PUSH BUTTON

WiFi Protected Setup (WPS) Push Button Configuration support for simple and secure setup of your wireless network.

• BEST CHANNEL SELECTION

In places where there are many wireless networks, the TRAVEL ROUTER will select the channel with the least interference for maximum reception and performance.

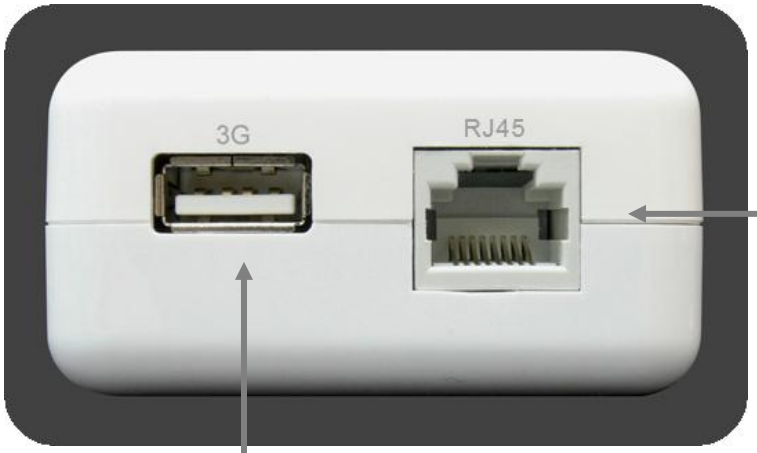
• MULTI-SSID

Up to 4 different wireless networks can be created with different security encryption methods. They can even be isolated so each wireless network has their own access policies.

• ADVANCED FIREWALL AND ACCESS CONTROL

Dual Firewall is featured to prevent unwanted access from the Internet. URL, MAC and IP Filters allows control over who can connect to your LAN, and what Internet sites they can connect to.

5. Hardware Overview



3G USB
Attach a 3G USB adapter to share your 3G Internet connection.

When 3G USB adapter is connected, RJ45 automatically is set to LAN mode.

RJ45
This RJ45 port can be configured as WAN or LAN modes.

WAN: Connect to the Internet using DSL/Cable modem.

LAN: Connect to a computer, switch or hub.

LED Lights	icon	Description
Mobile 3G		Color – Blue Lights when 3G USB adapter is connected. Blinks when 3G data transfer.
Wireless LAN		Color – Blue Lights when Wireless signal is activated. Blinks when Wireless data transfer.
WPS		Color – Blue Blinks when WPS handshake is initialized.
LAN		Color – Blue Lights when wired network device is connected to RJ45 port. Blinks when data transfer occurs on RJ45 port.
Power		Color – Blue Lights when device is powered ON. Blinks device is Reset.
Mode		Indicates which mode the TRAVEL ROUTER is set to. Orange – AP Router Blue – Access Point Green – Client Bridge
Buttons	**icon**	**Description**
WPS		Press this button to initialize WPS process. Hold this button for 10 seconds to Reset to Factory Defaults.

6. Before you Begin

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

6.1 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.

6.2 AP Router / AP / Client Bridge Modes

There are three main modes to select from which will influence the installation of the TRAVEL ROUTER. This section will help you determine which mode works with your setup.

AP Router Mode

AP Router Mode allows you to share an Internet connection to multiple computers.

AP Mode

AP mode allows you to have a wired or wireless router.

Client Bridge Mode

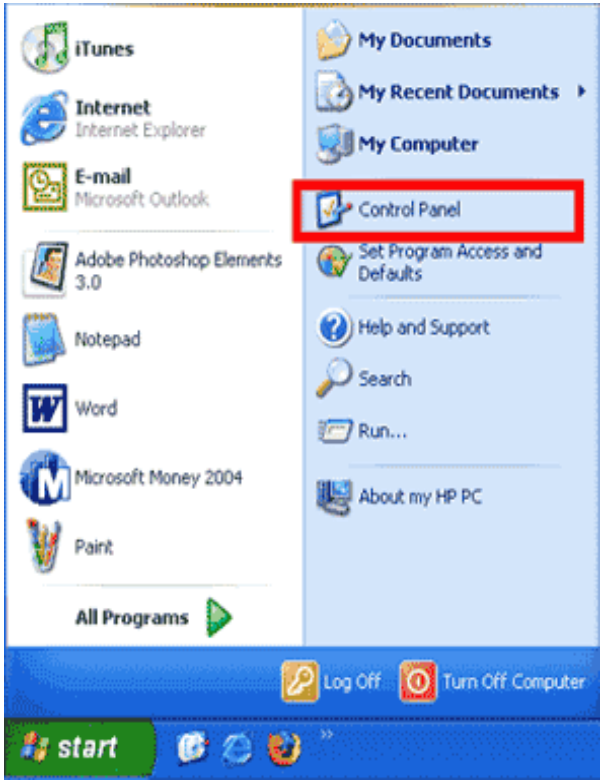
Client Bridge Mode allows a wired network device to connect to your wireless network, or create a point-to-point bridge.

Change mode from the top right of the User Interface.

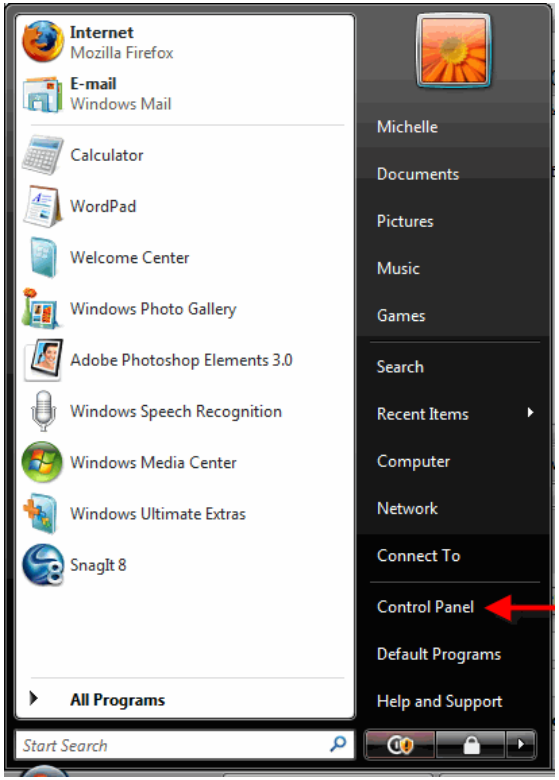
Please see ***Configuring the TRAVEL ROUTER*** for instructions to access the Web-Based User Interface.

6.3 Check Network Settings (Windows XP/Vista)

1. Click Start button and open Control Panel.



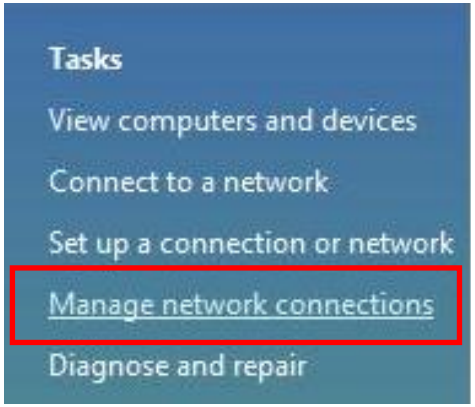
Windows XP



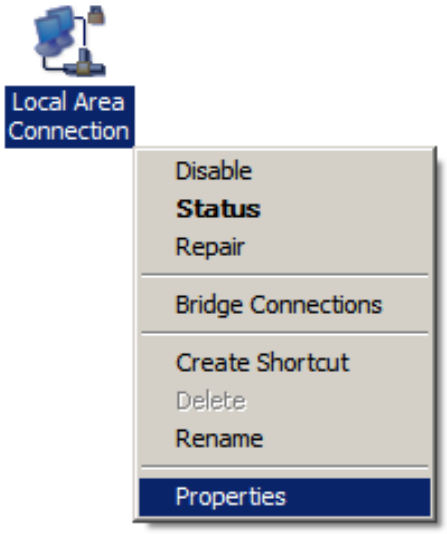
Windows Vista

2. Windows XP, click [**Network Connection]**

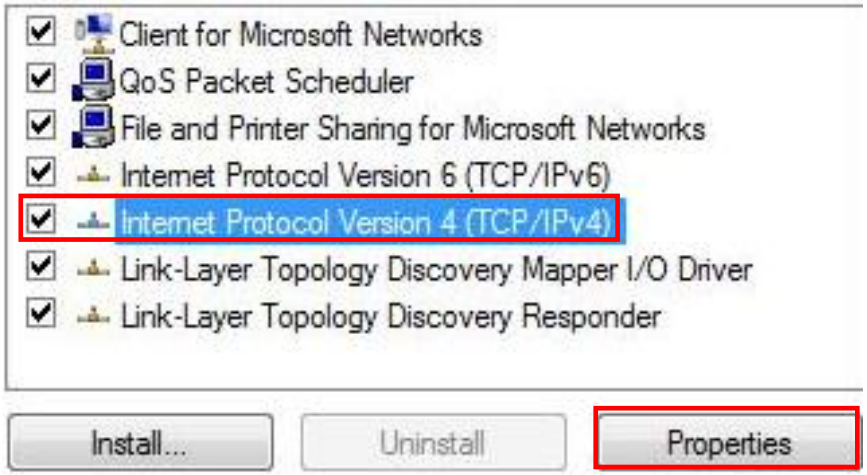
Windows Vista, click [**View Network Status and Tasks**] then [**Manage Network Connections**]



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

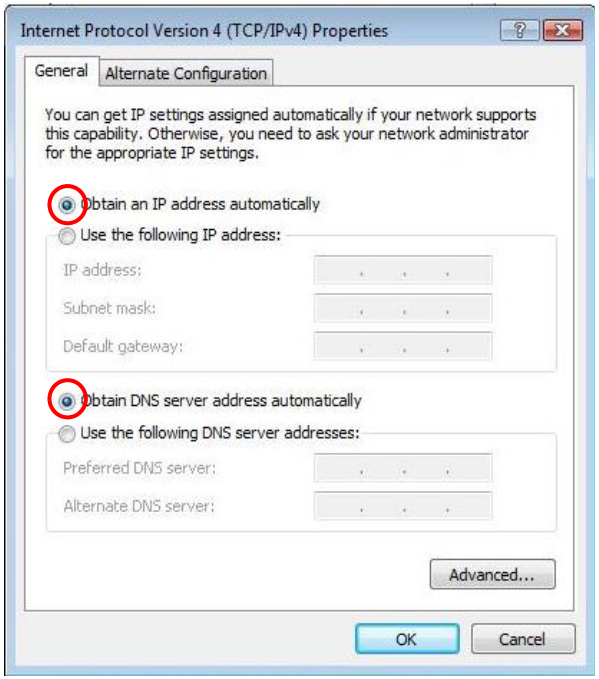


4. Check **“Client for Microsoft Networks”, “File and Printer Sharing”**, and **“Internet Protocol (TCP/IP)** is ticked. If not, please install them.



5. Select **“Internet Protocol (TCP/IP)”** and click [**Properties**]

6. Select **“Obtain an IP Address automatically”** and **“Obtain DNS server address automatically”** and click [**OK**].

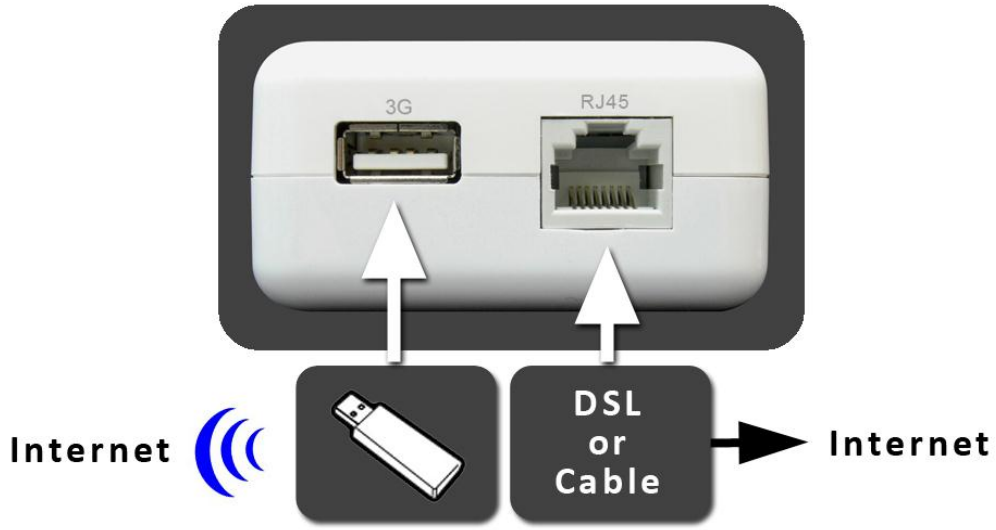


7. Hardware Installation

AP Router Mode:

One type of Internet connection is required. Please either connect the network cable from your DSL/Cable modem to the RJ45 port on the TRAVEL ROUTER or connect a 3G adapter to the USB port.

Note: When 3G USB adapter is connected, RJ45 automatically is set to LAN mode.



AP Mode:

Connect the network cable to the RJ45 port.

Power On :

Use the AC Power cord to connect TRAVEL ROUTER and outlet or any other power supplies to provide the electricity to the device.

8. Configuring Travel 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 TRAVEL ROUTER.

Default Settings

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

Note: *xxxxxx* mentioned 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.

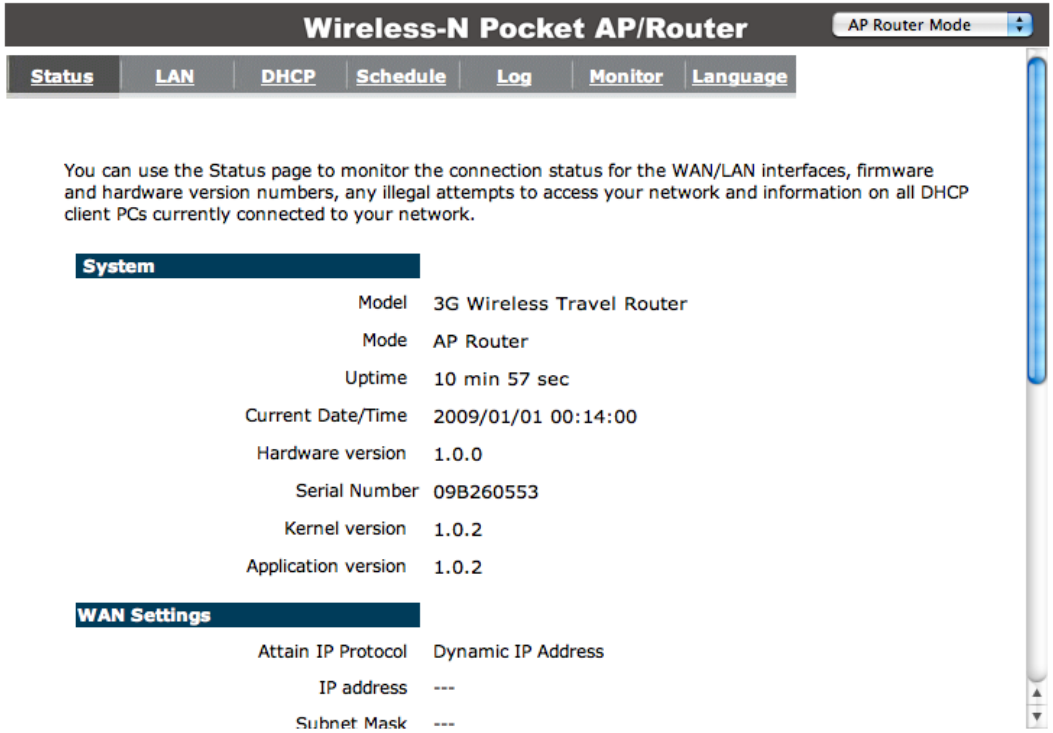
8.1 Setup Wizard

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

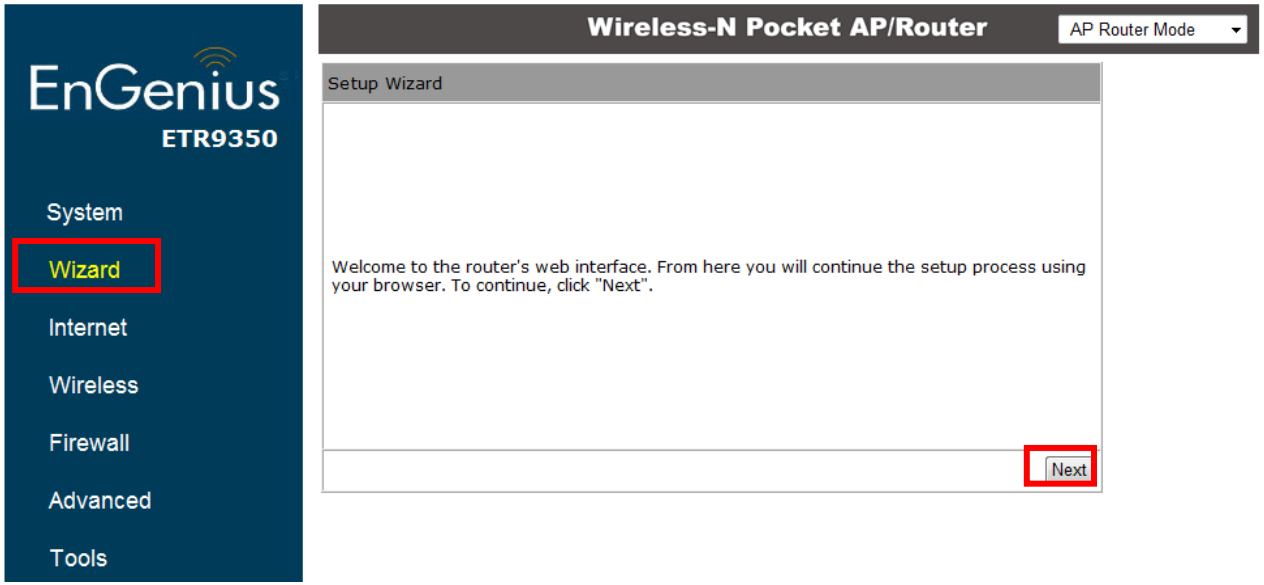
   Note: If you have changed the default IP Address assigned to the TRAVEL ROUTER, ensure you enter the correct IP Address.

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

3. You will see the following screen if the log on process is successful.

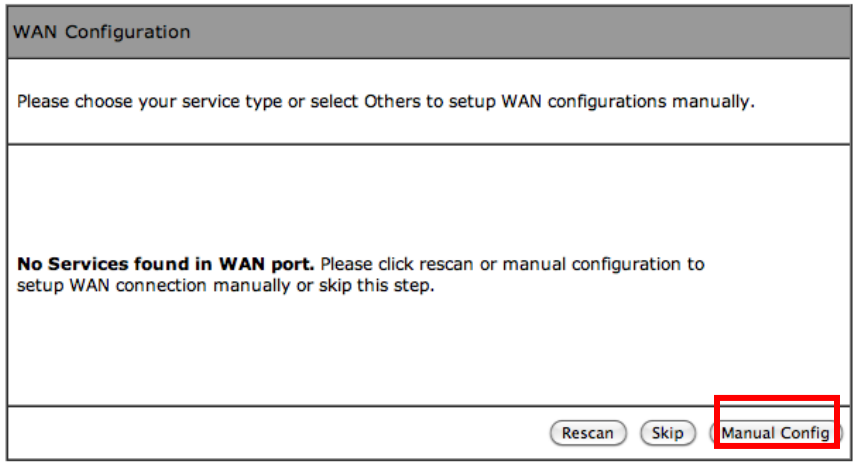


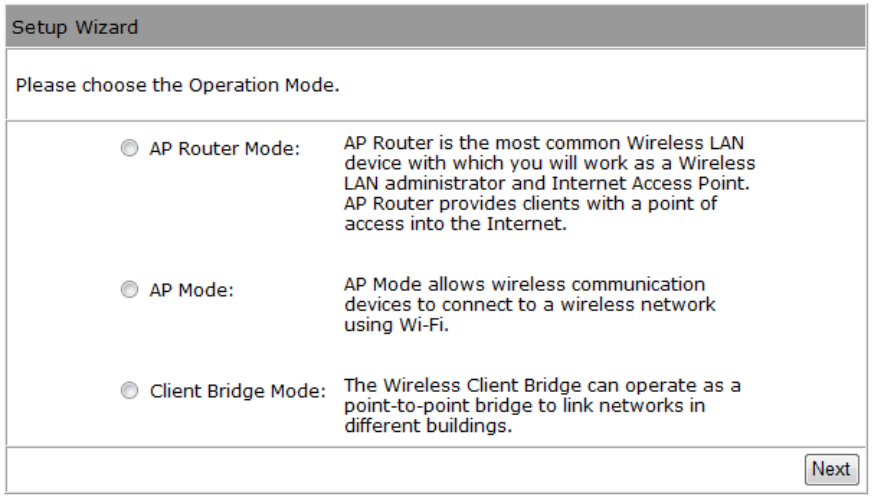
4. Click **Wizard** to enter the Setup Wizard.
Then click **Next** to begin the wizard.


EnGenius
ETR9350
System
Wizard
Internet
Wireless
Firewall
Advanced
Tools
Wireless-N Pocket AP/Router
AP Router Mode
Setup Wizard
Welcome to the router's web interface. From here you will continue the setup process using your browser. To continue, click "Next".
Next

5. Select the Operation Mode.

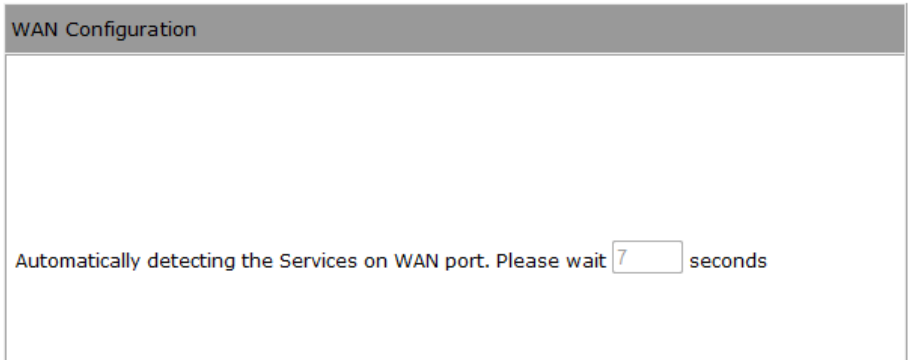
Please ensure you have the proper cables connected as described in the Hardware Installation section.



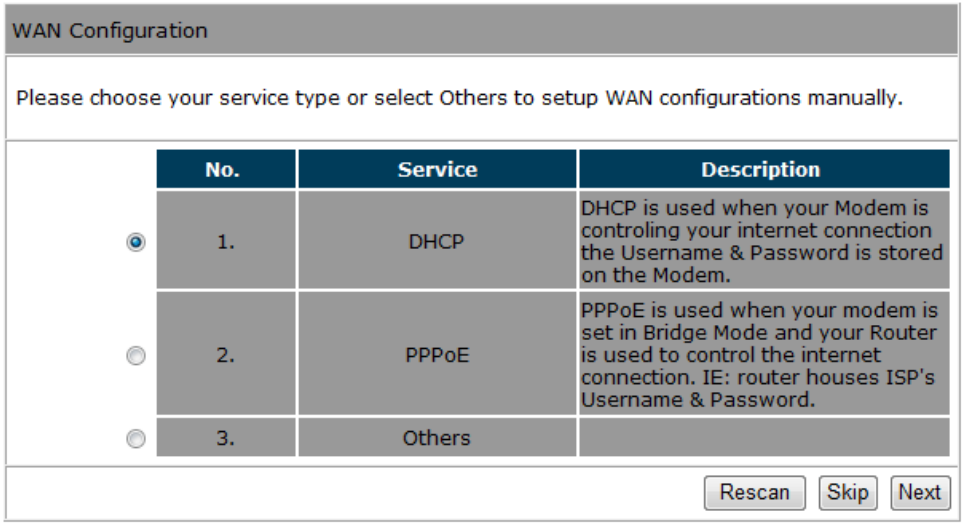


8.1.1 AP Router Mode

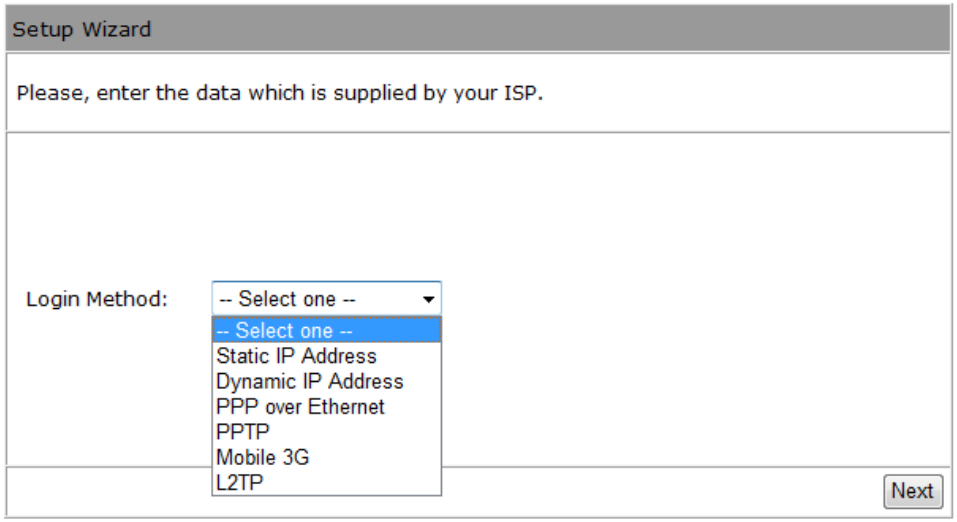
a) The device will now automatically search for the correct Internet settings.



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.

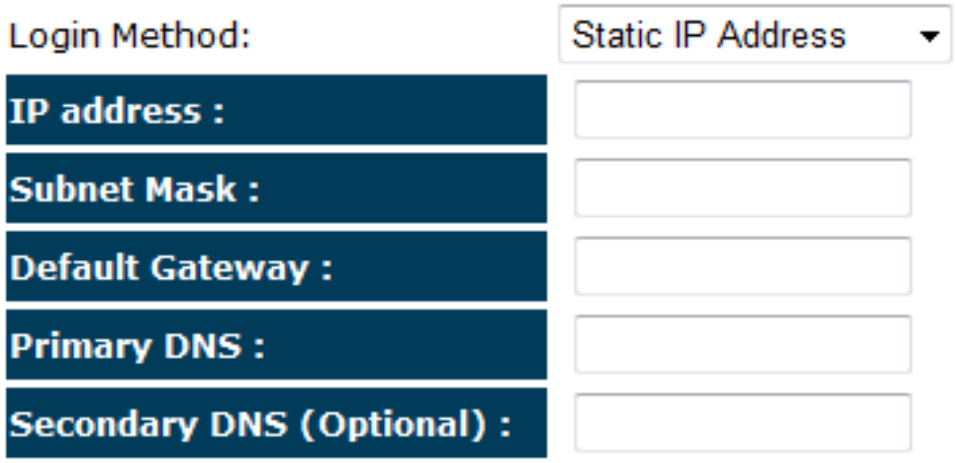


c) There are many WAN service types available. Please obtain the correct settings from your Internet Service Provider (ISP).



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.

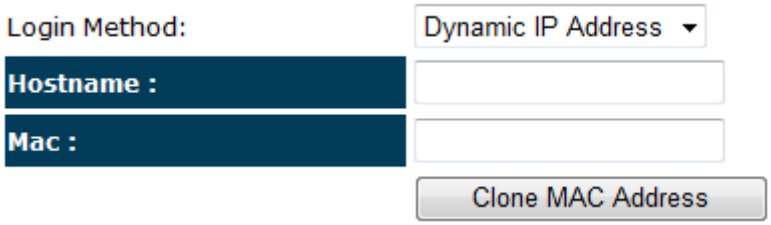


Dynamic IP Address

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.

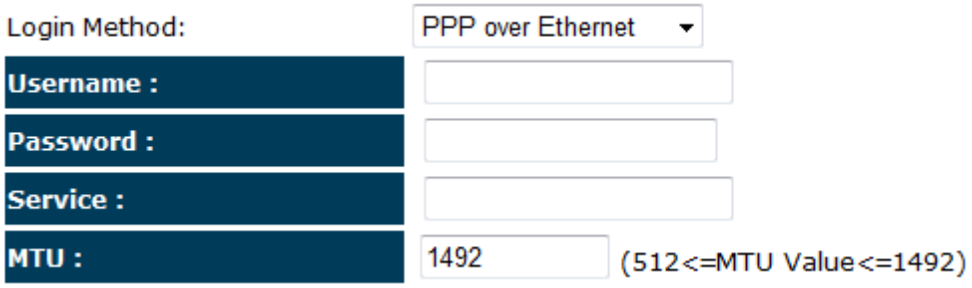
If your ISP has recorded the MAC address of your computer's Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC Address** button.

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.



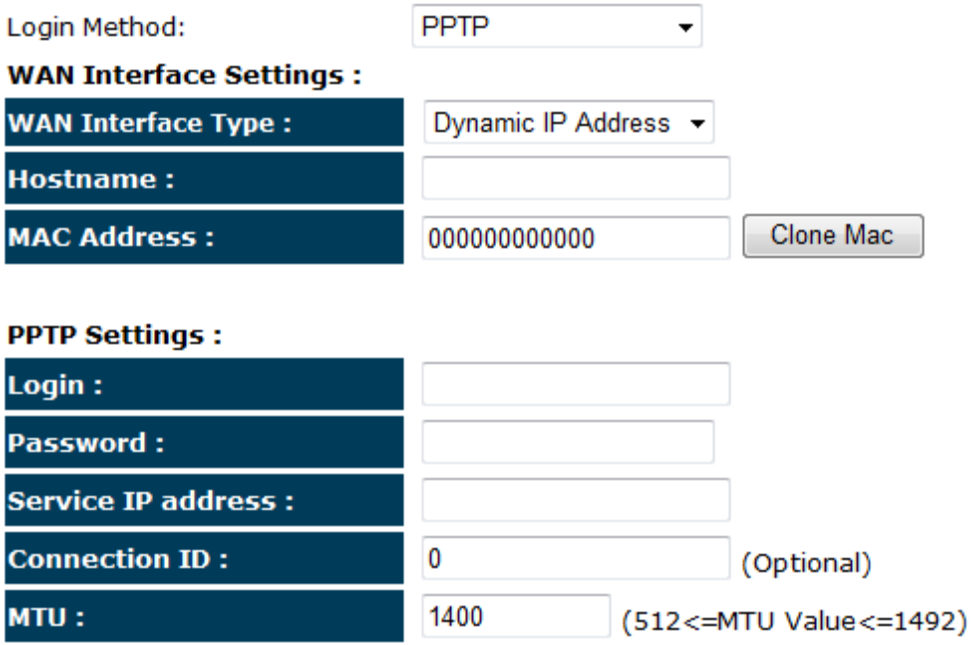
Dynamic IP Address	
Hostname:	This is optional. Only required if specified by ISP
MAC:	The MAC Address that is used to connect to the ISP.

PPP over Ethernet
ISP requires an account username and password.



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.

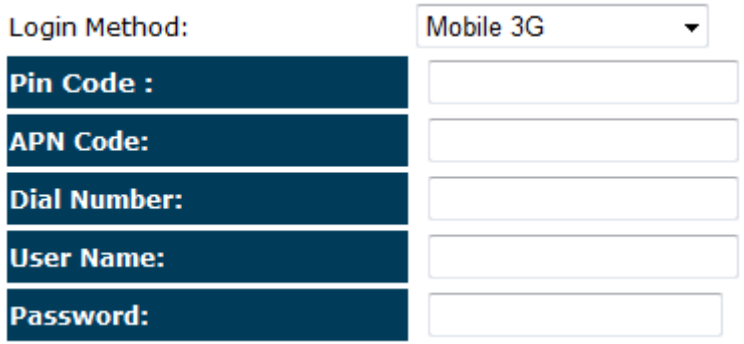
Point-to-Point Tunneling Protocol (PPTP)
PPTP is used by some ISPs.



PPTP WAN Interface Settings	
WAN Interface Type:	Select whether the ISP is set to Static IP or Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP
MAC:	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.

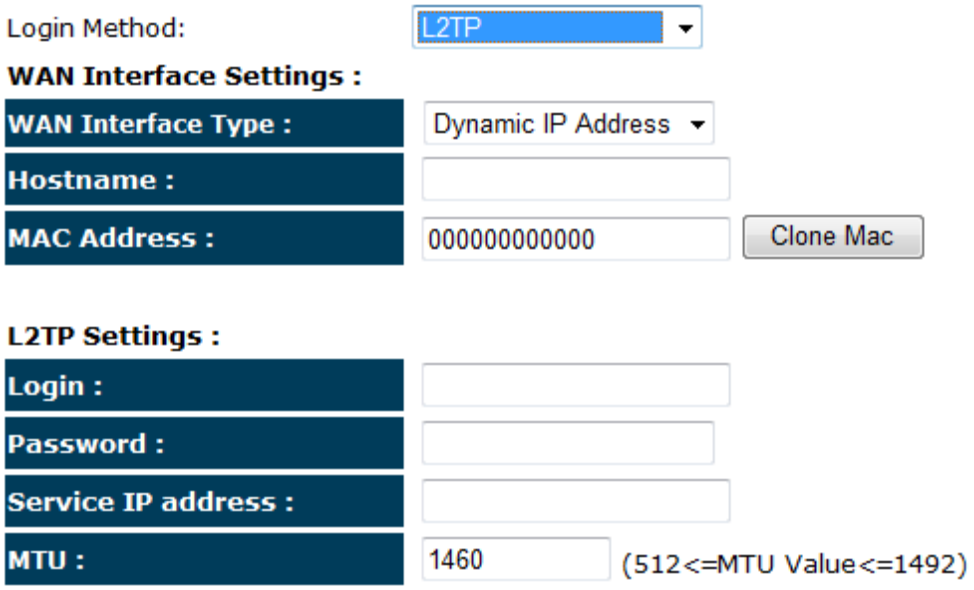
Mobile 3G

Please ensure your 3G USB card is connected to the TRAVEL ROUTER and has an active USIM card inserted.



Mobile 3G	
Pin Code:	Enter the Pin code for your USIM card if required.
APN Code:	Enter the APN code for the network provider
Dial Number:	Only required if specified by ISP
User Name:	Account Username. Only required if specified by ISP
Password:	Account Password. Only required if specified by ISP

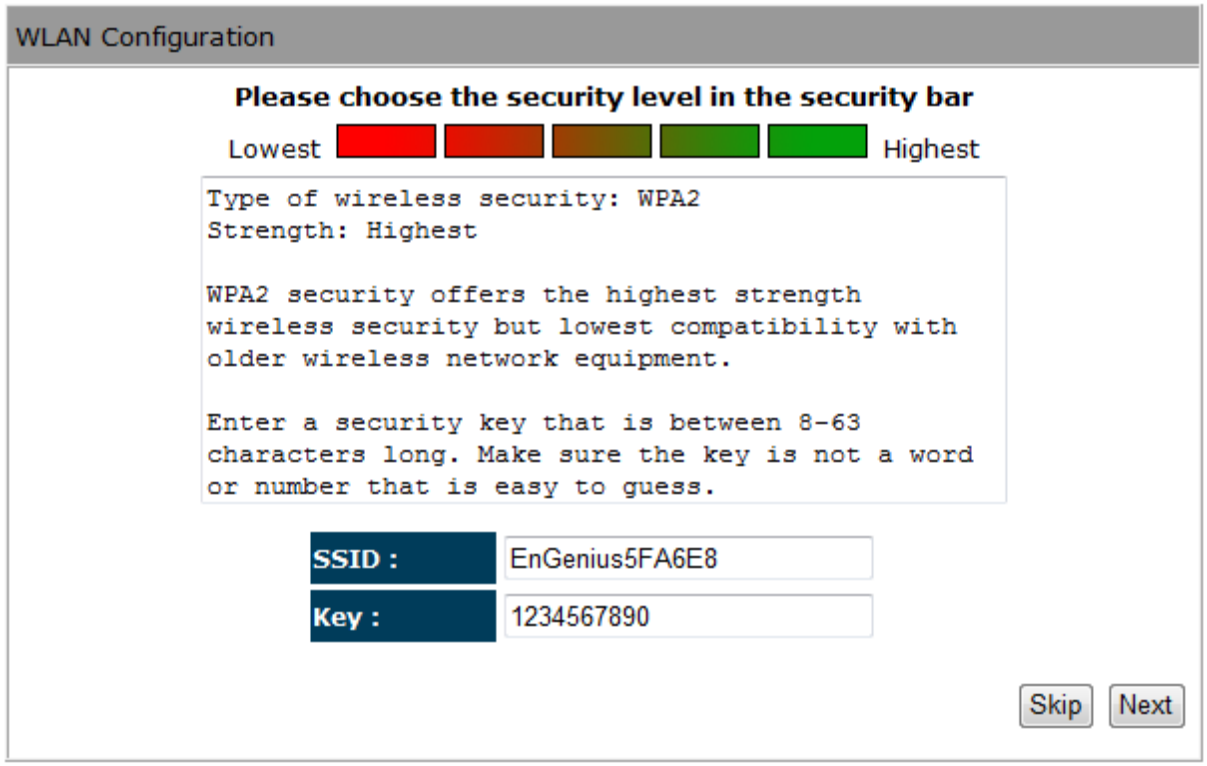
Layer-2 Tunneling Protocol (L2TP)



L2TP WAN Interface Settings	
WAN Interface Type:	Select whether the ISP is set to Static IP or Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP
MAC:	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.

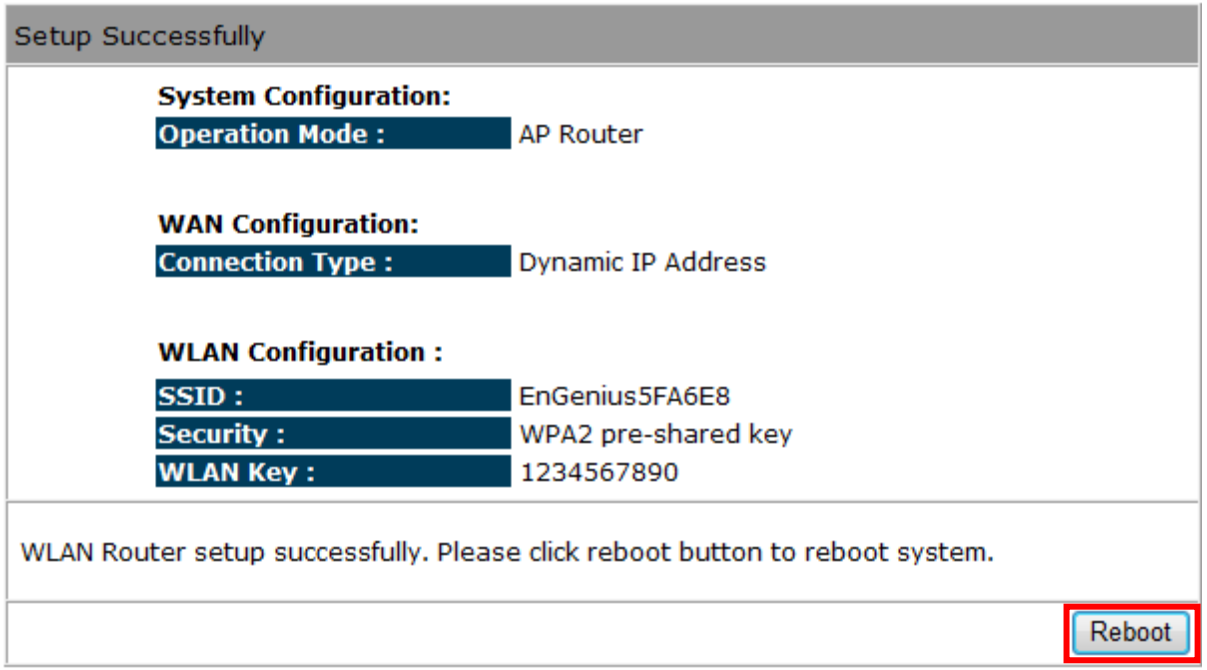
Note: 802.11n wireless speeds may not be achievable if the security is setup to Lowest and Low level.



SSID: Enter the name of your wireless network.

Key: Enter the security key for your wireless network.

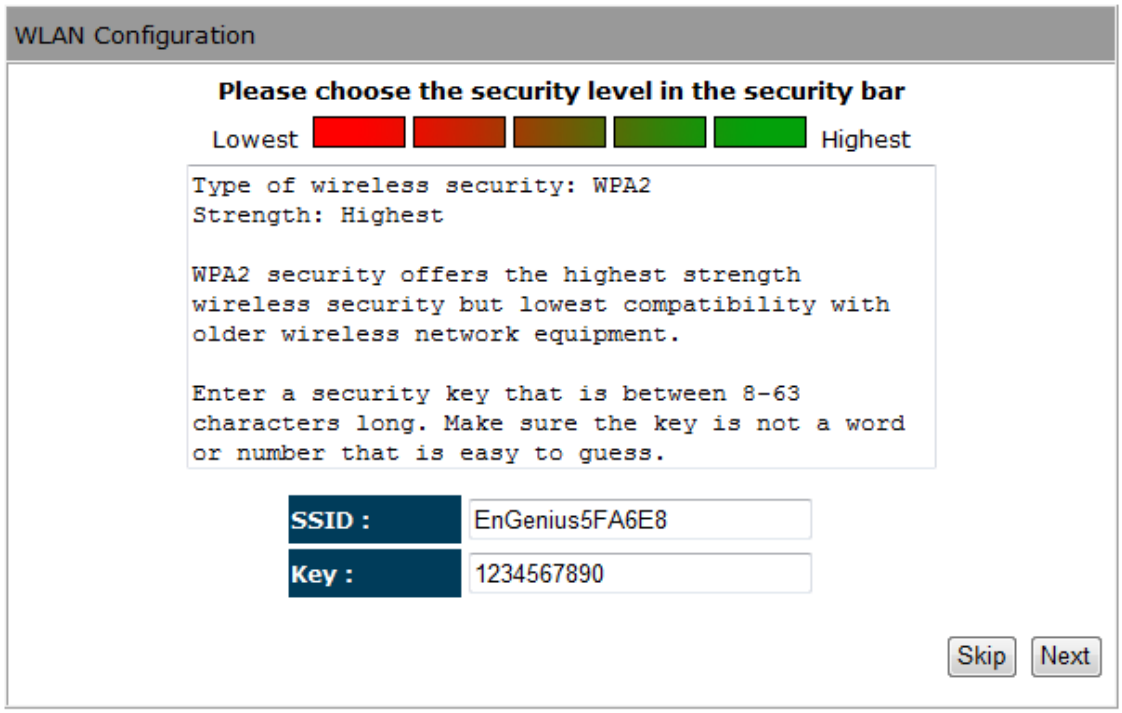
e) Check the settings are correct, and then click **Reboot** to apply the settings.



8.1.2 AP Mode

a) Select the level of wireless security to be used.
EnGenius recommends the **Highest** level of security to be used.

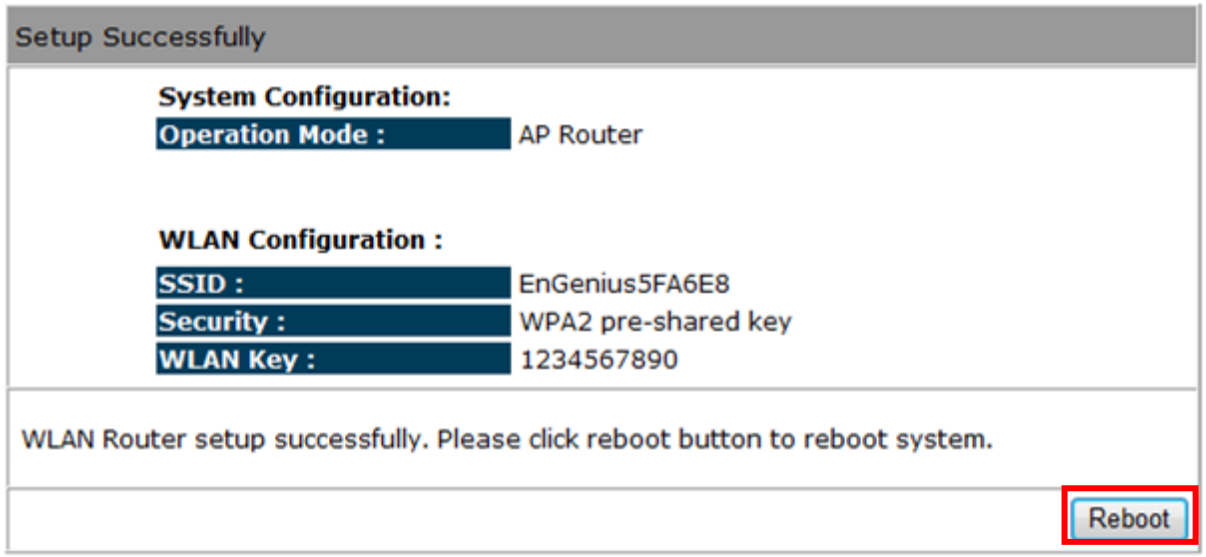
Note: 802.11n wireless speeds may not be achievable if the security is setup to Lowest and Low level.



SSID: Enter the name of your wireless network.

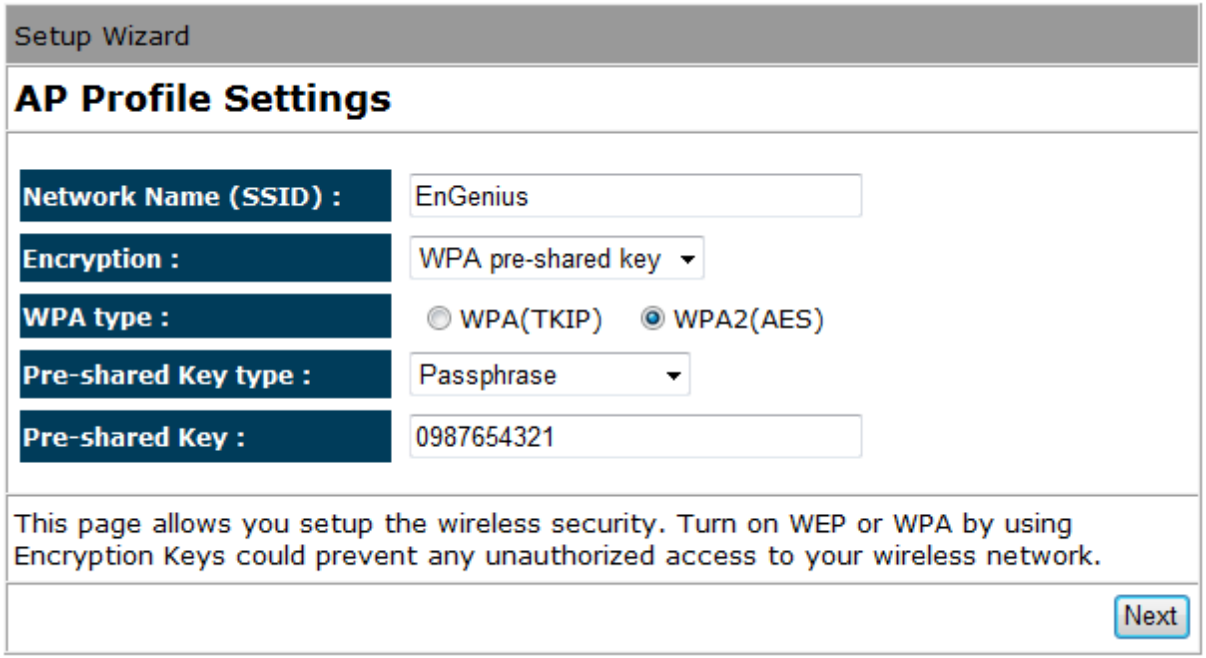
Key: Enter the security key for your wireless network.

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

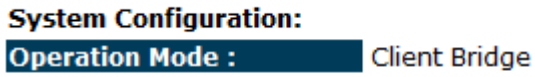


8.1.3 Client Bridge Mode

a) In this mode, the TRAVEL ROUTER will connect to a wireless network as a client device. Please enter the SSID and security settings of that wireless network.



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



8.2 Web-Based Configuration

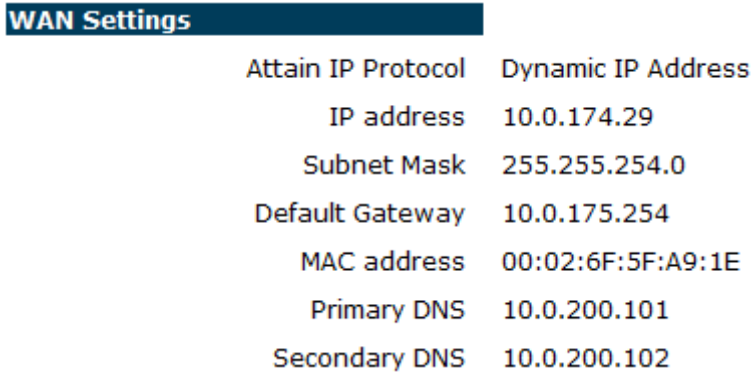
8.2.1 System

Status

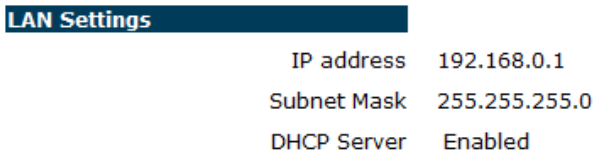
This page allows you to monitor the status of the device.

System	
Model	3G Wireless Router
Mode	AP Router
Uptime	33 min 35 sec
Current Date/Time	2009/01/01 00:53:01
Hardware version	1.0.0
Serial Number	000000111
Kernel version	1.0.2
Application version	1.0.2

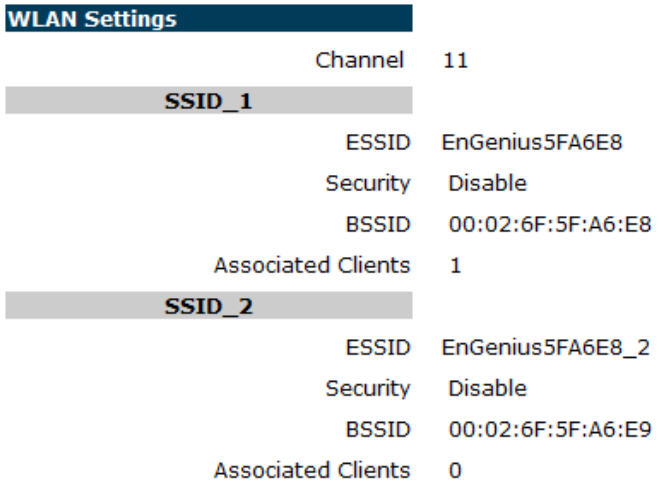
Status	
Model:	Description of this device.
Mode:	The device is currently in which mode.
Uptime:	The duration about the device has been operating without powering down or reboot.
Current Date/Time:	The device's system time. If this is incorrect, please set the time in the Tools / Time page.
Hardware version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



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.



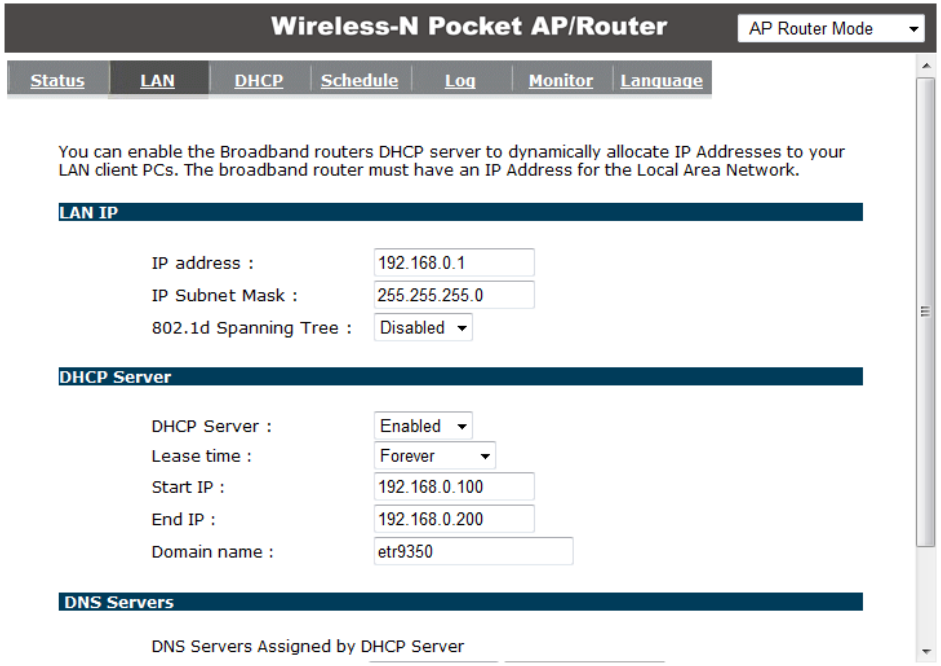
LAN Settings	
IP address:	The LAN IP Address of the device.
Subnet Mask	The LAN Subnet Mask of the device.
DHCP Server	Whether the DHCP server is Enabled or Disabled.

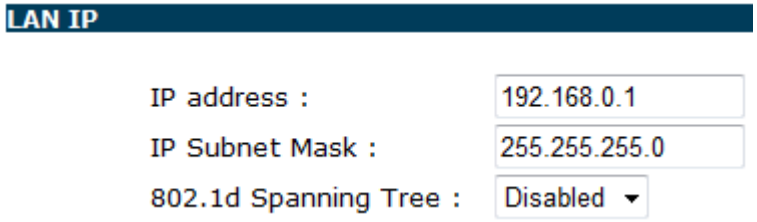


WLAN Settings	
Channel:	The wireless channel in use.
ESSID:	The SSID (Network Name) of the wireless network. (up to 4 SSID's are supported)
Security:	Wireless encryption is enabled for this SSID.
BSSID:	The MAC address of this SSID.
Associated Clients:	The number of wireless clients connected to this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

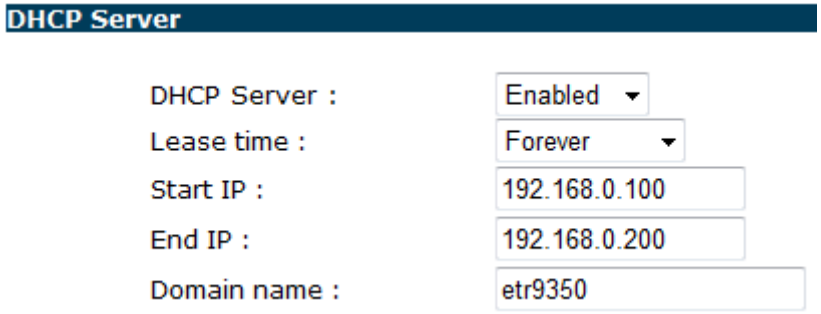
LAN

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

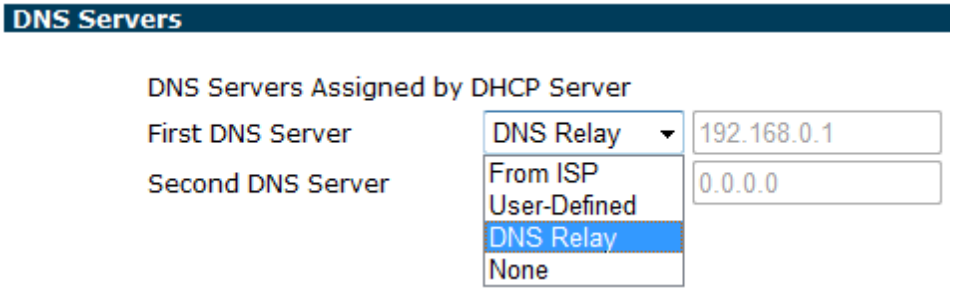




LAN IP	
IP address:	The LAN IP Address of this device.
IP Subnet Mask:	The LAN Subnet Mask of this device.
802.1d Spanning Tree:	When Enabled, the Spanning Tree protocol will prevent network loops in your LAN network.



DHCP Server	
DHCP Server:	The DHCP Server automatically allocates IP addresses to your LAN devices.
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 devices.
Domain name:	The domain name for this LAN network.

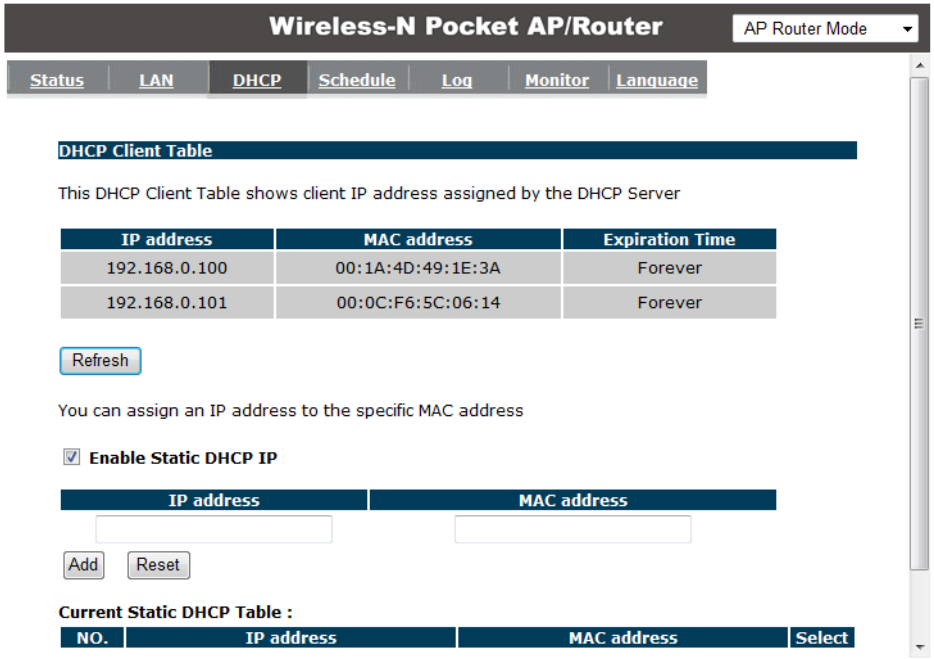


Two DNS servers can be assigned for use by your LAN devices.
There are three modes available.

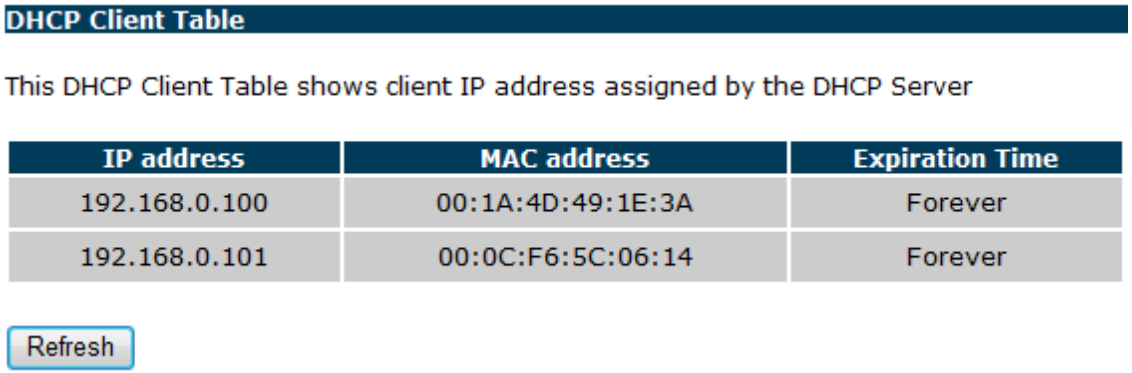
DNS Servers	
From ISP:	The DNS server IP address is assigned from your ISP.
User-Defined:	The DNS server IP address is assigned manually.
DNS Relay:	LAN clients are assigned the device's IP address as the DNS server. DNS requests are relayed to the ISP's DNS server.

DHCP

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

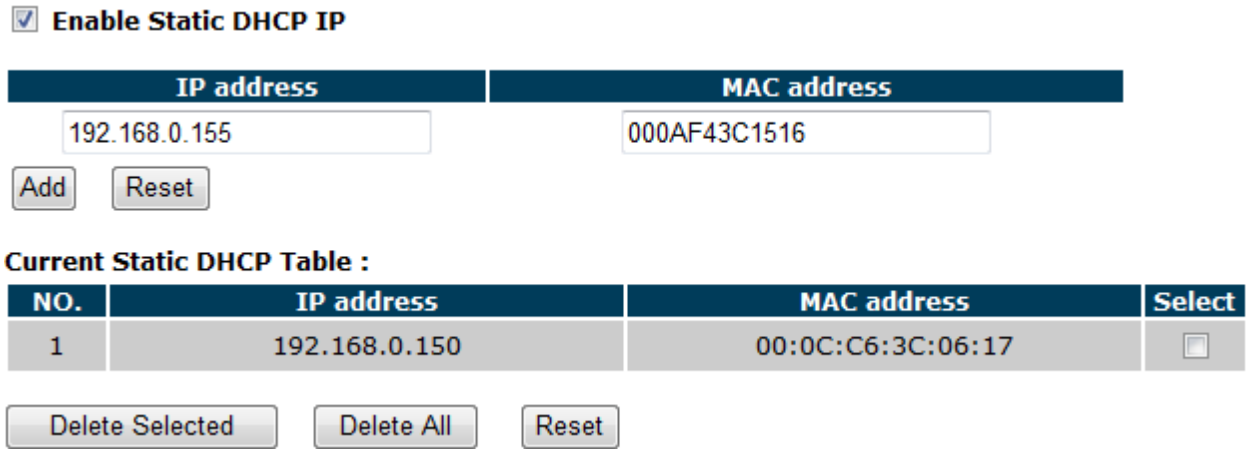


The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server



.

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.



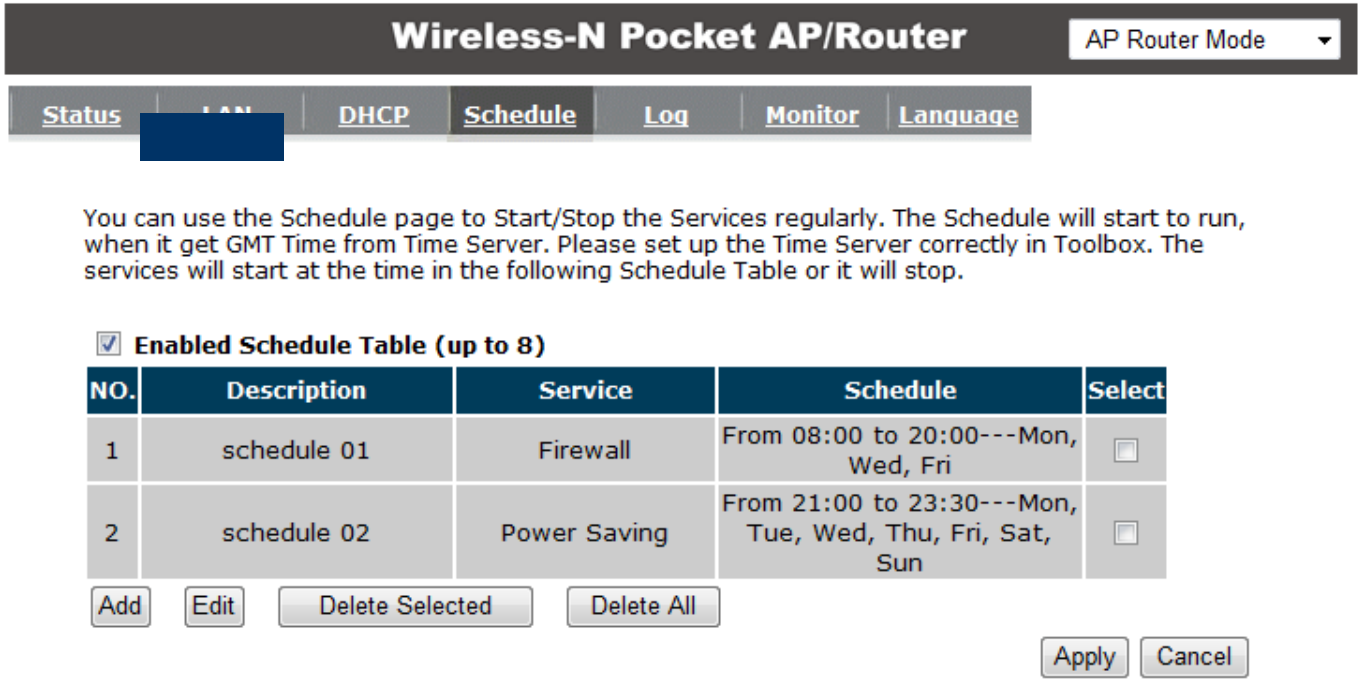
You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

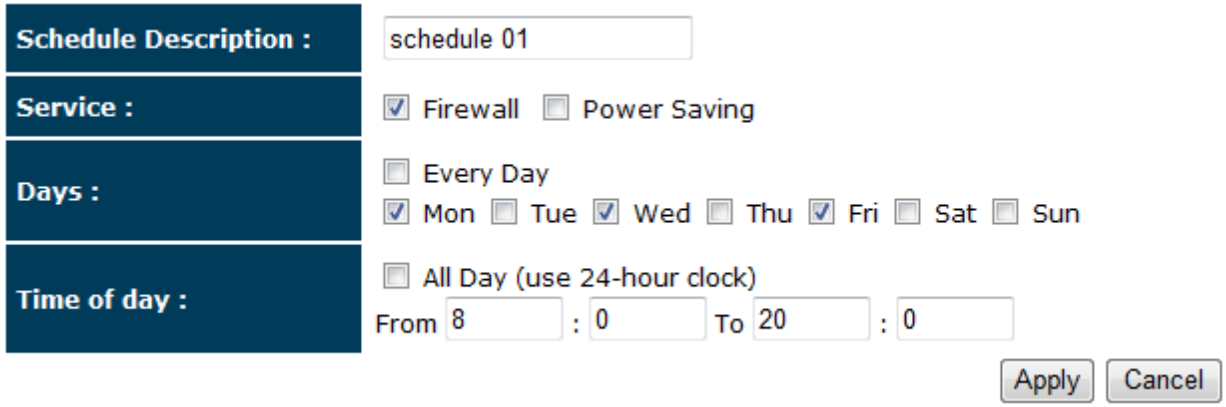
Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

Schedule

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

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

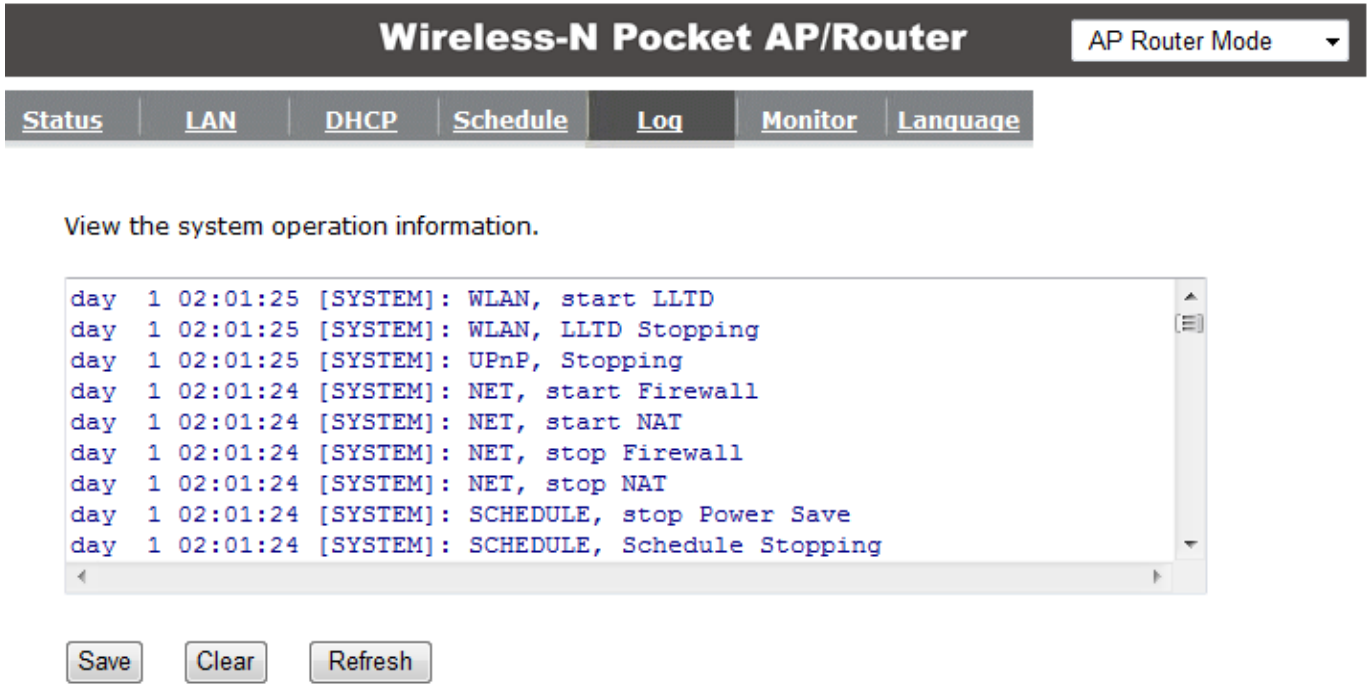




Schedule	
Schedule Description:	Assign a name to the schedule.
Service:	The service provides for the schedule.
Days:	Define the Days to activate or deactivate the schedule.
Time of day:	Define the Time of day to activate or deactivated the schedule. Please use 24-hour clock format.

Log

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

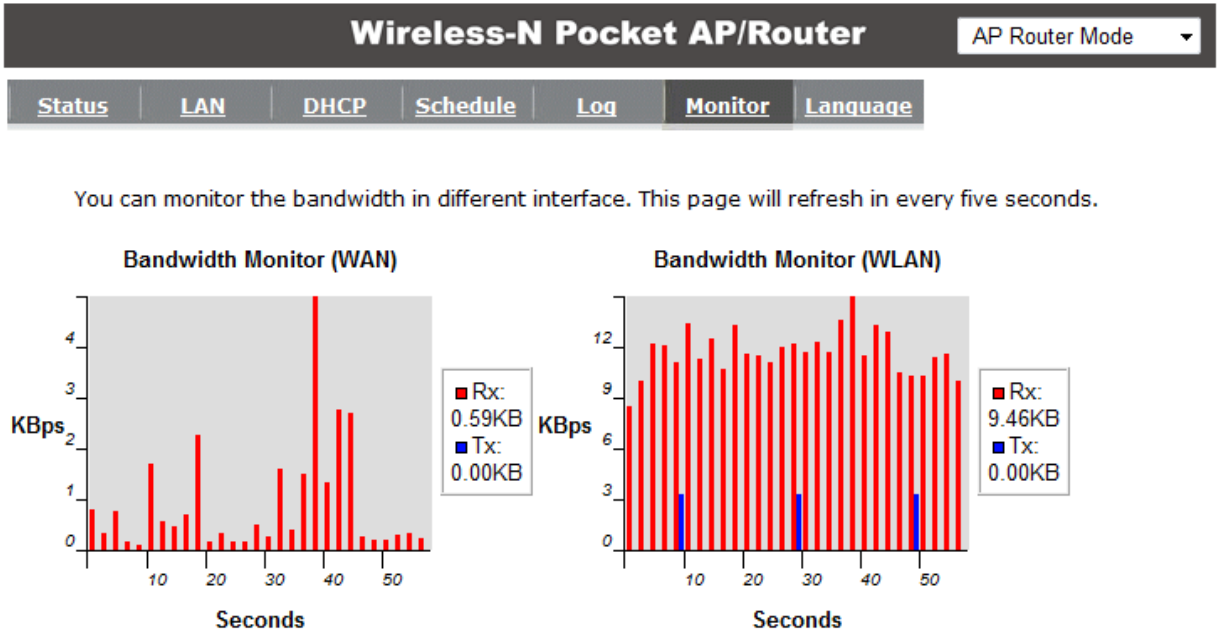


Log	
Save:	Save the log to a file.
Clear:	Clears the log.
Refresh:	Updates the log.

Monitor

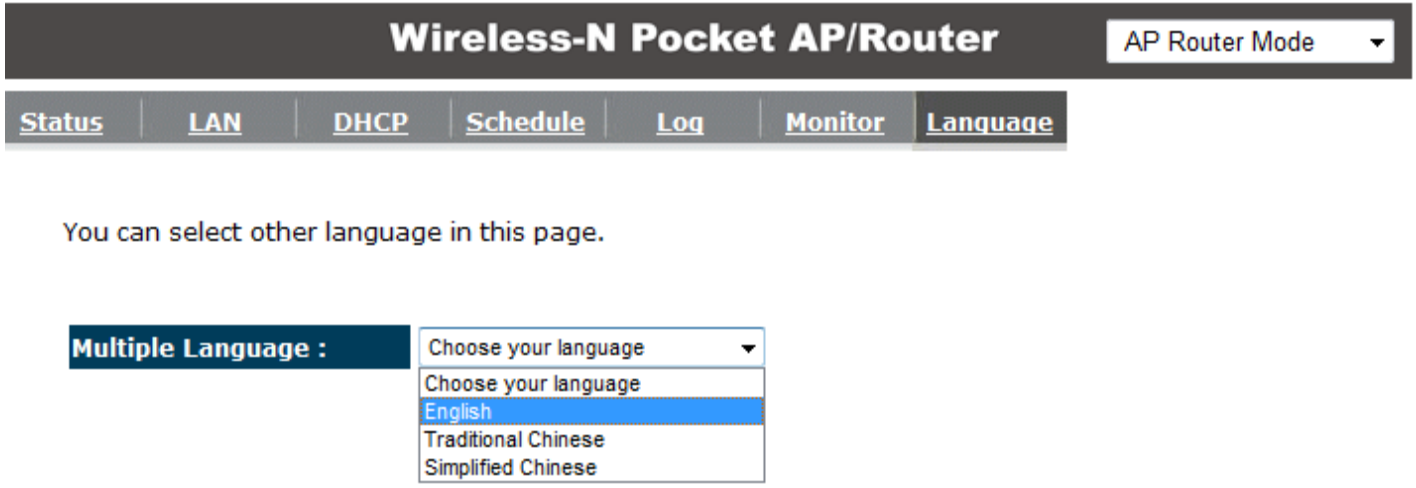
This page shows a histogram of the WAN and Wireless LAN traffic.

The information is automatically updated every five seconds.



Language

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

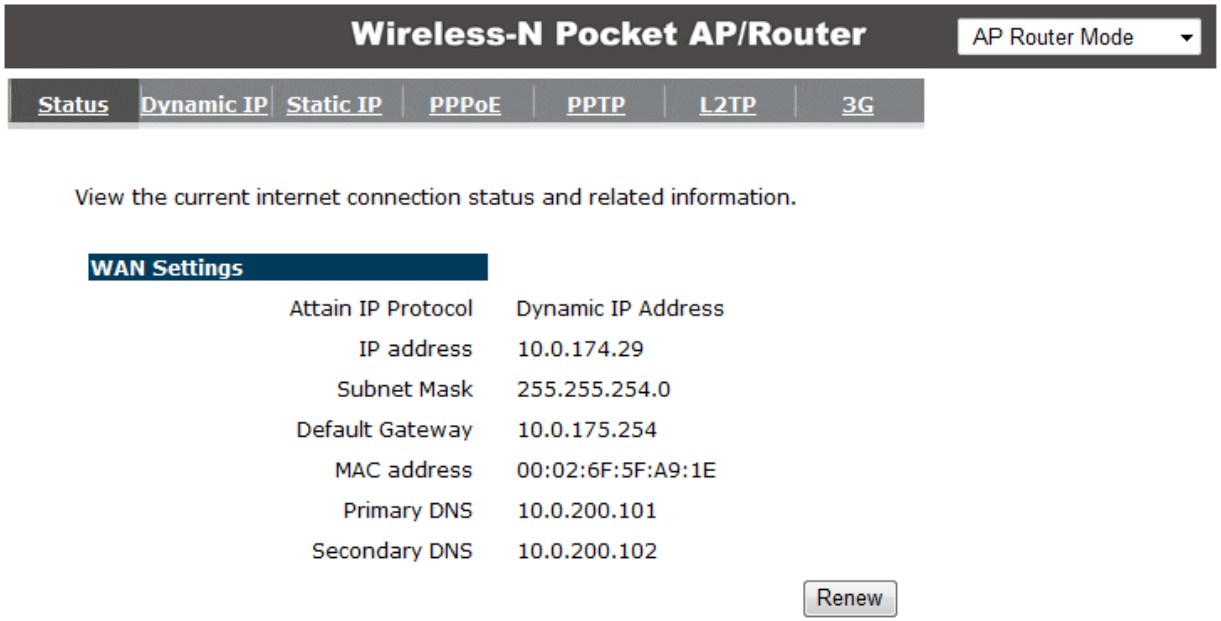


8.2.2 Internet

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

Status

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

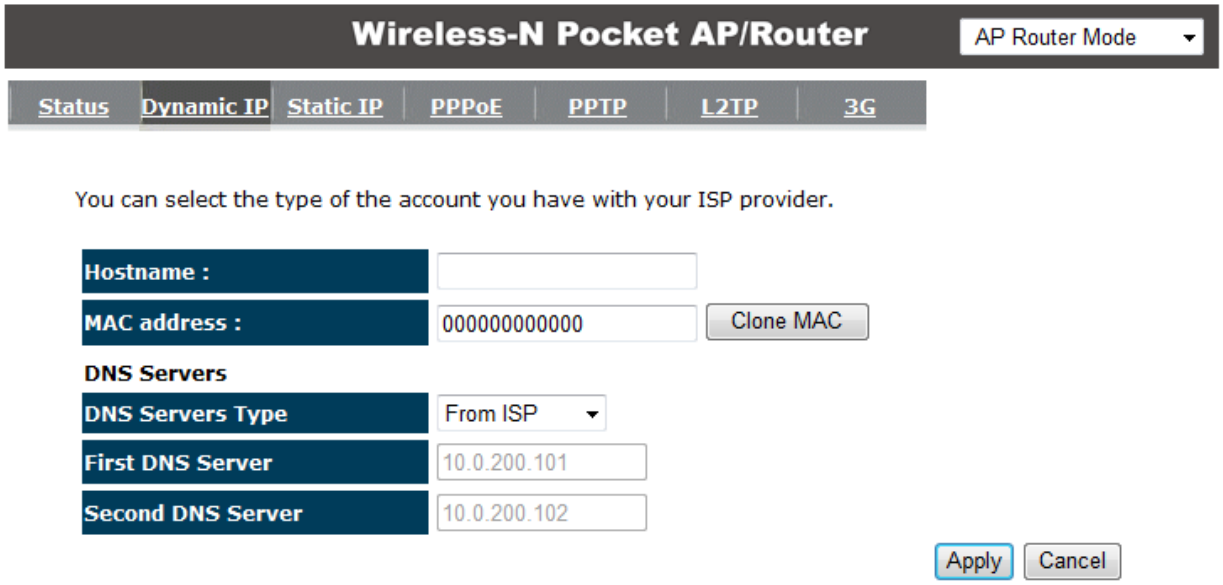


Dynamic IP Address

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.

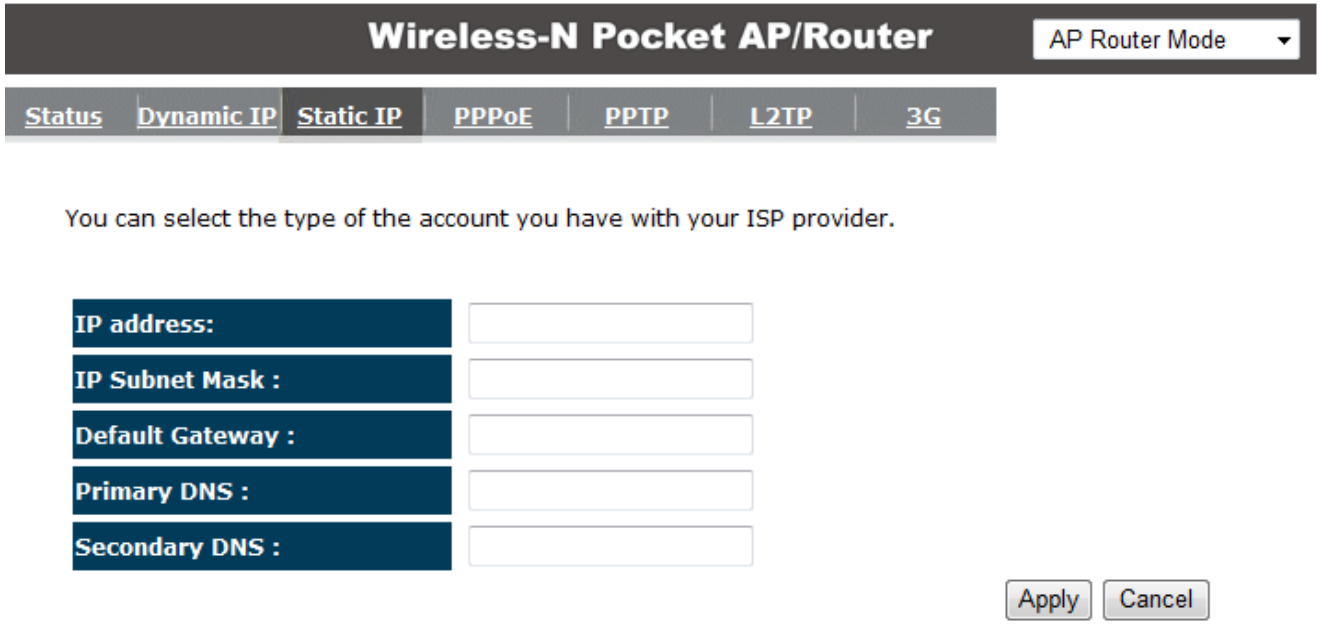
This will replace the AP Router MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.



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.

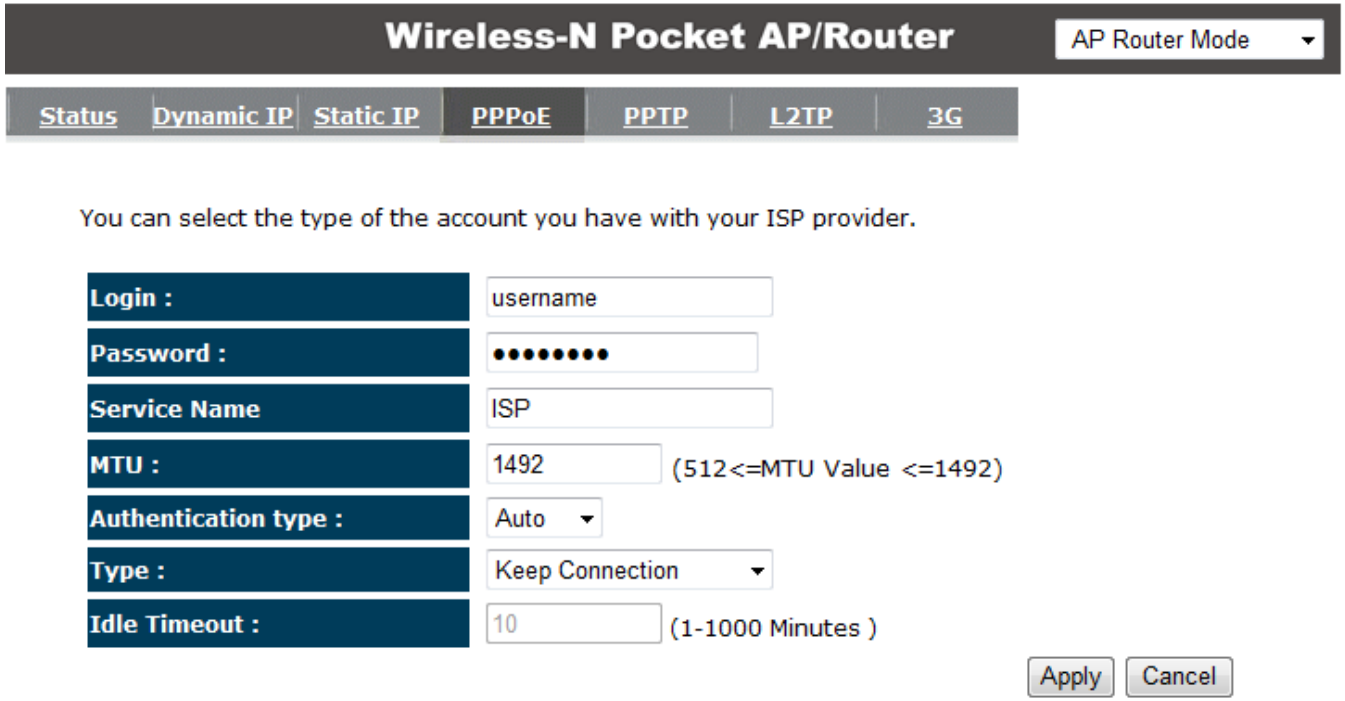
Static IP Address

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.


Wireless-N Pocket AP/Router
AP Router Mode
Status
Dynamic IP
Static IP
PPPoE
PPTP
L2TP
3G
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 :
Apply
Cancel

PPP over Ethernet

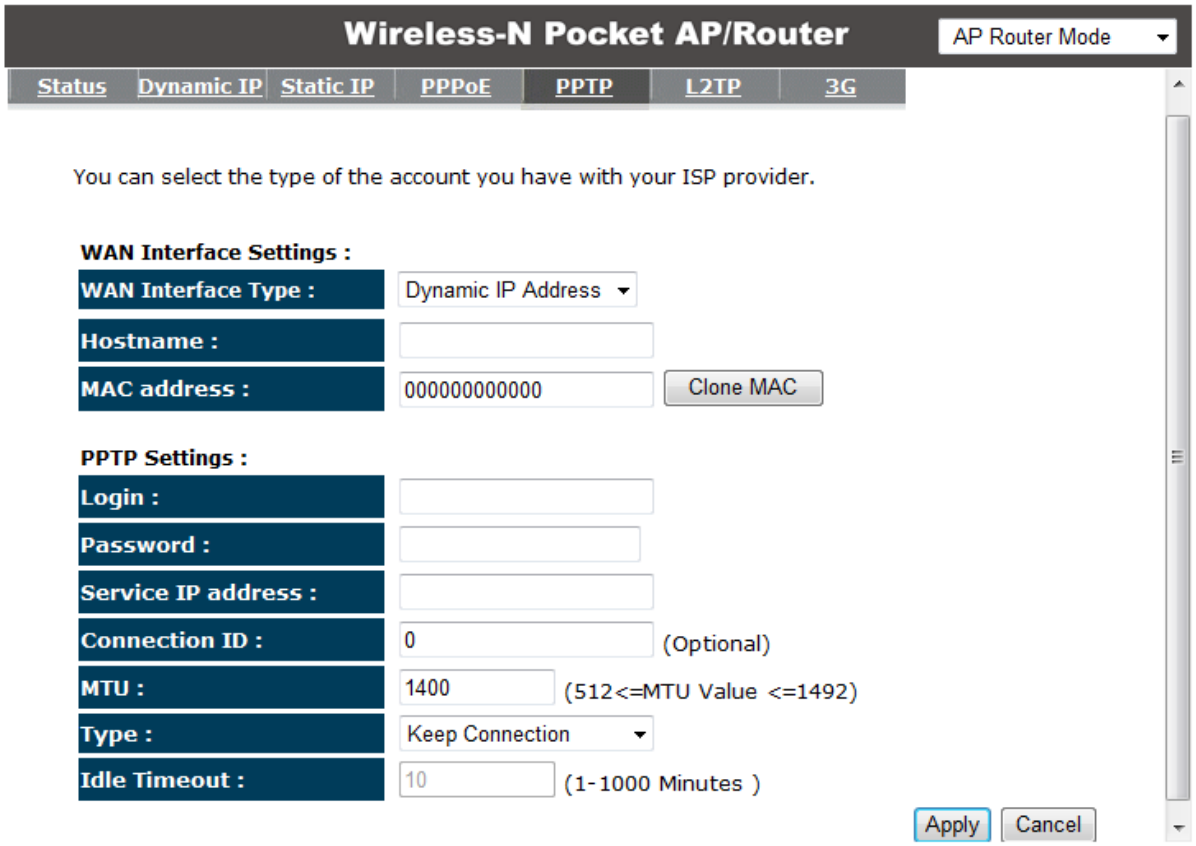
ISP requires an account username and password.



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.

Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by some ISPs.

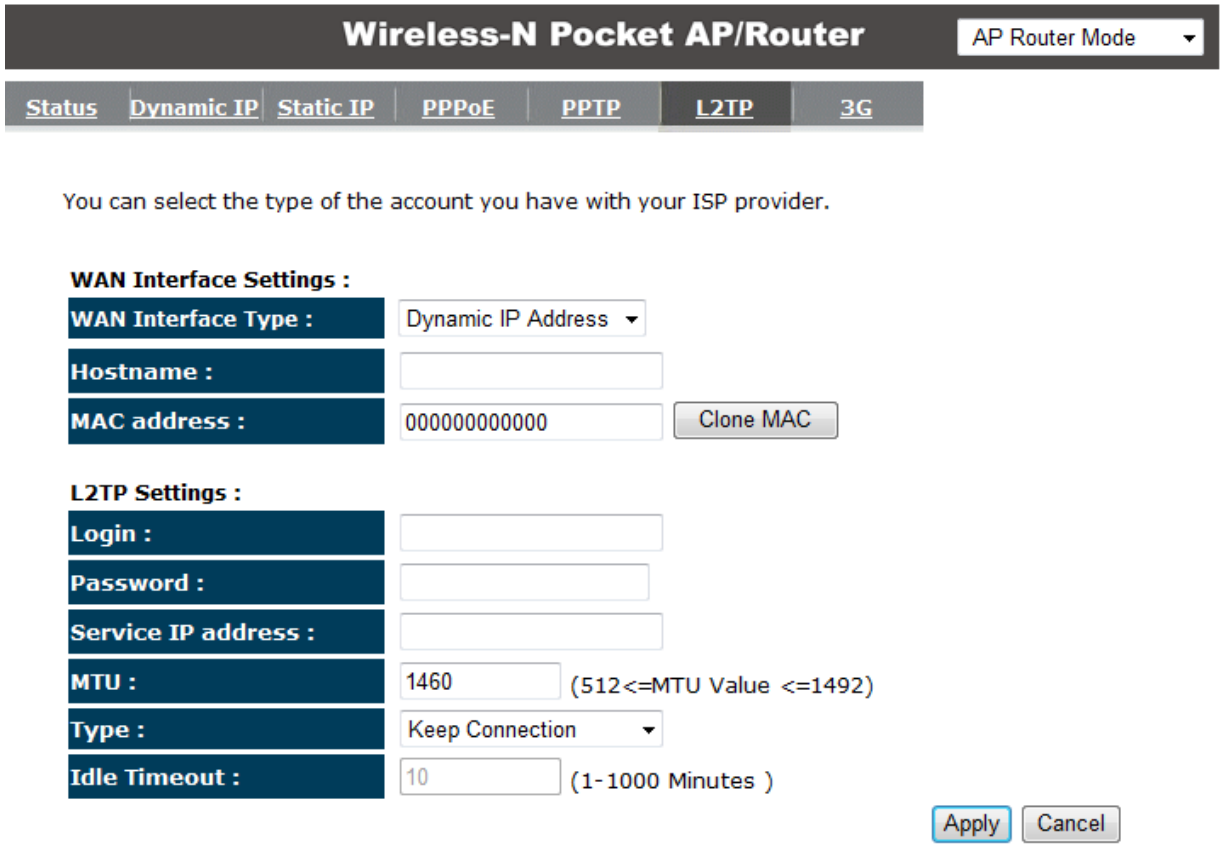


Point-to-Point Tunneling Protocol (PPTP)	
WAN Interface Type:	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.

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

Layer-2 Tunneling Protocol (L2TP)

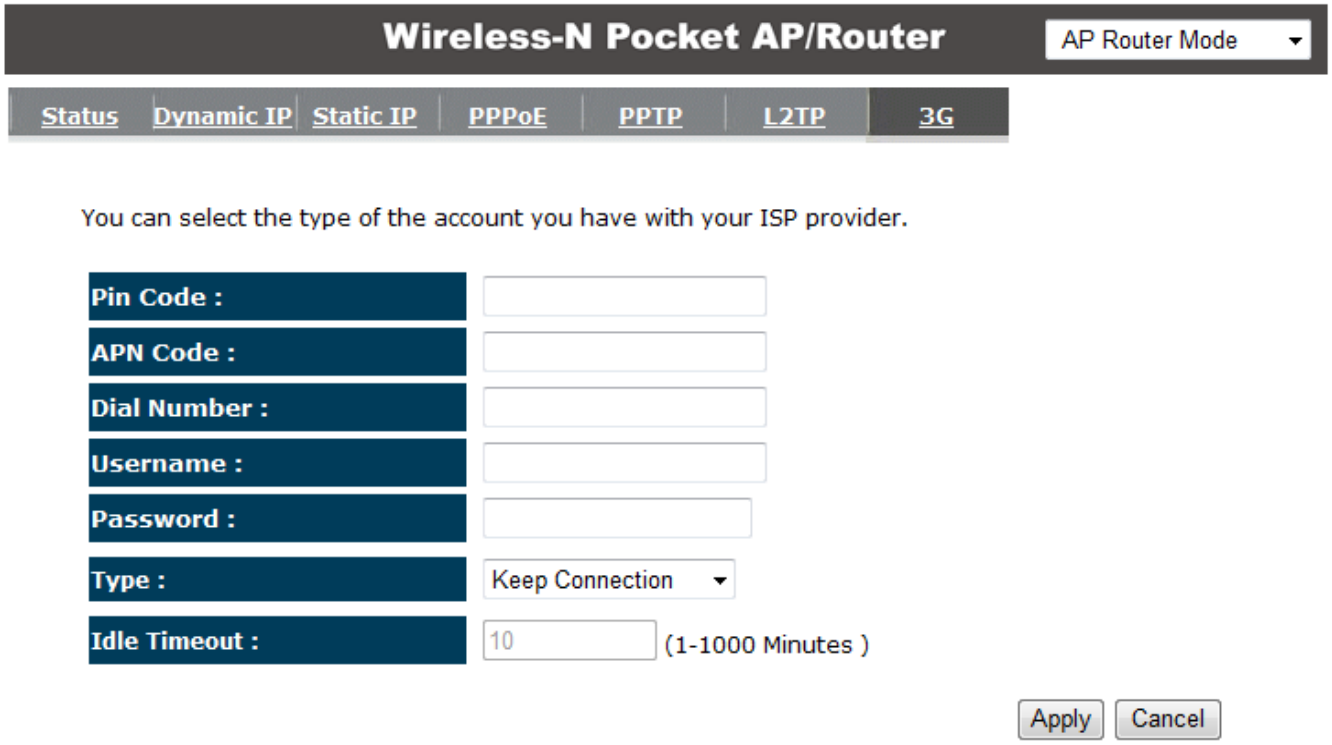
L2TP is used by some ISPs.



Layer-2 Tunneling Protocol (L2TP)	
WAN Interface Type:	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP
MAC:	The MAC Address that is used to connect to the ISP.
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.
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.

Mobile 3G

Please ensure your 3G USB card is connected to the TRAVEL ROUTER and has an active USIM card inserted.



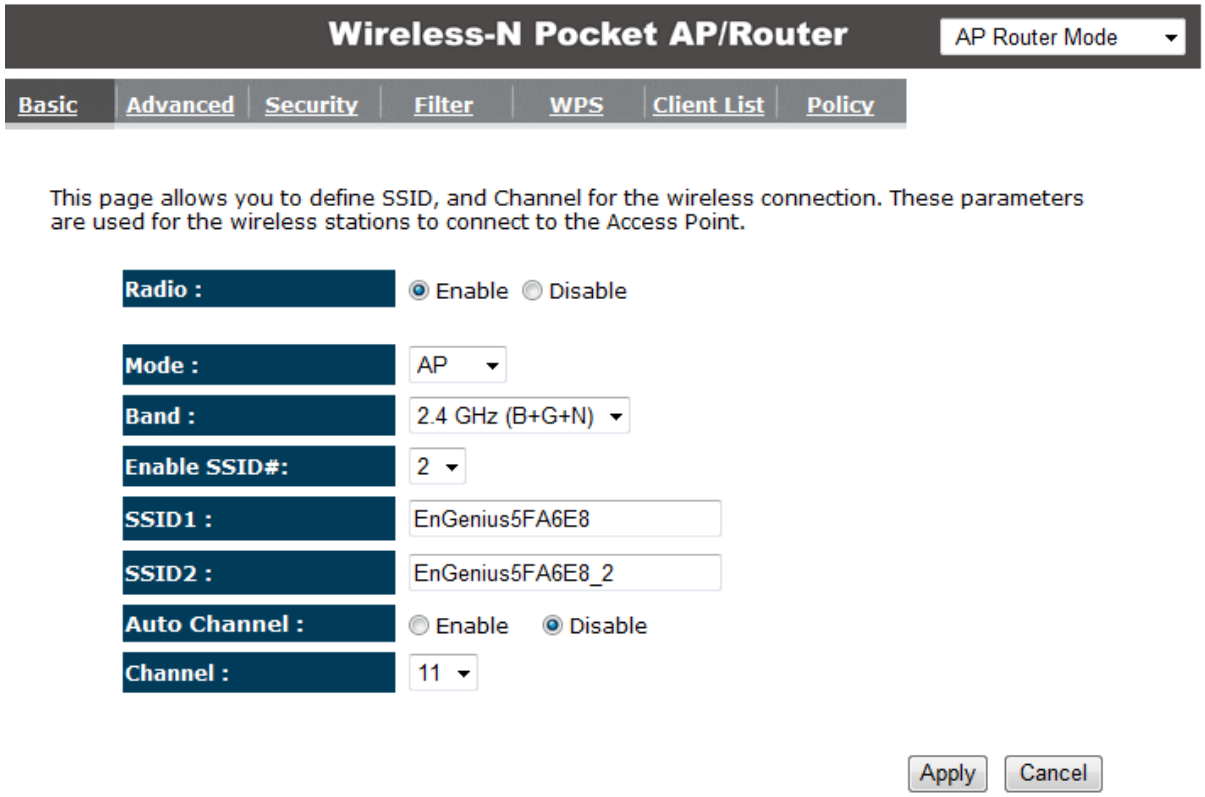
Mobile 3G	
Pin Code:	Enter the Pin code for your USIM card if required.
APN Code:	Enter the APN code for the network provider
Dial Number:	Only required if specified by ISP
User Name:	Account Username. Only required if specified by ISP
Password:	Account Password. Only required if specified by ISP
Type:	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.

8.2.3 Wireless

The Wireless section allows you to configure the Wireless settings.

Status

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



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)** 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.

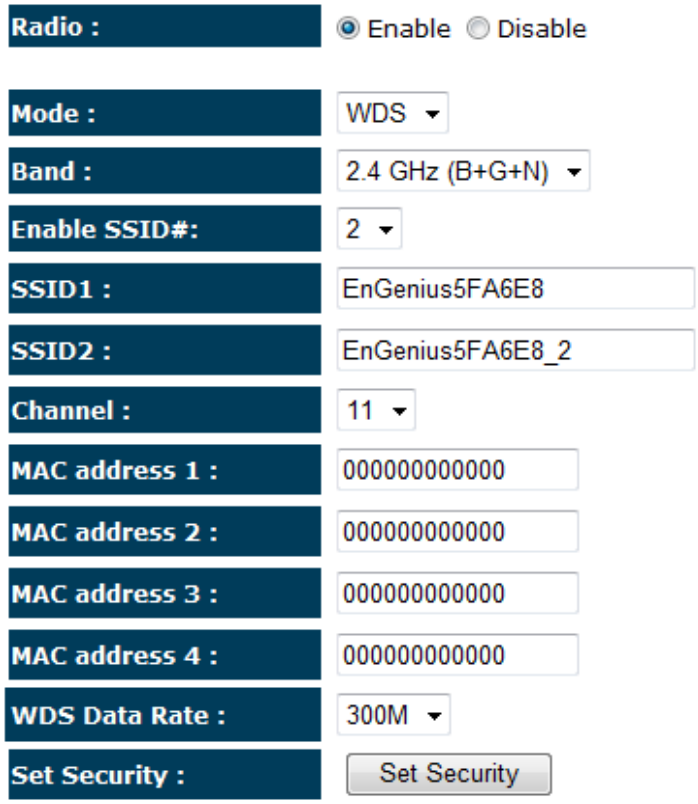
Wireless Distribution System (WDS)

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.

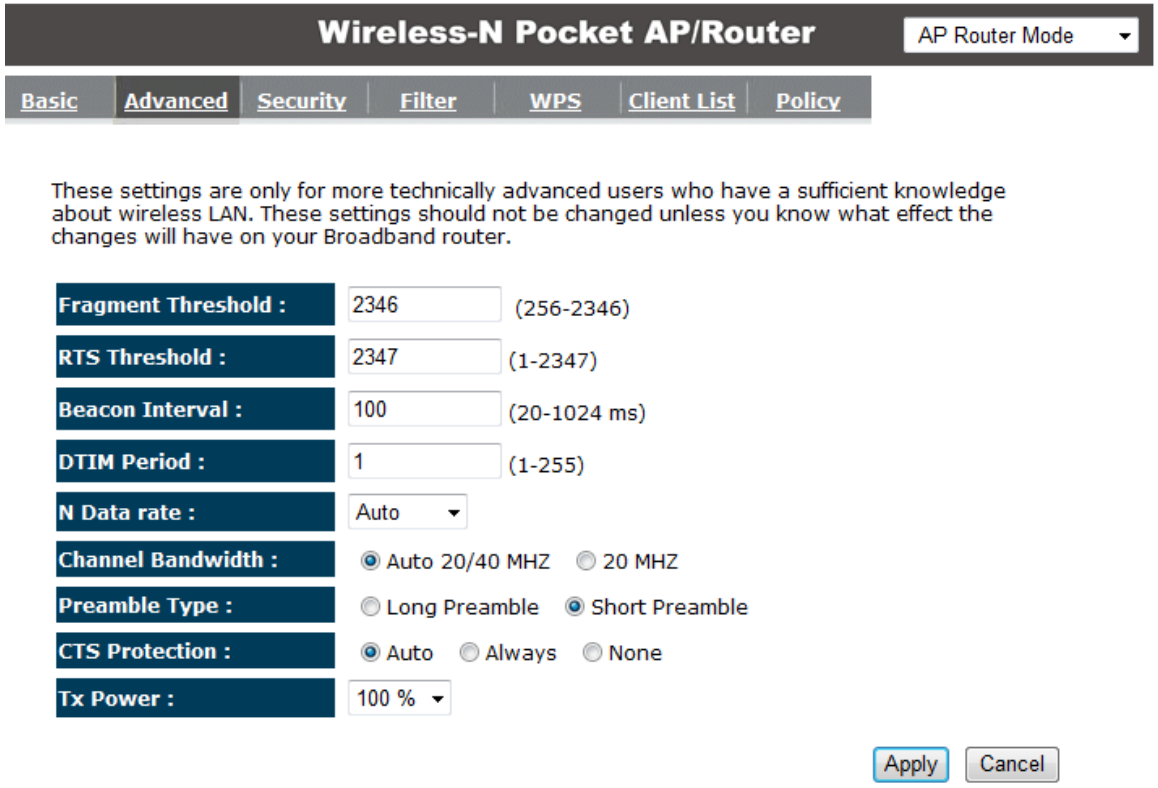
Also note that all Access Points in the WDS network needs to use the same Channel and Security settings.

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.



Advanced

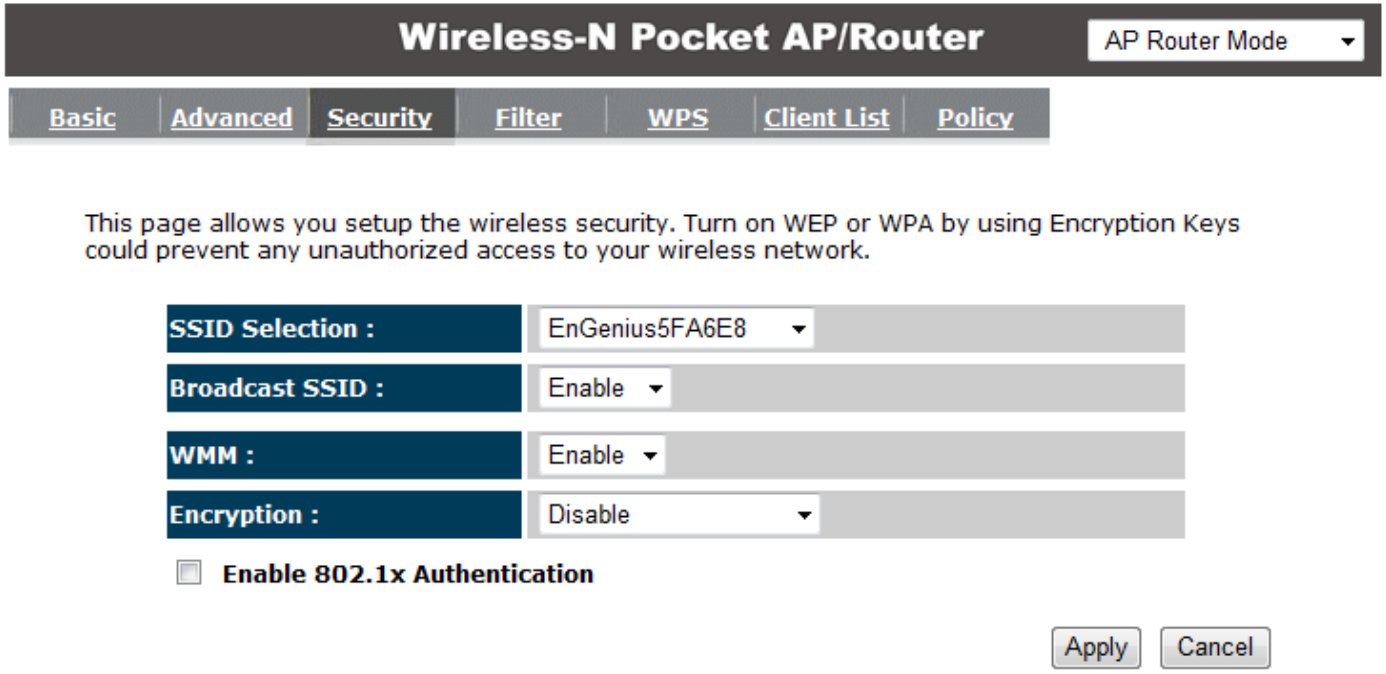
This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.



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.

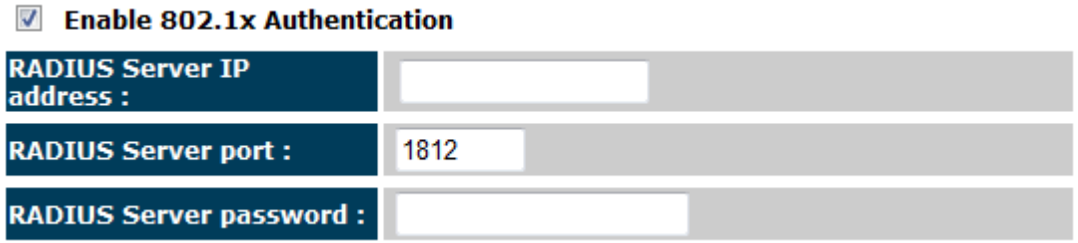
Security

This page allows you to set the wireless security settings.



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:	WiFi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, 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.

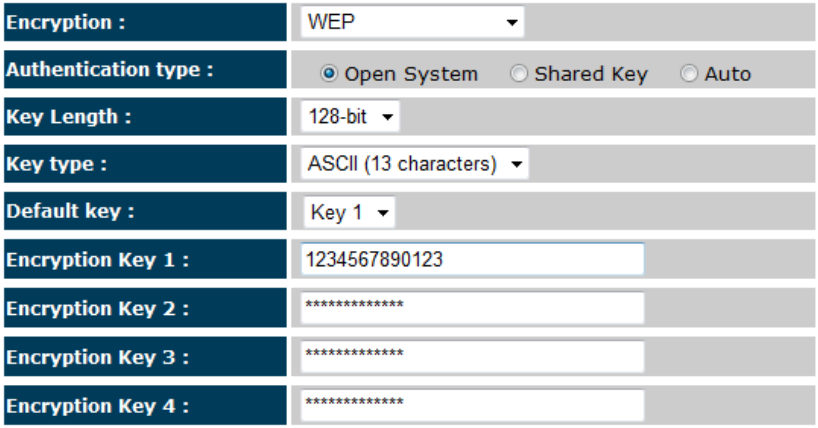
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.



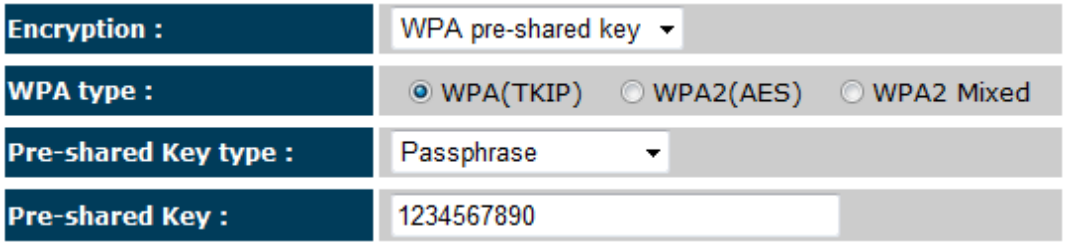
802.1x Authentication	
RADIUS Server IP Address:	The IP Address of the RADIUS Server
RADIUS Server port:	The port of the RADIUS Server.
RADIUS Server password:	The RADIUS Server's password.

WEP Encryption:

WEP Encryption	
Authentication Type:	Please ensure that your wireless clients use the same authentication type.
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.

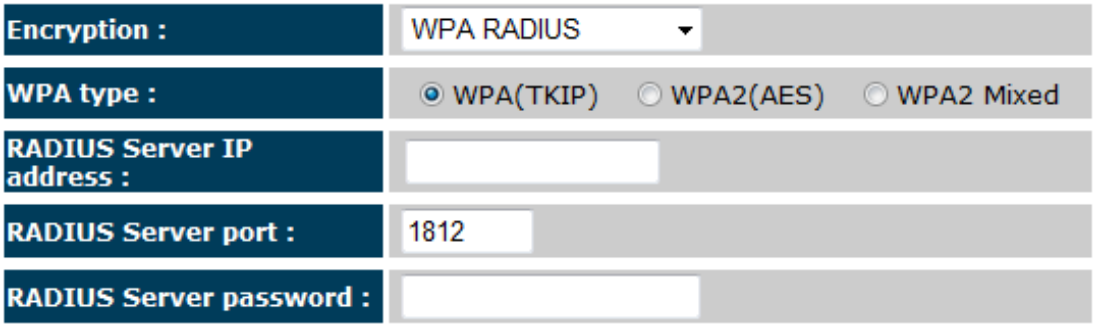


WPA Pre-Shared Key Encryption:



WPA 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.

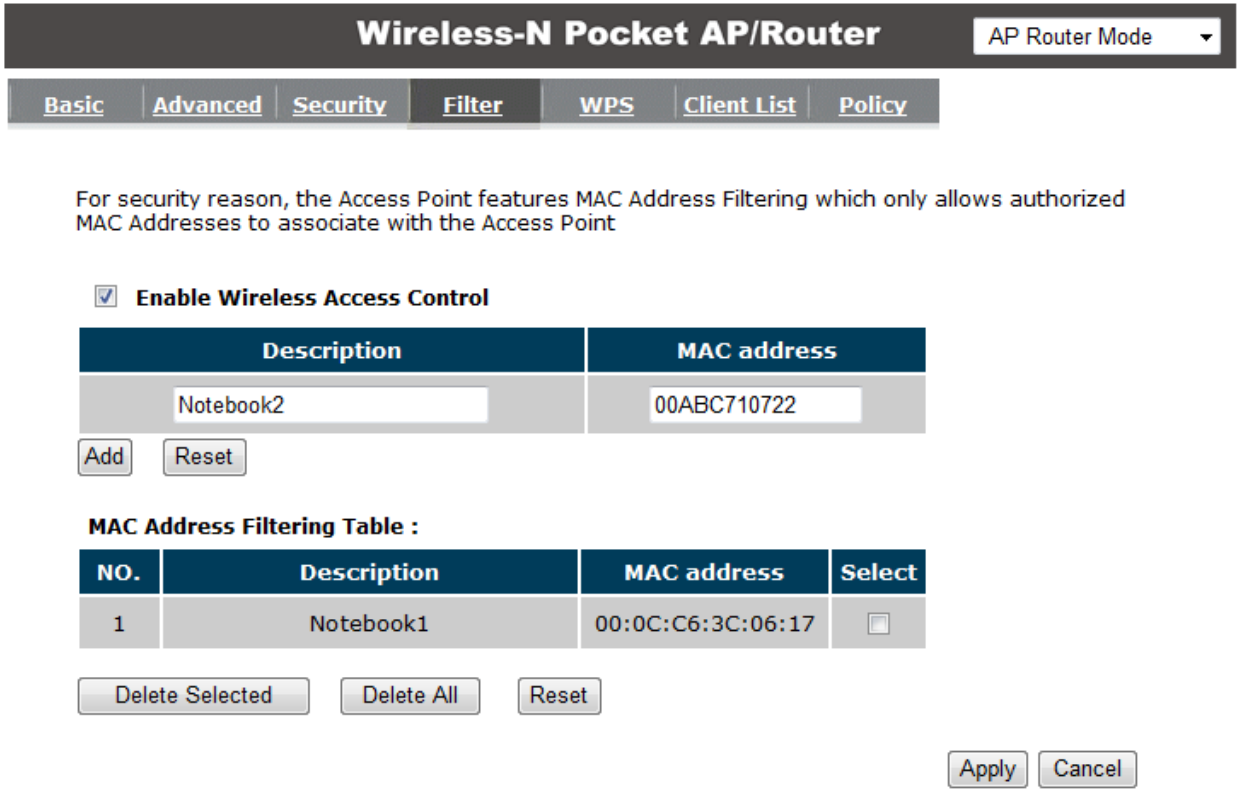
WPA RADIUS Encryption:



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.

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.

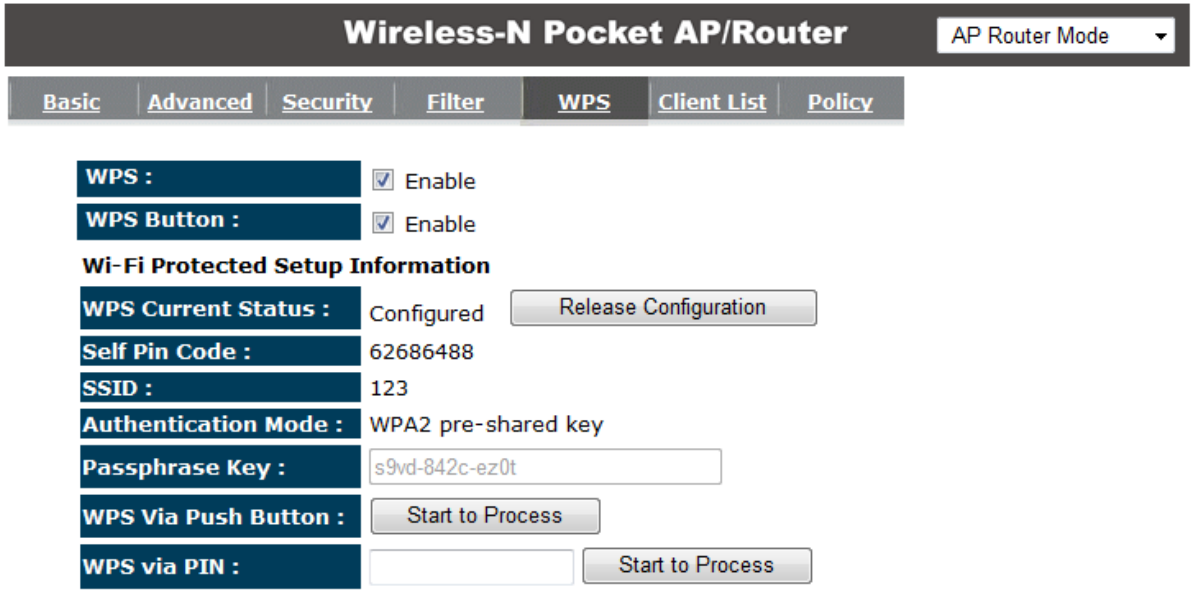


Wireless Filter	
Enable Wireless Access Control:	Tick the box to Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description:	Enter a name or description for this entry.
MAC address:	Enter the MAC address of the wireless client that you wish 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.

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.



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 **Unconfigured**. 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.

Initializing WPS Feature

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

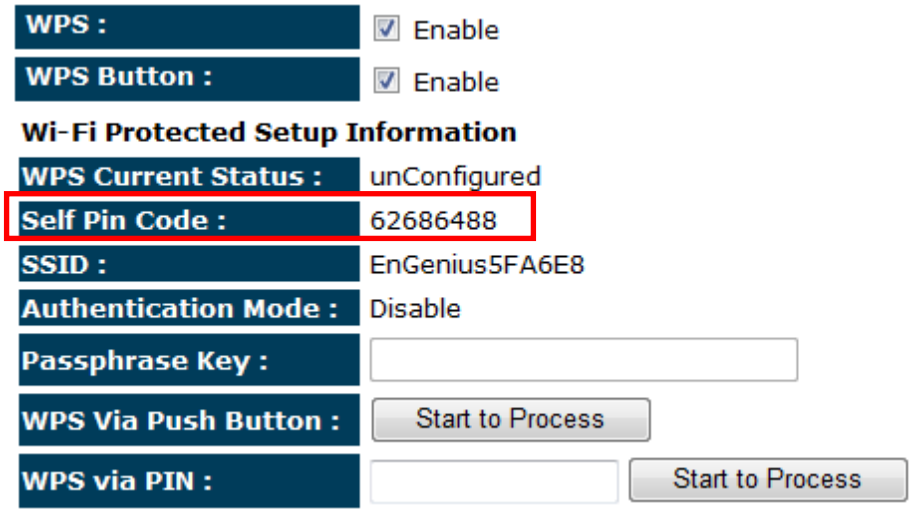
1. WPS Push Button Method

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

While the WPS LED is flashing on the TRAVEL 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 TRAVEL ROUTER device.

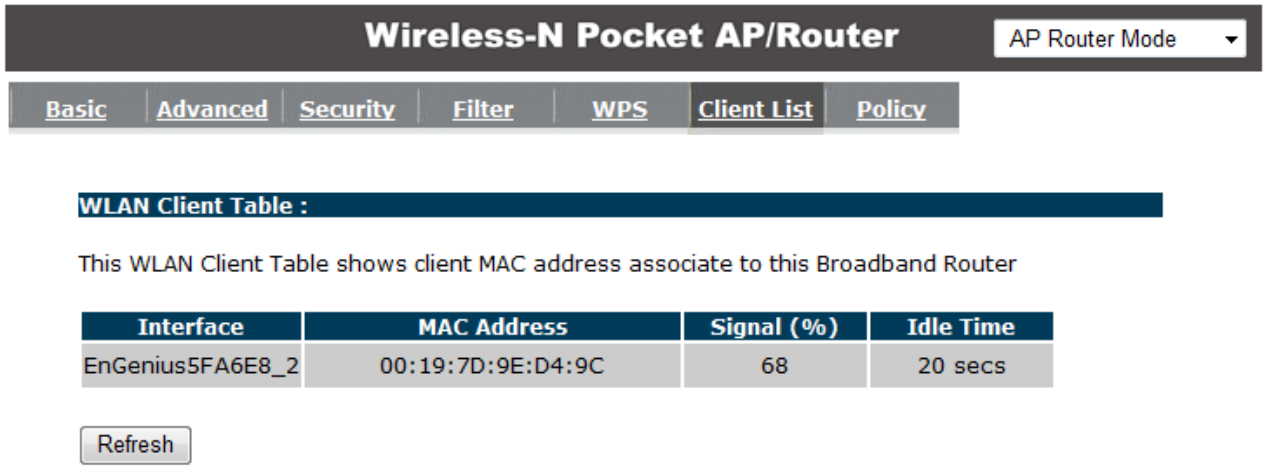


Please use this Pin code to initialize the WPS process from the wireless client configuration utility.

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

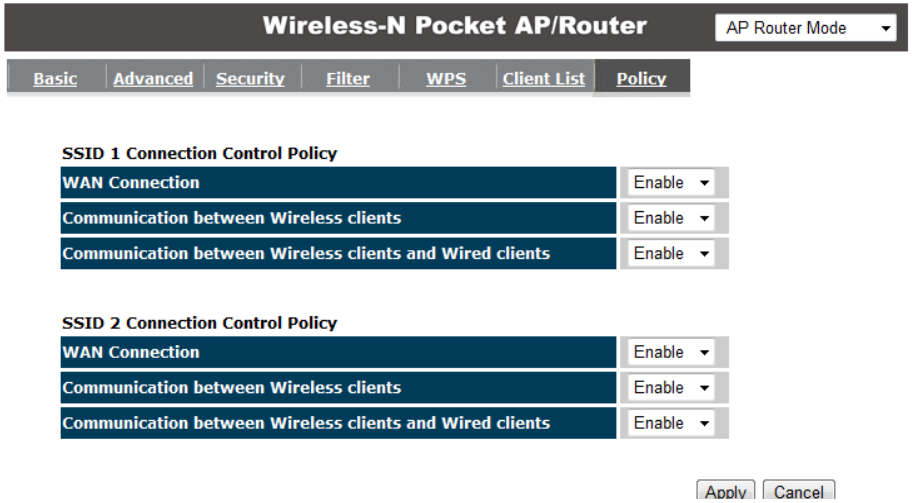
Client List

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



Policy

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



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.

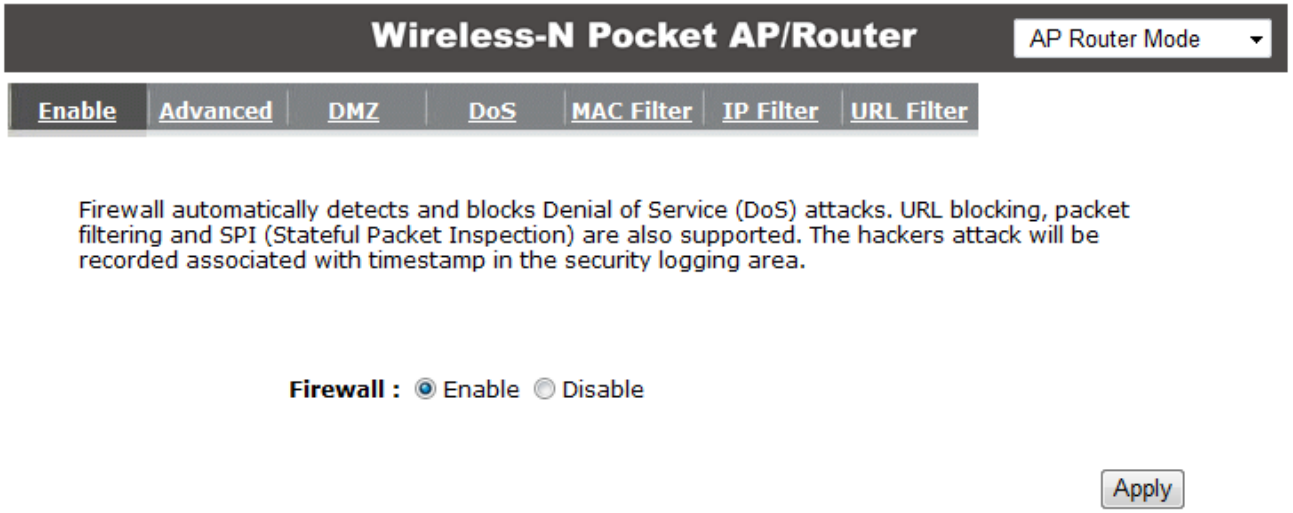
8.2.4 Firewall

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

Enable

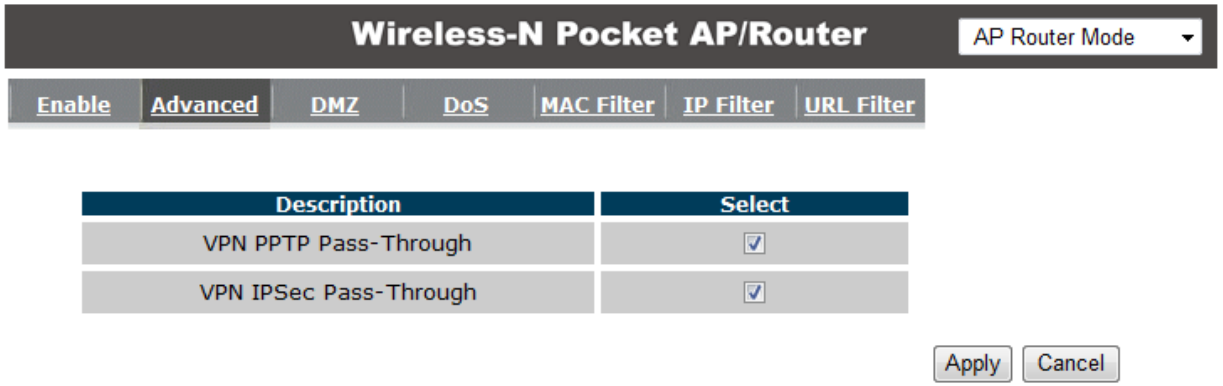
This page allows you to Enable / Disable the Firewall features.

When Enabled, Denial of Service (DoS) and SPI (Stateful Packet Inspection) features are also be enabled.



Advanced

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

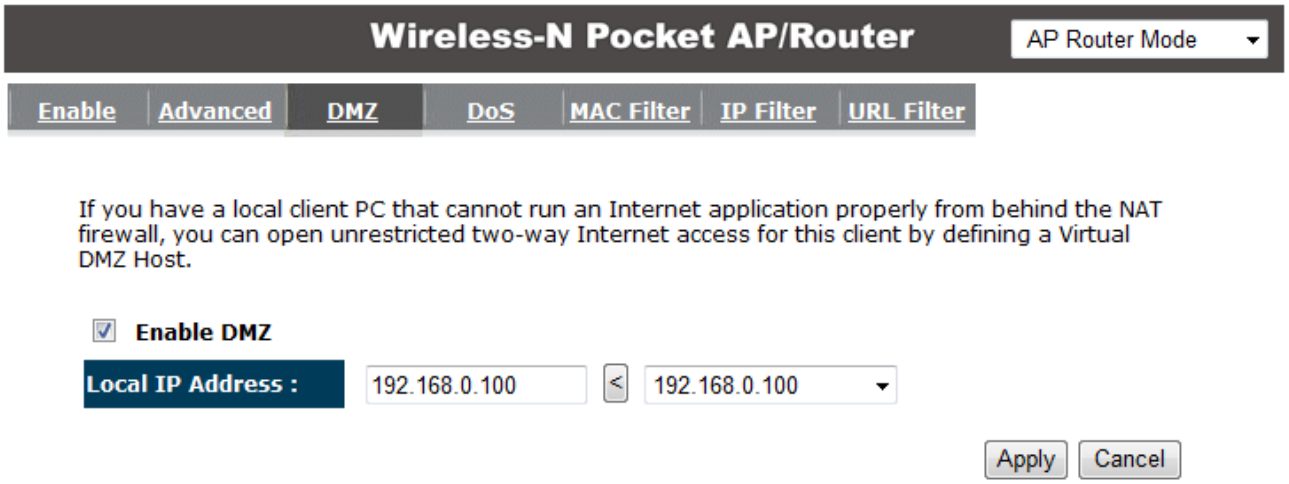


DMZ

This feature, if enabled, 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 “DMZ PC”
- 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”

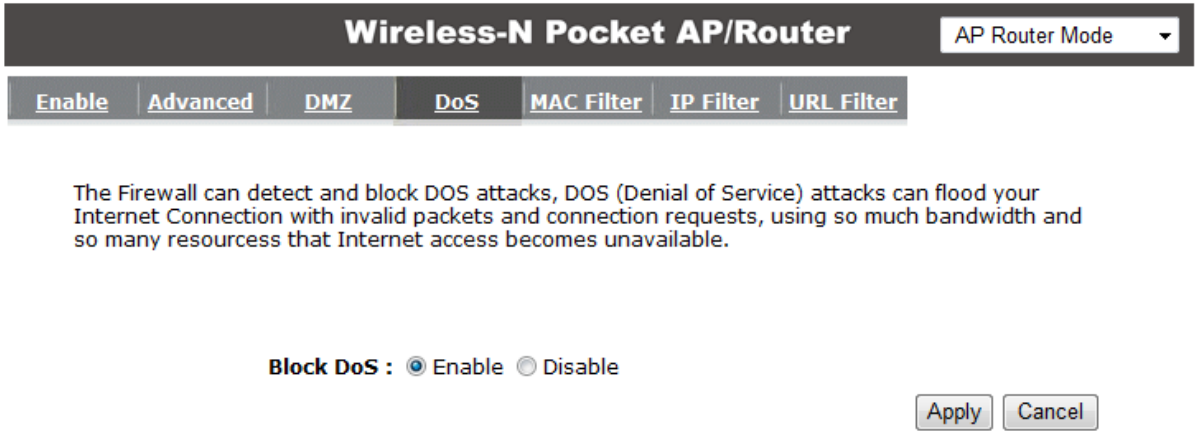
Note: The “DMZ PC” is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.



Denial of Service (DoS)

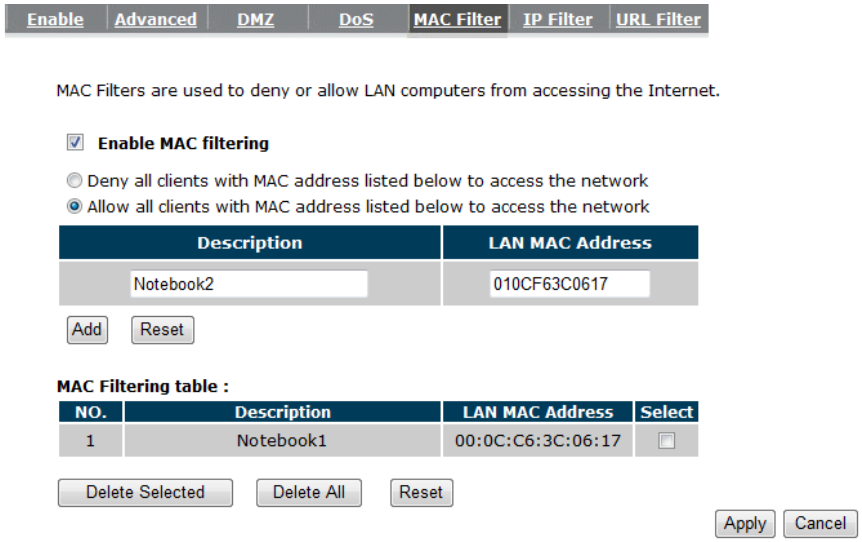
Denial of Service (Denial of Service) is a type of Internet attack that sends a high amount of data to you with the intent to overload your Internet connection.

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



MAC Filter

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

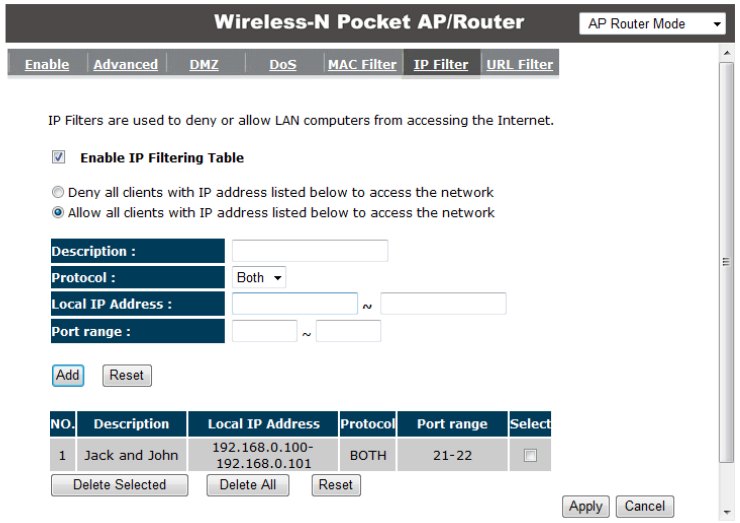


MAC Filter	
Enable MAC filtering:	Tick this box to Enable the MAC filtering feature.
Deny all clients with MAC addresses listed below to access the network:	When selected, the computers listed in the MAC Filtering table will be **Denied** access to the Internet.
Allow all clients with MAC addresses listed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

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.

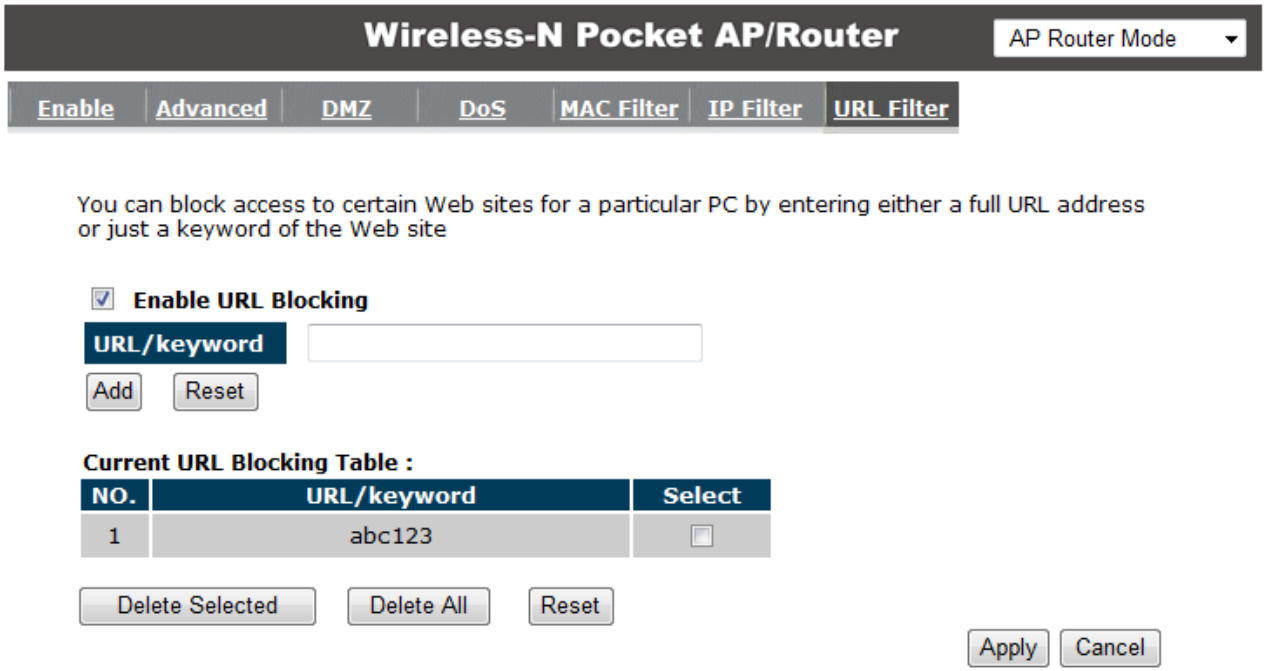


IP Filter	
Enable IP filtering:	Tick this box to Enable the IP filtering feature.
Deny all clients with IP addresses listed below to access the network:	When selected, the computers with IP addresses specified will be **Denied** access to the indicated Internet ports.
Allow all clients with IP addresses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

URL Filter

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

For example, “abc123” has been added to the URL Blocking Table. Any web address that includes “abc123” will be blocked.



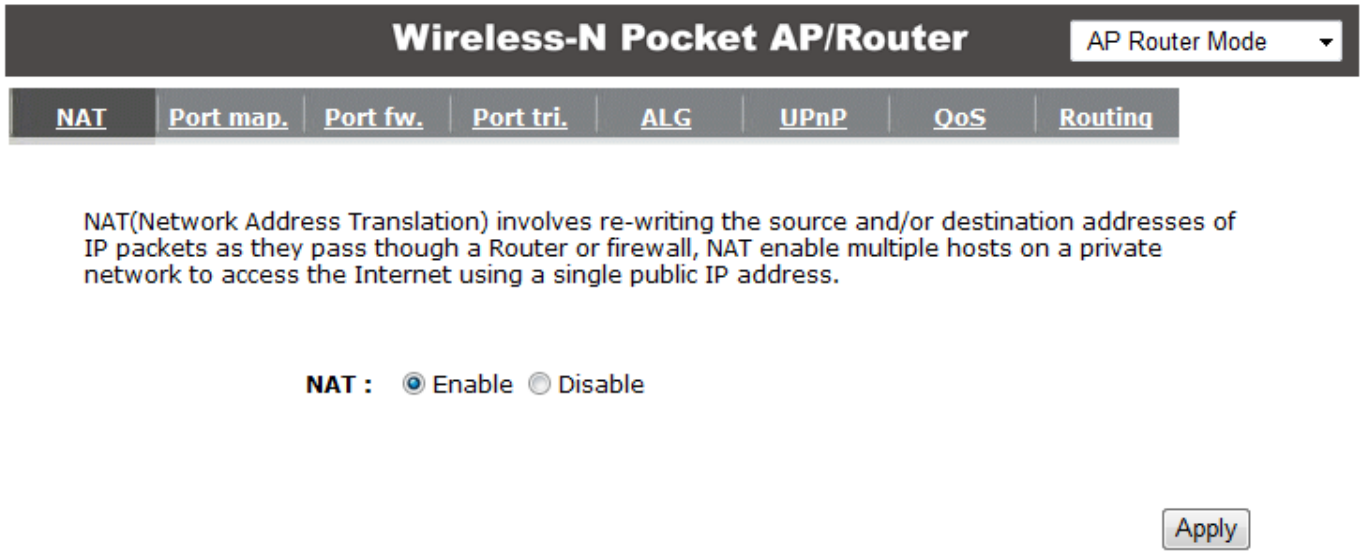
8.2.5 Advanced

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

Network Address Translation (NAT)

This page allows you to Enable / Disable the Network Address Translation (NAT) feature. The NAT is required to share one Internet account with multiple LAN users.

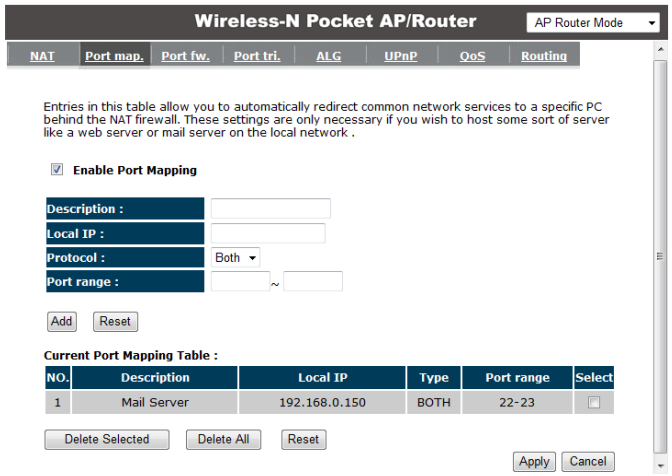
It also is required for certain Firewall features to work properly.



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 22 to 23.
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.



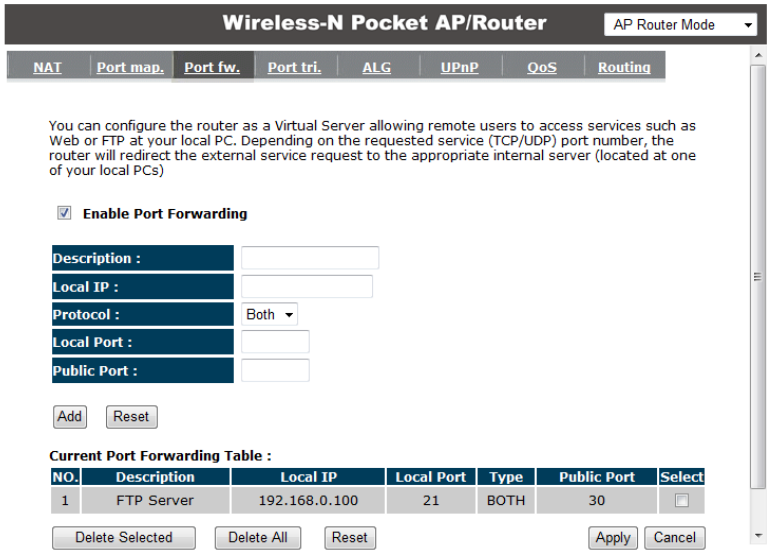
Port Mapping	
Enable Port Mapping	Tick this box to Enable the Port Mapping feature.
Description:	Enter a name or description to help you identify this entry.
Local IP:	The local IP address of the computer the server is hosted on.
Protocol:	Select to apply the feature to either TCP, UDP or Both types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

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 FTP Server running on port 21 on the LAN.
For security reasons, the Administrator would like to provide this server to Internet connection on port 30.

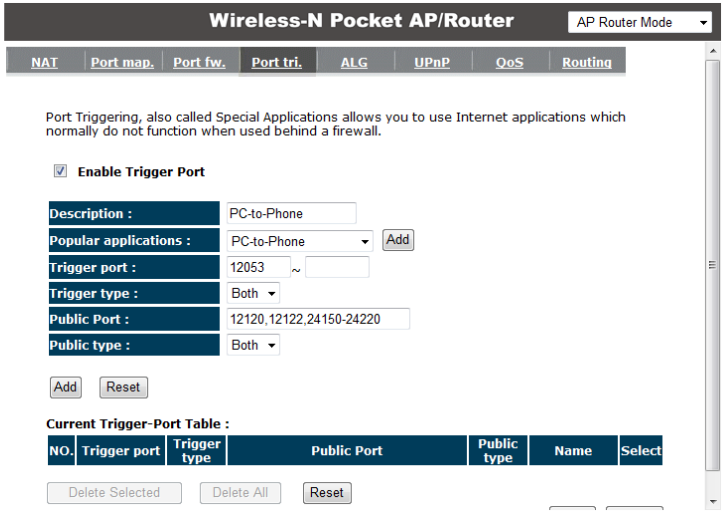
Therefore then there is a connection from the Internet on port 30, it will be forwarded to the computer with the IP address 192.168.0.100 and changed to port 21.



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.

Port Trigger

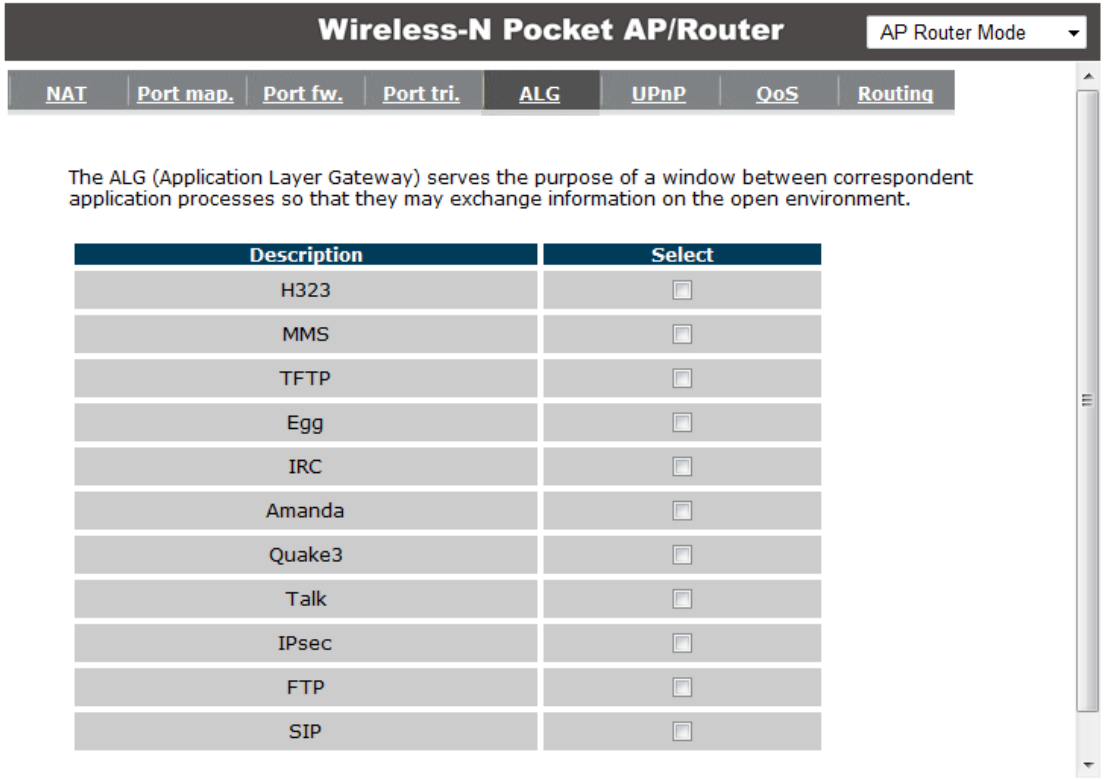
If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Trigger will be required for these applications to work.



Port 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.

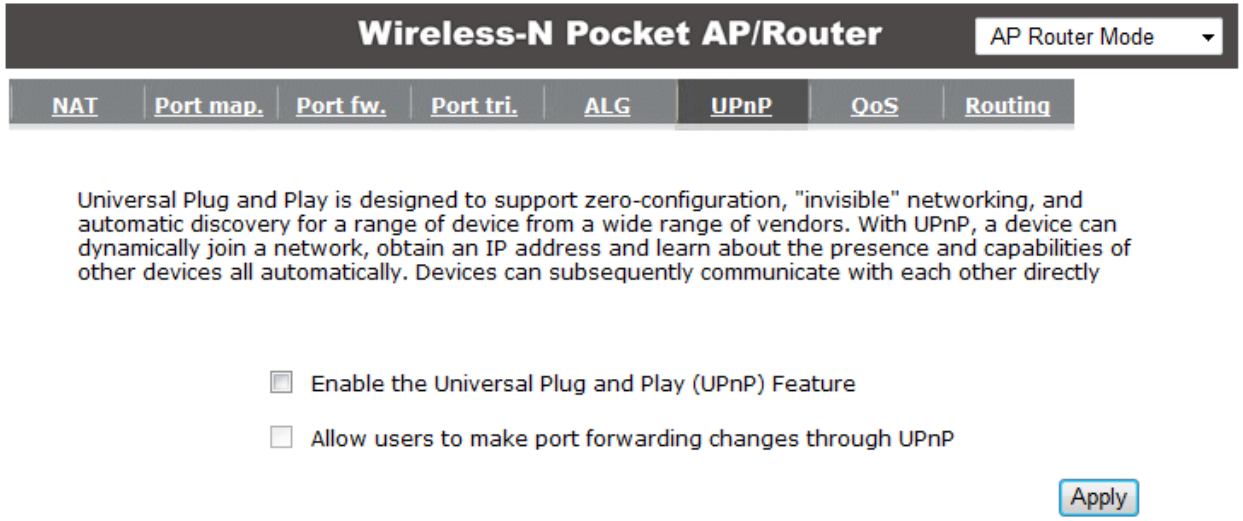
Application Layer Gateway (ALG)

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.



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.



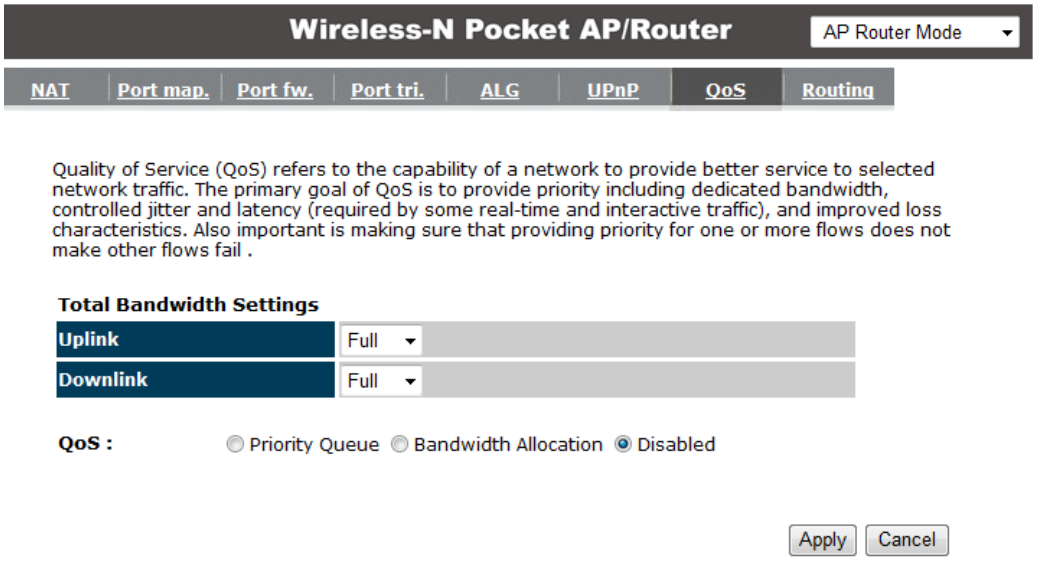
Universal Plug and Play (UPnP)	
Enable the UPnP Feature:	Tick this box to Enable the UPnP feature to allow supported devices to be visible on the network.
Allow users to make port forwarding changes through UPnP:	Tick this box to allow applications to automatically set their port forwarding rules to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

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.

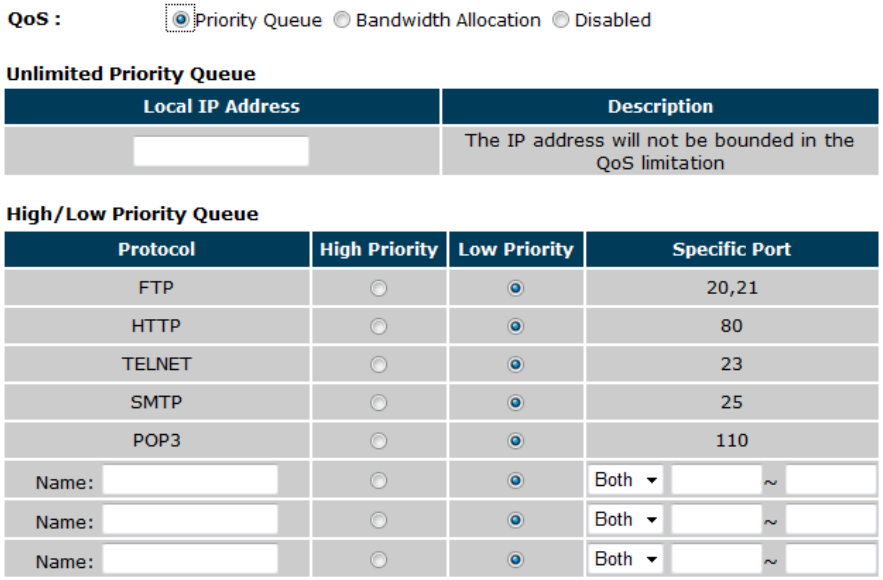
In order for this feature to function properly, the user should first set the Uplink and Downlink bandwidth provided by your Internet Service Provider.



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

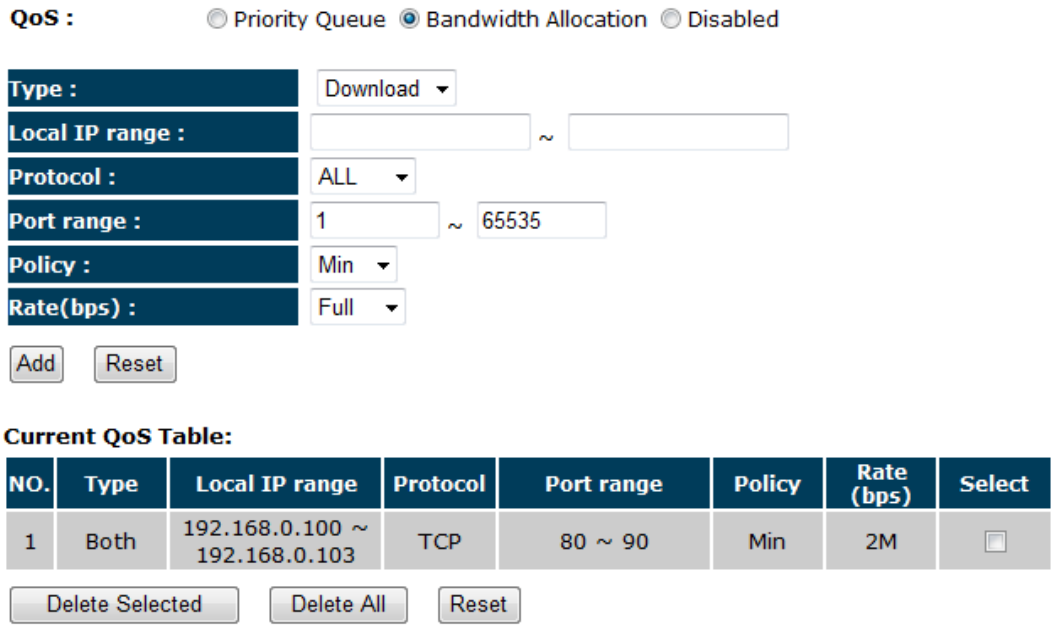
Bandwidth priority is set to either High or Low. The transmissions in the High queue will be processed first.



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.

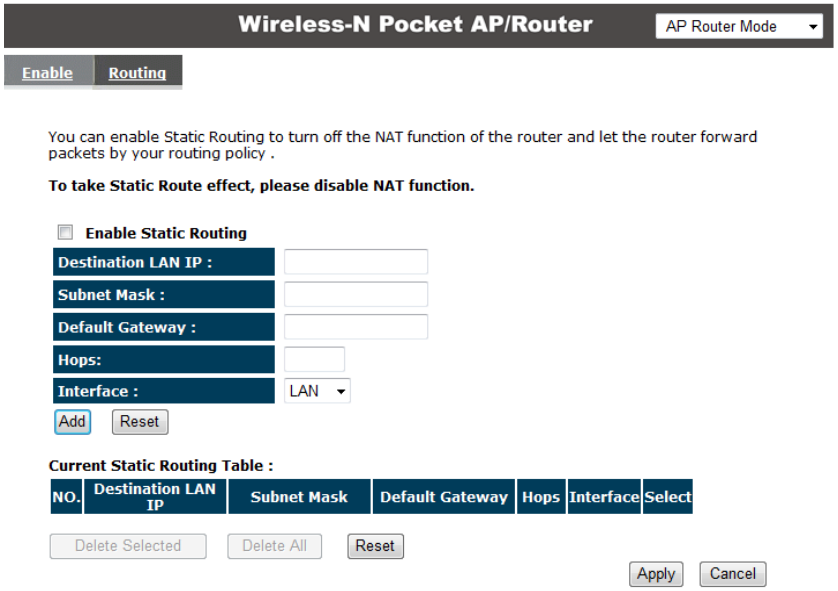


Bandwidth Allocation	
Type:	Set whether the QoS rules apply to transmission that are Download, Upload or Both directions.
Local IP range:	Enter the IP address range of the computers that you would like the QoS rules to apply to.
Protocol:	Select from this list of protocols to automatic set the related 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.

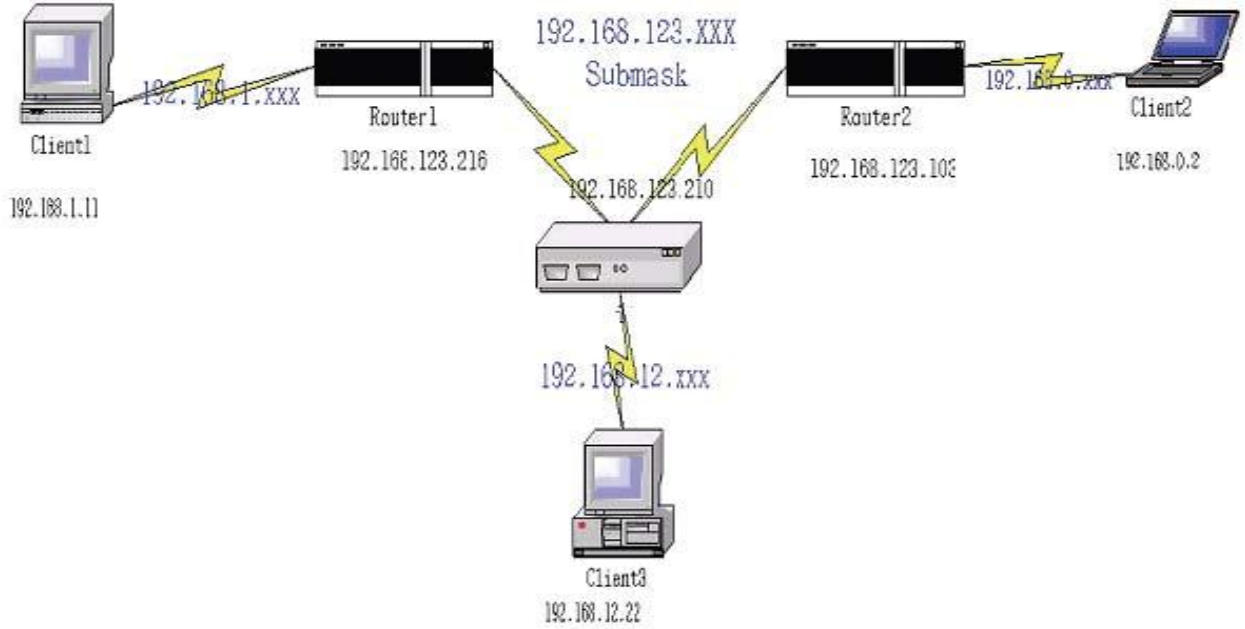
Routing

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

Note: NAT function needs to be disabled for the Routing feature to be enabled.



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
192.168.1.0	255.255.255.0	192.168.123.216	1	LAN
192.168.0.0	255.255.255.0	192.168.123.103	1	LAN

So if, for example, Client3 wants to send an IP data packet to 192.168.0.2 (Client 2), it would use the above table to determine that it had to go via 192.168.123.103 (Router 2)

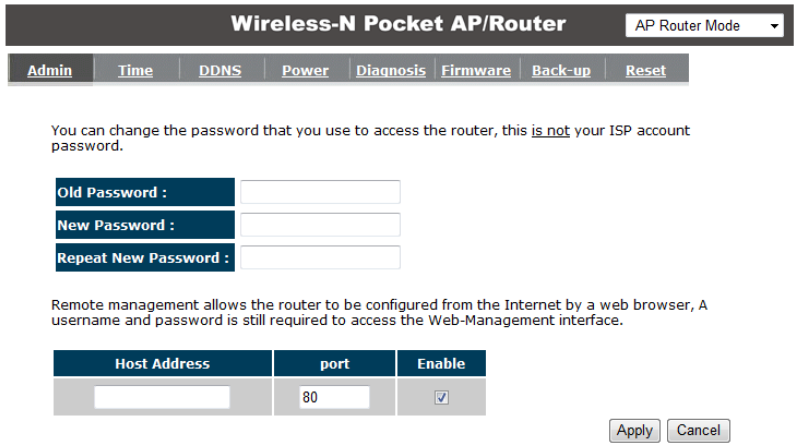
And if it sends Packets to 192.168.1.11 (Client 1) will go via 192.168.123.216 (Router 1).

8.2.6 Tools

This section allows you to configure some device system settings.

Admin

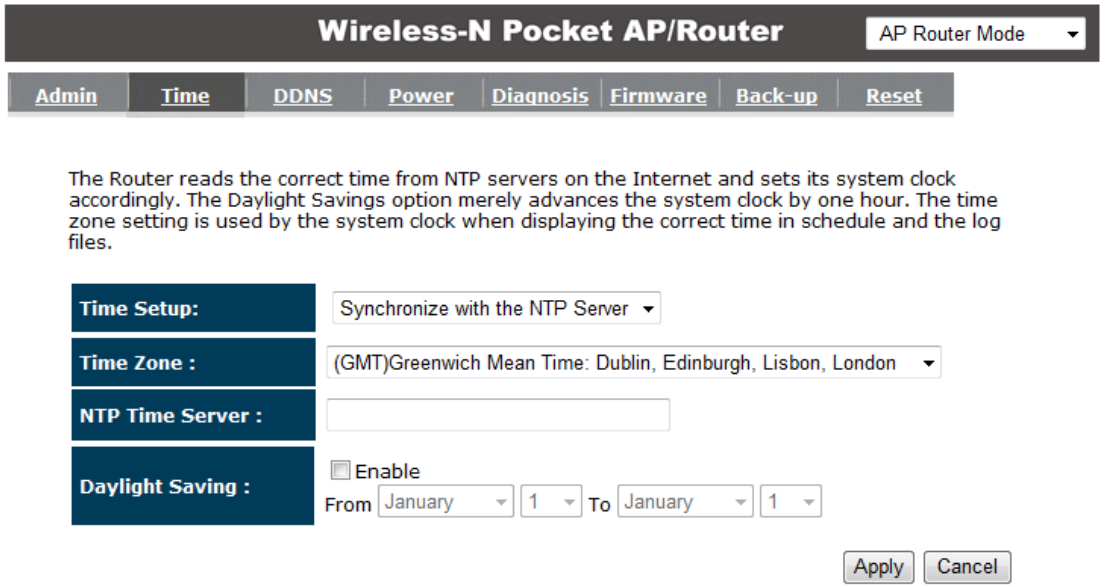
This page allows you to change the system password and to configure remote management.



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.

Time

This page allows you to set the system time.

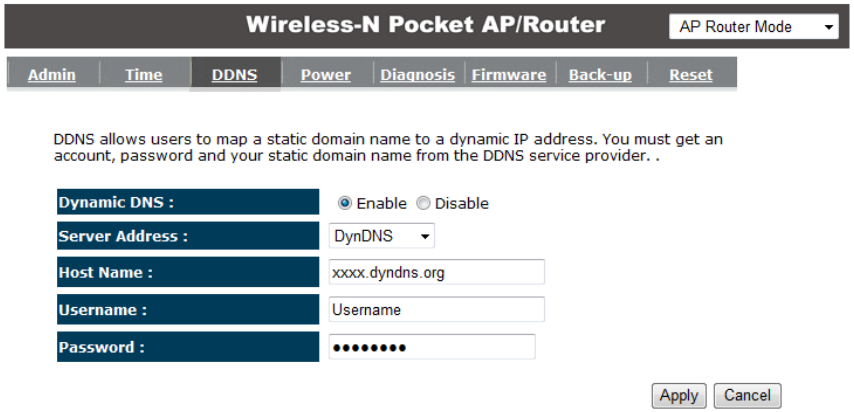


Time	
Time Setup:	Select the method you want to set the time.
Time Zone:	Select the time zone for your current location.
NTP Time Server:	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
Daylight Savings:	Check whether daylight savings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

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.



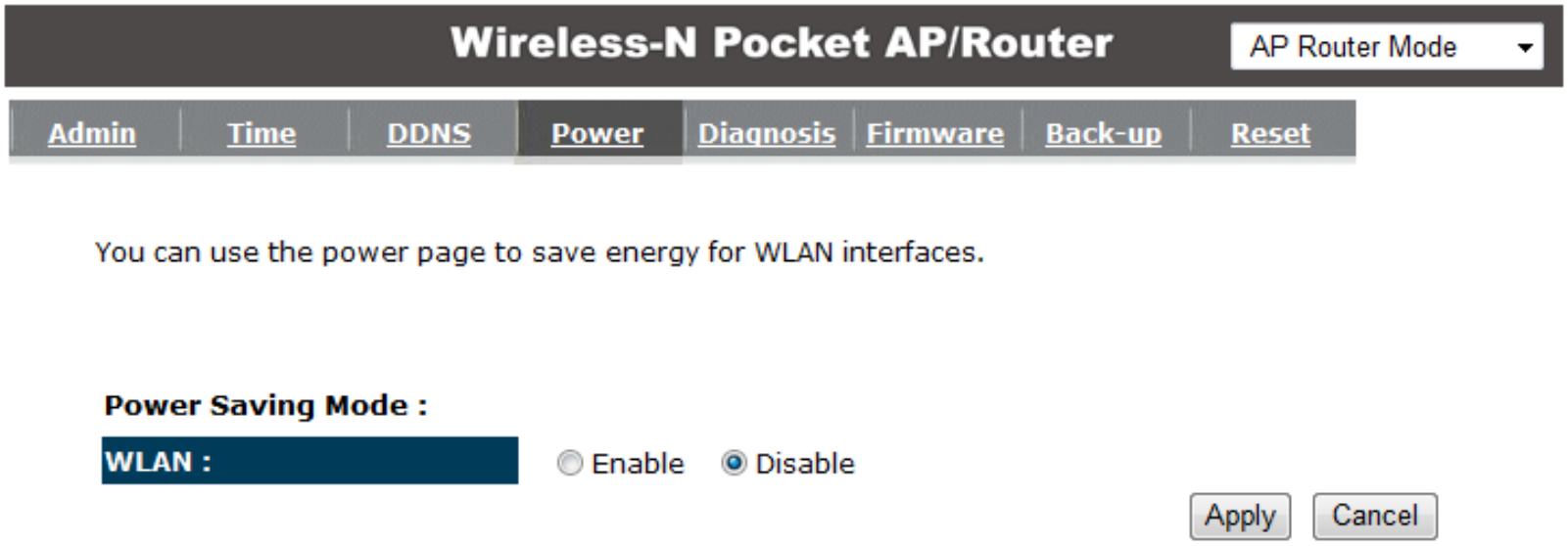
DDNS Services work as follows:

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 ETR-9305'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.

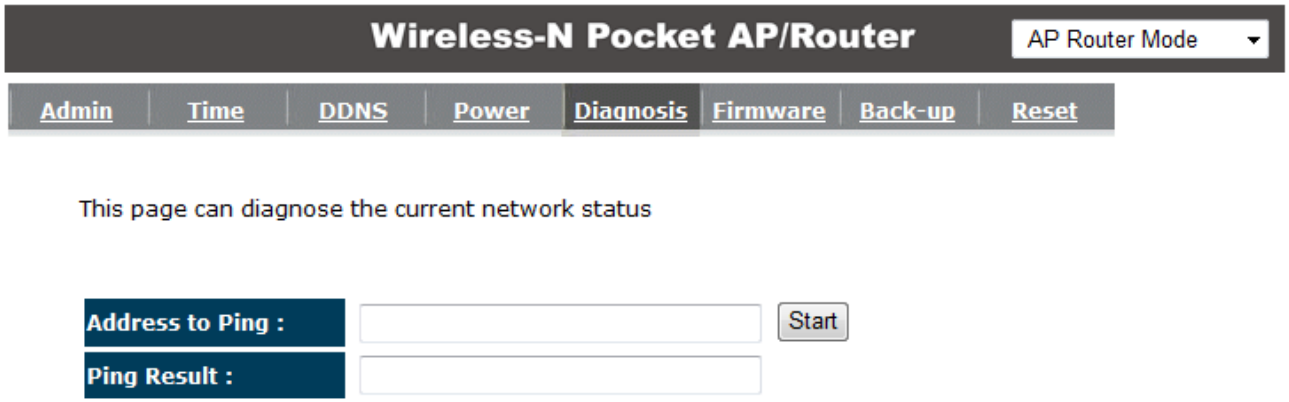
Power

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



Diagnosis

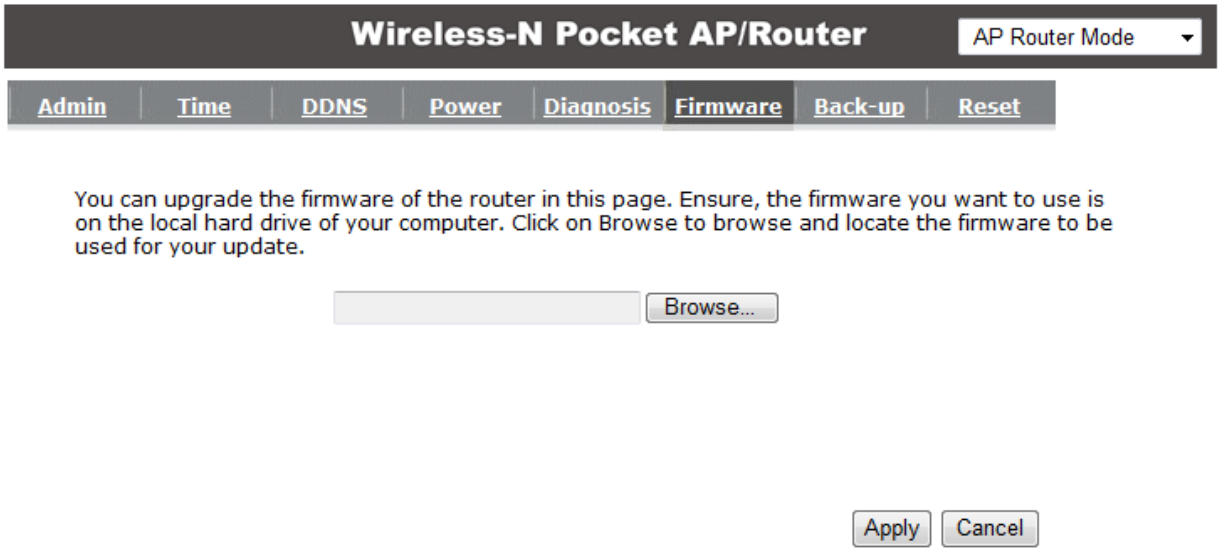
This page allows you determine if the TRAVEL ROUTER device has an active Internet connection.



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.

Firmware

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

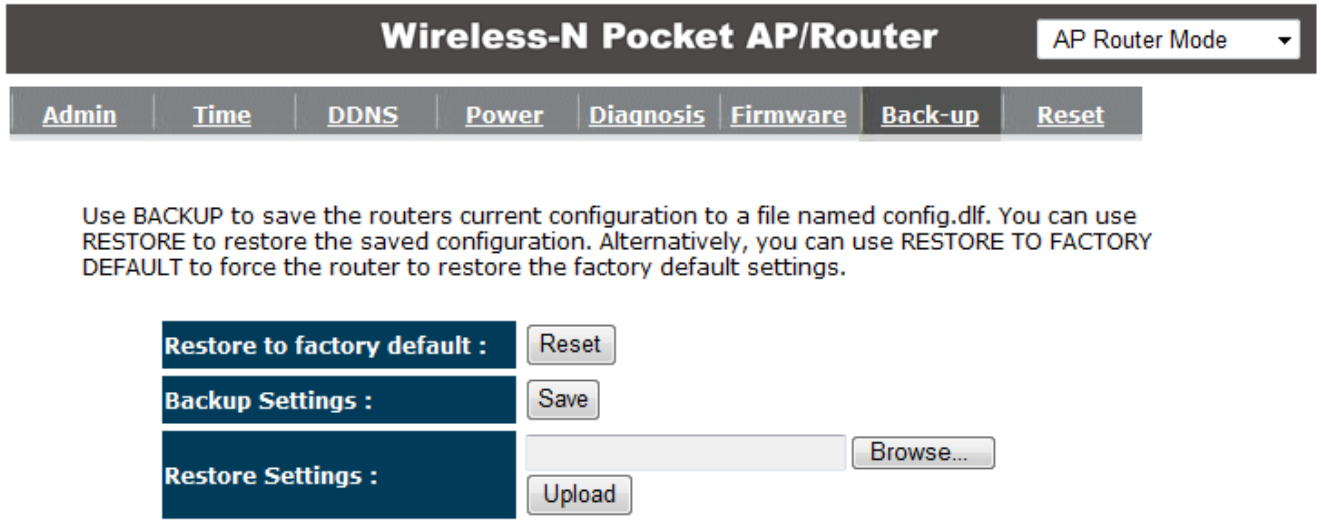


To perform the Firmware Upgrade:

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.

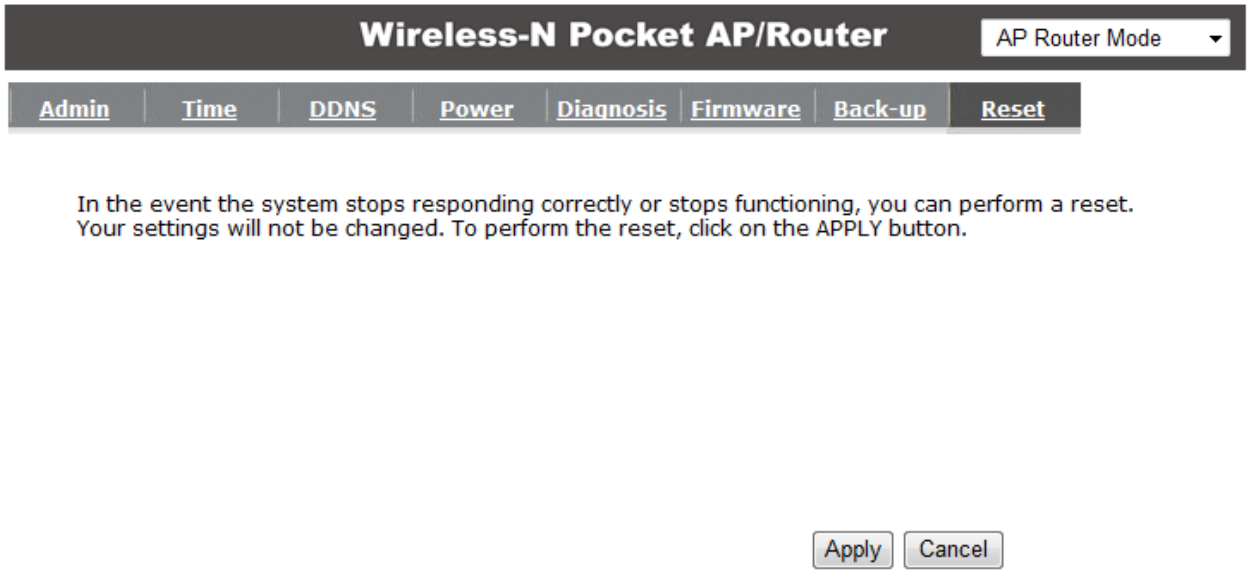
Back-up



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.

Reset

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



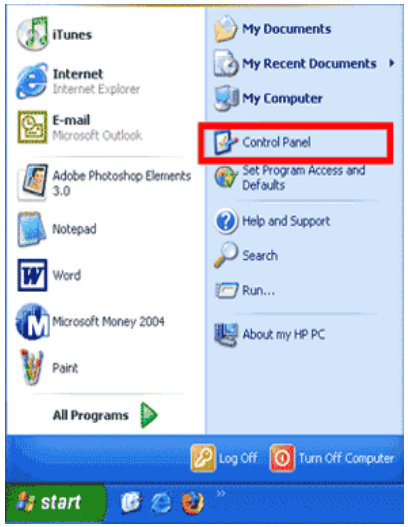
8.3 AP and Client Bridge Modes

When the TRAVEL ROUTER device is set to AP or Client Bridge modes, it will no longer allocate IP addresses to its wireless clients.

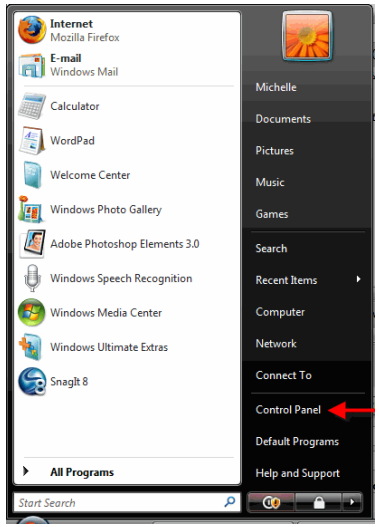
To access the Web-Based configuration page, please follow the following steps to set a static IP address (Windows XP/Vista).

1. Connect to the TRAVEL ROUTER using an Ethernet CAT.5 LAN Cable.

2. Click Start and open Control Panel.



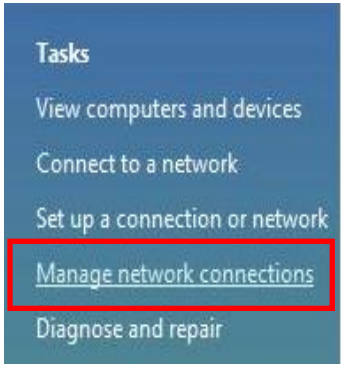
Windows XP



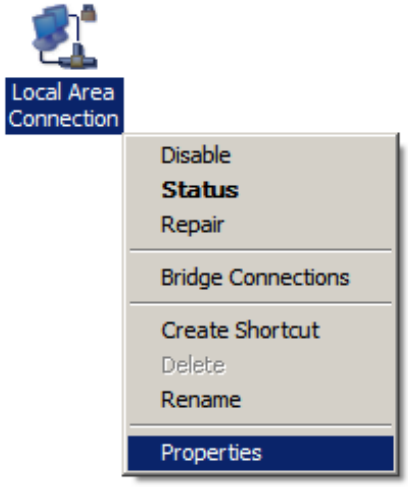
Windows Vista

3. Windows XP, click [**Network Connection]**

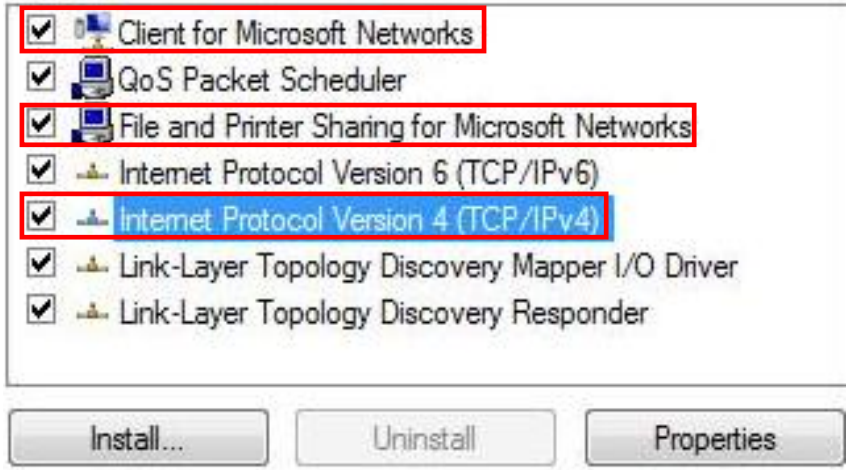
Windows Vista, click **[View Network Status and Tasks]** then **[Manage Network Connections]**



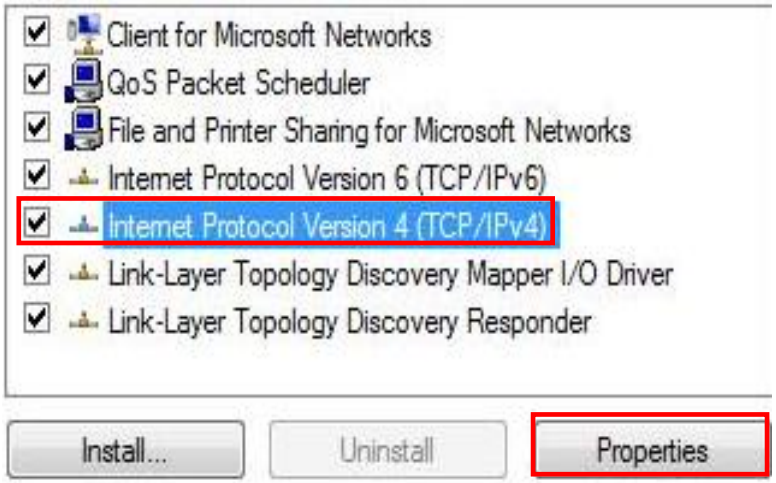
4. Right click on [**Local Area Connection**] and choose [**Properties**].



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



6. Select **“Internet Protocol (TCP/IP)”** and click [**Properties**]

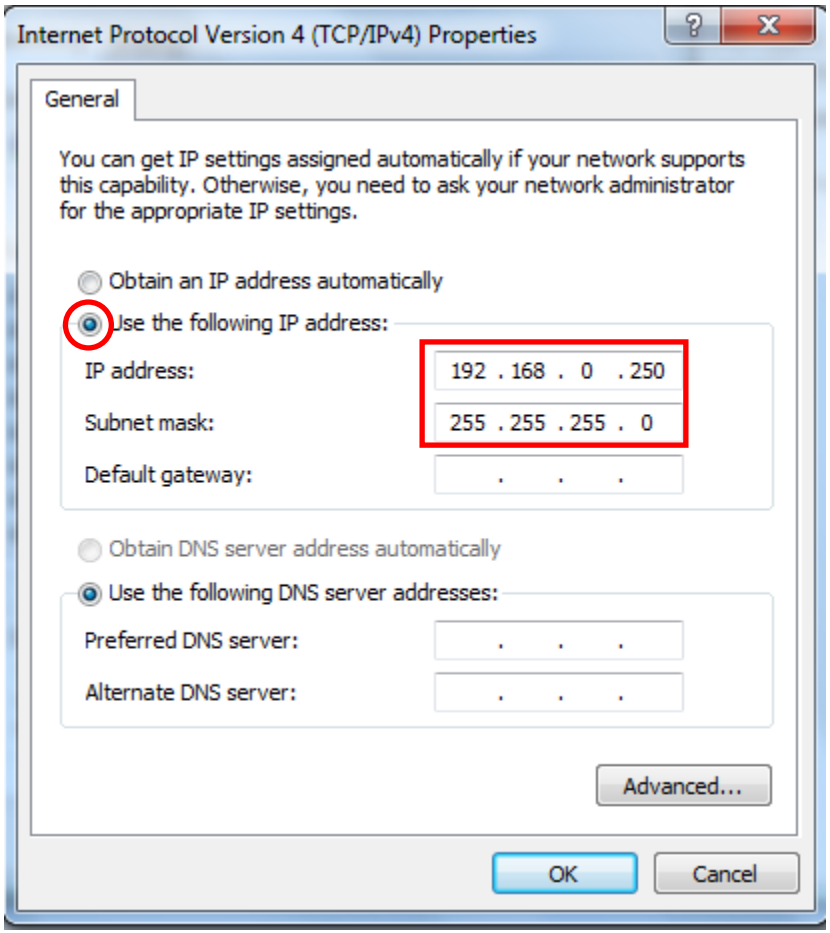


7. Manually set the IP Address. Then click **[OK]**

For example:

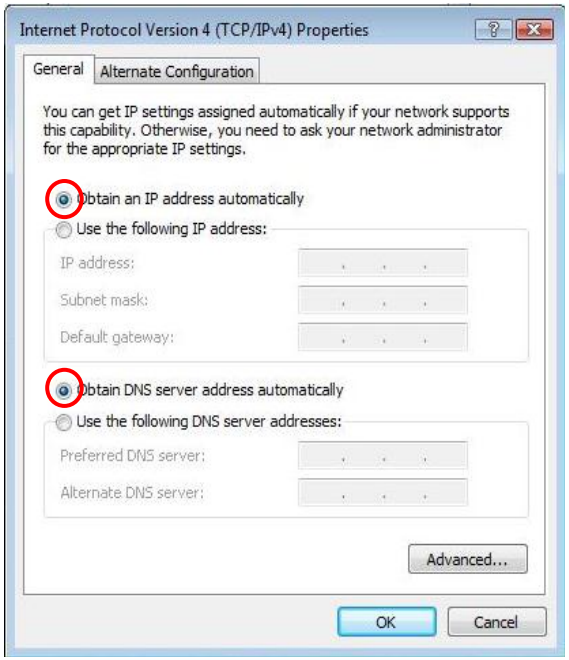
IP Address: 192.168.0.250

Subnet Mask: 255.255.255.0



8. You should now be able to access the Web-Based configuration in your Web Browser.

9. Remember to configure the settings back to **Obtain an IP Address Automatically** and **Obtain DNS Server Address Automatically** once you complete configuring the Web-Based interface.



8.4 Client Bridge Mode

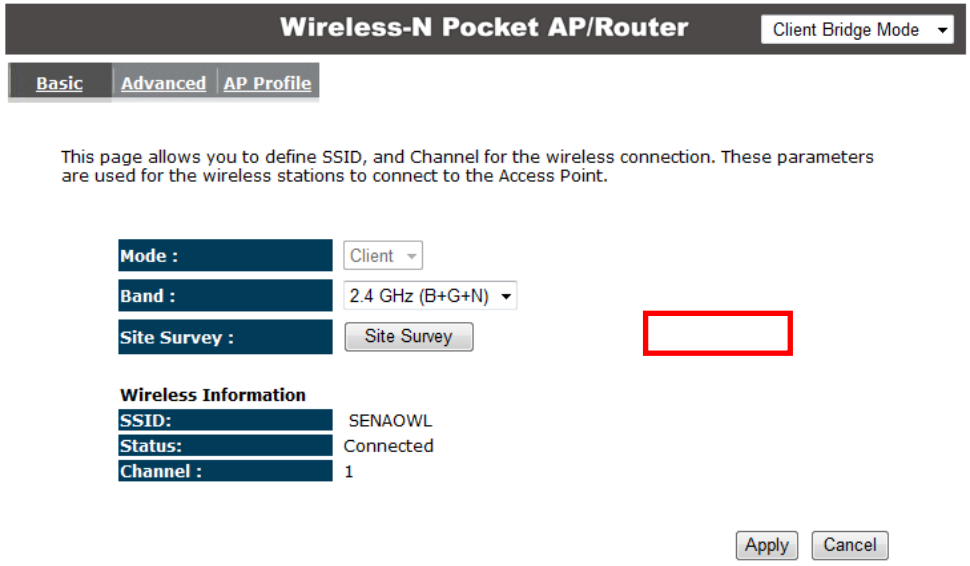
The Client Bridge mode turns the TRAVEL ROUTER into a wireless client, which then allows non-wireless devices to use its RJ45 port to access the network wirelessly.

8.4.1 Wireless

This section allows you to configure which wireless network the TRAVEL ROUTER will connect to.

Basic

1. Configure which wireless network the TRAVEL ROUTER will connect to in the Wireless Basic page.
2. Use the **Site Survey** button to scan the area for available wireless networks.



3. Select the SSID (wireless network) that you would like to connect to, and then click **Add to AP Profile**.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Auth	Signal (%)	Mode
1	◉	1	SENAOWL	00:97:53:AA:11:1C	WEP	AUTOWEP	65	11b/g/n
2	○	1	SENAOWL	00:02:6F:53:0C:9B	WEP	AUTOWEP	81	11b/g
3	○	1	SENAOWL	00:02:6F:36:9C:9A	WEP	AUTOWEP	70	11b
4	○	1	SENAOVIP	00:02:6F:E0:02:12	NONE	OPEN	44	11b/g
5	○	1	EnGenius2	06:02:6F:10:10:12	NONE	OPEN	44	11b/g
6	○	1	EnGenius1	00:02:6F:10:10:12	NONE	OPEN	34	11b/g
7	○	1	SENAOWL	00:02:6F:48:0D:87	WEP	AUTOWEP	55	11b/g

4. Enter the wireless security settings for this SSID. Then click **Save** to apply the settings.

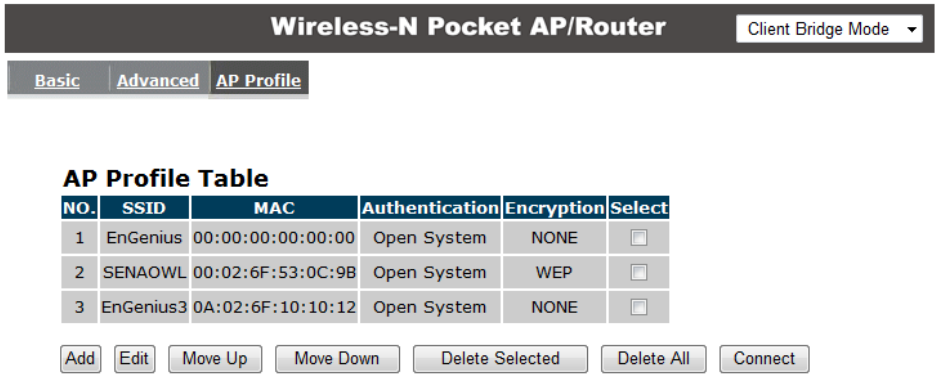
AP Profile Settings

Network Name (SSID) :	SENAOWL
Encryption :	WEP
Authentication Type :	◉ Open System ○ Shared Key
Key Length :	64-bit
Key type :	Hex (10 characters)
Default key :	Key 1
Encryption Key 1 :	**********
Encryption Key 2 :	**********
Encryption Key 3 :	**********
Encryption Key 4 :	**********

5. Change your IP Address settings back to **Obtain your IP Address Automatically**.
You should now be connected to the wireless network through the TRAVEL ROUTER.

AP Profiles

You can save the settings up to three wireless networks. The TRAVEL ROUTER will automatically connect to the wireless network in order of priority.



AP Profile	
Add:	Manually Add a new SSID (wireless network) profile.
Edit:	Edit the SSID settings.
Move Up / Down:	Change the priority that the TRAVEL ROUTER will connect to these SSID's.
Delete Selected:	Deletes the selected SSID profile.
Delete All:	Deletes all SSID profiles.
Connect:	Force connection to this SSID.

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.