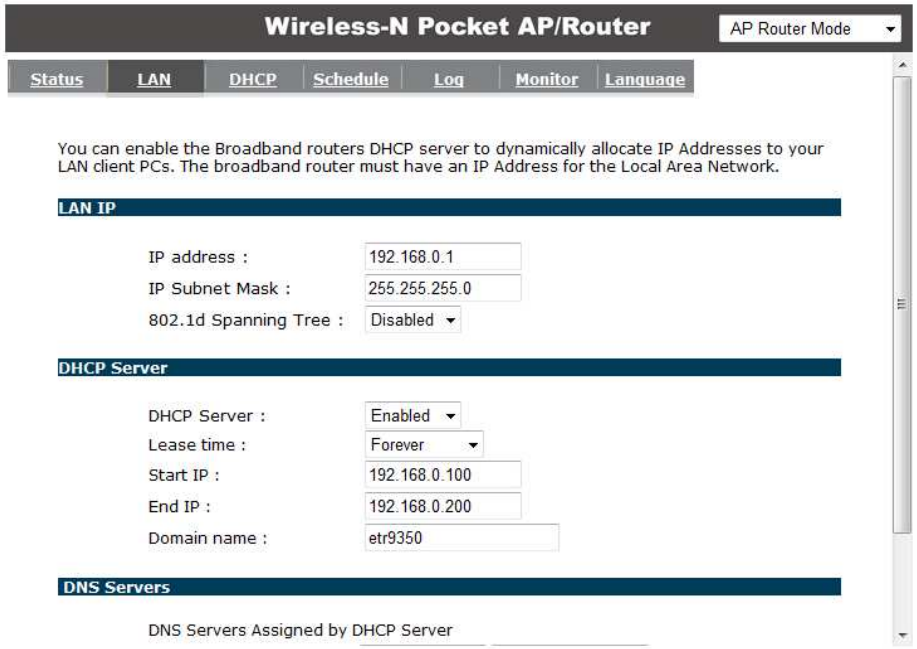
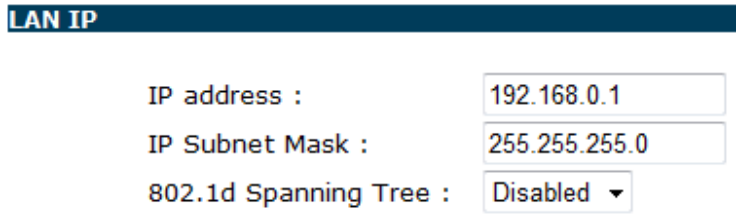
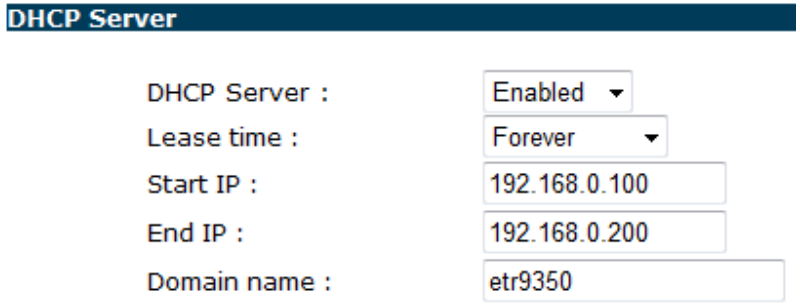
LAN

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

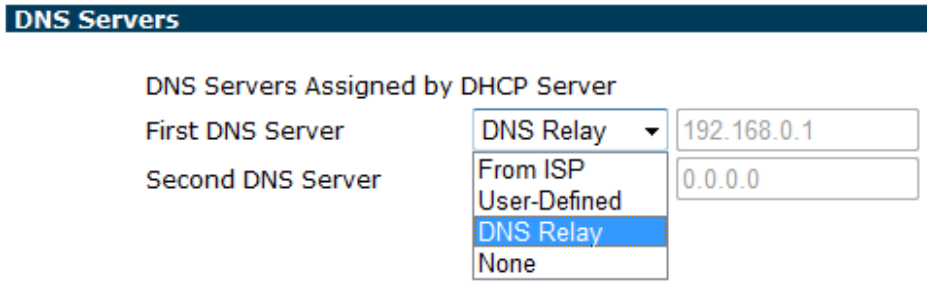




LAN IP	
IP address:	The LAN IP Address of this device.
IP Subnet Mask:	The LAN Subnet Mask of this device.
802.1d Spanning Tree:	When Enabled, the Spanning Tree protocol will prevent network loops in your LAN network.



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.

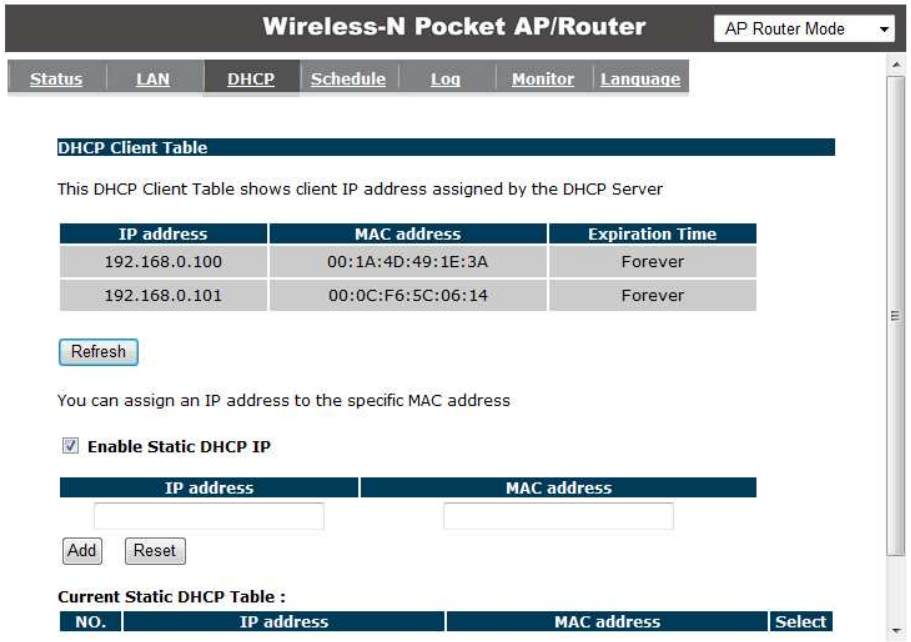


Two DNS servers can be assigned for use by your LAN devices.
There are three modes available.

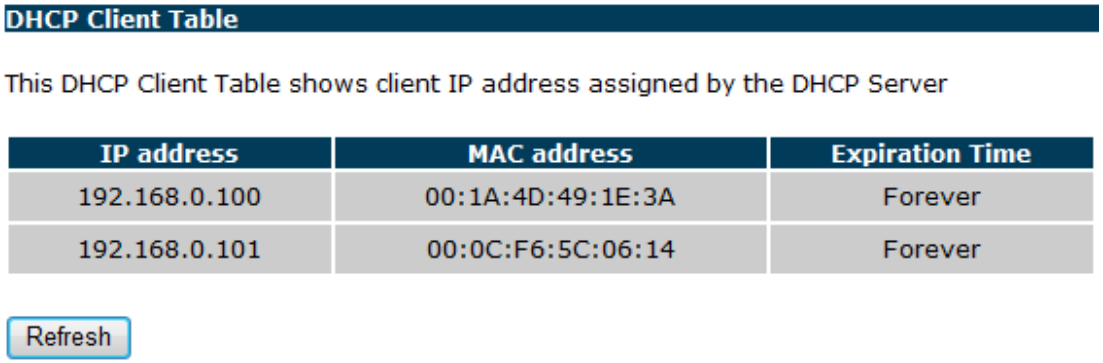
DNS Servers	
From ISP:	The DNS server IP address is assigned from your ISP.
User-Defined:	The DNS server IP address is assigned manually.
DNS Relay:	LAN clients are assigned the device's IP address as the DNS server. DNS requests are relayed to the ISP's DNS server.

DHCP

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

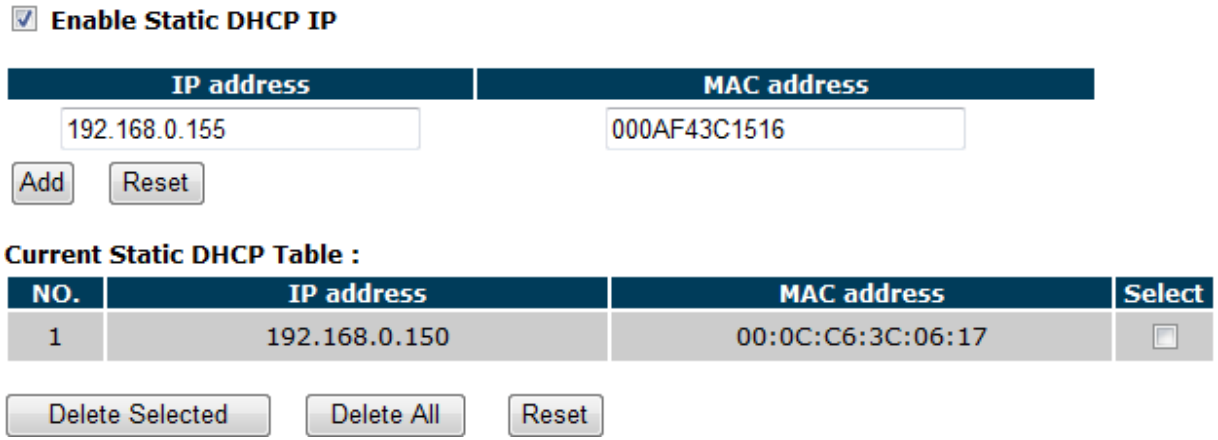


The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server



.

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.



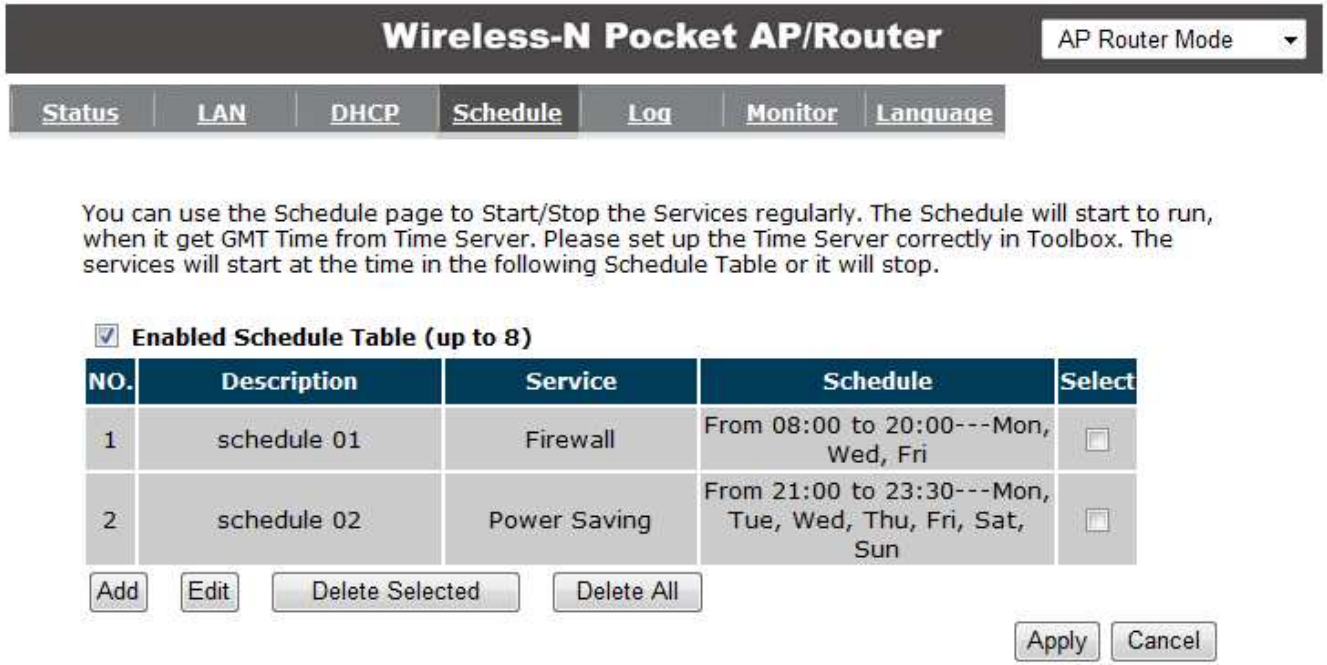
You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

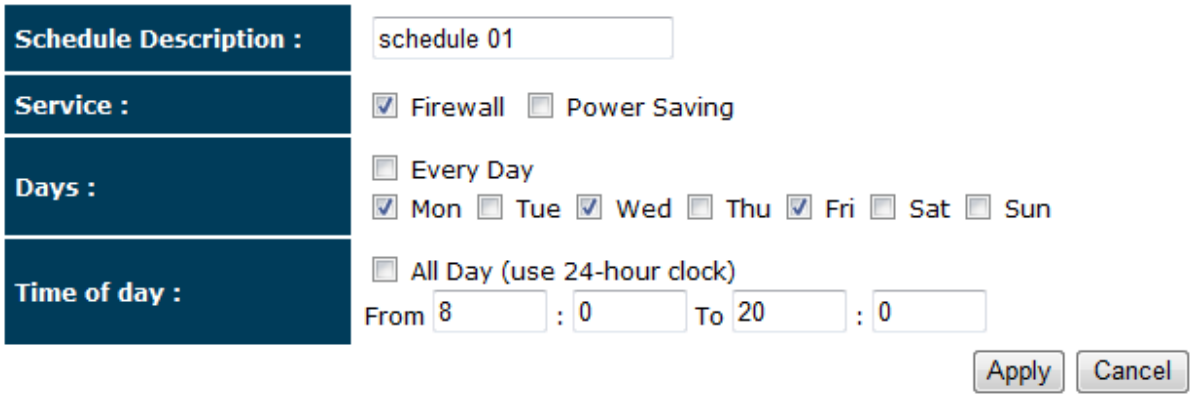
Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

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.

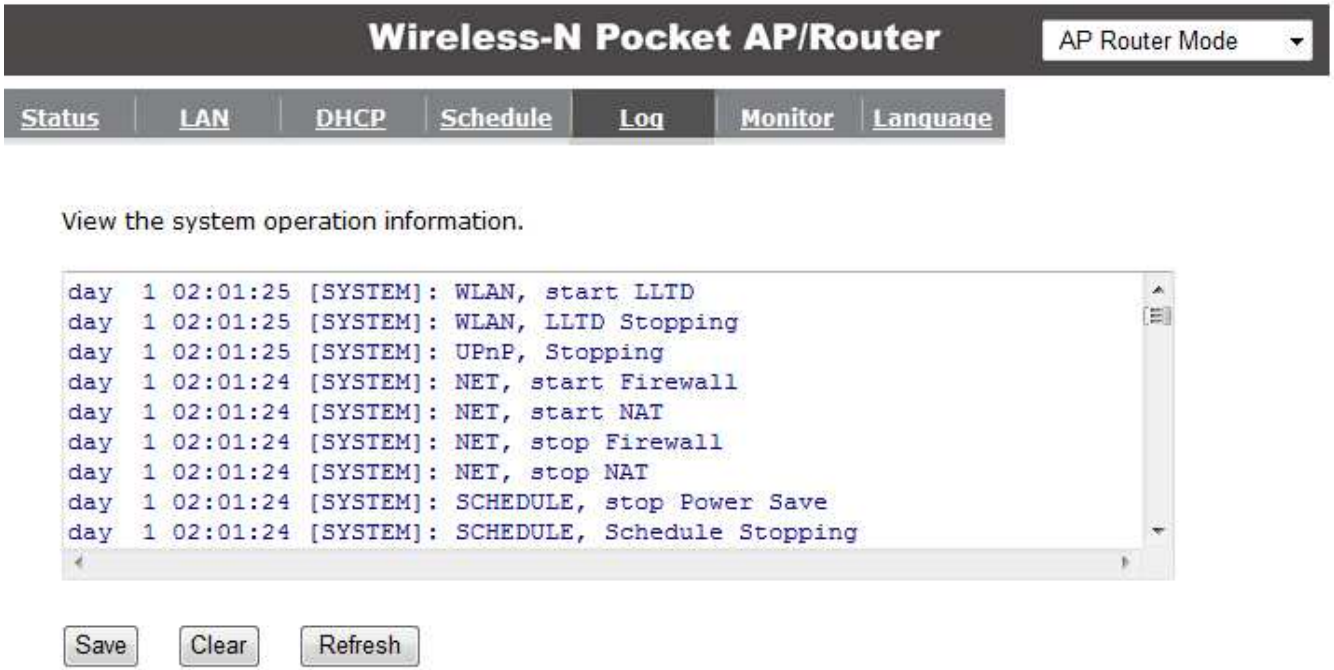




Schedule	
Schedule Description:	Assign a name to the schedule.
Service:	The service provides for the schedule.
Days:	Define the Days to activate or deactivate the schedule.
Time of day:	Define the Time of day to activate or deactivated the schedule. Please use 24-hour clock format.

Log

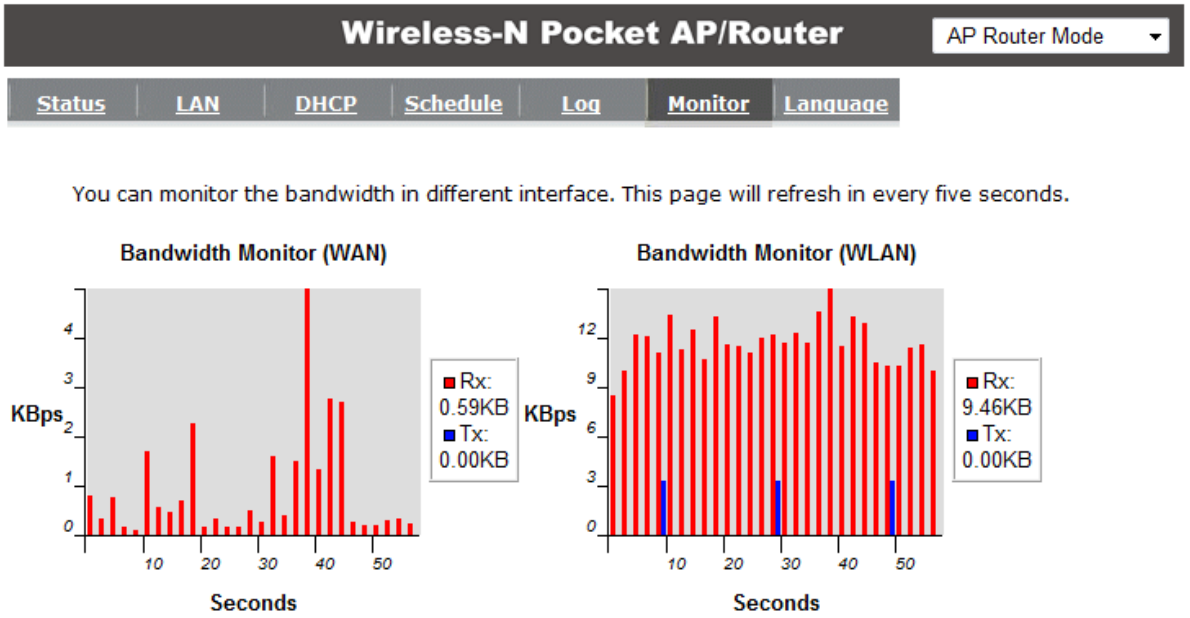
This page displays the system log of the device. When powered down or rebooted, the log will be cleared.



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

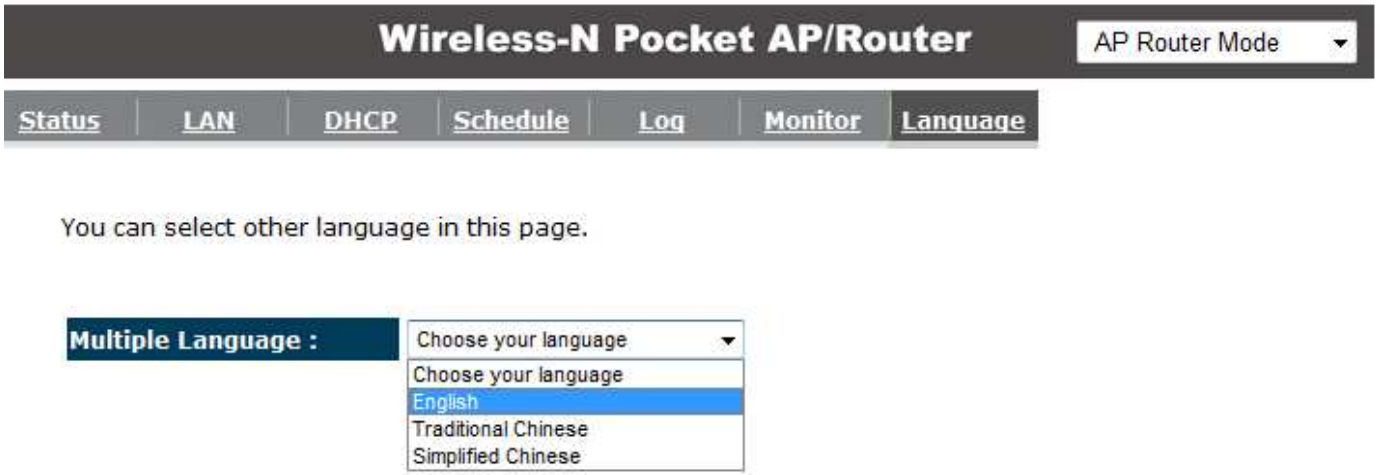
Monitor

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.

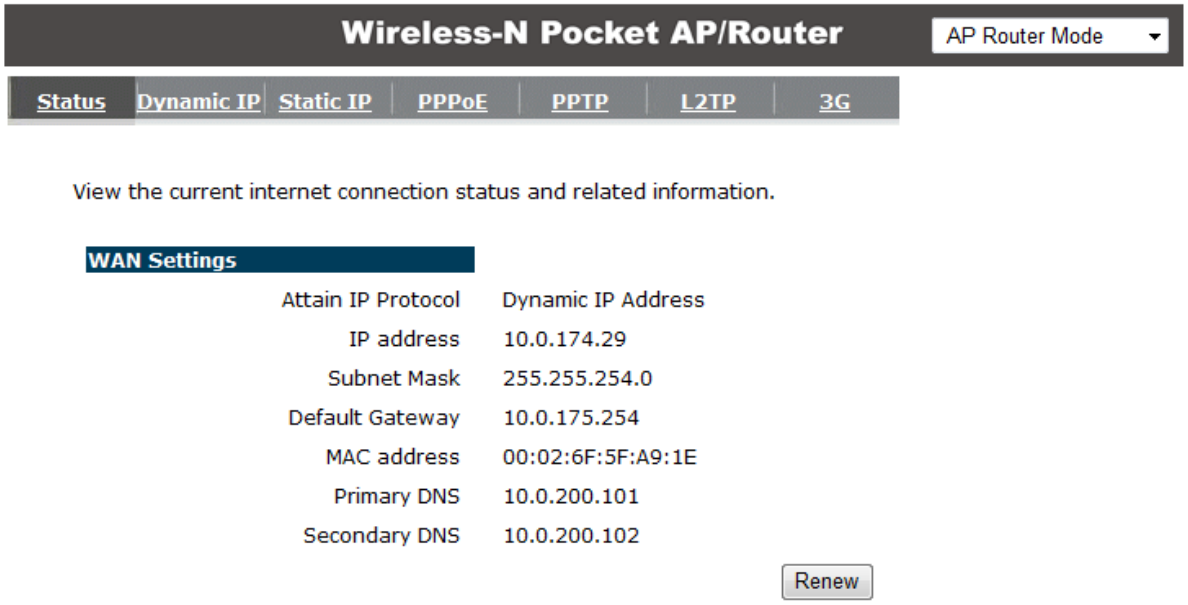


8.2.2 Internet

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.

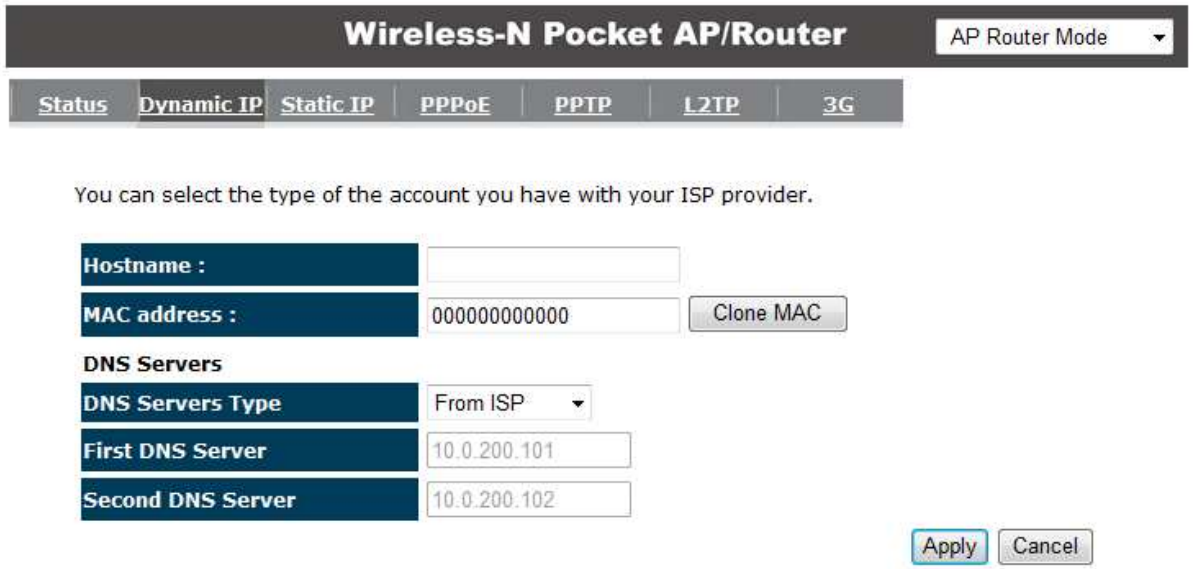


Dynamic IP Address

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.

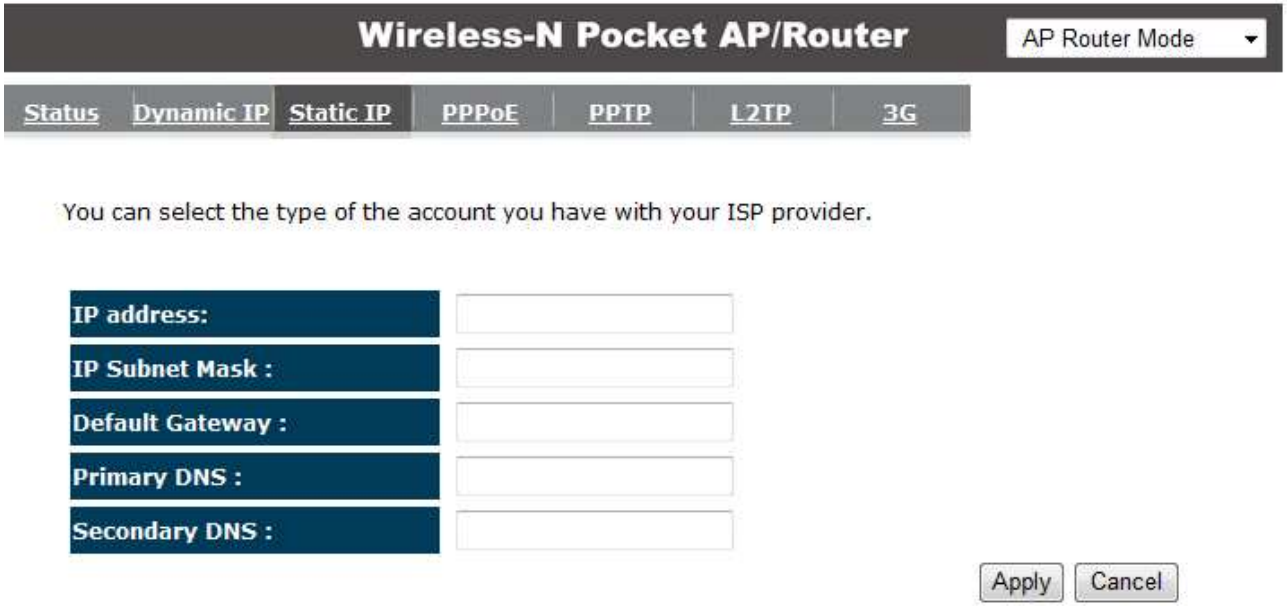
This will replace the AP Router MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.



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.

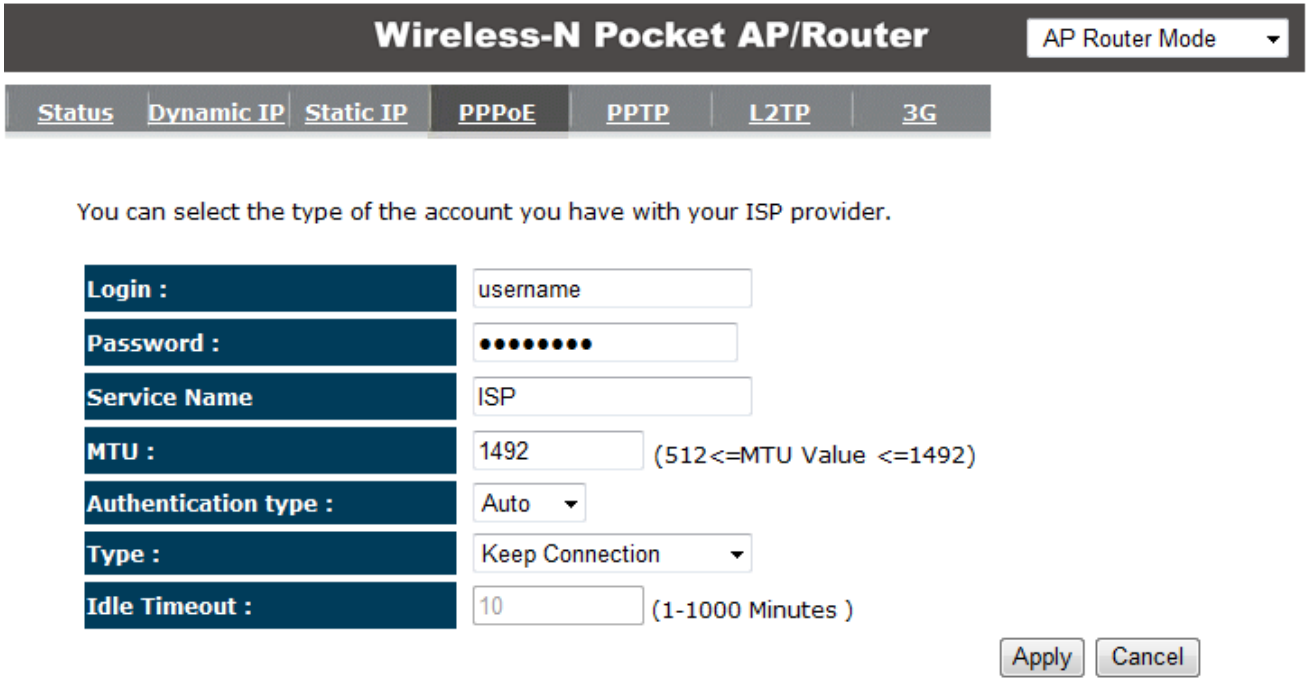
Static IP Address

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

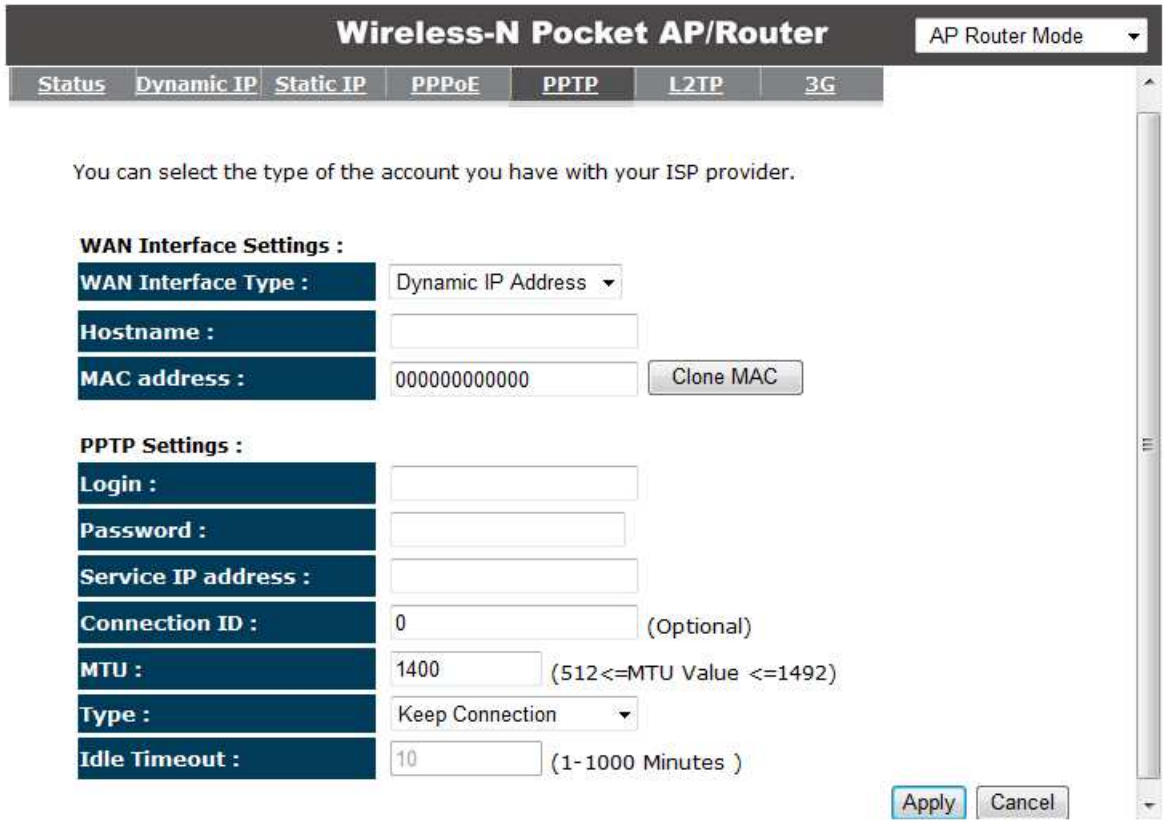
ISP requires an account username and password.



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.

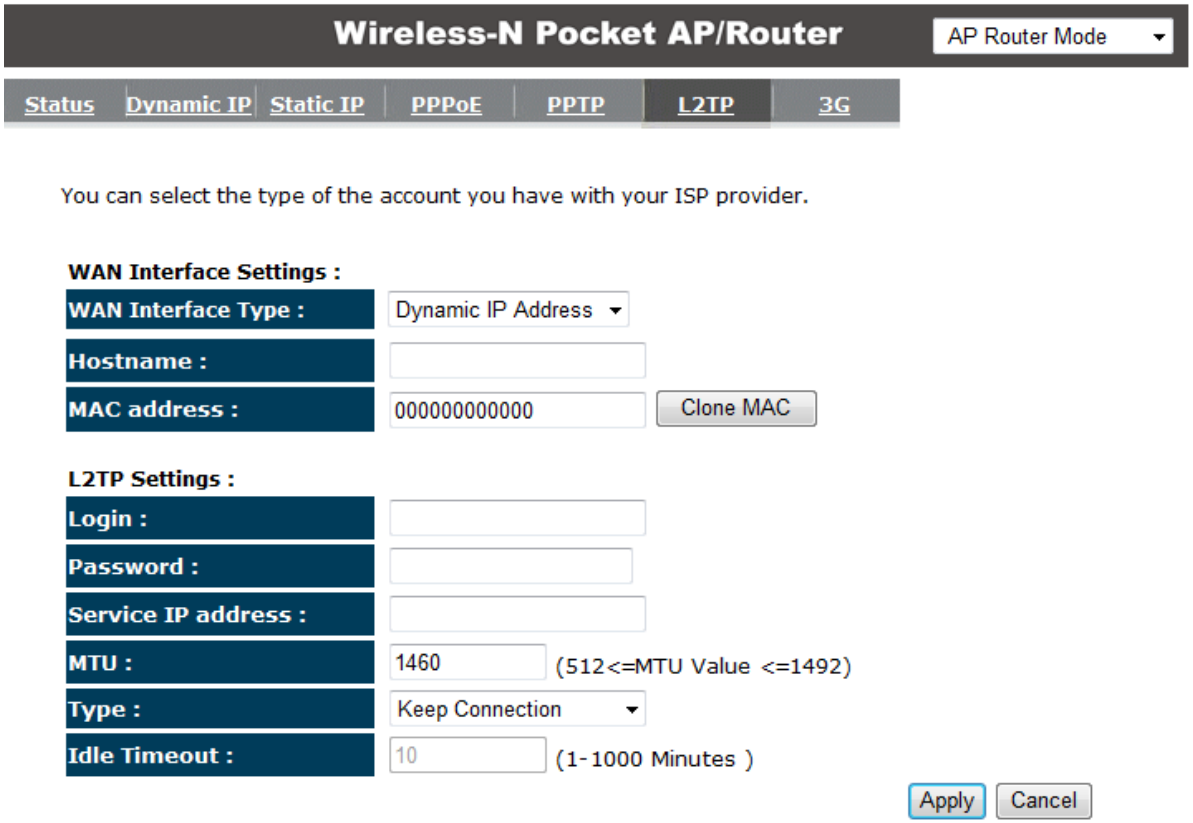


Point-to-Point Tunneling Protocol (PPTP)	
WAN Interface Type:	Select whether the ISP is set to Static IP or will allocate Dynamic IP addresses.
Hostname:	This is optional. Only required if specified by ISP

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)

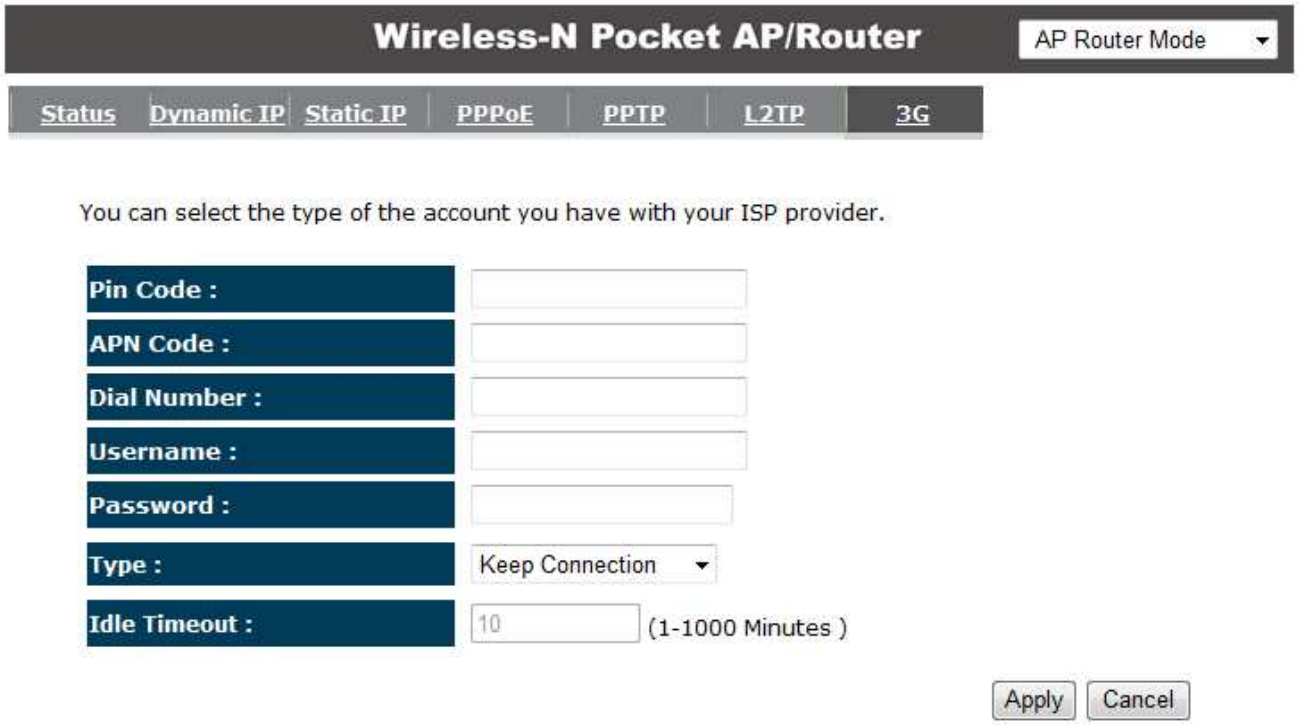
L2TP is used by some ISPs.



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.



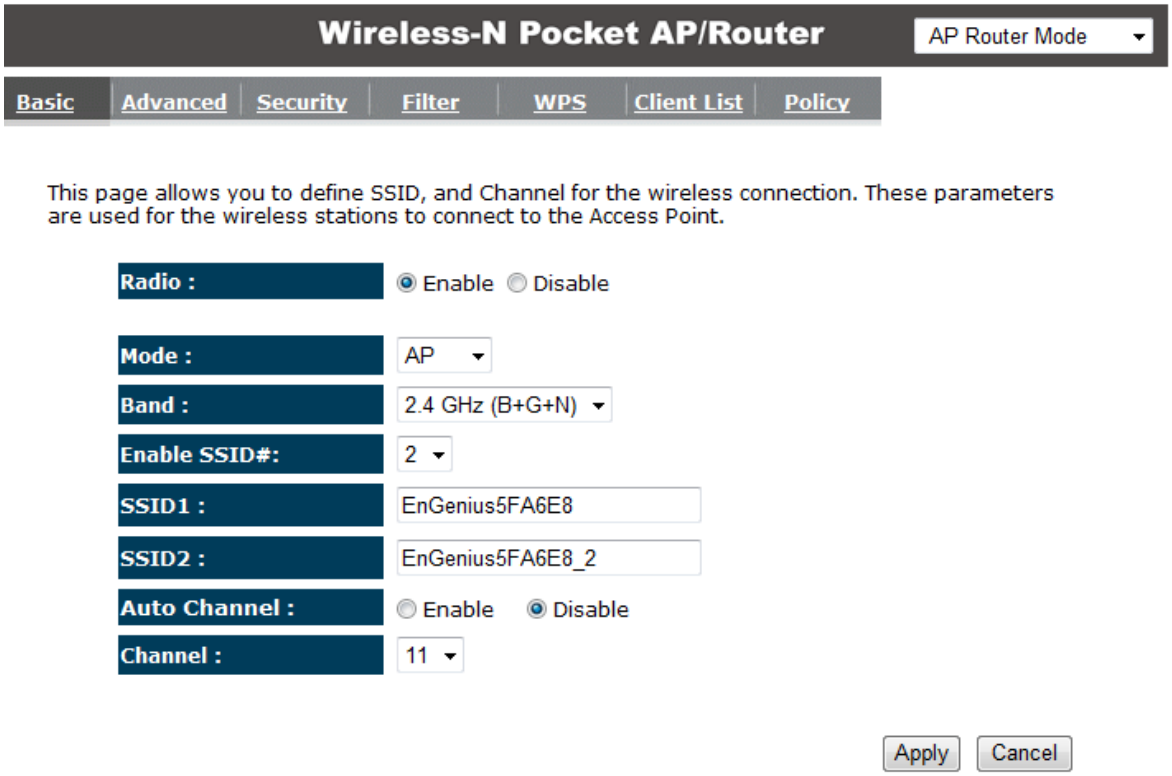
Mobile 3G	
Pin Code:	Enter the Pin code for your USIM card if required.
APN Code:	Enter the APN code for the network provider
Dial Number:	Only required if specified by ISP
User Name:	Account Username. Only required if specified by ISP
Password:	Account Password. Only required if specified by ISP
Type: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

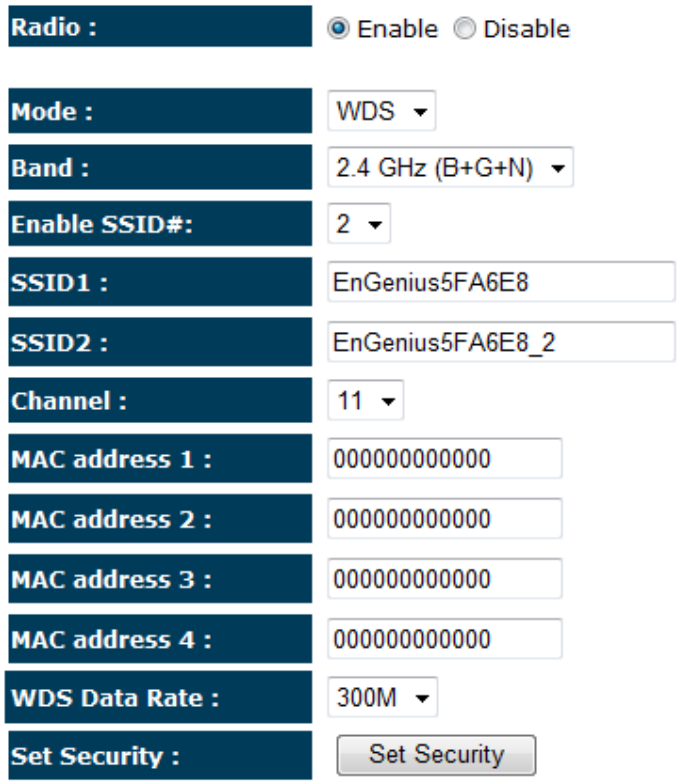
Wireless Distribution System (WDS)

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.

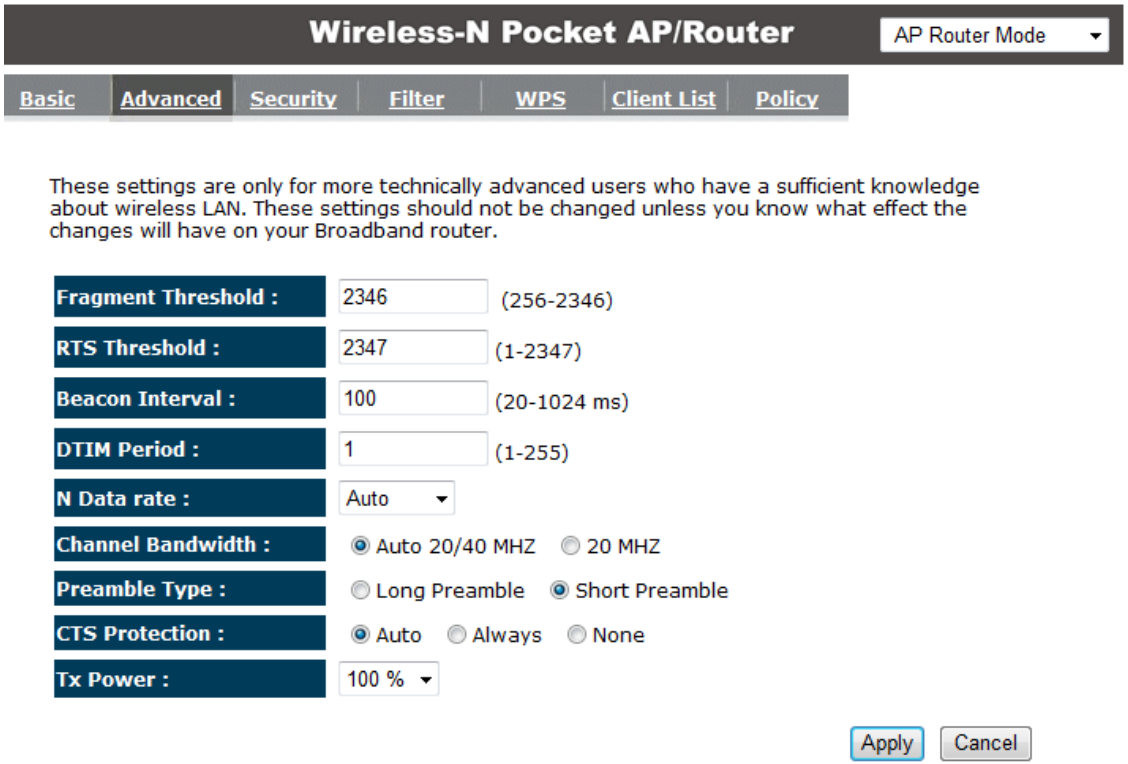
Also note that all Access Points in the WDS network needs to use the same Channel and Security settings.

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

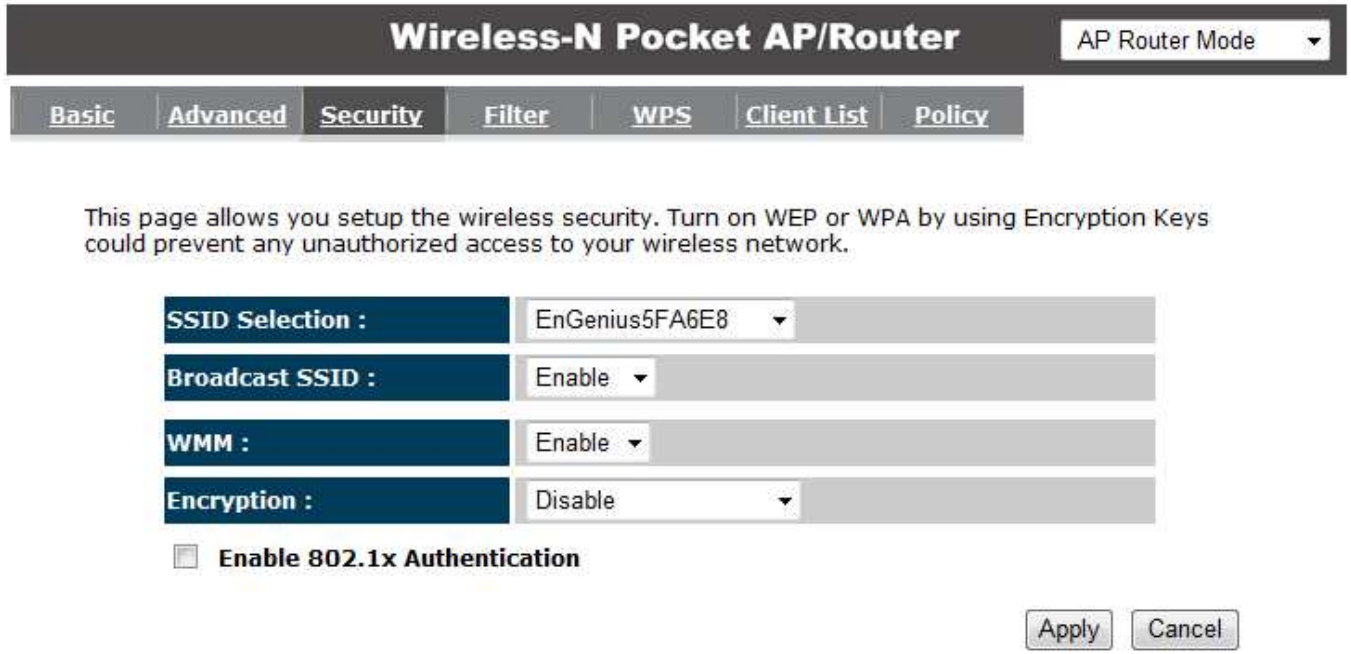
This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.



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.

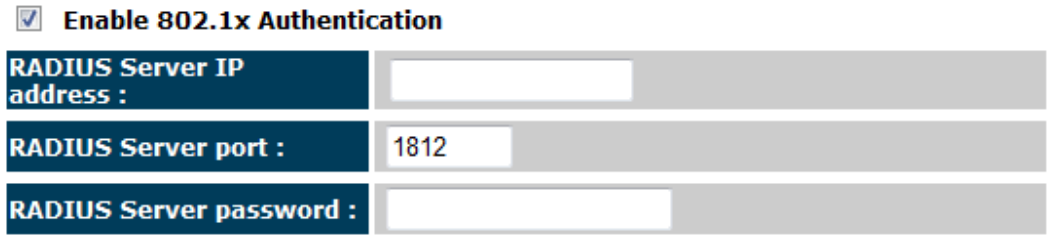
Security

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.

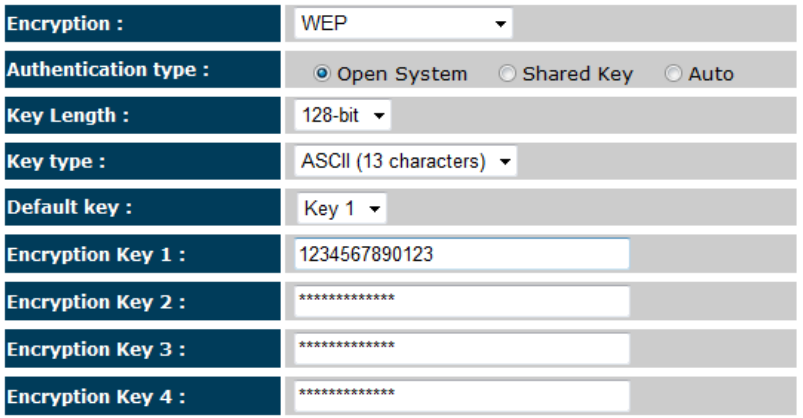
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.



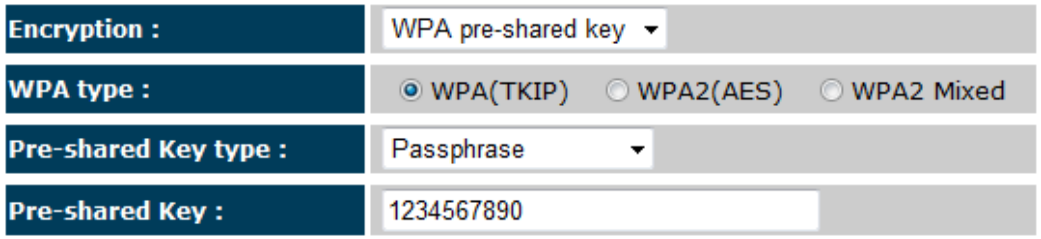
802.1x Authentication	
RADIUS Server IP Address:	The IP Address of the RADIUS Server
RADIUS Server port:	The port of the RADIUS Server.
RADIUS Server password:	The RADIUS Server's password.

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.

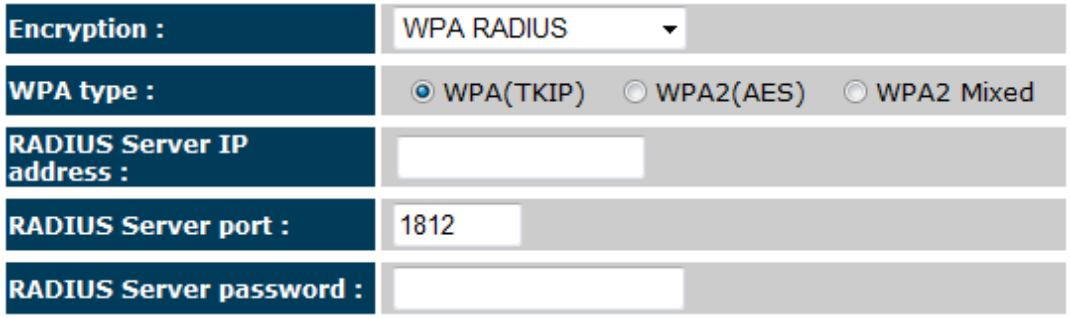


WPA Pre-Shared Key Encryption:



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.

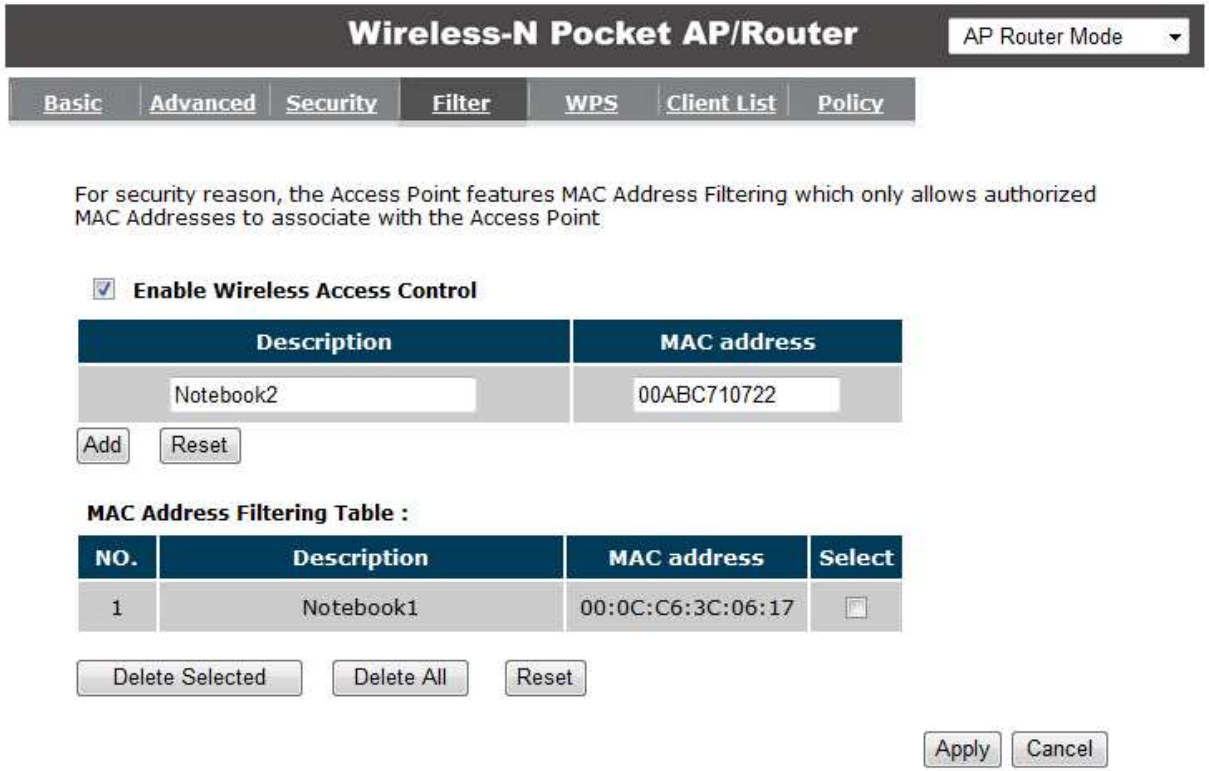
WPA RADIUS Encryption:



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.

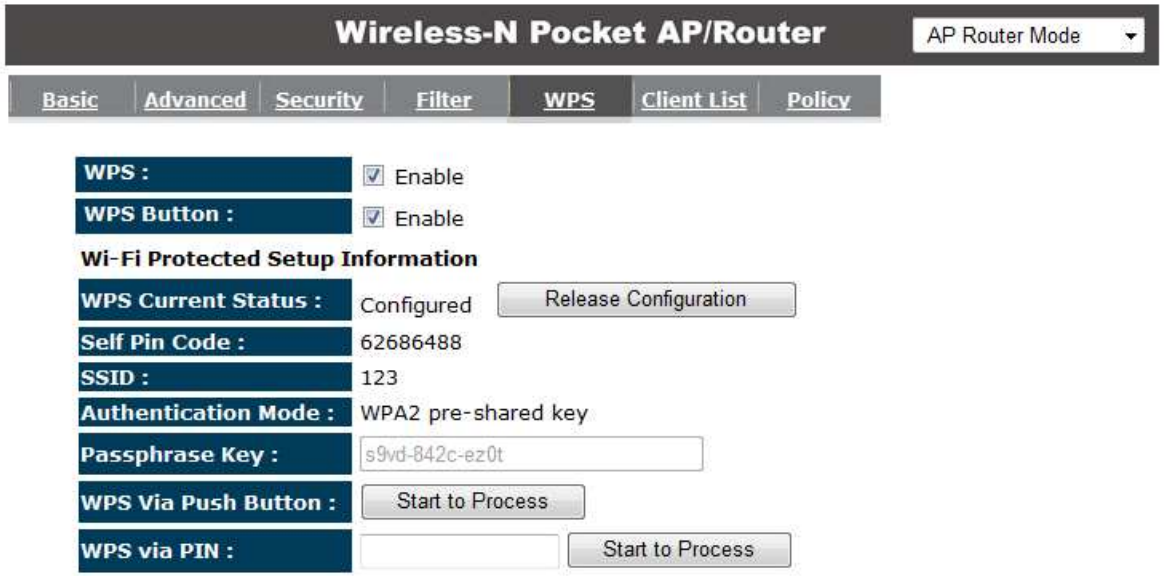


Wireless Filter	
Enable Wireless Access Control:	Tick the box to Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description:	Enter a name or description for this entry.
MAC address:	Enter the MAC address of the wireless client that you wish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



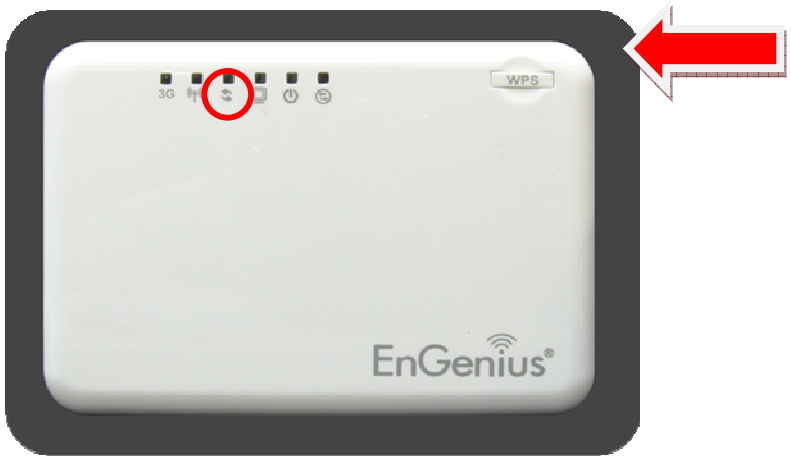
Wi-Fi Protected Setup (WPS)	
WPS:	Tick to Enable the WPS feature.
WPS Button:	Tick to Enable the WPS push button.
Wi-Fi Protected Setup Information	
WPS Current Status:	Shows whether the WPS function is **Configured** or **Unconfigured**. Configured means that WPS has been used to authorize connection 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.