

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:	<p>Wi-Fi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background.</p> <p>Note that in certain situations, WMM needs to be enabled to achieve 11n transfer speeds.</p>
Encryption:	<p>The encryption method to be applied.</p> <p>You can choose from WEP, WPA pre-shared key or WPA RADIUS.</p> <ul style="list-style-type: none"> • 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. <p>If this option is selected:</p> <ul style="list-style-type: none"> • This Access Point must have a "client login" on the Radius Server. • Each user must have a "user login" on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

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

Enable 802.1x Authentication

RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	<input type="text" value="1812"/>
RADIUS Server password :	<input type="text"/>

802.1x Authentication

RADIUS Server IP Address:	The IP Address of the RADIUS Server
RADIUS Server port:	The port number of the RADIUS Server.
RADIUS Server password:	The RADIUS Server's password.

WEP Encryption:

WEP Encryption	
Authentication Type:	Please ensure that your wireless clients use the same authentication type.
Key type	<ul style="list-style-type: none"> • ASCII: regular text (recommended) • HEX: for advanced users
Key Length:	Select the desired option, and ensure the wireless clients use the same setting. <ul style="list-style-type: none"> • 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.

Encryption :	WEP ▾
Authentication type :	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> Auto
Key Length :	128-bit ▾
Key type :	ASCII (13 characters) ▾
Default key :	Key 1 ▾
Encryption Key 1 :	1234567890123
Encryption Key 2 :	*****
Encryption Key 3 :	*****
Encryption Key 4 :	*****

WPA Pre-Shared Key Encryption:

Encryption :	WPA pre-shared key ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase ▾
Pre-shared Key :	1234567890

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

WPA RADIUS Encryption:

Encryption :	WPA RADIUS ▾
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	<input type="text"/>
RADIUS Server port :	1812
RADIUS Server password :	<input type="text"/>

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-N Pocket AP/Router
AP Router Mode ▾

Basic
Advanced
Security
Filter
WPS
Client List
Policy

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

Enable Wireless Access Control

Description	MAC address
Notebook2	00ABC710722

MAC Address Filtering Table :

NO.	Description	MAC address	Select
1	Notebook1	00:0C:C6:3C:06:17	<input type="checkbox"/>

Wireless Filter	
Enable Wireless Access Control:	<p>Tick the box to Enable Wireless Access Control.</p> <p>When Enabled, only wireless clients on the Filtering Table will be allowed.</p>
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.

Wireless-N Pocket AP/Router

AP Router Mode

[Basic](#) | [Advanced](#) | [Security](#) | [Filter](#) | **[WPS](#)** | [Client List](#) | [Policy](#)

WPS : Enable

WPS Button : Enable

Wi-Fi Protected Setup Information

WPS Current Status : Configured Release Configuration

Self Pin Code : 62686488

SSID : 123

Authentication Mode : WPA2 pre-shared key

Passphrase Key :

WPS Via Push Button : Start to Process

WPS via PIN : Start to Process

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

WPS :	<input checked="" type="checkbox"/> Enable
WPS Button :	<input checked="" type="checkbox"/> Enable
Wi-Fi Protected Setup Information	
WPS Current Status :	unConfigured
Self Pin Code :	62686488
SSID :	EnGenius5FA6E8
Authentication Mode :	Disable
Passphrase Key :	<input type="text"/>
WPS Via Push Button :	<input type="button" value="Start to Process"/>
WPS via PIN :	<input type="text"/> <input type="button" value="Start to Process"/>

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

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

Client List

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

Wireless-N Pocket AP/Router AP Router Mode

[Basic](#) [Advanced](#) [Security](#) [Filter](#) [WPS](#) [Client List](#) [Policy](#)

WLAN Client Table :

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

Interface	MAC Address	Signal (%)	Idle Time
EnGenius5FA6E8_2	00:19:7D:9E:D4:9C	68	20 secs

Policy

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

Wireless-N Pocket AP/Router
AP Router Mode ▾

Basic
Advanced
Security
Filter
WPS
Client List
Policy

SSID 1 Connection Control Policy

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

SSID 2 Connection Control Policy

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

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

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.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Enable](#) [Advanced](#) [DMZ](#) [DoS](#) [MAC Filter](#) [IP Filter](#) [URL Filter](#)

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

Firewall : Enable Disable

Advanced

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

Wireless-N Pocket AP/Router AP Router Mode ▾

[Enable](#) [Advanced](#) [DMZ](#) [DoS](#) [MAC Filter](#) [IP Filter](#) [URL Filter](#)

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

DMZ

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

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

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

Wireless-N Pocket AP/Router

AP Router Mode

[Enable](#) [Advanced](#) [DMZ](#) [DoS](#) [MAC Filter](#) [IP Filter](#) [URL Filter](#)

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

Enable DMZ

Local IP Address :

Denial of Service (DoS)

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

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

The screenshot shows the configuration page for a Wireless-N Pocket AP/Router. At the top, there is a title bar with the text "Wireless-N Pocket AP/Router" and a dropdown menu set to "AP Router Mode". Below the title bar is a navigation menu with tabs for "Enable", "Advanced", "DMZ", "DoS", "MAC Filter", "IP Filter", and "URL Filter". The "DoS" tab is currently selected. Below the navigation menu, there is a paragraph of text explaining the DoS firewall feature: "The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resourcess that Internet access becomes unavailable." Below this text, there is a "Block DoS" section with two radio buttons: "Enable" (which is selected) and "Disable". At the bottom right of the form, there are two buttons: "Apply" and "Cancel".

MAC Filter

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

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

Enable MAC filtering
 Deny all clients with MAC address listed below to access the network
 Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address
Notebook2	010CF63C0617

MAC Filtering table :

NO.	Description	LAN MAC Address	Select
1	Notebook1	00:0C:C6:3C:06:17	<input type="checkbox"/>

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.

Wireless-N Pocket AP/Router AP Router Mode

Enable Advanced DMZ DoS MAC Filter **IP Filter** URL Filter

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

Enable IP Filtering Table

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

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

Description :

Protocol : Both

Local IP Address : ~

Port range : ~

Add Reset

NO.	Description	Local IP Address	Protocol	Port range	Select
1	Jack and John	192.168.0.100-192.168.0.101	BOTH	21-22	<input type="checkbox"/>

Delete Selected Delete All Reset

Apply Cancel

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.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Enable](#) | [Advanced](#) | [DMZ](#) | [DoS](#) | [MAC Filter](#) | [IP Filter](#) | [URL Filter](#)

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

Enable URL Blocking

URL/keyword

Current URL Blocking Table :

NO.	URL/keyword	Select
1	abc123	<input type="checkbox"/>

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.



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

NAT : Enable Disable

Apply

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.

The screenshot shows the configuration interface for a Wireless-N Pocket AP/Router. The 'Port map.' tab is selected. Under 'Enable Port Mapping', the checkbox is checked. The 'Current Port Mapping Table' contains the following entry:

NO.	Description	Local IP	Type	Port range	Select
1	Mail Server	192.168.0.150	BOTH	22-23	<input type="checkbox"/>

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.

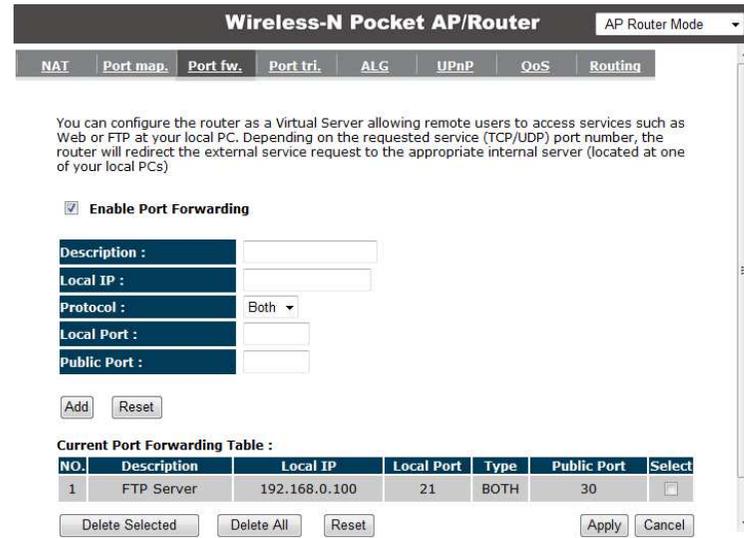
Port Forwarding

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.

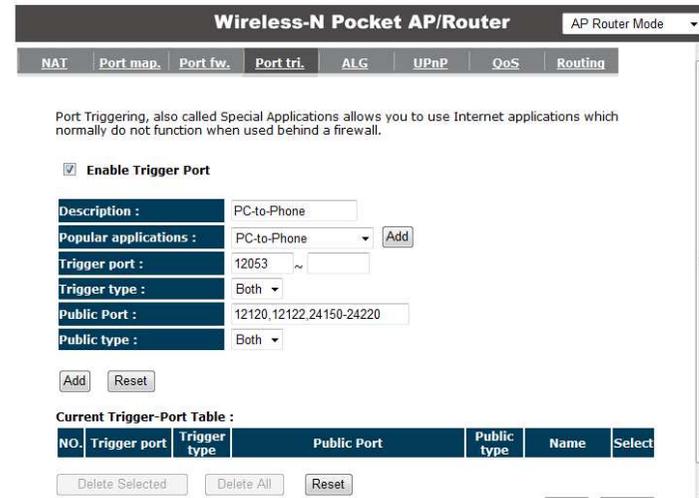
Therefore then there is a connection from the Internet on port 30, it will be forwarded to the computer with the IP address 192.168.0.100 and changed to port 21.



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

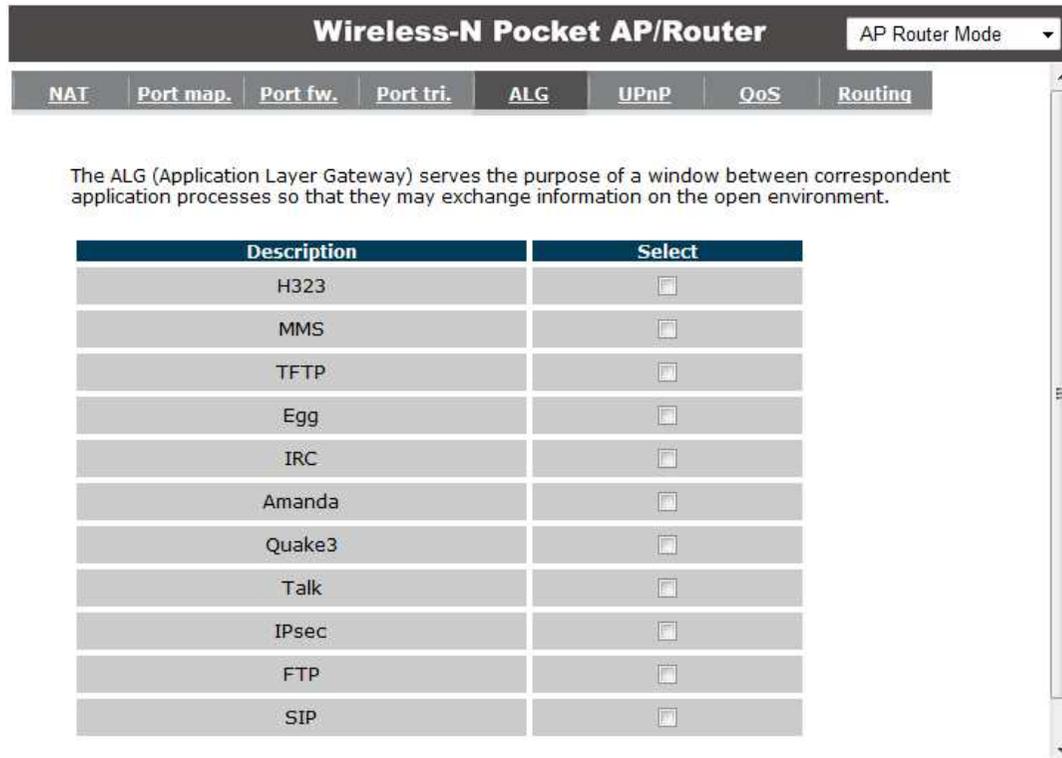
If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Trigger will be required for these applications to work.



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.



The screenshot shows the configuration interface for a Wireless-N Pocket AP/Router. At the top, there is a title bar with the text "Wireless-N Pocket AP/Router" and a dropdown menu set to "AP Router Mode". Below the title bar is a navigation menu with tabs for "NAT", "Port map.", "Port fw.", "Port tri.", "ALG", "UPnP", "QoS", and "Routing". The "ALG" tab is currently selected. Below the navigation menu, there is a descriptive paragraph: "The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment." Below this text is a table with two columns: "Description" and "Select". The table lists various applications with checkboxes in the "Select" column, all of which are currently unchecked.

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

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.

Wireless-N Pocket AP/Router
AP Router Mode ▾

NAT
Port map.
Port fw.
Port tri.
ALG
UPnP
QoS
Routing

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

Enable the Universal Plug and Play (UPnP) Feature
 Allow users to make port forwarding changes through UPnP

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

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.

Wireless-N Pocket AP/Router
AP Router Mode ▾

NAT
Port map.
Port fw.
Port tri.
ALG
UPnP
QoS
Routing

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

Total Bandwidth Settings

Uplink	Full ▾
Downlink	Full ▾

QoS : Priority Queue Bandwidth Allocation Disabled

Apply
Cancel

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

Priority Queue Method

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

QoS : Priority Queue Bandwidth Allocation Disabled

Unlimited Priority Queue

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

High/Low Priority Queue

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

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

Bandwidth Allocation Method

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

QoS : Priority Queue Bandwidth Allocation Disabled

Type : Download ▾

Local IP range : ~

Protocol : ALL ▾

Port range : 1 ~ 65535

Policy : Min ▾

Rate(bps) : Full ▾

Add Reset

Current QoS Table:

NO.	Type	Local IP range	Protocol	Port range	Policy	Rate (bps)	Select
1	Both	192.168.0.100 ~ 192.168.0.103	TCP	80 ~ 90	Min	2M	<input type="checkbox"/>

Delete Selected Delete All Reset

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 Minimum 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.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Enable
Routing

You can enable Static Routing to turn off the NAT function of the router and let the router forward packets by your routing policy .

To take Static Route effect, please disable NAT function.

Enable Static Routing

Destination LAN IP :

Subnet Mask :

Default Gateway :

Hops:

Interface :

LAN ▾

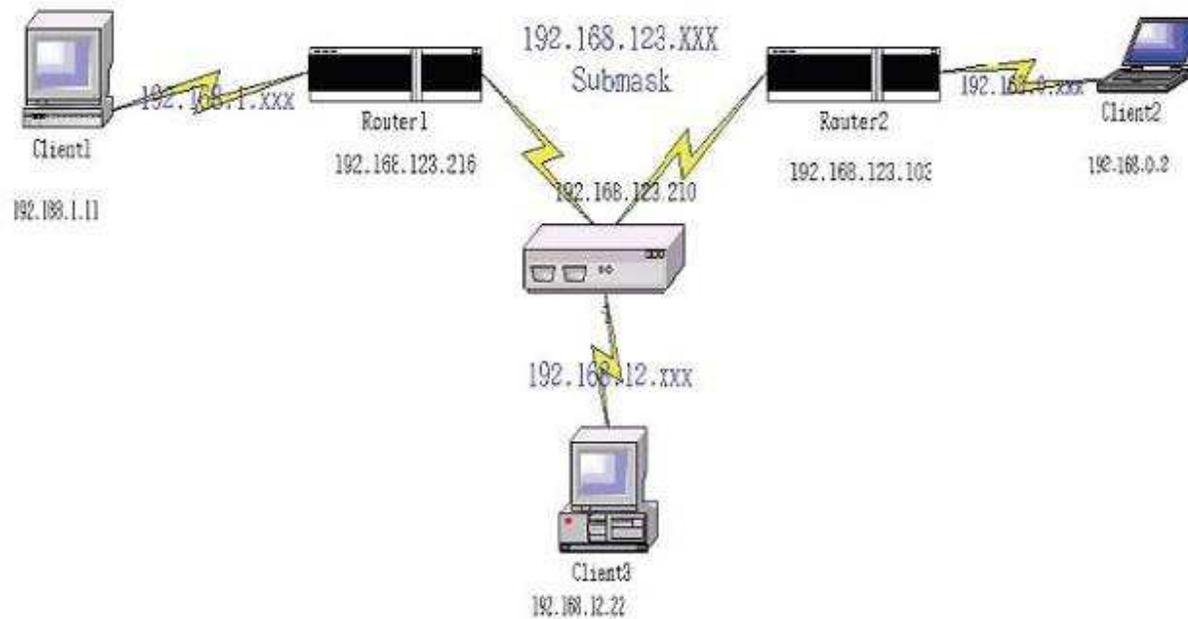
Add
Reset

Current Static Routing Table :

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Hops	Interface	Select
<div style="display: flex; justify-content: space-between; margin-top: 5px;"> Delete Selected Delete All Reset </div>						

Apply
Cancel

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.

Wireless-N Pocket AP/Router AP Router Mode ▾

Admin
Time
DDNS
Power
Diagnosis
Firmware
Back-up
Reset

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

Old Password :

New Password :

Repeat New Password :

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

Host Address	port	Enable
<input style="width: 95%;" type="text"/>	80	<input checked="" type="checkbox"/>

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.

Wireless-N Pocket AP/Router
AP Router Mode ▾

Admin
Time
DDNS
Power
Diagnosis
Firmware
Back-up
Reset

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

Time Setup:

Synchronize with the NTP Server ▾

Time Zone :

(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾

NTP Time Server :

Daylight Saving :

Enable
 From January ▾ 1 ▾ To January ▾ 1 ▾

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

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.

Wireless-N Pocket AP/Router AP Router Mode

Admin Time **DDNS** Power Diagnosis Firmware Back-up Reset

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

Dynamic DNS : Enable Disable

Server Address : DynDNS

Host Name : xxxx.dyndns.org

Username : Username

Password :

Apply Cancel

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.

Wireless-N Pocket AP/Router AP Router Mode ▾

[Admin](#) | [Time](#) | [DDNS](#) | **[Power](#)** | [Diagnosis](#) | [Firmware](#) | [Back-up](#) | [Reset](#)

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

Power Saving Mode :

WLAN :

Enable Disable

Apply

Cancel

Diagnosis

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

Wireless-N Pocket AP/Router
AP Router Mode ▾

Admin
Time
DDNS
Power
Diagnosis
Firmware
Back-up
Reset

This page can diagnose the current network status

Address to Ping :

Ping Result :

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

Firmware

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

The screenshot shows the web interface for a Wireless-N Pocket AP/Router. At the top, there is a header bar with the title "Wireless-N Pocket AP/Router" and a dropdown menu set to "AP Router Mode". Below the header is a navigation menu with tabs for "Admin", "Time", "DDNS", "Power", "Diagnosis", "Firmware", "Back-up", and "Reset". The "Firmware" tab is selected. The main content area contains the following text: "You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update." Below this text is a text input field and a "Browse..." button. At the bottom of the form are "Apply" and "Cancel" buttons.

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

Wireless-N Pocket AP/Router
AP Router Mode ▾

Admin
Time
DDNS
Power
Diagnosis
Firmware
Back-up
Reset

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

Restore to factory default :	<input type="button" value="Reset"/>
Backup Settings :	<input type="button" value="Save"/>
Restore Settings :	<input style="width: 100%;" type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Upload"/>

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.



In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button.

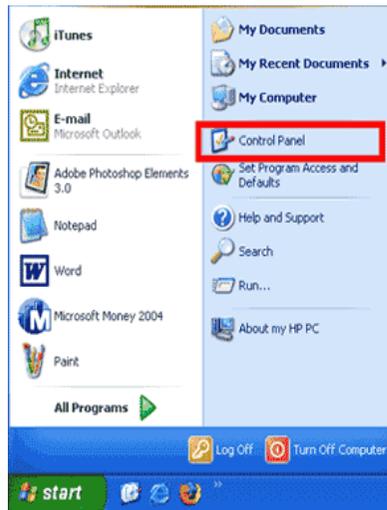
Apply Cancel

8.3 AP and Client Bridge Modes

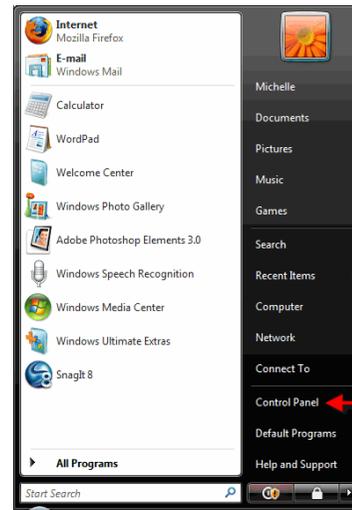
When the TRAVEL ROUTER device is set to AP or Client Bridge modes, it will no longer allocate IP addresses to its wireless clients.

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

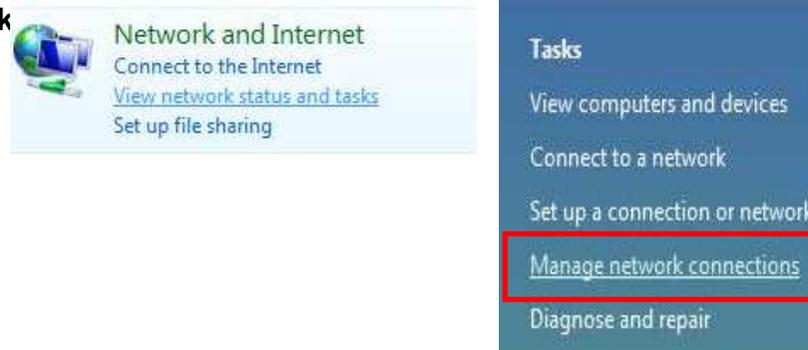


Windows Vista

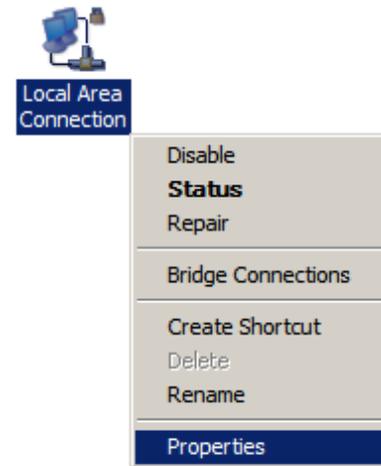
3. Windows XP, click **[Network Connection]**



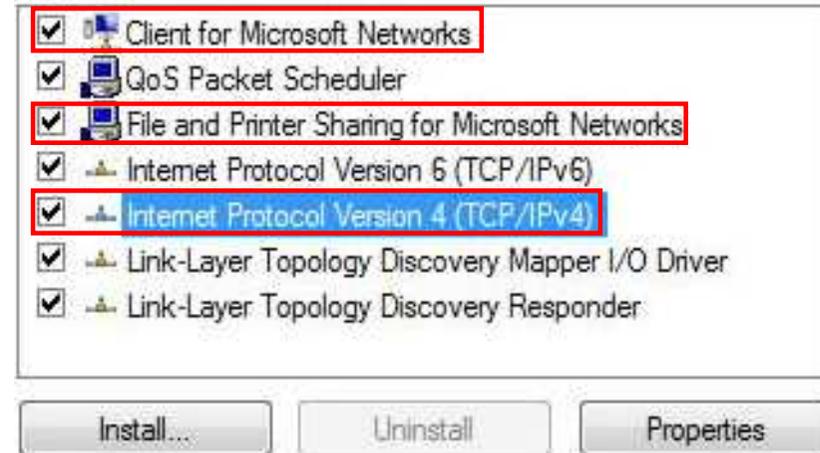
Windows Vista, click **[View Network Status and Task]** then **[Manage Network Connections]**



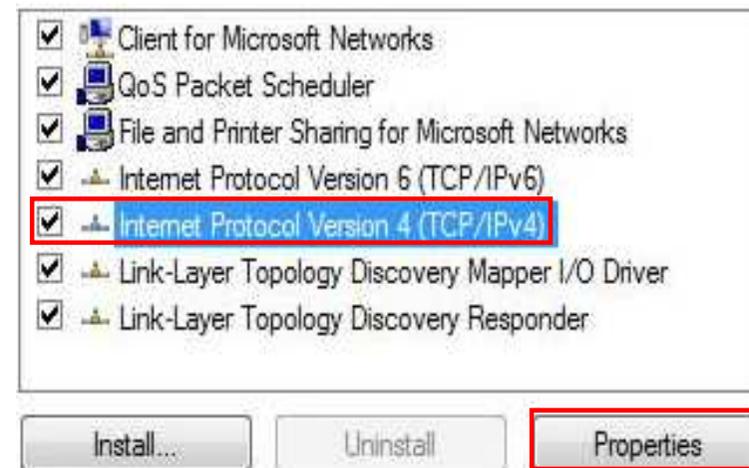
4. Right click on **[Local Area Connection]** and choose **[Properties]**.



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]

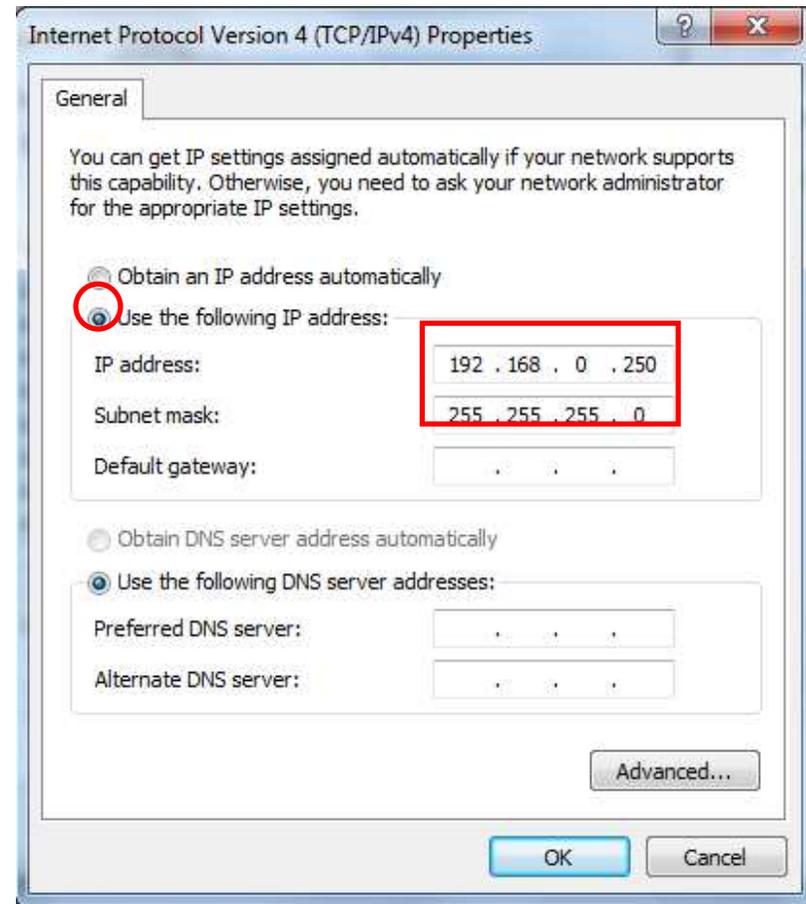


7. Manually set the IP Address. Then click [OK]

For example:

IP Address: 192.168.0.250

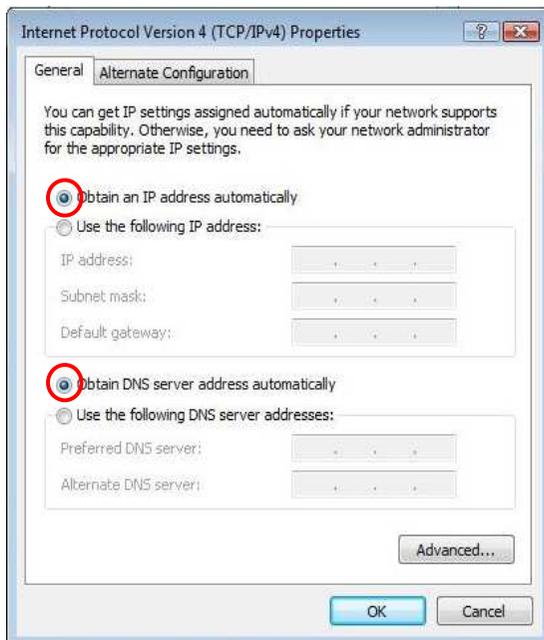
Subnet Mask: 255.255.255.0



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 in **Client Bridge Mode**.



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 RJ-45 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.

Wireless-N Pocket AP/Router Client Bridge Mode ▾

[Basic](#) [Advanced](#) [AP Profile](#)

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

Mode : Client ▾

Band : 2.4 GHz (B+G+N) ▾

Site Survey :

Wireless Information

SSID: SENAOWL

Status: Connected

Channel : 1

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	<input checked="" type="radio"/>	1	SENAOWL	00:97:53:AA:11:1C	WEP	AUTOWEP	65	11b/g/n
2	<input type="radio"/>	1	SENAOWL	00:02:6F:53:0C:9B	WEP	AUTOWEP	81	11b/g
3	<input type="radio"/>	1	SENAOWL	00:02:6F:36:9C:9A	WEP	AUTOWEP	70	11b
4	<input type="radio"/>	1	SENAOVIP	00:02:6F:E0:02:12	NONE	OPEN	44	11b/g
5	<input type="radio"/>	1	EnGenius2	06:02:6F:10:10:12	NONE	OPEN	44	11b/g
6	<input type="radio"/>	1	EnGenius1	00:02:6F:10:10:12	NONE	OPEN	34	11b/g
7	<input type="radio"/>	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 :	<input checked="" type="radio"/> Open System <input type="radio"/> 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.

Wireless-N Pocket AP/Router
Client Bridge Mode ▾

Basic
Advanced
AP Profile

AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	EnGenius	00:00:00:00:00:00	Open System	NONE	<input type="checkbox"/>
2	SENAOWL	00:02:6F:53:0C:9B	Open System	WEP	<input type="checkbox"/>
3	EnGenius3	0A:02:6F:10:10:12	Open System	NONE	<input type="checkbox"/>

Add
Edit
Move Up
Move Down
Delete Selected
Delete All
Connect

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:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

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:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.