



ENCORE
ELECTRONICS

ENHWI-N3

802.11n Wireless Router



User Manual

TABLE OF CONTENTS

1	INTRODUCTION	3
2	KEY FEATURES.....	4
3	PACKAGE CONTENTS.....	5
4	PRODUCT LAYOUT.....	6
5	NETWORK + SYSTEM REQUIREMENTS.....	8
6	ENHWI-N3 PLACEMENT.....	8
7	SETUP LAN, WAN.....	9
8	PC NETWORK ADAPTER SETUP (<i>WINDOWS XP</i>).....	10
9	BRING UP ENHWI-N3.....	12
10	SMART WIZARD	12
11	INITIAL SETUP ENHWI-N3.....	26
12	AP ROUTER MODE.....	27
13	REPEATER MODE	84
	APPENDIX A – FCC INTERFERENCE STATEMENT.....	96
	APPENDIX B – IC INTERFERENCE STATEMENT	97

I - Introduction

Congratulations on your purchase of ENHWI-N3 802.11n Wireless Router. ENHWI-N3 is backward compatible with wireless devices running under the 802.11g and 802.11b technologies. ENHWI-N3 is not only a Wireless Access Point, but also a wireless Repeater that extends your wireless coverage when used as a Repeater Mode in a established Local Area Networking or LAN, as well as 4-port 10/100 Mbps full-duplex Switch that connects your wired Ethernet LAN devices together at incredible speed.

At 150 Mbps wireless transmission rate, the Access Point built into the router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data into a single wireless channel providing a seamless access to multimedia contents. Its robust RF signal travels farther, eliminates dead spots and extends network range. For data protection, wireless security and privacy, the ENHWI-N3 encodes all wireless transmissions with WEP, WPA, and WPA2 data encryptions.

With built-in DHCP Server & a powerful SPI firewall, the ENHWI-N3 protects your computers against intruders and known Internet attacks, and still provides safe and secured VPN pass-through. With data rate at incredible speed and QoS function, the ENHWI-N3 is ideal for media-centric applications such as streaming video, internet gaming, and VoIP telephony to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

II - Key Features

Features	Advantages
Incredible Data Rate up to 150 Mbps**	Easily handled heavy data loads such as MPEG audio / video streaming,
IEEE 802.11b/g/n Compliant	Fully Interoperable with IEEE 802.11b/g/n compliant devices with legacy protection
Four 10/100 Mbps Fast Switch RJ-45 Ports (with Auto-Crossover)	Scalability. Extend your network computers.
Firewall supports, DMZ, MAC Filter, IP Filter, URL Filter, ICMP Blocking, SPI, Port Mapping, Port Forwarding, Port Trigger	Use to prevent attacks from hackers or viruses from the internet
Support 802.1x Authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security)
WDS (Wireless Distribution System)	Make Wireless AP and Bridge mode simultaneously as a wireless repeater

*** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

III - Package Contents





Check and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original packaging.

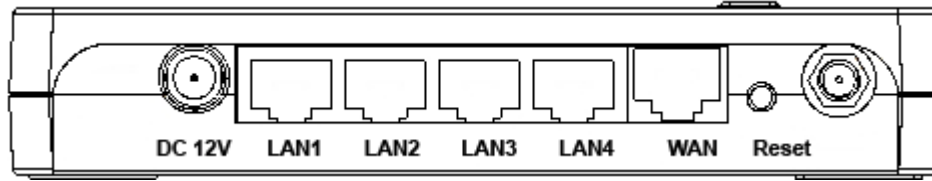
1. ENHWI-N3 Wireless 802.11n Router
2. 100V~240V Power Adapter (Use only the supplied power adapter)
3. One piece 2 dBi 2.4 GHz SMA Upgradeable Antenna
4. Quick Installation Guide
5. CD-ROM (Smart Install and User's Manual)

IV - Product Layout



Front Panel View

LED Lights	Description
 POWER	Lights up in Red when powered ON. Blinks on TEST/RESET
 WLAN	Lights up in Green when Wireless LAN is enabled. Blinks on traffic
 1 to 4	Blinks in Green on data traffic
 WAN	Lights up in Green when WAN port is use



Rear View

Item	Description
Reset	Press and release this button to reboot the device. Press and hold this button for 10 seconds to load the factory default settings of the system.
WPS™	Click this button to start WPS™ function.
DC 12V	Power connector, connects to DC 12V 1As Power Adapter
LAN1 ~ LAN4	Ports 1 to 4 Local Area Network (LAN)10/100 Mbps RJ-45 ports
WAN	Wide Area Network (WAN) port or Internet Port. Connects to xDSL or Cable Modem

V - Network + System Requirements

To begin using the ENHWI-N3, make sure you meet the following as minimum requirements:

- PC / Notebook Computer
- Operating System – Microsoft™ Windows® 98SE/ME/XP/2000/Windows Vista™
- 1 Free Ethernet port
- Wi-Fi adapter card – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- A Web Browser (Internet Explorer, Safari, Firefox, Opera etc.)
- Few Ethernet compatible CAT5 or better cables.

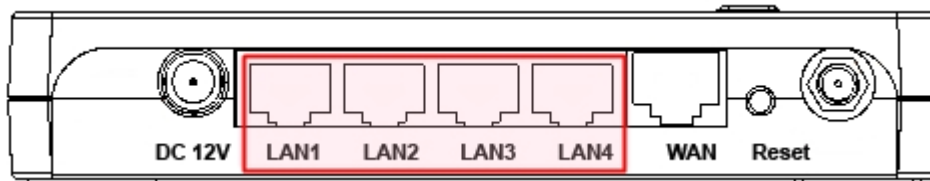
VI - ENHWI-N3 - Where to place

You can place ENHWI-N3 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your ENHWI-N3 Wireless Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem. If the antennas are not positioned correctly, performance loss can occur.

VII - Setup LAN, WAN

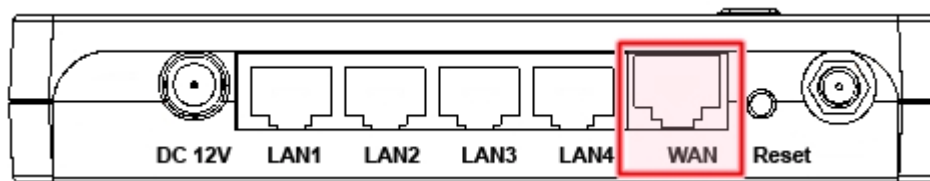
LAN connection:

Connect Ethernet cable between your PC/Notebook LAN port & one of the 4 available LAN ports on ENHWI-N3.



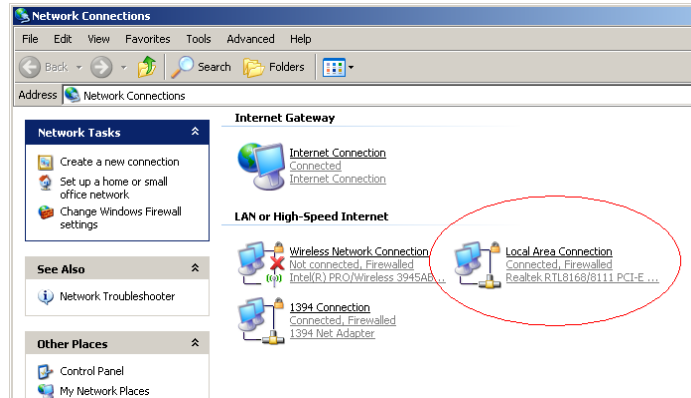
WAN connection:

Connect Ethernet cable between WAN port of your ADSL/CABLE modem & WAN port of ENHWI-N3. Make sure your ADSL/CABLE modem is already setup and working well. Contact your ISP (Internet Service Provider) if you have any questions.

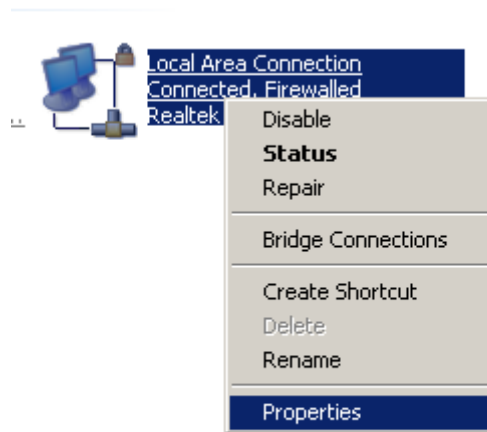


VIII - PC Network Adapter Setup (*Windows XP*)

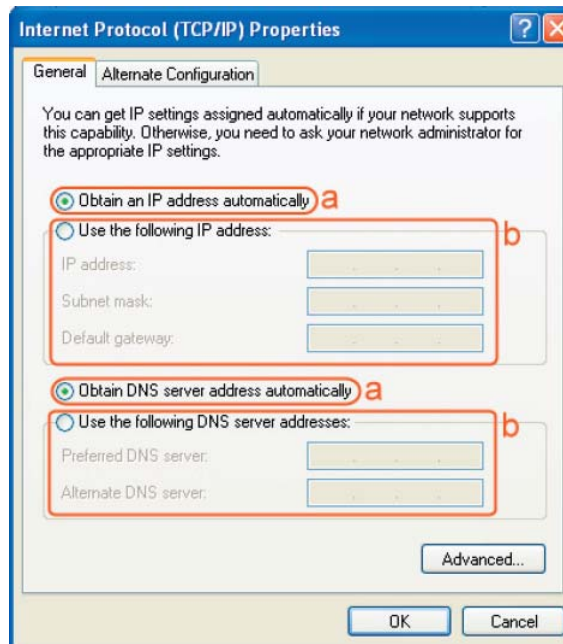
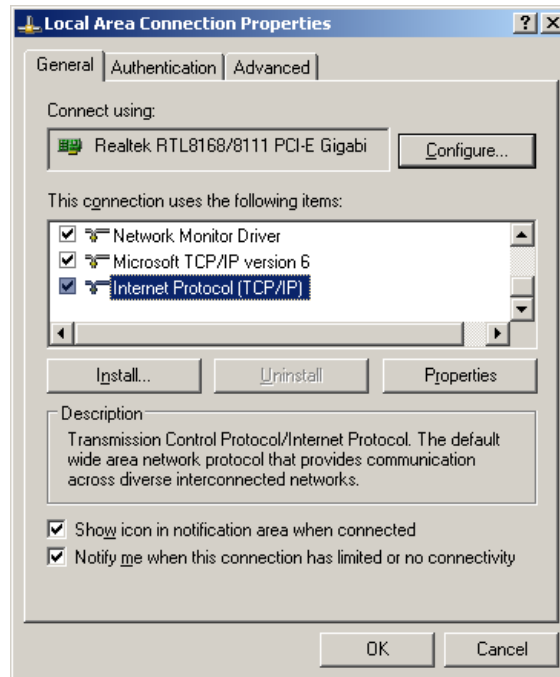
- Assuming your PC or Laptop is equipped with a Network Interface Card. Click on **START** → select “**Control panel**” → From the Control Panel Window select “**Network Connections**”



- Right-click (Use the right button of your mouse) the “**Local Area Connection**” icon then select and click “**Properties**”



- Click to Highlight the “**Internet Protocol (TCP/IP)**” then click “**Properties**” button



- Select the “General” tab.
 - ENHWI-N3 supports the DHCP function, please select both “**Obtain an IP address automatically**” and “**Obtain DNS server address automatically**”

***IX* - Power up the ENHWI-N3**

Connect the supplied power-adaptor to the power port and connect it to a wall power outlet. The ENHWI-N3 automatically enters and run the self-test phase. The Power LED will light a steady red light indicating that the ENHWI-N3 is ready for operation.

***X* - Smart Wizard**

Before you start the ENHWI-N3 router's Smart Wizard check for the followings:

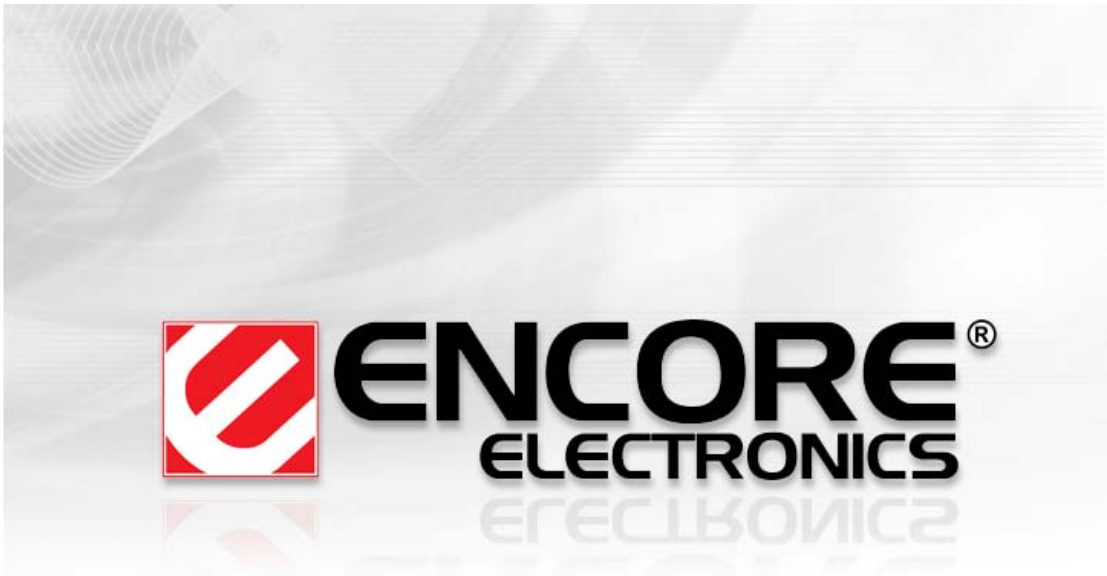
- Internet connection should be setup & ready to use (ADSL or cable modem).
- Modem must provide an RJ-45 port to connect with a ENHWI-N3 Router
- Microsoft Windows compatible PC/Notebook with UPnP enabled Network Interface Card adapter. (This can be found in your network cards advanced properties within MS Windows)
- CAT 5 network cable(s), RJ-45 port on PC/Notebook.

Step 1: Connect ENHWI-N3 “WAN” port & your Modem’s LAN port with RJ45 cable.

Step 2: Power-up the ENHWI-N3. The red power LED in the front the panel should light up & stay on to indicate that the router is ready

Step 3: Connect one of the four available LAN ports to the PC/Notebook RJ-45 NIC port with a CAT 5 RJ-45 network cable.

Step 4: Insert the ENHWI-N3 CD into your CDROM drive and the “SMART WIZARD” should run automatically after just a few seconds. If not, open the Windows Explorer, go to the root directory of the CD. Double click on the Wizard.exe file.



Making Connections Easy

Copyright©2009 Encore Electronics Inc.

A welcome screen will pop up a few seconds and then will disappear.



NOTE: The product picture may be different from what you have

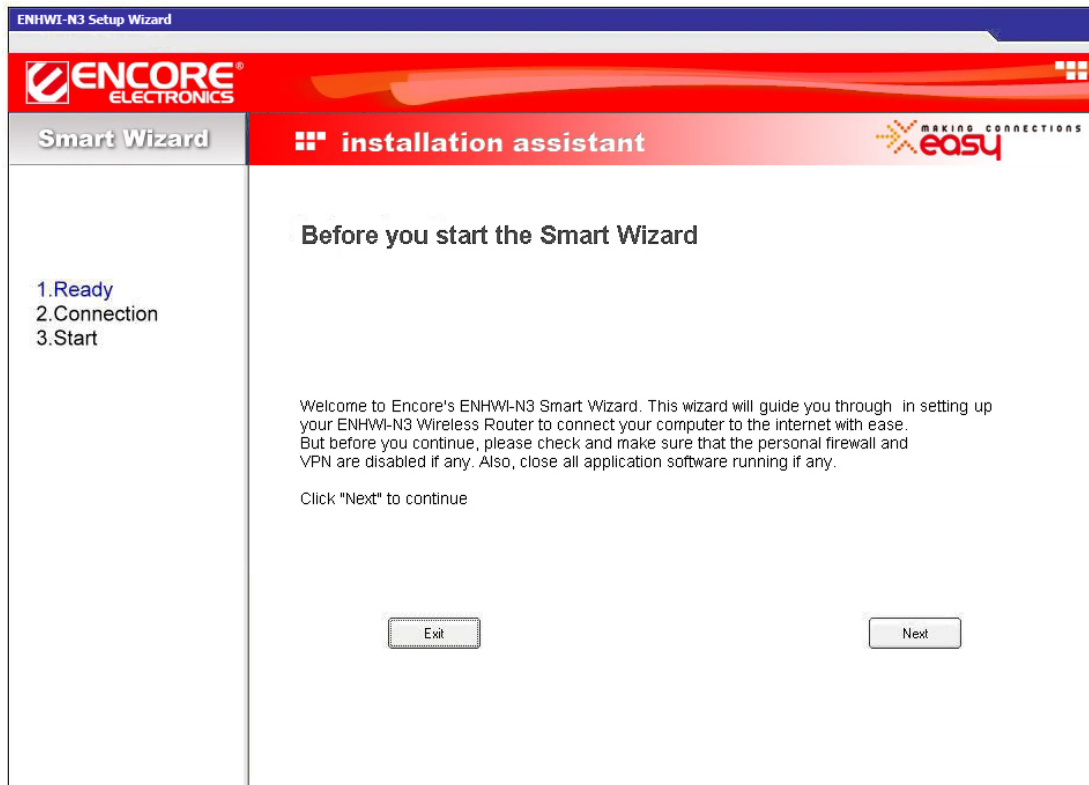
Click **Setup Wizard** to run basic setup settings of your ENHWI-N3.

Click **User Manual** to open the user manual.

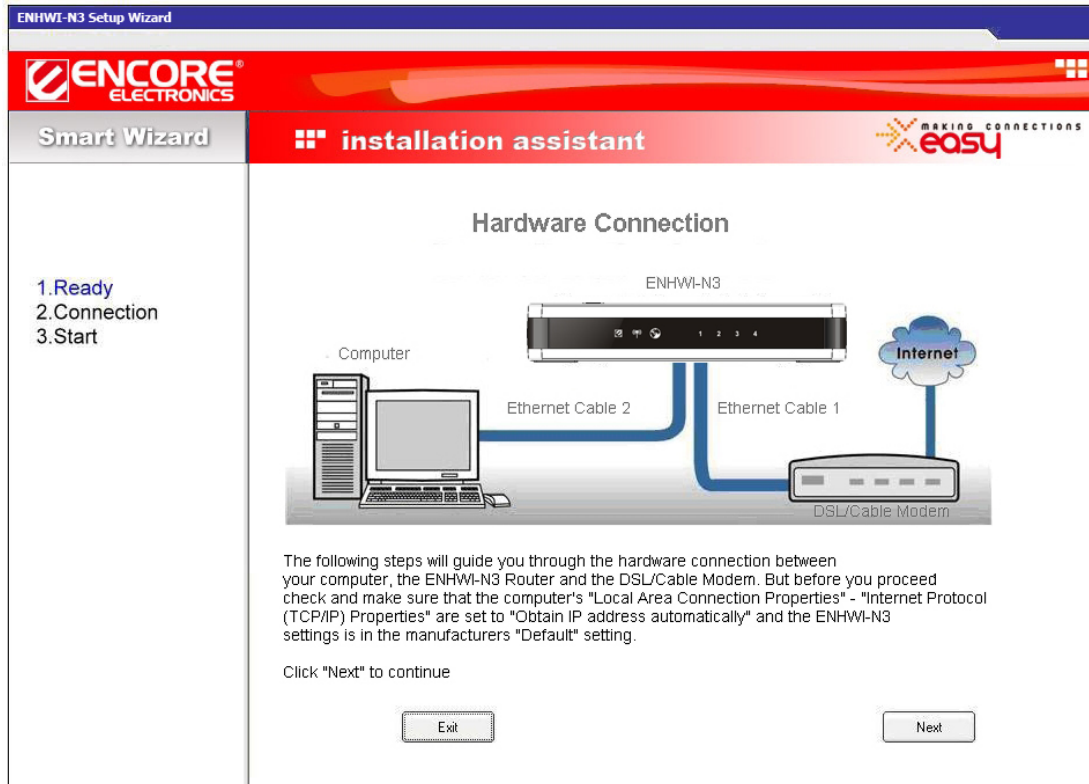
Click **Adobe Reader** to install Adobe Acrobat reader on your PC/Notebook.

Click **EXIT** when finish or anytime you want to abort.

Setup Wizard

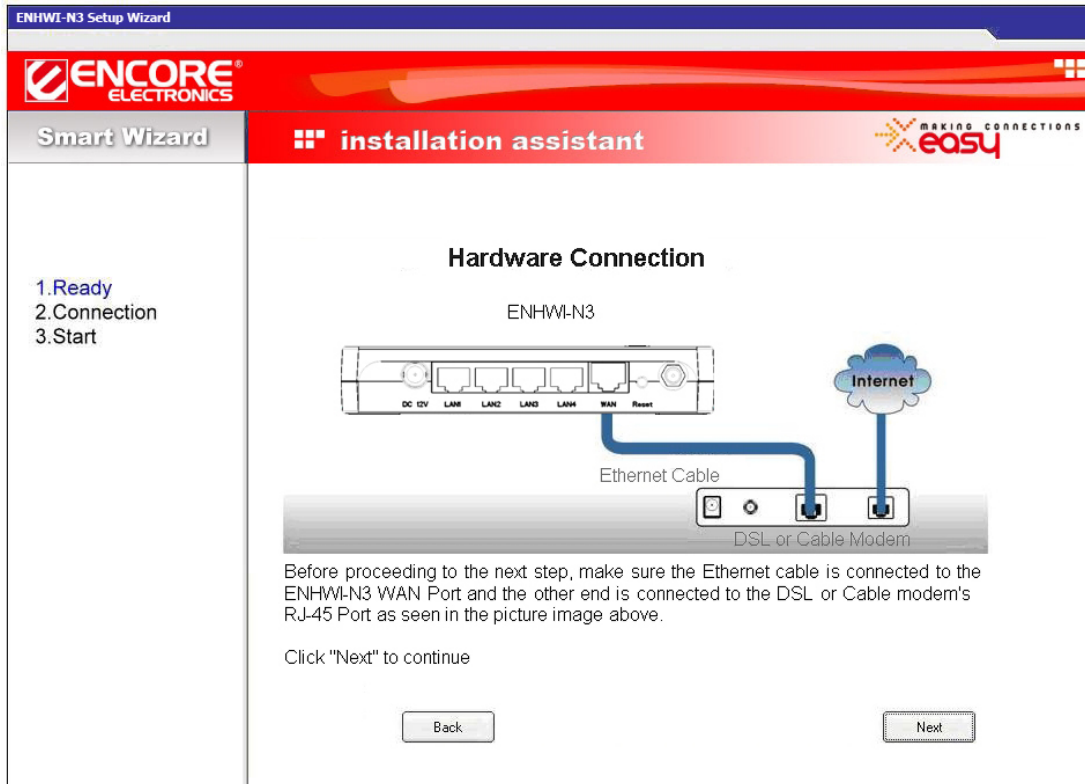


Click to proceed. Click **<Exit>** to abort.

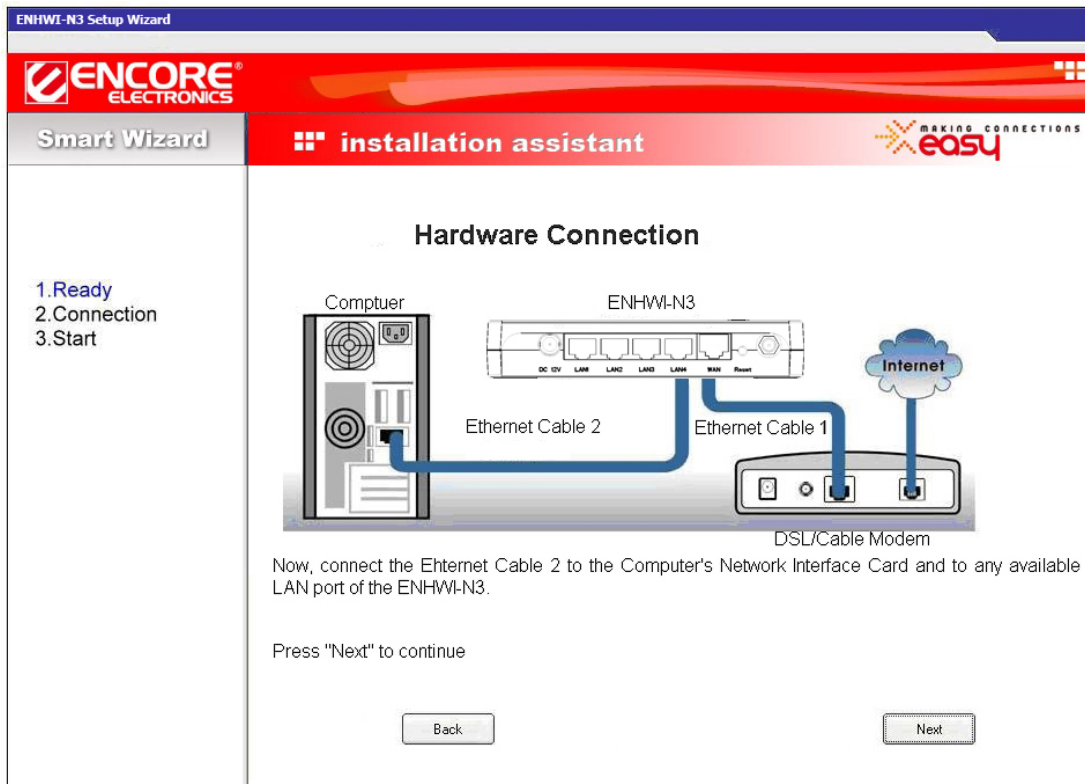


Make sure your **DSL/CABLE modem** is setup and working prior to this installation procedures. If not, call your Internet Service Provider and have them check and help you in setting up your DSL/Cable modem.

Click to proceed.



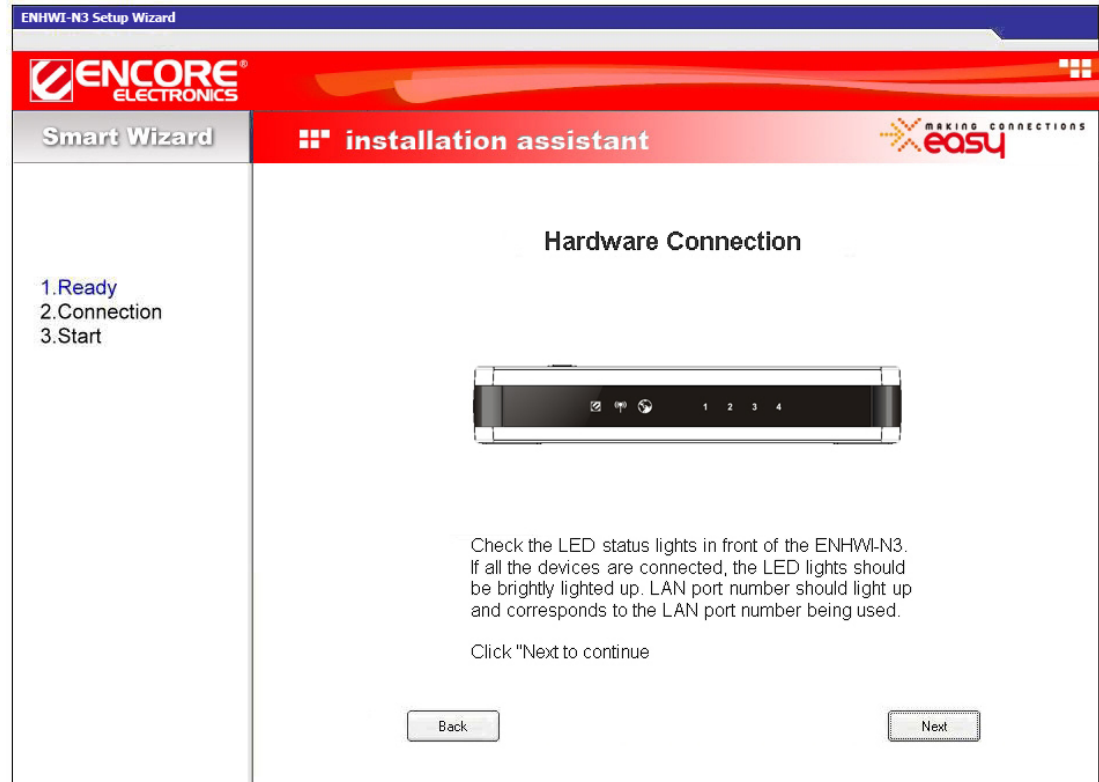
Check the MODEM and ENHWI-N3 connection. It should be as shown below.



Check power connection for modem as well as ENHWI-N3.

Make sure the antenna is connected to rear panel of ENHWI-N3.

Click **<Next>** to proceed.



Notice the LED will light up at this stage. If not, check your procedures again.

Click to configure WAN & Wireless settings.

ENHWI-N3 Setup Wizard

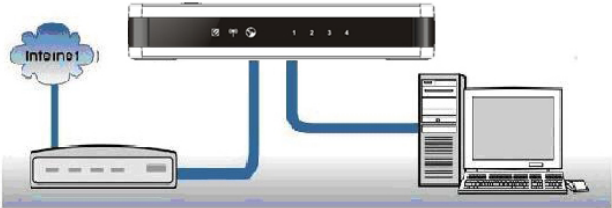
ENCORE
ELECTRONICS

Smart Wizard

installation assistant

making connections
easy

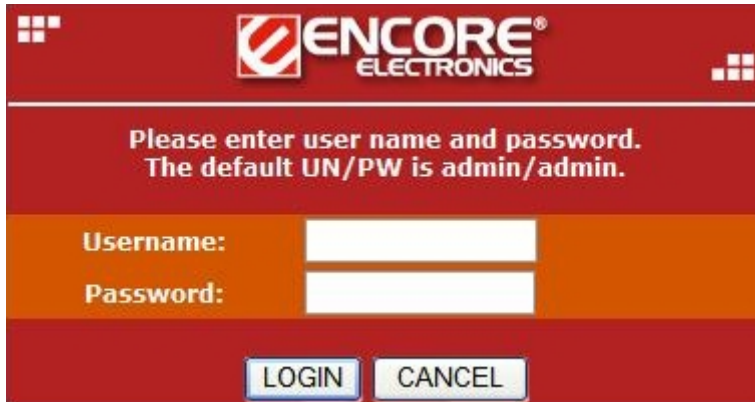
Hardware Connection




1. Ready
2. Connection
3. Start

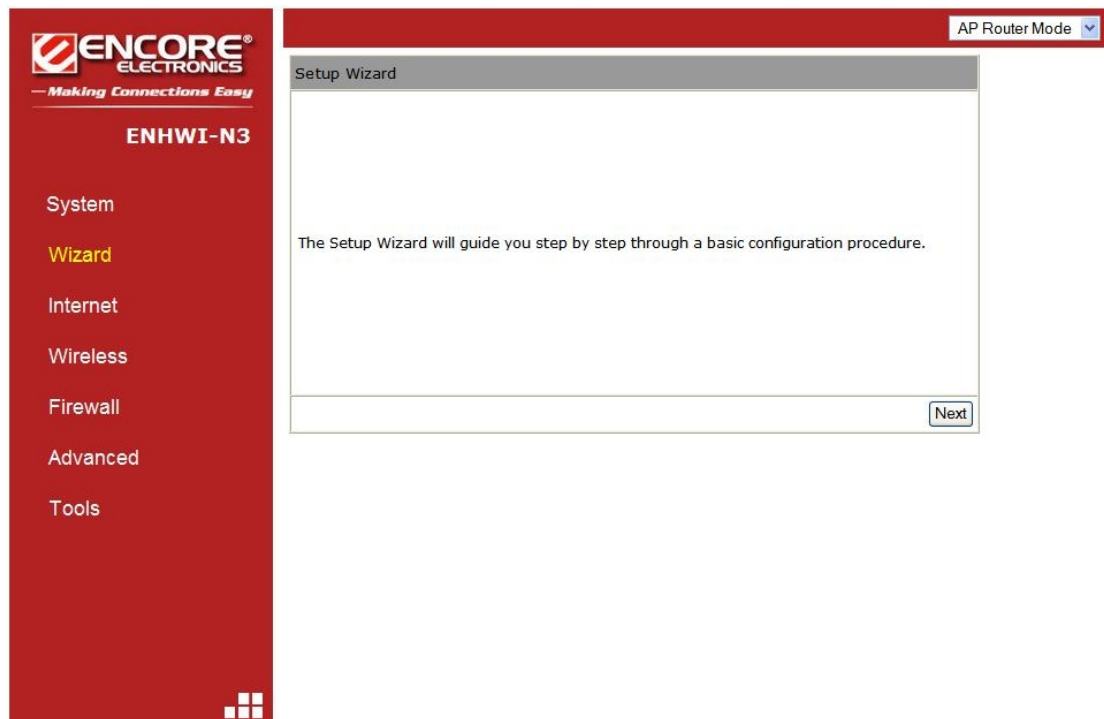
In the next **setup procedures**, you will be redirected to the ENHWI-N3 Setup Wizard screens. You will be prompted to fill up some fields for security settings and other vital information to setup your wireless LAN and WAN settings, and to connect your computer to the internet through a secured wireless connections.

Click "Next" to continue to the ENHWI-N3 Web Based setup




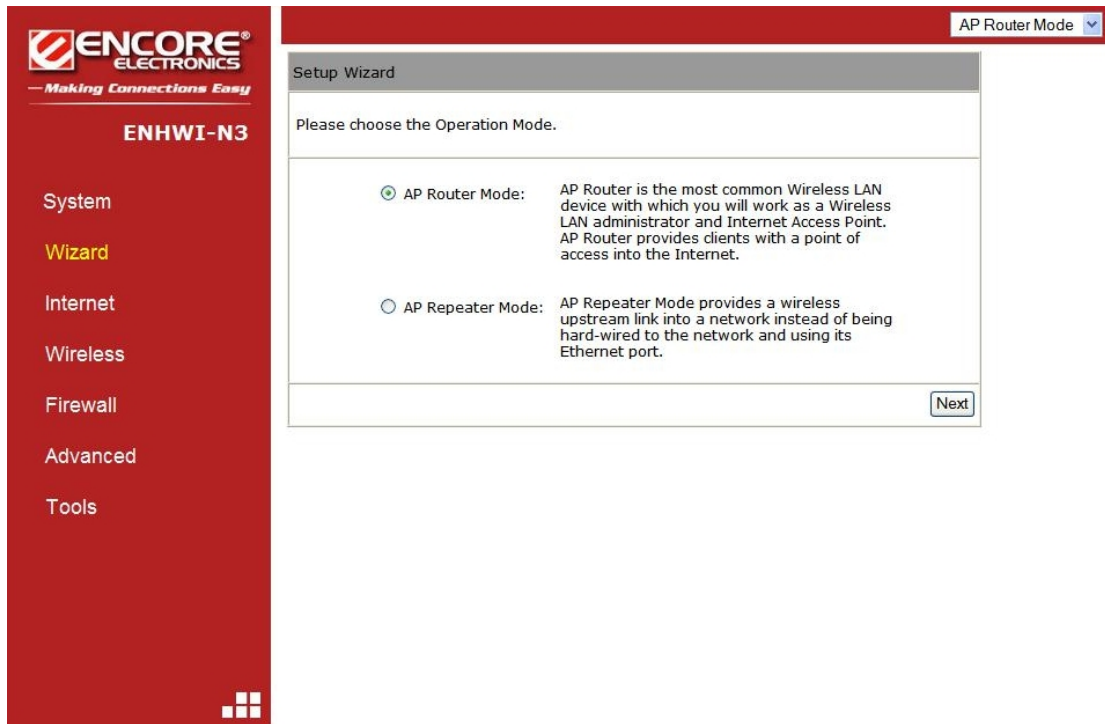
The image shows the login screen for Encore Electronics. At the top, there is a red header with the Encore Electronics logo and the text "Please enter user name and password. The default UN/PW is admin/admin." Below this, there are two input fields: "Username:" and "Password:". At the bottom, there are two buttons: "LOGIN" and "CANCEL".

Enter the factory default username is **admin** and password is also **admin**. Click  to continue. Your default browser screen will connect to the ENHWI-N3 User Interface screen using the factory default address <http://192.168.0.1> .



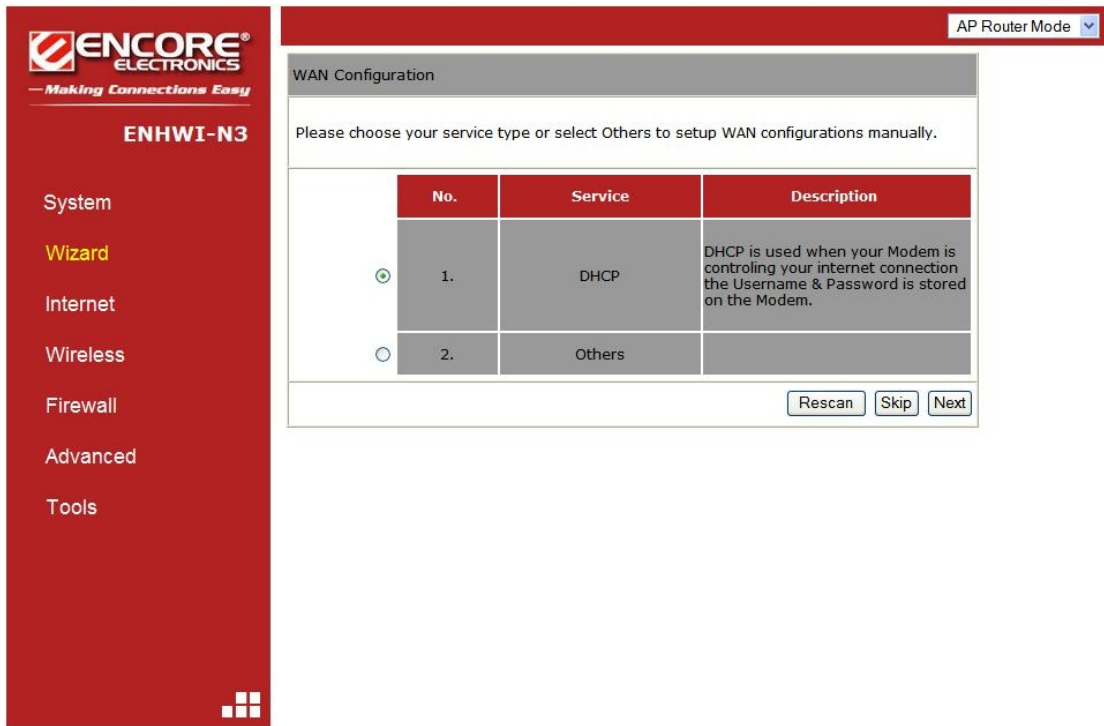
The image shows the Setup Wizard screen for the ENHWI-N3 device. The top right corner displays "AP Router Mode" with a dropdown arrow. The main content area is titled "Setup Wizard" and contains the text: "The Setup Wizard will guide you step by step through a basic configuration procedure." At the bottom right of the main content area, there is a "Next" button. On the left side, there is a red sidebar with the Encore Electronics logo and the text "Making Connections Easy". Below this, the device model "ENHWI-N3" is displayed. The sidebar contains a list of menu items: "System", "Wizard" (highlighted in yellow), "Internet", "Wireless", "Firewall", "Advanced", and "Tools".

Click  to enter the mode selection screen.



Select the mode your ENHWI-N3 is going to use. The Setup Wizard will skip the WAN configuration under **AP Repeater Mode**.

Click and your ENHWI-N3 will automatically detect your “Internet” Network settings.



The Smart Wizard will detect the DHCP and PPPoE connections automatically. In the picture above it shows that the Smart Wizard detected a DHCP server. You can choose the detected service type or select “**Others**” to setup the WAN settings manually.

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

AP Router Mode

Setup Wizard

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

Login Method: Dynamic IP Address

Hostname :

Mac :

Clone MAC Address

Next

Here, you can configure the host name and MAC address of the ENHWI-N3. The **“Clone MAC Address”** button clones the MAC address of your PC and use it as the MAC address of your ENHWI-N3 router instead of the real MAC address of the router.

The Smart Wizard has finished setting up the **WAN Configuration** portion. Click **Next** to proceed to other portions.

Setting up Wireless LAN

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

AP Router Mode

WLAN Configuration

Please choose the security level in the security bar

Lowest [Red] [Orange] [Yellow] [Green] [Dark Green] Highest

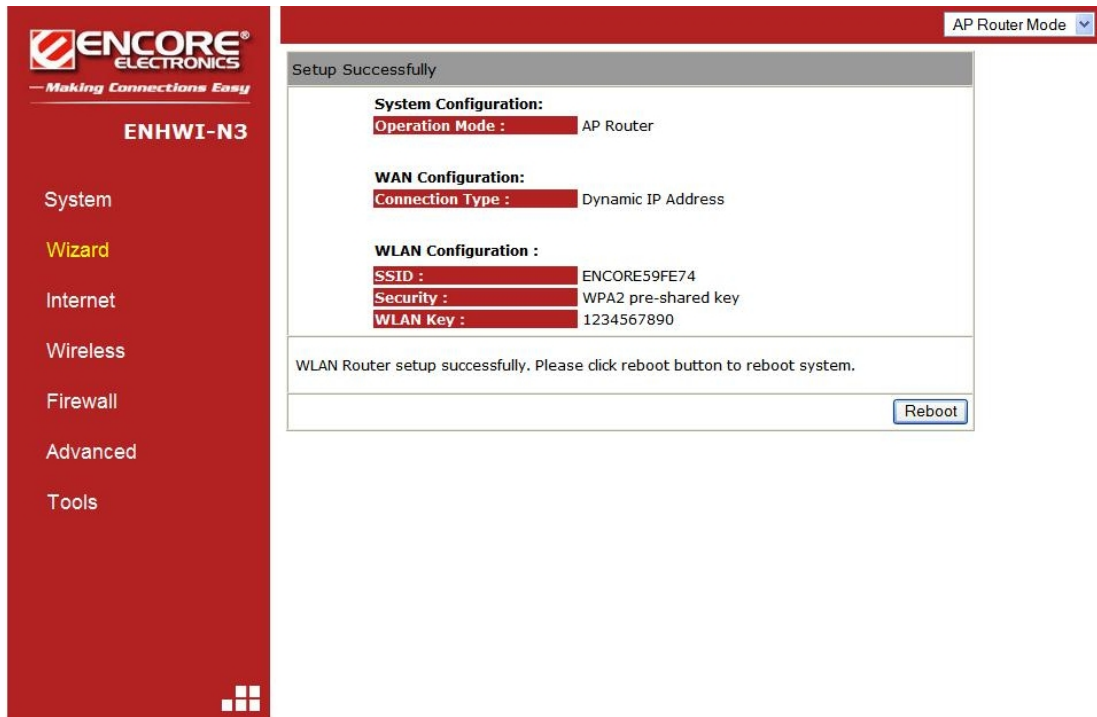
Encryption method: WPA2 PSK
Authentication Type: AES
Please input SSID in the following box.
Please input 8 ~ 63 ascii characters or 64 hexadecimal characters in the following key box.

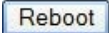
SSID : ENCORE59FE74
Key : 1234567890

Skip Next

Enter the name for your wireless network SSID (the default is ENCORE59FE74) and security key (default is 1234567890). Move and point your mouse over to the security level blocks from the weakest (red block) to the strongest (green block), and click on the selected block to select the level of security you desired. The “Key” type will depend on the wireless security you selected. If you choose WEP as the wireless security you will be prompted whether an ASCII or Hexadecimal is your preferred key type. Hexadecimal requires 10 character digits on the KEY: field.

Click to proceed



To save configuration changes click 

NOTE:

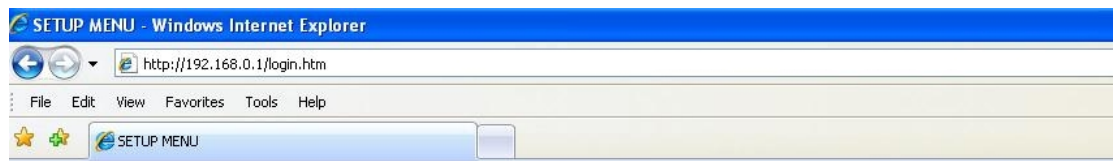
After the Wireless settings are saved and the ENHWI-N3 is rebooted, you need to reconnect your WLAN client using the new security settings you just changed. You will need to reenter the new wireless security key for the client and the ENHWI-N3 reestablish wireless connections.

XI – How to login to the ENHWI-N3 web based Graphical User Interface

The ENHWI-N3 use a web based user interface for setting up your router's configuration, it can be access through your web browser such as Internet Explorer or Mozilla Firefox.

ENHWI-N3 web based user interface login procedure

1. OPEN your browser (Example: Internet Explorer, Mozilla, Netscape, etc).
2. Type-in **http://192.168.0.1** exactly in address field and hit the **[Enter]** key on your keyboard.

A login form for ENCORE ELECTRONICS. The form has a red header with the ENCORE ELECTRONICS logo. Below the header, it says "Please enter user name and password. The default UN/PW is admin/admin." There are two input fields: "Username:" and "Password:". At the bottom, there are two buttons: "LOGIN" and "CANCEL".

3. Type-in the ENHWI-N3 Username and Password (the factory default is admin and admin)
4. Click **LOGIN** to navigate into the ENHWI-N3 configuration home page.
5. You will see the configuration home page of the ENHWI-N3 as follows.

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

AP Router Mode

Status LAN DHCP Schedule Log Monitor Language

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

System

Model	Wireless Network Broadband Router
Mode	AP Router
Uptime	2 days 17 hours 20 min 58 sec
Current Date/Time	2009/01/03 17:20:59
Hardware version	1.0.0
Serial Number	00000016
Kernel version	1.0.0
Application version	1.0.6

WAN Settings

Attain IP Protocol	Dynamic IP Address
Authentication Mode	---
Subnet Mask	---
Default Gateway	---
MAC address	00:02:6F:59:FE:D8

ENHW-N3 Home Page Screen

XII - The AP Router Mode

■ SYSTEM

Shows the Uptime, Hardware information, Serial number as well as the Firmware version information and other vital information

● Status Tab

This page allows you to monitor the status of your router.

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

AP Router Mode

Status LAN DHCP Schedule Log Monitor Language

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

System

Model	Wireless Network Broadband Router
Mode	AP Router
Uptime	2 days 17 hours 20 min 58 sec
Current Date/Time	2009/01/03 17:20:59
Hardware version	1.0.0
Serial Number	00000016
Kernel version	1.0.0
Application version	1.0.6

WAN Settings

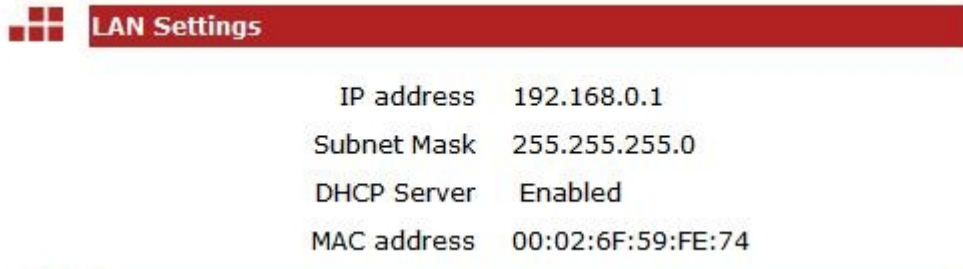
Attain IP Protocol	Dynamic IP Address
Authentication Mode	---
Subnet Mask	---
Default Gateway	---
MAC address	00:02:6F:59:FE:D8

4 WAN Settings: Scroll down to see the full information. This section displays whether the WAN port is connected to a Cable / DSL modem. It also displays the router's WAN IP address, Subnet Mask, ISP Gateway, MAC address and the Primary DNS.

WAN Settings

Attain IP Protocol	Dynamic IP Address
Authentication Mode	---
Subnet Mask	---
Default Gateway	---
MAC address	00:02:6F:59:FE:D8
Primary DNS	---

2. LAN Settings: Scroll down to see this section. Displays the ENHWI-N3 Router LAN port's current information. It also shows whether the DHCP Server is enabled or disabled.



The screenshot shows the LAN Settings page with a red header bar containing a grid icon and the text "LAN Settings". Below the header, the following information is displayed:

IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC address	00:02:6F:59:FE:74

2. WLAN Settings: Scroll down to see this section. This section displays the current WLAN configuration settings. The wireless configuration details such as the SSID, Security settings, ESSID, BSSID, Channel number and wireless clients connected info are briefly shown.



The screenshot shows the WLAN Settings page with a red header bar containing a grid icon and the text "WLAN Settings". Below the header, the following information is displayed:

Channel	11
SSID_1	
ESSID	ENCORE59FE74
Security	WPA2 pre-shared key
BSSID	00:02:6F:59:FE:74
Associated Clients	0

● LAN Tab

The screenshot shows the ENCORE ELECTRONICS ENHWI-N3 web interface. The top navigation bar includes 'Status', 'LAN', 'DHCP', 'Schedule', 'Log', 'Monitor', and 'Language'. The 'LAN' tab is selected. Below the navigation bar, there is a message: 'You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.' The 'LAN IP' section contains three input fields: 'IP address' (192.168.0.1), 'IP Subnet Mask' (255.255.255.0), and '802.1d Spanning Tree' (Disabled). The 'DHCP Server' section contains five input fields: 'DHCP Server' (Enabled), 'Lease time' (Forever), 'Start IP' (192.168.0.100), 'End IP' (192.168.0.200), and 'Domain name' (enhwi-n3). At the bottom right of the form are 'Apply' and 'Cancel' buttons.

The LAN Tab is where LAN settings can be change. If you are an entry level user, after hooking up the cables, try to access the internet from your computer. If you can open a website with no problem, leave the settings as it is. If changes were made, click the button to save the changed configurations.

LAN IP

IP address: 192.168.0.1 is the router’s LAN manufacturers default IP address (this will also be the “Default Gateway” IP address of your LAN clients). It can be change based on your LAN design and configurations. Typical designs don’t need to change this IP address.

IP Subnet Mask: 255.255.255.0 specifies the Subnet Mask address for your LAN segment. This is based on the IP address range used.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server

DHCP Server: This can be enabled or disabled, “Enabled” by default.

Lease time: Lease time assigned to all IP address by the DHCP server.

Start IP: This is the first IP address in the IP pool range in which are being assigned and leased to DHCP clients.

End IP: This is the end of the IP address pool range

Domain Name: The Domain Name for the existing or customized network.

● DHCP Tab

The screenshot shows the DHCP Client Table configuration page. The interface includes a navigation menu on the left with options like System, Wizard, Internet, Wireless, Firewall, Advanced, and Tools. The main content area displays the DHCP Client Table with a single entry for IP address 192.168.0.100 and MAC address 00:21:70:BE:37:B2. Below the table, there is a section for enabling static DHCP IP, which includes input fields for IP address and MAC address, and buttons for Add, Reset, and Apply. The current static DHCP table is also shown with columns for NO., IP address, MAC address, and Select, along with buttons for Delete Selected, Delete All, and Reset.

AP Router Mode ▾

Status LAN **DHCP** Schedule Log Monitor Language

DHCP Client Table

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

IP address	MAC address	Expiration Time
192.168.0.100	00:21:70:BE:37:B2	Forever

Refresh

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select
-----	------------	-------------	--------

Delete Selected Delete All Reset

Apply Cancel

This is where to view the current LAN clients that have assigned or leased IP address by the DHCP server. This screen also shows all the DHCP clients that are currently connected to your network. The table shows the assigned or leased IP address, MAC address and the lease expiration data for each DHCP clients. Use

the **<Refresh>** button to update the available information. Click the **<Refresh>** button to get the updated table.

You can click to put a check mark on “**Enable Static DHCP IP**”. It is possible to add more static DHCP IP addresses. They are listed in the table “**Current Static DHCP Table**”. IP address can be deleted if wanted to.

Click the **<Apply>** button to save the changes made to the configuration.

● Schedule Tab

This page allows users to set up a scheduled function for the Firewall and Power Saving features of the ENHWI-N3 router.

The screenshot shows the 'Schedule' tab selected in a navigation menu. The page title is 'AP Router Mode'. Below the menu, there is a descriptive paragraph: 'You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.' Below this is a checkbox labeled 'Enabled Schedule Table (up to 8)'. A table with the following data is displayed:

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	All Time---Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

Below the table are buttons for 'Add', 'Edit', 'Delete Selected', and 'Delete All'. At the bottom right are 'Apply' and 'Cancel' buttons.

Edit the scheduled function to allow configuration for firewall or power savings services. Fill in the schedule and select type of service you desired. Click **<Apply>** to save the

settings.


AP Router Mode ▾

Status | LAN | DHCP | **Schedule** | Log | Monitor | Language

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

Schedule Description :	<input type="text" value="schedule 01"/>
Service :	<input type="checkbox"/> Firewall <input checked="" type="checkbox"/> Power Saving
Days :	<input checked="" type="checkbox"/> Every Day <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time of day :	<input checked="" type="checkbox"/> All Day (use 24-hour clock) From <input type="text"/> : <input type="text"/> To <input type="text"/> : <input type="text"/>

The “Schedule” table screen lists the pre-scheduled services. Select any of the schedules by using the check box located on the right side of each line to edit or Delete selected schedule line.



ENHWI-N3

- System
- Wizard
- Internet
- Wireless
- Firewall
- Advanced
- Tools

AP Router Mode ▾

Status | LAN | DHCP | **Schedule** | Log | Monitor | Language

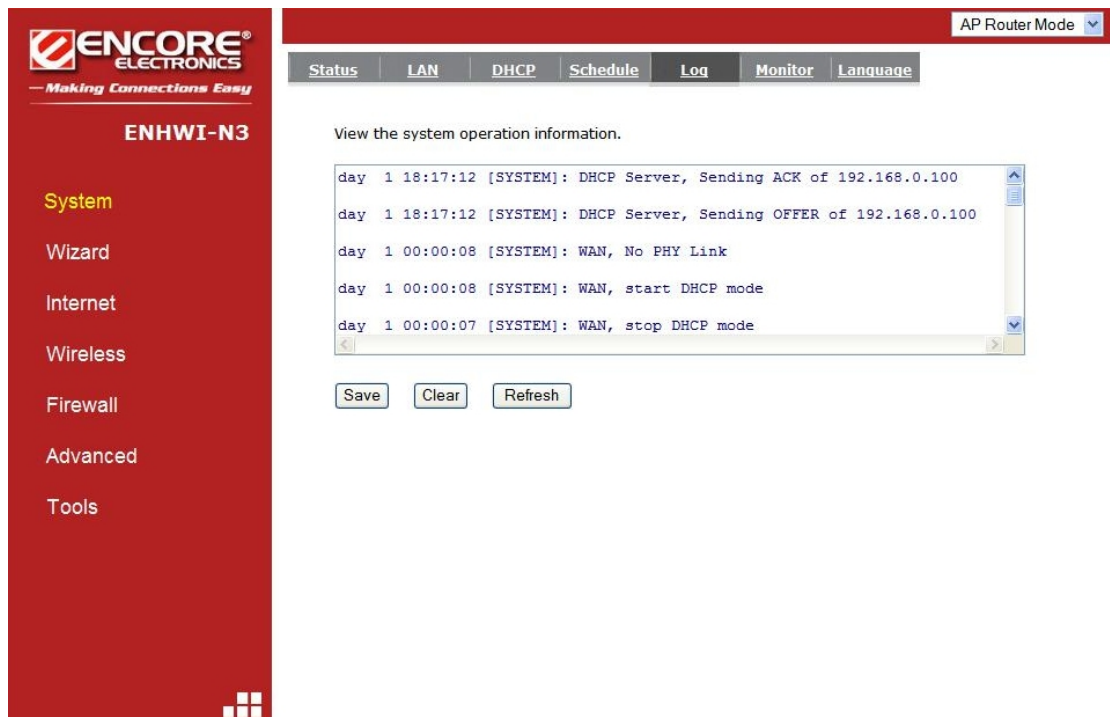
You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	All Time--Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>
2	schedule 02	Firewall	All Time--Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>
3	schedule 03	Power Saving+Firewall	All Time--Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

● Event Log Tab

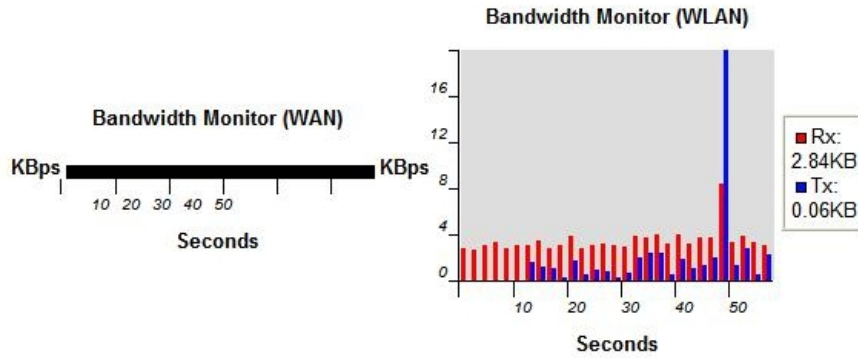
On this “Event Log” screen, it displays all events and events information occurred after the start-up. Scroll down to see more. The Event Log can be saved to the local file-storage device such as hard disc drive by using the **<Save>** button, or the Event Log can be emptied using the **<Clear>** button. Use the **<Refresh>** button to reset the Event Log and to get the most updated information. When the router is powered OFF, the Event Log will be wiped out and will come up empty. The saved logs can be uploaded and viewed again.



● Monitor Tab


This screen shows the histogram of the network connection on WAN, LAN & WLAN. Auto refresh keeps information updated frequently.

You can monitor the bandwidth in different interface. This page will refresh in every five seconds.



● Language Tab

This is where you select preferred language.



ENHWI-N3

- System
- Wizard
- Internet
- Wireless
- Firewall
- Advanced
- Tools

AP Router Mode ▼

Status | LAN | DHCP | Schedule | Log | Monitor | **Language**

You can select other language in this page.

Multiple Language :

Choose your language

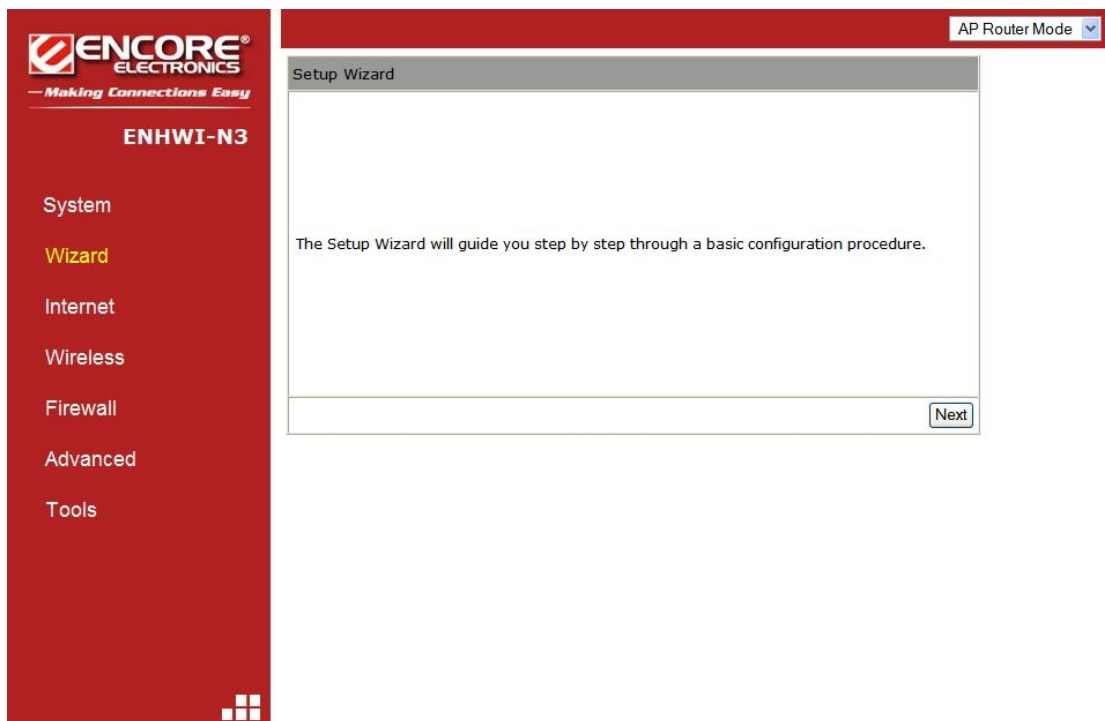
Choose your language

English

Italiano

■ WIZARD

Click **Wizard** to configure the basic functionalities of the ENHWI-N3 Router. A popup Setup Wizard Window will be immediately displayed. If the popup window for Setup Wizard failed to appear check your Popup Settings and make sure popup is allowed at least temporarily for this purpose. Before you continue, check all the needed cables if they are properly hooked up. Check your DSL or Cable Modem if working properly and is connected to your ISP and then click **<Next>**. Refer to the **Smart Wizard** section for more details.



■ INTERNET

- Status

This page shows the current Internet connection type and status

The screenshot shows the web interface for the ENHWI-N3 router. The top navigation bar includes the Encore Electronics logo and the slogan "Making Connections Easy". The model number "ENHWI-N3" is displayed. A dropdown menu is set to "AP Router Mode". Below the navigation bar, there are tabs for "Status", "Dynamic IP", "Static IP", "PPPoE", and "PPTP". The "Dynamic IP" tab is selected, and the page displays the current internet connection status and related information. The "WAN Settings" section shows the following configuration:

WAN Settings	
Attain IP Protocol	Dynamic IP Address
IP address	192.168.1.62
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC address	00:02:6F:59:FE:D8
Primary DNS	68.238.64.12,68.238.128.12

A "Renew" button is located at the bottom right of the WAN Settings section.

- Dynamic IP

Use the MAC address when registering for the Internet service, and do not change it unless required by your ISP. If your ISP use the MAC address of the Ethernet card as an identifier, connect only the PC with the registered MAC address to the broadband router and click the **<Clone MAC Address>** button. This will replace the current MAC address with the already registered Ethernet card MAC address.

The screenshot shows the web interface for the ENHWI-N3 router. The top navigation bar includes the Encore Electronics logo and the slogan "Making Connections Easy". The main menu on the left lists: System, Wizard, Internet (highlighted in yellow), Wireless, Firewall, Advanced, and Tools. The top right corner shows "AP Router Mode" with a dropdown arrow. Below the navigation bar, there are tabs for "Status", "Dynamic IP", "Static IP", "PPPoE", and "PPTP". The "Dynamic IP" tab is selected. The main content area contains the text: "You can select the type of the account you have with your ISP provider." Below this text are two input fields: "Hostname :" and "MAC address :". The "MAC address" field contains the value "000000000000" and has a "Clone MAC" button next to it. At the bottom right of the form area are "Apply" and "Cancel" buttons.

Host Name: This is optional.

MAC address: The default value is set to the WAN's physical address or MAC of the broadband router.

- Static IP

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

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

- System
- Wizard
- Internet
- Wireless
- Firewall
- Advanced
- Tools

AP Router Mode

Status Dynamic IP Static IP PPPoE PPTP

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

IP address:	172.1.1.1
IP Subnet Mask :	255.255.0.0
Default Gateway :	172.1.1.254
Primary DNS :	
Secondary DNS :	

Apply Cancel

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

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

- System
- Wizard
- Internet
- Wireless
- Firewall
- Advanced
- Tools

AP Router Mode

Status Dynamic IP Static IP PPPoE PPTP

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

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

Apply Cancel

Login / Password: Enter the PPPoE username and password assigned by your ISP Provider.

Service Name: This is optional.

Maximum Transmission Unit (MTU): This is the maximum size of the packets.

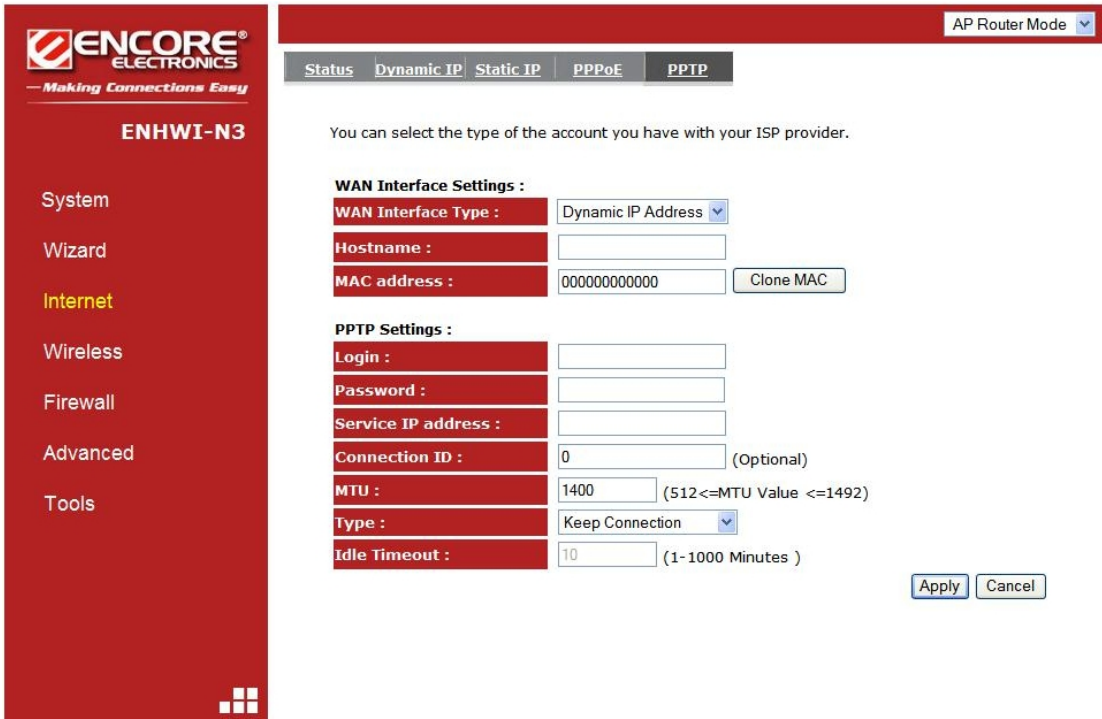
Type: **Keep Connection** - will stay connected to the Internet

Automatic Connection - automatically connects to the Internet when an application needs it, and drops the connection after the designated idle time period.

Manual Connection – manually connect and disconnect to the internet by the user

Idle Timeout (available only under Automatic Connection): This is a maximum period of time for which the Internet connection is maintained during inactivity. If the application is inactive for certain time designated here the internet connection will be automatically dropped.

- Point-to-Point Tunneling Protocol (PPTP)



PPTP allows the secure connection over the Internet by simply dialing in to a local point provided by your ISP provider. The image screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

Click **<Apply>** to save configuration and connect to ISP provider.

■ WIRELESS

- Basic

In basic setting page, you can set wireless Radio, Mode, Band, SSID, and Channel.

AP Router Mode ▾

Basic | **Advanced** | Security | Filter | WPS | Client List | Policy

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

Radio : Enable Disable

Mode : AP ▾

Band : 2.4 GHz (B+G+N) ▾

Enable SSID#: 1 ▾

SSID1 : ENCORE59FE74

Auto Channel : Enable Disable

Channel : 11 ▾

Apply Cancel

Radio: You can turn on/off wireless radio. If wireless Radio is turned off, the ENHWI-N3 will not take wireless connections.

Mode: Three operation modes for selections, the **AP router** and **AP router with WDS**. If you choose **AP Router Mode**, there will be two selections under it, the **AP** or **WDS** function in the drop-down menu.

Band: You can select the wireless standards running on your network environment such as the following:

- 2.4 GHz(B):** If all your clients are using 802.11b
- 2.4 GHz(N):** If all your clients are using 802.11n
- 2.4 GHz(B+G):** If both 802.11b or a 802.11g
- 2.4 GHz(G):** If all your clients are using 802.11g
- 2.4 GHz(B+G+N):** If your clients are mixed using 802.11b, 802.11g, or 802.11n

Enable ESSID: ENHWI-N3 supports up to 4 SSID. Use the down arrow to select the number of SSID you wanted to have in your wireless LAN. Once established you can set the security policy settings for each. See “Policy” section for more details.

ESSID1 to ESSID4: ESSID is the name of your wireless network. It is recommended to use a unique name to identify your wireless device in the LAN. This is case sensitive and up to 32 printable characters.

Auto Channel: Disable by default. If Enabled will automatically search all channels and automatically change to the clearest channel detected. Different items are visible below the **Auto Channel**.

Channel: Channel 11 by default. This is visible only when the **Auto Channel** is disabled. You can enter your preferred channel number here for the ENHWI-N3 wireless LAN.

Check Channel Time: This menu is visible only when the **Auto Channel** is enabled. Selections are from One Hour to One Week. This is the duration of when will the ENHWI-N3 check for and use the clearest channel in the area automatically.

- **WDS with AP Router**

Wireless Distribution System. The WDS is a way of interconnecting wireless routers and allow an extended wireless network coverage using multiple wireless routers without the use of a wired backbone. Each WDS AP requires the same channel and encryption type to work.

AP Router Mode ▾

Basic | **Advanced** | Security | Filter | WPS | Client List | Policy

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

Radio : Enable Disable

Mode : WDS ▾

Band : 2.4 GHz (B+G+N) ▾

Enable SSID#: 1 ▾

SSID1 : ENCORE59FE74

Auto Channel : Enable Disable

Channel : 11 ▾

MAC address 1 : 000000000000

MAC address 2 : 000000000000

MAC address 3 : 000000000000

MAC address 4 : 000000000000

Set Security :

MAC address 1~4: Please enter the MAC address(es) of the neighboring APs that participates in the WDS. A maximum of 4 devices are allowed.

Set Security: WDS Security depends on your AP security settings. Note: It does not support **mixed mode** such as WPA-PSK/WPA2-PSK Mixed mode.

- Advanced

On this tab you can set the advanced wireless settings. If you're in doubt what to enter or use here, leave these settings as it is. This is for advance users only. Wrong parameters can make the router un-operational.

The screenshot shows the configuration interface for an ENCORE ELECTRONICS ENHWI-N3 router. The interface is in the 'Advanced' tab, which is highlighted in red. The top navigation bar includes 'Basic', 'Advanced', 'Security', 'Filter', 'WPS', 'Client List', and 'Policy'. The 'Advanced' tab is selected. The main content area is titled 'ENHWI-N3' and contains a warning message: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.' Below the warning, there are several configuration fields:

- Fragment Threshold :** 2346 (256-2346)
- RTS Threshold :** 2347 (1-2347)
- Beacon Interval :** 100 (20-1024 ms)
- DTIM Period :** 1 (1-10)
- Data rate :** Auto
- N Data rate :** Auto
- Channel Bandwidth :** Auto 20/40 MHz 20 MHz
- Preamble Type :** Long Preamble Short Preamble
- CTS Protection :** Auto Always None
- Tx Power :** 100 %

At the bottom right of the configuration area, there are 'Apply' and 'Cancel' buttons.

Fragment Threshold: Default value is 2346. Specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in a bad performance.

RTS Threshold: Default value is 2347. When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval: Default value is 100. This is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

DTIM Period: Default value is 1. Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Data Rate: The “Data Rate” is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate: The “Data Rate” is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth: This is the range of frequencies that will be used.

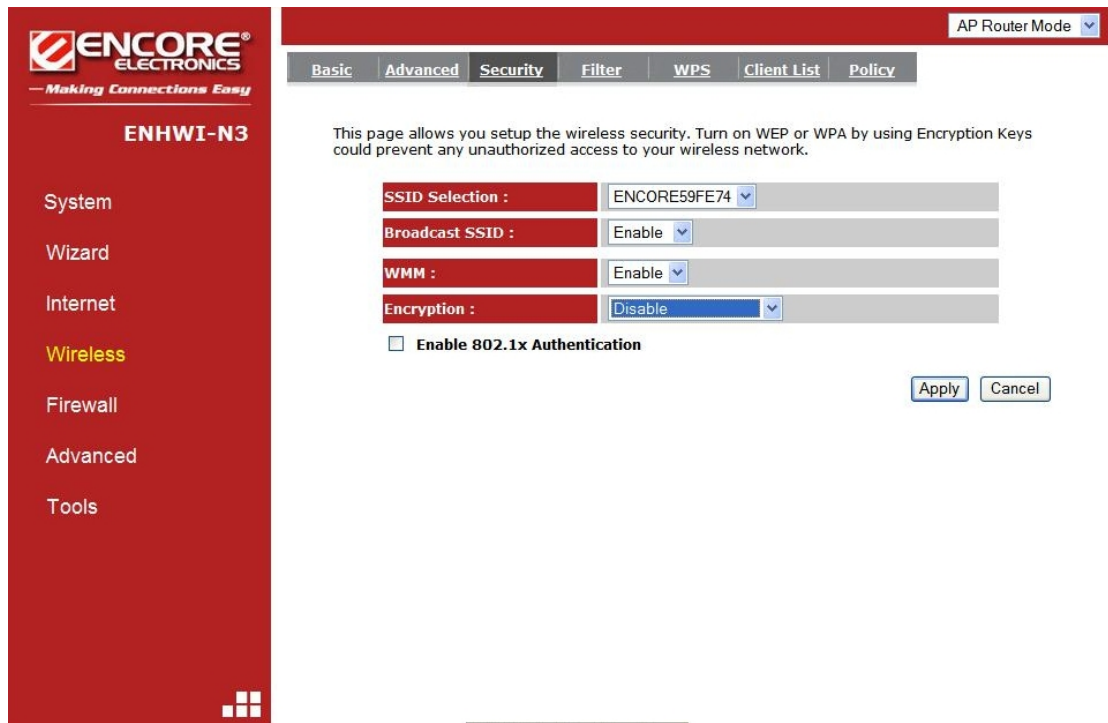
Preamble Type: The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a lower due to an increase of data frame transmission.

TX Power: 10% to 100%. Default value is 100%.

- Security

ENHWI-N3 provides complete wireless LAN security types. Selections are WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key or PSK and WPA with RADIUS. With these wireless securities, unauthorized access can be prevented. Make sure all other wireless stations use the same security type, and were setup with the same security key.



ESSID Selection: ENHWI-N3 router supports multiple ESSID, you can name your wireless ESSID here.

Broadcast ESSID: If you enabled “Broadcast ESSID”, every wireless station located within the coverage of this Router can see this ESSID. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.

WMM: Wi-Fi Multi Media if enabled supports QoS to dedicate line and other resource for better audio, video and voice streaming to a particular station and applications.

Encryption: If set to Disable, the router will have no protection against uninvited wireless guests, your LAN will be prone to hackers. It is highly recommended to Enable this function and set your own wireless security.

Enable 802.1x Authentication

IEEE 802.1x is an authentication protocol using RADIUS server. When this is Enabled, every LAN user must use an 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.

The screenshot shows the ENCORE Electronics web interface. The top navigation bar includes 'Basic', 'Advanced', 'Security', 'Filter', 'WPS', 'Client List', and 'Policy'. The 'Security' tab is selected. The page title is 'ENHWI-N3'. The left sidebar contains menu items: System, Wizard, Internet, Wireless (highlighted), Firewall, Advanced, and Tools. The main content area has a sub-header 'AP Router Mode' and a description: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this are several configuration fields: 'SSID Selection' (ENCORE59FE74), 'Broadcast SSID' (Enable), 'WMM' (Enable), and 'Encryption' (Disable). A checkbox labeled 'Enable 802.1x Authentication' is checked. Below it are three input fields: 'RADIUS Server IP address', 'RADIUS Server port' (1812), and 'RADIUS Server password'. 'Apply' and 'Cancel' buttons are at the bottom right.

WEP Encryption

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter up to four WEP keys and select one of them as a default key. The AP can receive any packet encrypted by one of the four keys.

ENCORE[®] ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

AP Router Mode

Basic Advanced **Security** Filter WPS Client List Policy

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

SSID Selection : ENCORE59FE74

Broadcast SSID : Enable

WMM : Enable

Encryption : WEP

Authentication type : Open System Shared Key Auto

Key Length : 64-bit

Key type : ASCII (5 characters)

Default key : Key 1

Encryption Key 1 : *****

Encryption Key 2 : *****

Encryption Key 3 : *****

Encryption Key 4 : *****

Enable 802.1x Authentication

Apply Cancel

Authentication Type: There are two authentication types: "**Open System**" and "**Shared Key**". Both AP and wireless client must be configured with the same authentication type.

Key Length: You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Type: You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Default Key: It's the key used to encrypt data.

Key1 - Key4: The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device.

64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys.

128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click **<Apply>** at the bottom of the screen to save the above configurations.

WPA Pre-Shared Key Encryption

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. The encryption key is not easy to be cracked by hackers. This is the best security available.

The screenshot shows the configuration interface for an ENCORE ELECTRONICS ENHWI-N3 router. The interface is in "AP Router Mode" and the "Security" tab is selected. The settings are as follows:

SSID Selection :	ENCORE59FE74
Broadcast SSID :	Enable
WMM :	Enable
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

Buttons for "Apply" and "Cancel" are located at the bottom right of the configuration area.

WPA-RADIUS Encryption

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication.

It uses **TKIP** or **CCMP (AES)** to change the encryption key frequently. Press **<Apply>** button when you are done.

The screenshot displays the configuration interface for an ENCORE Electronics device, specifically the ENHWI-N3 model. The interface is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes options for System, Wizard, Internet, **Wireless** (highlighted), Firewall, Advanced, and Tools. The main configuration area is titled "AP Router Mode" and contains several tabs: Basic, Advanced, Security (selected), Filter, WPS, Client List, and Policy. Below the tabs, a message states: "This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network." The configuration fields are as follows:

SSID Selection :	ENCORE59FE74
Broadcast SSID :	Enable
WMM :	Enable
Encryption :	WPA RADIUS
WPA type :	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA2 Mixed
RADIUS Server IP address :	
RADIUS Server port :	1812
RADIUS Server password :	

At the bottom right of the configuration area, there are two buttons: "Apply" and "Cancel".

- MAC Address Filtering

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

ENCORE ELECTRONICS
— Making Connections Easy

ENHWI-N3

System
Wizard
Internet
Wireless
Firewall
Advanced
Tools

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
<input type="text"/>	<input type="text"/>

Add Reset

MAC Address Filtering Table :

NO.	Description	MAC address	Select
-----	-------------	-------------	--------

Delete Selected Delete All Reset

Apply Cancel

Enable wireless access control: Enable the wireless access control function

Adding an address into the list

Enter the "MAC Address" and "Description" of the wireless station to be added and then click **<Add>**. The wireless station will now be added into the "MAC Address Filtering Table" below. If you are having any difficulties filling in the fields, just click "Reset" and both "MAC Address" and "Description" fields will be cleared.

Remove an address from the list

If you want to remove a MAC address from the "MAC Address Filtering Table", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Wi-Fi Protected Setup™ (WPS™)

WPS™ is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you.

The wireless router supports two types of WPS, the WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

 Enable'. Below is 'Wi-Fi Protected Setup Information' with fields: WPS Current Status (Configured), Self Pin Code (58978443), SSID (ENCORE59FE74), Authentication Mode (WPA/WPA2 pre-shared key), Passphrase Key (encore-usa), WPS Via Push Button (Start to Process), and WPS via PIN (Start to Process)."/>

AP Router Mode

Basic Advanced Security Filter **WPS** Client List Policy

WPS : Enable

Wi-Fi Protected Setup Information

WPS Current Status : Configured [Release Configuration](#)

Self Pin Code : 58978443

SSID : ENCORE59FE74

Authentication Mode : WPA/WPA2 pre-shared key

Passphrase Key :

WPS Via Push Button : [Start to Process](#)

WPS via PIN : [Start to Process](#)

WPS: Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status: If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see '**UnConfigured**'. Click the "Release Configuration" can clear the security settings of the 1st SSID.

Self Pin Code: This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID: This is the network broadcast name (SSID) of the router.

Authentication Mode: It shows the active authentication mode for the wireless connection.

Passphrase Key: It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

Interface: If device is set to repeater mode, you can choose "**Client**" interface to connect with other AP by using WPS, otherwise you may choose "**AP**" interface to do WPS with other clients.

WPS via Push Button: Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN: You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

- Client List

WLAN Client Table shows the Wireless clients associated to this Wireless Router.

The screenshot shows the 'Client List' tab selected in a router's configuration interface. At the top right, there is a dropdown menu for 'AP Router Mode'. Below the navigation tabs, the 'WLAN Client Table' section is titled. It contains a text box stating 'This WLAN Client Table shows client MAC address associate to this Broadband Router'. Below this is a table with columns for 'Interface', 'MAC Address', 'Signal (%)', and 'Idle Time'. The table is currently empty, displaying the message 'No client connecting to the Router.' A 'Refresh' button is located below the table.

Interface	MAC Address	Signal (%)	Idle Time
No client connecting to the Router.			

- Policy

The Broadband router can allow you to set up the Wireless Access Policy up to 4 SSID's.

The screenshot shows the 'Policy' tab selected in a router's configuration interface. At the top right, there is a dropdown menu for 'AP Router Mode'. Below the navigation tabs, the 'Policy' section is titled. It contains four sections, each for a different SSID (SSID 1, SSID 2, SSID 3, and SSID 4). Each section has three rows of configuration options, each with a dropdown menu set to 'Enable':

- 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
- SSID 3 Connection Control Policy**
 - WAN Connection: Enable
 - Communication between Wireless clients: Enable
 - Communication between Wireless clients and Wired clients: Enable
- SSID 4 Connection Control Policy**
 - WAN Connection: Enable
 - Communication between Wireless clients: Enable

■ FIREWALL

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

AP Router Mode ▼

EnableAdvancedDMZDoSMAC FilterIP FilterURL 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

Note:

To enable the Firewall settings select Enable and click Apply

- Advanced

You can allow the VPN packets to pass through this Broadband router.

AP Router Mode ▼

EnableAdvancedDMZDoSMAC FilterIP FilterURL Filter

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

- Demilitarized Zone (DMZ)

If you have a client PC that cannot run an Internet application (e.g. Games) properly behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) from your WAN IP address to a particular LAN client/server.

The screenshot shows a router's configuration page for DMZ. At the top right, there is a red bar with 'AP Router Mode' and a dropdown arrow. Below this is a navigation menu with tabs: 'Enable', 'Advanced', 'DMZ' (which is highlighted), 'DoS', 'MAC Filter', 'IP Filter', and 'URL Filter'. The main content area contains the following text: '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.' Below this text is a checkbox labeled 'Enable DMZ' which is currently unchecked. Underneath the checkbox is a label 'Local IP Address :' followed by an empty text input field, a left-pointing arrow button, and a dropdown menu with the text 'Please select a PC.' At the bottom right of the form are two buttons: 'Apply' and 'Cancel'.

Enable DMZ: Enable / Disable DMZ

LAN IP Address: Fill-in the IP address of a particular host in your LAN Network or select a PC from the list on the right that will receive all the packets originally from the WAN port/Public IP address.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

The screenshot shows a web interface for a router's firewall configuration. At the top right, there is a red header bar with a dropdown menu set to "AP Router Mode". Below this is a navigation bar with tabs for "Enable", "Advanced", "DMZ", "DoS", "MAC Filter", "IP Filter", and "URL Filter". The "DoS" tab is currently selected. Below the navigation bar, there is a descriptive text: "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 resources that Internet access becomes unavailable." Underneath this text, there is a "Block DoS" section with two radio buttons: "Enable" (which is selected) and "Disable". At the bottom right of this section, there are two buttons: "Apply" and "Cancel".

Flood: Protects the router from Sync Flood attack.

- MAC Filter

If you want to restrict users from accessing certain Internet applications / services (e.g. Internet websites, email, FTP etc.), and then this is the place to set that configuration. MAC Filter allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

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

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
<input type="text"/>	<input type="text"/>

MAC Filtering table :

NO.	Description	LAN MAC Address	Select
-----	-------------	-----------------	--------

Enable MAC Filtering: Check to enable or disable MAC Filtering.

Deny: If you select “**Deny**” then all clients will be allowed to access Internet except the clients in the list below.

Allow: If you select “**Allow**” then all clients will be denied to access Internet except the PCs in the list below.

Add PC MAC Address

Fill in "**LAN MAC Address**" and **<Description>** of the PC that is allowed / denied to access the Internet, and then click **<Add>**. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

Remove PC MAC Address

If you want to remove some PC from the "**MAC Filtering Table**", select the PC you want to remove in the table and then click **<Delete Selected>**. If you want to remove all PCs from the table, just click the **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset>**.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- IP Filter

AP Router Mode ▼

EnableAdvancedDMZDoSMAC FilterIP FilterURL 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 :	<input style="width: 90%;" type="text"/>
Protocol :	Both ▼
Local IP Address :	<input style="width: 40%;" type="text"/> ~ <input style="width: 40%;" type="text"/>
Port range :	<input style="width: 20%;" type="text"/> ~ <input style="width: 20%;" type="text"/>

NO.	Description	Local IP Address	Protocol	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

Enable IP Filtering: Check to enable or uncheck to disable IP Filtering.

Deny: If you select “Deny” then all clients will be allowed to access Internet except for the clients in the list below.

Allow: If you select “Allow” then all clients will be denied to access Internet except for the PCs in the list below.

Add PC IP Address

You can click **<Add>** PC to add an access control rule for users by an IP address or IP address range.

Remove PC IP Address

If you want to remove some PC IP from the **<IP Filtering Table>**,

select the PC you want to remove in the table and then click **<Delete Selected>**. If you want to remove all PCs from the table, just click the **<Delete All>** button.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- URL Filter

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

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

Add Reset

Current URL Blocking Table :

NO.	URL/keyword	Select
-----	-------------	--------

Delete Selected Delete All Reset

Apply Cancel

Enable URL Blocking: Enable or disable URL Blocking

Add a URL Keyword

Fill-in the "URL/Keyword" field with your ur l/ keyword, and then click **<Add>**. You can enter the full URL address or the keyword of the web site you want to block. If you happen to make a mistake and want to retype again, just click "Reset" and the field will be cleared.

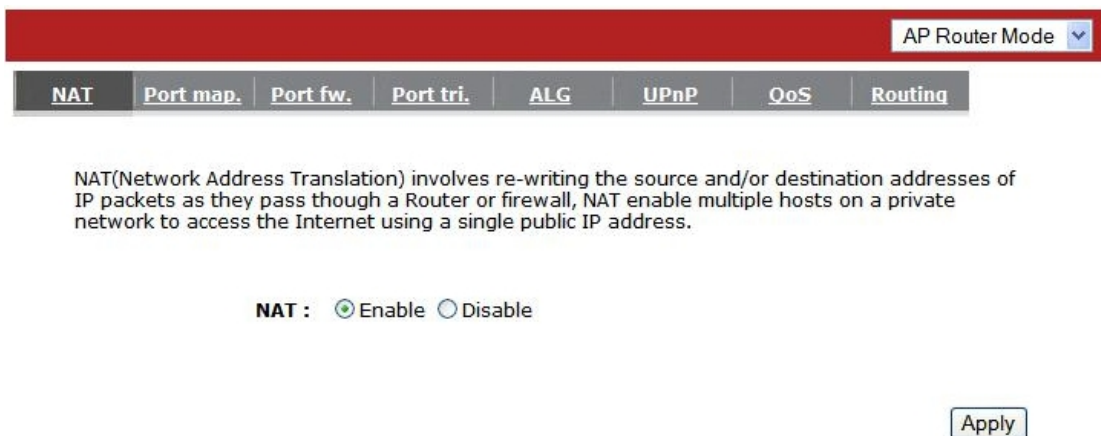
Remove URL Keyword

If you want to remove some URL keywords from the "**Current URL Blocking Table**", select the URL keyword you want to remove in the table and then click **<Delete Selected>**. If you want remove all URL keywords from the table, click **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset>**. Click **<Apply>** to save the above configurations

■ ADVANCED

- Network Address Translation (NAT)

Network Address Translation (NAT) allows multiple users at your local LAN site to access the Internet using a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.



The screenshot shows a configuration interface for a router. At the top right, there is a dropdown menu labeled "AP Router Mode" with a downward arrow. Below this is a horizontal navigation bar with several tabs: "NAT", "Port map.", "Port fw.", "Port tri.", "ALG", "UPnP", "QoS", and "Routing". The "NAT" tab is currently selected. Below the navigation bar, there is a text block explaining NAT: "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." Below this text, there are two radio buttons: "NAT : Enable Disable". At the bottom right of the configuration area, there is an "Apply" button.

- Port Mapping

Port Mapping allows you to re-direct a particular range of service port numbers (from the Internet / WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.

AP Router Mode ▾

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

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

Enable Port Mapping

Description :

Local IP :

Protocol : Both ▾

Port range : ~

Current Port Mapping Table :

NO.	Description	Local IP	Type	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

Enable Port Mapping: Enable or disable port mapping function.

Description: description of this setting.

Local IP: This is the local IP of the server behind the NAT firewall.

Protocol: This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only, or select “BOTH” to forward both “TCP” and “UDP” packets.

Port Range: The range of ports to be forward to the private IP.

Add Port Mapping

Fill in the "**Local IP**", "**Protocol**", "**Port Range**" and "**Description**" of the setting to be added and then click "**Add**". Then this Port Mapping setting will be added into the "**Current Port Mapping Table**" below. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

Remove Port Mapping

If you want to remove a Port Mapping setting from the "**Current Port Mapping Table**", select the Port Mapping setting that you want to remove in the table and then click **D<Delete Selected>**. If you want to remove all Port Mapping settings from the table, click **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Port Forwarding (Virtual Server)

Use the Port Forwarding (Virtual Server) function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address (See Glossary for an explanation on Port number).

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

Enable Port Forwarding

Description :

Local IP :

Protocol : Both ▼

Local Port :

Public Port :

Current Port Forwarding Table :

NO.	Description	Local IP	Local Port	Type	Public Port	Select
-----	-------------	----------	------------	------	-------------	--------

Enable Port Forwarding: Enable or disable Port Forwarding.

Description: The description of this setting.

Local IP / Local Port: This is the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.

Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default “both” setting. Public Port enters the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN Network.

Public Port: Port number will be changed to Local Port when the packet enters your LAN Network.

Add Port Forwarding

Fill in the "**Description**" , "**Local IP**", "**Local Port**", "**Protocol**" and "**Public Port**" of the setting to be added and then click **<Add>** button. Then this Virtual Server setting will be added into the "**Current Port Forwarding Table**" below. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

Remove Port Forwarding

If you want to remove Port Forwarding settings from the "**Current Port Forwarding Table**", select the Port Forwarding settings you want to remove in the table and then click "**Delete Selected**". If you want to remove all Port Forwarding settings from the table, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Port Triggering (Special Applications)

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

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

Enable Trigger Port

Description :

Popular applications : ▾

Trigger port : ~

Trigger type : ▾

Public Port :

Public type : ▾

Current Trigger-Port Table :

NO.	Trigger port	Trigger type	Public Port	Public type	Name	Select
-----	--------------	--------------	-------------	-------------	------	--------

Enable Trigger Port: Enable or disable the Port Trigger function.

Trigger Port: This is the outgoing (Outbound) range of port numbers for this particular application.

Trigger Type: Select whether the outbound port protocol is “TCP”, “UDP” or “BOTH”.

Public Port: Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)

Public Type: Select the Inbound port protocol type: “TCP”, “UDP” or “BOTH”

Popular Applications: This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-5) in the “Add” selection box and then click the <Add> button. This will automatically list the Public Ports required for this popular application in the location (1-5) you specified.

Add Port Triggering

Fill in the "**Trigger Port**", "**Trigger Type**", "**Public Port**", "**Public Type**", "**Public Port**" and "**Description**" of the setting to be added and then Click **<Add>**. The Port Triggering setting will be added into the "**Current Trigger-Port Table**" below. If you happen to make a mistake, just click **<Reset>** and the fields will be cleared.

Remove Port Triggering

If you want to remove Special Application settings from the "**Current Trigger-Port Table**", select the Port Triggering settings you want to remove in the table and then click **<Delete Selected>**. If you want remove all Port Triggering settings from the table, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

- Application Layer Gateway (ALG)

You can select applications that need **ALG** support. The router will let the selected application to correctly pass through the NAT gateway.

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

Description	Select
H323	<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"/>

Apply Cancel

- UPNP

With UPnP, all PCs in you Intranet will discover this router automatically. So, you don't have to configure your PC and it can easily access the Internet through this router.

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

Apply

Enable / Disable UPnP: You can enable or Disable the UPnP feature here.

After you enabled the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

- Quality of Service (QoS)

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule "Others".

Priority Queue

This can put the packets of specific protocols in High/Low Queue. The packets in High Queue will process first.

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 .

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"/>

Unlimited Priority Queue: The LAN IP address will not be bounded in the QoS limitation.

High/Low Priority Queue: This can put the packets in the protocol and port range to High/Low QoS Queue.

Bandwidth Allocation:

This can reserve / limit the throughput of specific protocols and port range. You can set the upper bound and Lower bound.

AP Router Mode v

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 .

QoS : Priority Queue Bandwidth Allocation Disabled

Type : Download v

Local IP range : ~

Protocol : ALL v

Port range : 1 ~ 65535

Policy : Min v

Rate(bps) : Full v

Current QoS Table:

NO.	Type	Local IP range	Protocol	Port range	Policy	Rate (bps)	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>							

Type: Specify the direction of packets. Upload / Download or both.

IP range: Specify the IP address range. You could also fill one IP address

Protocol: Specify the packet type. The default ALL will put all packets in the QoS priority Queue.

Port range: Specify the Port range. You could also fill one Port.

Policy: Specify the policy of QoS, **Min** option will reserve the selected data rate in QoS queue. **Max** option will limit the selected data rate in QoS queue.

Rate: The data rate of QoS queue.

Disabled: This turn off QoS Service.

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 .

QoS : Priority Queue Bandwidth Allocation Disabled

- Routing

You can set Enable Static Routing to let the router forward packets using your routing policy.

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 ▼

Current Static Routing Table :

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

Destination LAN IP: Specify the destination LAN IP address of static routing rule.

Subnet Mask: Specify the Subnet Mask of static routing rule.

Default Gateway: Specify the default gateway of static routing rule.

Hops: Specify the Max Hops number of static routing rule.

Interface: Specify the Interface of static routing rule.

■ TOOLS

- Admin

You can change the password required to log into the broadband router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

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 type="text"/>	8080	<input type="checkbox"/>

Old Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and type it again in **Repeat New Password** for verification purposes

Remote management

Allows you to designate a host in the Internet. The ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address: This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the above configurations.

- Time

The Time Zone allows your router to refer or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Setting Up Time:

Synchronize with the NTP server

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 :	<input type="checkbox"/> Enable From January 1 To January 1

Apply Reset

Time Zone: Select the time zone of the country you are currently located. The router will set its time based on your selection.

NTP Time Server: The router can be set up to use external NTP Time Server.

Daylight Savings: The router can also be set to automatically adjust to the Daylight Savings changes. If you wish to use this function, you must select the Daylight Savings Time period and put a checkmark on the Enable box to enable your daylight savings time configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Synchronize with your PC

You could synchronize timer with your computers time.

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

Time Setup:	Synchronize with PC ▾
PC Date and Time:	Thursday, May 21, 2009 12:10:51 PM
Daylight Saving :	<input type="checkbox"/> Enable From January ▾ 1 ▾ To January ▾ 1 ▾

PC Date and Time: This field would display your computer's date and time.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must register to a DDNS services and to get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

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 :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Address :	3322(qdns) ▾
Host Name :	<input type="text"/>
Username :	<input type="text"/>
Password :	<input type="text"/>

Enable/Disable DDNS: Enable or disable the DDNS function of this router

Server Address: Select a DDNS service provider

Host Name: Fill in your static domain name that uses DDNS.

Username: The account that your DDNS service provider assigned to you.

Password: The password you set for the DDNS service account above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Power

Saving power in WLAN mode can be enabled / disabled in this page.

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

- Diagnosis

In this page lets you run diagnosis to your network status.

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 :

- Firmware

This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page.

You can also use the Browse button to find the firmware file in your PC.

AP Router Mode

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

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.

Browse...

Apply Cancel

Once you've selected the new firmware file, click **<Apply>** at the bottom of the screen to start the upgrade process

- Back-up

This page allows you to save the current router configurations. When you save the configurations, you also can restore the saved configurations into the router through the **Restore Settings**. If extreme problems occur you can use the **Restore to Factory Defaults** to set all configurations to its original default settings. Warning: You will lose any saved data and settings when you set back to the manufacturer's default settings, but you can re-enter your previous settings manually.

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: 150px;" type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Upload"/>

Backup Settings: This can save the current Broadband router configuration to a file named "config.bin" on your PC. You can also use the **<Upload>** button to restore the saved configuration to the Broadband router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the Broadband router to perform a power reset and restore the original factory settings.

- Reset

You can reset the broadband router when system stops responding correctly or stop functions.

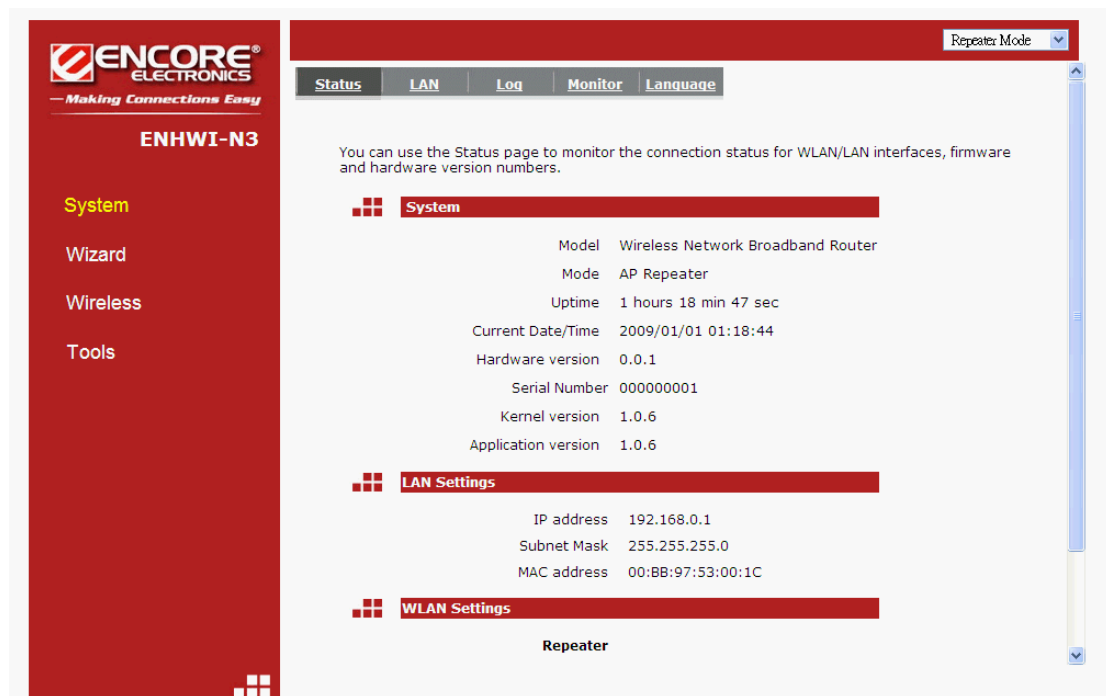
In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking .

XIII - Repeater Mode

Repeater mode has limited settings compared to the AP mode. Choose “Repeater mode” on the top right corner of the configuration page.

System restarts and connects to the IP address `http://192.168..0.1`

You will see the configuration homepage under “**REPEATER**” mode now.



The screenshot displays the configuration interface for the ENHWI-N3 router in Repeater Mode. The left sidebar contains navigation options: System (highlighted), Wizard, Wireless, and Tools. The main content area is titled 'Status' and includes a dropdown menu for 'Repeater Mode'. Below the navigation tabs (Status, LAN, Log, Monitor, Language), there is a descriptive text: 'You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.' The 'System' section lists the following details:

Model	Wireless Network Broadband Router
Mode	AP Repeater
Uptime	1 hours 18 min 47 sec
Current Date/Time	2009/01/01 01:18:44
Hardware version	0.0.1
Serial Number	000000001
Kernel version	1.0.6
Application version	1.0.6

The 'LAN Settings' section shows:

IP address	192.168.0.1
Subnet Mask	255.255.255.0
MAC address	00:BB:97:53:00:1C

The 'WLAN Settings' section is currently empty, with the word 'Repeater' centered below it.

■ System

- Status

System status section allows you to monitor the current status of your router.

You can see the Uptime, hardware information, serial number as well as firmware version information.

LAN Settings: This page displays the Broadband router LAN port's current LAN information.

WLAN Settings: Wireless configuration details such as SSID, Status(Connected/Disconnected), Security and Channel are briefly shown.

- LAN

The LAN Tabs shows LAN settings. LAN settings can be change as needed. If you are an entry level user, try opening a website from your computer. If you're successful and able to connect and browse the web site you opened without any problem, do not change any of the settings.

Click **<Apply>** at the bottom of this screen to save the changed configurations.

Repeater Mode ▼

Status LAN Log Monitor Language

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

LAN IP

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

Apply Cancel

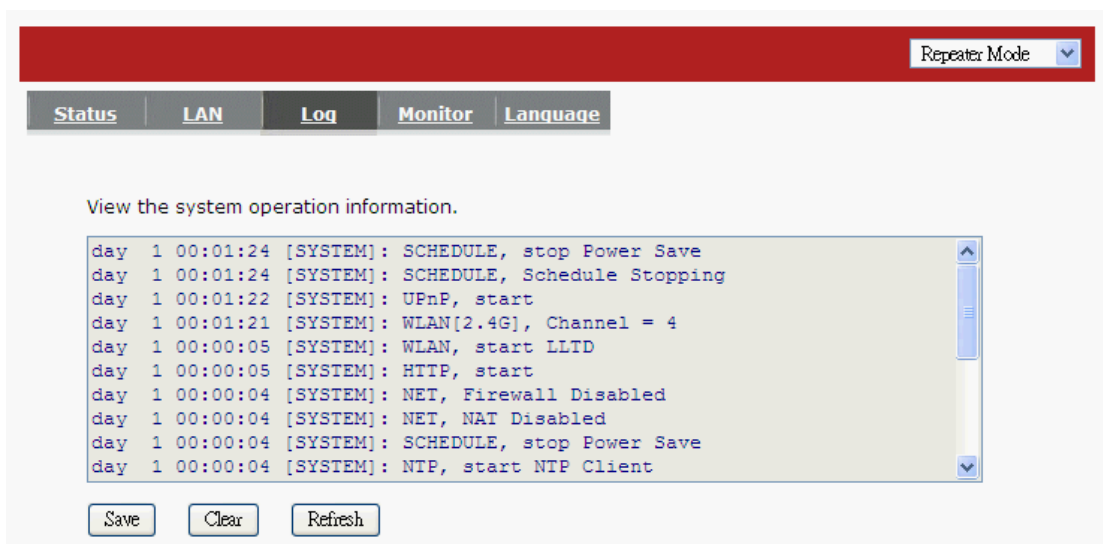
IP address: This is the router's LAN IP address (Your LAN clients default gateway IP address). It can be changed based on your network architecture.

IP Subnet Mask: Specify a Subnet Mask IP address for your LAN segment.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

- Event Log

View operations log of the **ENHWI-N3**. This page shows the current system log of the ENHWI-N3 router. It displays any event occurred after system start up. Use the scroll bar to go down to the bottom of the page, the system log can be saved **<Save>** to a local file for future use or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



Repeater Mode

Status LAN **Log** Monitor Language

View the system operation information.

```
day 1 00:01:24 [SYSTEM]: SCHEDULE, stop Power Save
day 1 00:01:24 [SYSTEM]: SCHEDULE, Schedule Stopping
day 1 00:01:22 [SYSTEM]: UPnP, start
day 1 00:01:21 [SYSTEM]: WLAN[2.4G], Channel = 4
day 1 00:00:05 [SYSTEM]: WLAN, start LLTD
day 1 00:00:05 [SYSTEM]: HTTP, start
day 1 00:00:04 [SYSTEM]: NET, Firewall Disabled
day 1 00:00:04 [SYSTEM]: NET, NAT Disabled
day 1 00:00:04 [SYSTEM]: SCHEDULE, stop Power Save
day 1 00:00:04 [SYSTEM]: NTP, start NTP Client
```

Save Clear Refresh

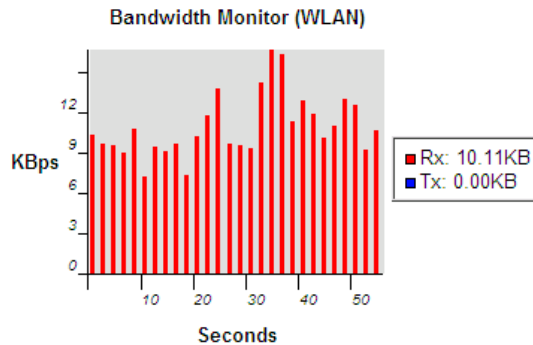
- Monitor

The Monitor Tab shows the bandwidth monitoring feature of each network interface of the ENHWI-N3 router, wireless or wired and of the network packet histogram for the network connection on WLAN. Auto refresh keeps information updated frequently.

Repeater Mode

[Status](#) | [LAN](#) | [Log](#) | **Monitor** | [Language](#)

You can monitor the bandwidth in different interface. This page will refresh in every five seconds.



- Language

This Wireless Router supports multiple languages for user interface. Select your preferred language.

Repeater Mode

[Status](#) | [LAN](#) | [Log](#) | [Monitor](#) | **Language**

You can select other language in this page.

Multiple Language :

- Choose your language
- English
- Italiano

■ Wireless

- Basic

You can set parameters use by the wireless stations to connect to this router. The parameter includes Mode, ESSID, Channel Number and Associated Client.

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

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	Repeater ▾
Band :	2.4 GHz (B+G+N) ▾
Enable SSID#:	1 ▾
SSID1 :	ENCORE59FE74
Site Survey :	Site Survey
Wireless Information	
SSID:	ENCORE59FE74
Status:	Disconnected
Channel :	

Apply Cancel

Radio: Enable or Disable Wireless function

Band: Allows you to set the frequency band of the router. Fix at 802.11b, 802.11g or 802.11n modes. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.

Enable ESSID: You can specify the maximum ESSID number.

ESSID1~3: Allow you to specify ESSID of WLAN.

Site Survey: Click this button to scan the available wireless routers that can be set as this router's parent router. By doing so this ENHWI-N3 router will become a wireless extender / repeater of the selected parent router. Select one router from the list for that router to become this router's parent router.

Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Auth	Signal(%)	Mode
1	<input type="radio"/>	1	Encore	00:02:6F:4F:5A:7F	TKIPAES	WPAPSKWPA2PSK	5	11b/g
2	<input type="radio"/>	1	SENAOWL	00:02:6F:53:0C:9B	WEP	AUTOWEP	55	11b/g
3	<input type="radio"/>	11	SQA_ADSL	00:0C:F6:47:C0:4C	TKIPAES	WPAPSKWPA2PSK	100	11b/g/n
4	<input type="radio"/>	3	SNADSL	00:02:6F:48:0D:8F	WEP	AUTOWEP	20	11b/g
5	<input type="radio"/>	4	SQA7750B	00:02:6F:5D:16:E8	NONE	OPEN	100	11b/g/n

- Client List

This WLAN Client Table shows the Wireless client associated to this Wireless Router.

Repeater Mode

Basic **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
ENCORE59FE74	00:23:4D:36:D7:BE	100	0 secs

- Policy

The Broadband router allows you to set up the Wireless Access Policy. If multiple SSID is created, this is the place to set the policy for each SSID.

Communication between Wireless clients:

This function is to allow other Wireless Client to communicate with another Wireless Client on the LAN connected on the same SSID.

Communication between Wireless clients and wired clients:

This function allows the Wireless Client to communicate with other Wireless Client in the LAN on specific SSID as well as the Wired Client connected to the switch portion of this router.

The screenshot shows the 'SSID 1 Connection Control Policy' configuration page. At the top right, there is a 'Repeater Mode' dropdown menu. Below it are three tabs: 'Basic', 'Client List', and 'Policy'. The 'Policy' tab is selected. Under the heading 'SSID 1 Connection Control Policy', there are two rows of configuration options. The first row is 'Communication between Wireless clients' with an 'Enable' dropdown menu. The second row is 'Communication between Wireless clients and Wired clients' with an 'Enable' dropdown menu. At the bottom right, there are 'Apply' and 'Cancel' buttons.

■ Tools

- Admin

You can change the password that is required to log into the broadband router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

The screenshot shows the 'Admin' password change page. At the top right, there is a 'Repeater Mode' dropdown menu. Below it are six tabs: 'Admin', 'Time', 'Diagnosis', 'Firmware', 'Back-up', and 'Reset'. The 'Admin' tab is selected. The page contains the following text: 'You can change the password that you use to access the router, this is not your ISP account password.' Below this text are three input fields: 'Old Password :', 'New Password :', and 'Repeat New Password :'. At the bottom right, there are 'Apply' and 'Reset' buttons.

Old Password: Fill-in the current password to be replaced. This is required to allow changing to a new password.

New Password: Enter your new password and again in **Repeat New Password** for verification purpose

Click **<Apply>** at the bottom of the screen to save the above configurations

- Time

The Time Zone allows your router to use external source to time synchronizations. This affects other functions such as Event Log entries and Schedule settings that use time to do its tasks.

How to Set up Time:

Synchronize with the NTP server

The screenshot shows the 'Time' configuration page of a router. At the top right, there is a 'Repeater Mode' dropdown menu. Below it is a navigation bar with tabs for 'Admin', 'Time', 'Diagnosis', 'Firmware', 'Back-up', and 'Reset'. The main content area contains a descriptive paragraph: '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.' Below this are four configuration sections: 'Time Setup:' with a dropdown menu set to 'Synchronize with the NTP Server'; 'Time Zone :' with a dropdown menu set to '(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'; 'NTP Time Server :' with an empty text input field; and 'Daylight Saving :' with an unchecked 'Enable' checkbox and 'From' and 'To' date pickers both set to 'January 1'. At the bottom right, there are 'Apply' and 'Reset' buttons.

Time Zone: Select the time zone of the country you are located. The router will set its time based on your selection.

NTP Time Server: Enter the NTP Time Server address or URL here. This also accepts local the IP address if the NTP Time Server is on the same LAN.

Daylight Savings: The router can also setup to automatically adjust the Daylight Savings Time changes each time DST changes. To use this feature, click to put a checkmark on the Enable box then enter the dates the DST would starts and ends.

Click **<Apply>** at the bottom of the screen to save the above configurations

Synchronize and use your computer's clock

The ENHWI-N3 can be synchronized the time to your computer's time.

Repeater Mode

Admin Time 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 PC

PC Date and Time: June 04, 2009 11:33:46

Daylight Saving : Enable
From January 1 To January 1

Apply Reset

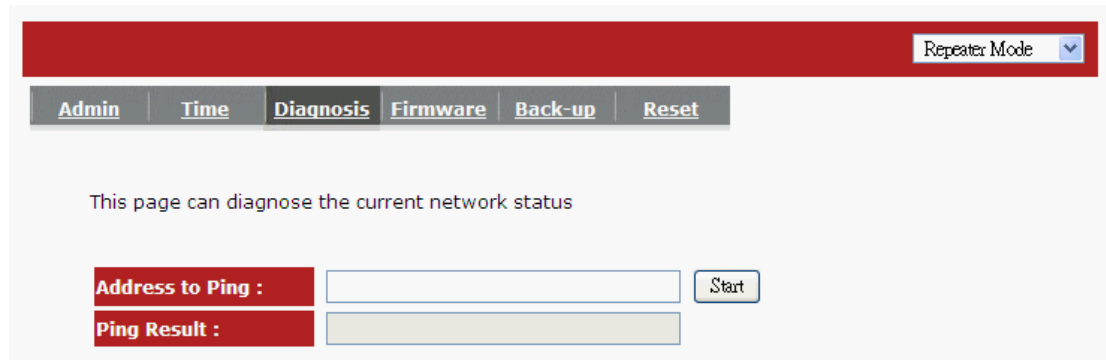
PC Date and Time: This field would display the user computers date and time.

Daylight Savings: The router can also setup to automatically adjust the Daylight Savings Time changes each time DST changes. To use this feature, click to put a checkmark on the Enable box then enter the dates the DST would starts and ends.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Diagnosis

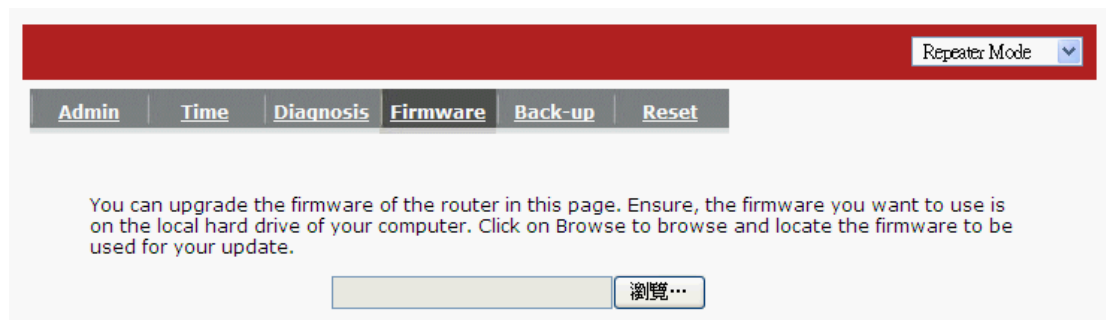
This page lets you diagnose the connection problem and the network status by executing the Ping function. The result tells you whether the connection is broken or successful.



The screenshot shows the 'Diagnosis' tab selected in a router's web interface. At the top right, there is a dropdown menu set to 'Repeater Mode'. Below the navigation tabs, a message states: 'This page can diagnose the current network status'. There are two input fields: 'Address to Ping :' and 'Ping Result :'. A 'Start' button is positioned to the right of the 'Address to Ping :' field.

- Firmware

This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.



The screenshot shows the 'Firmware' tab selected in a router's web interface. At the top right, there is a dropdown menu set to 'Repeater Mode'. Below the navigation tabs, a message states: '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.' There is a large empty text input field and a '瀏覽...' (Browse) button to its right.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process. Warning: Once the loading of the new firmware started, do not power down the router.

- Back-up

The page allows you to save (Backup) the router's current configuration settings.

The saved backup can be restored again if needed by using the **Restore Settings** selection and browse the saved backup file to restore back to the expected settings. If restore is not an option the **Restore to Factory Default** may be the only way to recover the router from damage. **Using Restore to Factory Default** will reset all configurations and settings to its original factory default settings (e.g. when you first purchased the router).

The screenshot shows a web-based configuration interface for a router. At the top, there is a red header bar with a dropdown menu labeled "Repeater Mode". Below the header is a navigation menu with tabs for "Admin", "Time", "Diagnosis", "Firmware", "Back-up", and "Reset". The "Back-up" tab is currently selected. Below the navigation menu, there is a text box with the following instructions: "Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings." Below the text box, there are three main sections: "Restore to factory default :" with a "Reset" button; "Backup Settings :" with a "Save" button; and "Restore Settings :" with a text input field, a "Browse" button, and an "Upload" button.

Backup Settings: Use this function to save the router's current settings and configuration to a file named "**config.bin**" to your computer. You can also use the **<Upload>** button to restore the saved configuration to the router. Alternatively, you can use the "**Restore to Factory Defaults**" to force the Broadband router to perform a power reset and restore the original factory settings.

- Reset

You can software reset the broadband router when system stops responding or stop working. This is different from the hardware reset that can reset the settings by physically pressing the button.



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. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.

Apply Cancel

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.