BROWAN
Wireless Broadband Anywhere

User Guide V1.0

BW1230

SMB Wireless Router

www.browan.com

Copyright

Notice

BROWAN reserves the right to change specifications without prior notice.

While the information in this document has been compiled with great care, it may not be deemed an assurance of product characteristics. BROWAN shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from BROWAN.

Trademarks

The product described in this book is a licensed product of BROWAN.

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.

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.

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.

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.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2001
  Safety of Information Technology Equipment

- EN50385 : (2002-08)
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
-
- EN 300 328 V1.6.1 (2004-11)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
-
  EN 301 489-1 V1.6.1: (2005-09)
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-17 V1.2.1 (2002-08)
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius

[Lithuanian]	reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Contents

About this Guide

Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the **BROWAN BW1230 SMB Wireless Router.**

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

!!!	Very important information. Failure to observe this may result in damage.
!	Important information that should be observed.
i	Additional information that may be helpful but which is not required.
bold	Menu commands, buttons and input fields are displayed in bold
`code`	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
`<value>`	Placeholder for certain values, e.g. user inputs
[value]	Input field format, limitations, and/or restrictions.
Words in **Bold**	The texts in **Bold** mean that those words are the **Key Words**.
Words in **Bold** and *Italic*	The texts in **Bold** and *Italic* mean that there are the *Explanations* about the words.

Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to:

manuals@browan.com

Browan Technical Support

If you encounter problems when installing or using this product, please consult the Browan website at www.browan.com for:

- Direct contact to the Browan support centers.
- Frequently Asked Questions (FAQ).
- Download area for the latest software, user documentation and product updates.

Chapter 1 – Introduction

Thank you for choosing **BROWAN BW1230 SMB Wireless Router**. You could have the better and easier wireless network with a series of BROWAN's products.

Product Overview

The **BW1230 SMB Wireless Router** is an integrated router, ***IEEE 802.11g*** wireless access point, four-port switch, and firewall to provide a high-speed, secure, affordable and easy-to-use wireless LAN solution that combines the flexibility of wireless networking and services required in Small Medium Business networks.

Shared and Rapid Connectivity

The BW1230 is designed in an attractive, compact plastic enclosure, with cutting-edge RF technology, providing shared Internet access for wireless and wired users within robust wireless network in offices or similar RF environments. The BW1230 not only supports either local power supply or inline Power-over-Ethernet (optional) but also keeps full backward compatibility with legacy 802.11b devices to ensure interoperability with all IEEE 802.11g and IEEE 802.11b client devices, extending the security, scalability, reliability, ease of deployment, and manageability available in wired networks to the wireless LAN.

Sophisticated Firewall and Advanced Security

Integrated with sophisticated firewall functionalities including a ***stateful packet inspection firewall***, hacker pattern detection, IP and MAC address filtering and other security features help protect the entire enterprise network from attacks and other Internet security risks. In addition, the advanced wireless security offers a strong level of protection for the wireless connection by 128-bit enhanced encryption (Wireless Protected Access) with ***TKIP/AES*** encryption for better security, along with 64/128-bits static and dynamic *WEP* encryption for legacy clients.

Virtual AP technology

BW1230 supports multiple BSSIDs, so-called ***Virtual AP*** which delivers multiple services from one piece of hardware. It can create up to ***3 virtual AP*** with different wireless security settings respectively, allowing different users to access the services they need (e.g., guests only get Internet access). It prevents non-authorized users from logging on enterprise network in terms of confidentiality of company information.

stateful packet inspection firewall:

A **stateful firewall** (any firewall that performs **stateful packet inspection or stateful inspection**) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

TKIP:

TKIP (Temporal Key Integrity Protocol) is a security protocol used in Wi-Fi Protected Access (WPA).

TKIP ensures that every data packet is sent with its own unique encryption key.

AES:

Advanced Encryption Standard (AES) is a block cipher adopted as an encryption standard by the U.S. government. And a block cipher is a symmetric key cipher which operates on fixed-length groups of bits.

Features Highlight

- 802.11b+g compliant, 1-54Mbps with auto-fallback
- Support Multiple BSSID, up to 3 Virtual AP
- Concurrent 802.11b and 802.11g user association
- WDS supported
- Quality of Service, IEEE 802.11e (WMM)
- Static and Dynamic IP routing (RIP v1 and v2)
- NAT/NAPT (IP masquerading)
- Port-forwarding and up to 15 virtual servers supported
- Virtual DMZ
- Transparent VPN pass-through (PPTP, L2TP)
- PPPoE/PPTP/L2TP client
- DHCP server/relay/client
- Dynamic Domain Name Service (DDNS)
- Enhanced encryption (Wireless Protected Access) with TKIP or AES
- Wired Equivalent Privacy (WEP) using static or dynamic key of 64 or 128 bits
- IP, MAC, WEB, and Protocol filter
- URL and domain blocking
- Access Control (accepting and denying rules) based on MAC/IP address
- Hidden SSID
- Web-based configuration
- Remote management via http and SNMP
- Firmware upgrade via web UI
- Backup/Restore configuration file
- System log to log server

Chapter 2 - Installation

This chapter provides installation instructions for the hardware and software components of the **BROWAN BW1230 SMB Wireless Router**. It also includes the procedures for the following tasks:

- **The Product Package**
- **Hardware Introduction**
- **Hardware Installation**
- **Software Installation**

The Product Package

The items in the package:

	Item	Qty
1	**BROWAN BW1230 SMB Wireless Router**	1
2	Power adapter	1
3	RJ-45 Ethernet cable	1
4	External antenna	1
5	Installation CD with:: ◆ BW1230 User Guide (PDF) ◆ Product Firmware ◆ Release Notes ◆ Adobe Acrobat Reader	1
6	Printed 2 Years Warranty Card	1

If any of these items are missing or damaged, please contact your reseller or Browan sales representative immediately.

Hardware Introduction

General Overview

Cost-effective solution is the design concept of BW1230. Users could share a single broadband internet connection between several wired and wireless computers. Also BW1230 could present user a safe internet connection by block any unauthorized users to see your files or damage your computers. And users could manage BW1230 easier with Web-based configuration.

Figure 1 – BW1230 General View

TOP Cover View

The Top Cover of BW1230 contains some indicator lights (LEDs), and they could help you to know the status of your networking and connection operations.

Figure2 shows the Top Cover view of BW1230.

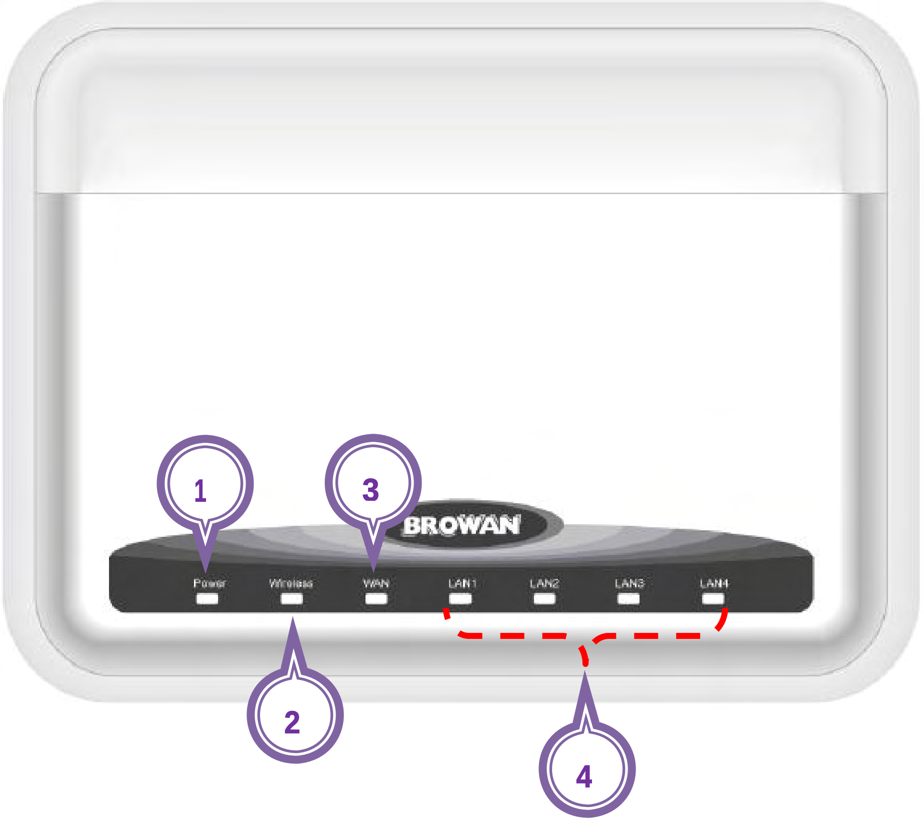


Figure 2 – BW1230 Top Cover View

1

Power LED:

It tells you the power is on or off.

2

Wireless LED:

1. If the Wireless LED is **on** it indicates your wireless networking is enable.
2. If the Wireless LED is **off** it indicates your wireless networking is disable.
3. If the Wireless LED is **flashing** it indicates your wireless networking is transmitting and receiving the data.

3

WAN LED:

1. If the WAN LED is **on** it indicates the connection between the BW1230 and your DSL/Cable Modem is working fine.
2. If the WAN LED is **off** it indicates the connection is failed.
3. If the WAN LED is **flashing** it indicates the connection between the BW1230 and your DSL/Cable Modem is working fine and it is transmitting and receiving the data.

4

LAN LED (Four Ports) :

1. If the LAN LED is **on** it indicates the connection between the BW1230 and your another network equipment is working fine.
2. If the LAN LED is **off** it indicates the connection is failed.
3. If the LAN LED is **flashing** it indicates the connection between the BW1230 and your another network equipment is working fine and it is transmitting and receiving the data.

The LED indication of BW1230 shown as below：

Item Number	LED	Status	Description
1.	Power	ON	Power is ON
		OFF	Power is OFF
2.	Wireless	ON	Wireless is activated
		OFF	Wireless is idle
		Flashing	Data is transmitting
3.	WAN	ON	WAN is activated
		OFF	WAN is idle
		Flashing	Data transmitting
4.	LAN 1 – LAN 4	ON	LAN is activated
		OFF	LAN is idle
		Flashing	Data is transmitting

Connection View

Figure3 shows the connectors of BW1230.

1 Power Adapter Socket

Please only use the power adapter provided by this BW1230 SMB Wireless Router.

2 Reset

You could press **Reset** button to restore your router back to the factory default.

3 WAN

Connect your WAN port to your DSL/Cable Modem for your broadband Internet access with a RJ-45 network cable.

4 LAN (From LAN1 to LAN4)

Connect your LAN port to your computers or any other network equipments (such as hubs or switches) with a RJ-45 network cable.

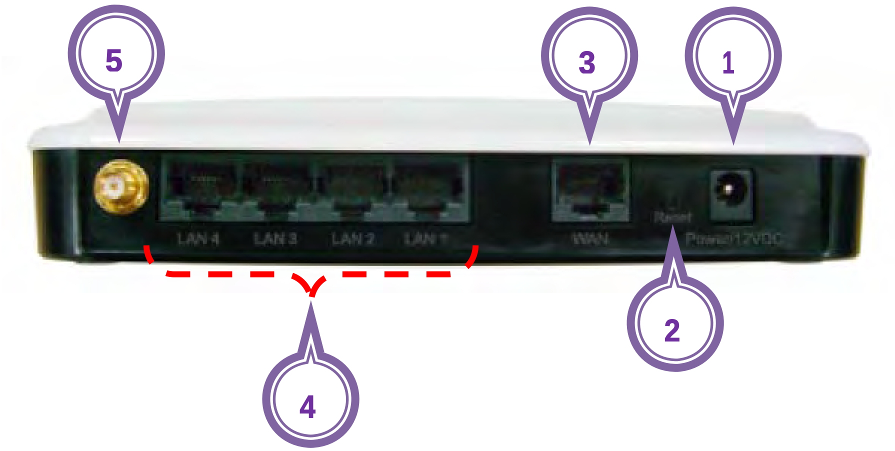


Figure 3 – BW1230 Connection View

5 External Antenna Socket

To install the BW1230 External Antenna.

!	Press the Reset button for less than 5 seconds to reboot the device. Press the Reset button for more than 5 seconds to set the device to factory defaults.

Bottom Case

You could find the **product label** on the bottom case, shown as Figure4.

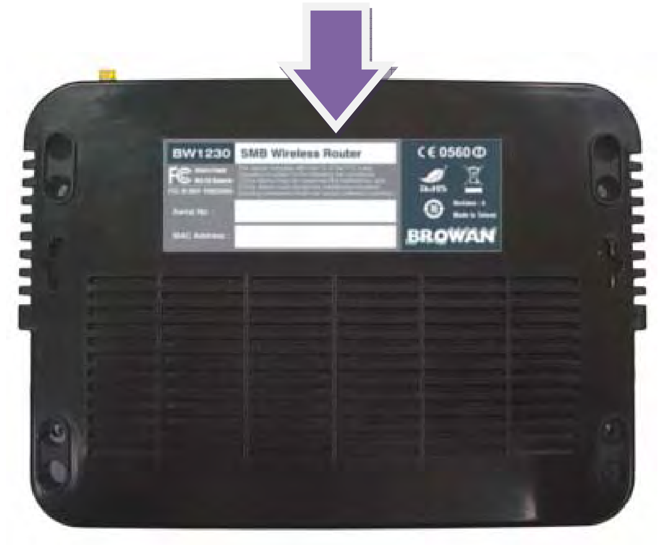
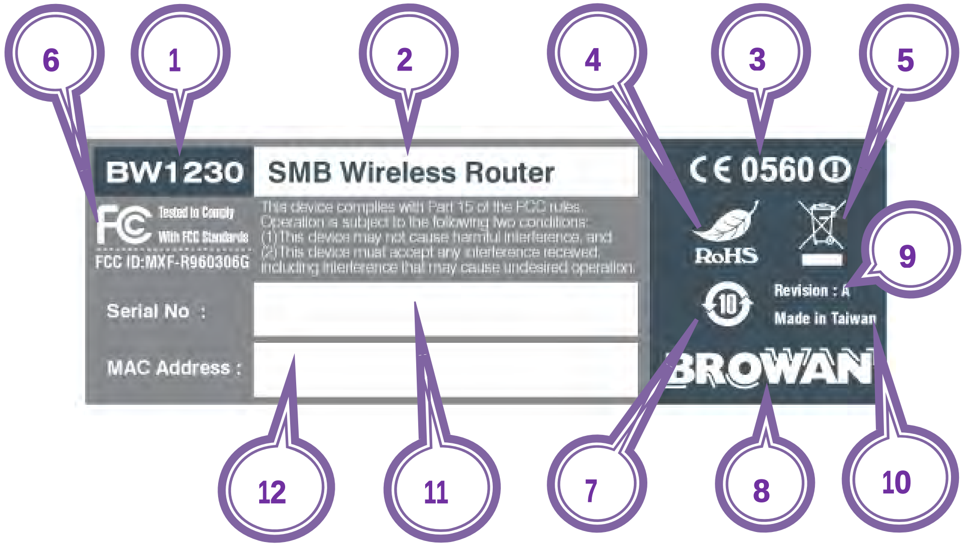

Product Label

Figure 4 – BW1230 Bottom Case

Product and Safety Label

This product label contains :

1. Product Model
2. Product name of BW1230.
3. BW1230 has passed the requirement of **CE.**
4. BW1230 has passed the requirement of **RoHS**.
5. BW1230 has passed the requirement of **WEEE**.
6. BW1230 has passed the requirement of **FCC**.
7. BW1230 has passed the requirement of **China RoHS**.
8. Browan Logo.
9. The Revision of BW1230.
10. This device has been made in Taiwan.
11. Serial number of BW1230.
12. MAC address of LAN in BW1230.



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.

Figure 5 – BW1230 Product Label

CE : The **CE** mark is a mandatory European marking for certain product groups to indicate conformity with the essential health and safety requirements set out in European Directives. To permit the use of a CE mark on a product, proof that the item meets the relevant requirements must be documented.

WEEE : The **Waste Electrical and Electronic Equipment Directive** (WEEE Directive) is the European Community directive on waste electrical and electronic equipment which, together with the **RoHS** Directive 2002/95/EC, became European Law in February 2003, setting collection, recycling and recovery targets for all types of electrical goods

RoHS : Restriction of Hazardous Substances Directive was adopted in February 2003 by the European Union. adopted in February 2003 by the European Union. The **RoHS** directive took effect on July 1, 2006, but is not a law; it is simply a directive. This directive restricts the use of six hazardous materials in the manufacture of various types of electronic and electrical equipment.

RoHS is often referred to as the lead-free directive, but it restricts the use of the following 6 substances:

1. Lead
2. Mercury
3. Cadmium
4. Hexavalent chromium (Chromium VI or Cr6+)
5. Polybrominated biphenyls (PBB)
6. Polybrominated diphenyl ether (PBDE)

China RoHS : China RoHS is a certification about the administration on the control of pollution caused by electronic information products.

Key Differences between **China RoHS** and **EU RoHS**:
The scope is different
The requirements are different
There are no exemptions ... yet
Labels, marks, and disclosure are required
The concept of **Put on the market** is different
The penalties are different
The responsibilities dictated by the law are different
Material testing down to the homogeneous materials in every single part you use to build your product may be required
The regulation is in force on March 1
You will have to design labels and issue change orders in order to comply
The standards that you have to comply with just became available in finalized versions

FCC : The Federal Communications Commission (FCC) is an independent United States government agency, created, directed, and empowered by Congressional statute.

The **FCC** was established by the Communications Act of 1934 as the successor to the Federal Radio Commission and is charged with regulating all non-Federal Government use of the radio spectrum (including radio and television broadcasting), and all interstate telecommunications (wire, satellite and cable) as well as all international communications that originate or terminate in the United States. It is an important factor in US telecommunication

	policy. The **FCC** took over wire communication regulation from the Interstate Commerce Commission. The **FCC**'s jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

Hardware Installation

Mounting the BW1230

Step 1 :
Please use a power drill to make two holes on the wall.

Step 2 :
Hammer the ①Wall Plugs into the two holes.

Step 3 :
And screw the ②Screws to the ①Wall Plug.

Step 4:
Now you could hang your ③BW1230 on the wall.

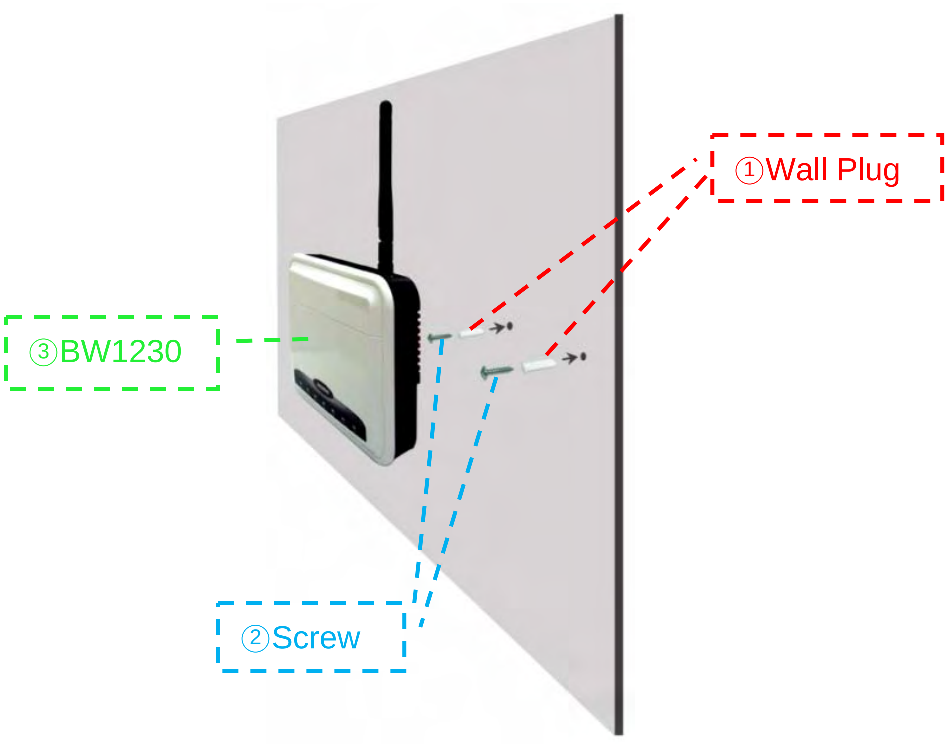
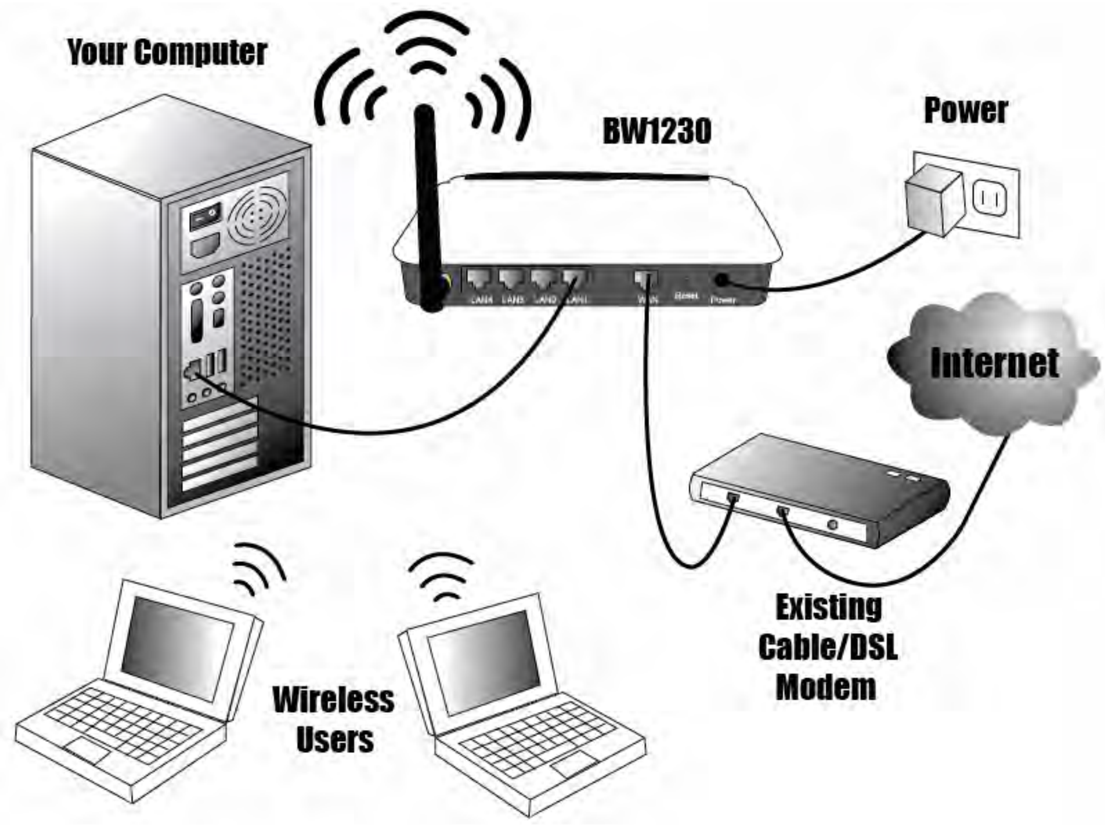


Figure 7 – Mounting the BW1230 on the wall

Installing the BW1230



Step1: Install the antenna and connect the power adapter.

Step2: Insert one end of RJ-45 network cable into the **WAN** Port, and insert another end of RJ-45 network cable into your existing Cable/DSL Modem.
You might check the connection status of the BW1230 and Cable/DSL modem from the **WAN LED** indicator.

Step3: Connect the Cable/DSL modem to your internet service with a RJ-45 network cable.

Step4: Connect your computer to any **LAN** Port of BW1230 with a RJ-45 network cable.
You might check the **LAN** connection status from the **LAN LED** indicator.

Step5: The Hardware installation now is

completed.
You could configure the BW1230 with your computer, and then you could set up other computers (including wireless computers) after the configuration completed

❗	**Directly** connect a computer to the any **LAN** Port of BW1230 for your preliminary configuration. Because you might lose contact with router if you configure the router from a wireless computer.

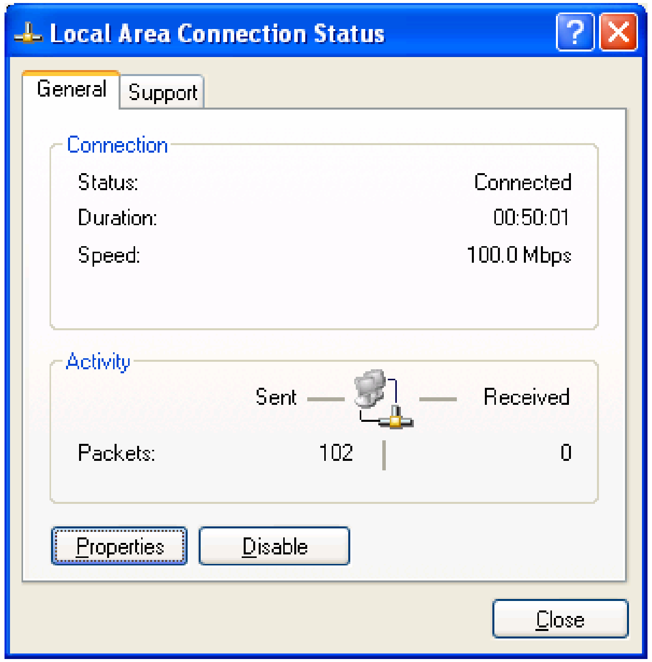
Software Installation

Accessing Your BW1230

- Use the **Web browser** to access

Step 1 :

- Please setup your **network connection**.
- Select **Local Area Connection Status**.
- Click on **Properties**.

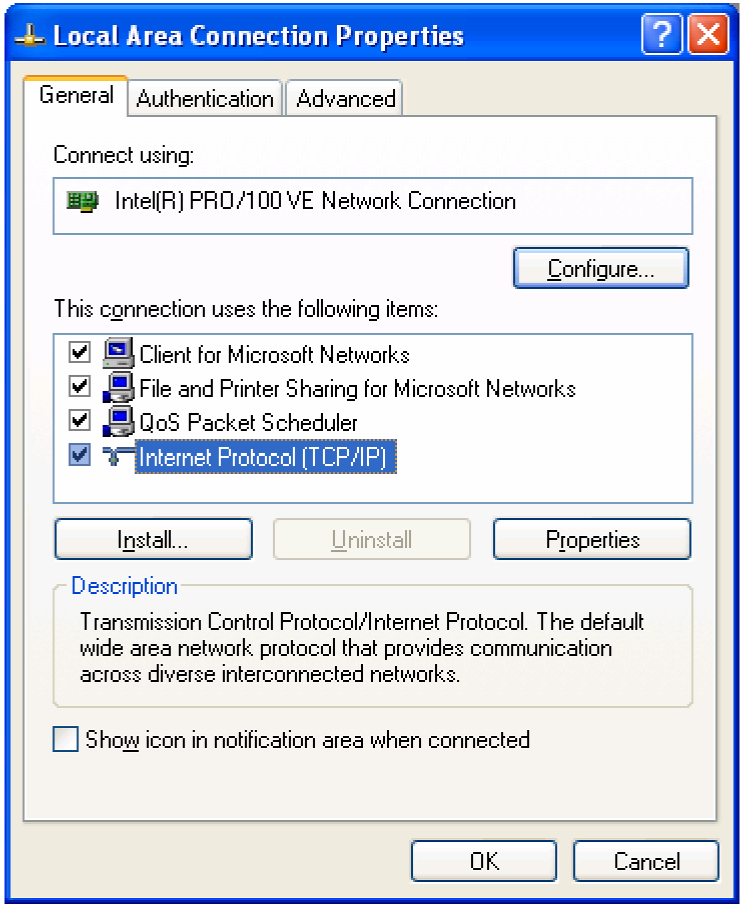


Status: Connected
Duration: 00:50:01
Speed: 100.0 Mbps

Sent — Received
Packets: 102 | 0

Figure 10-1 – Local Area Connection Status

- Double click on the Internet Protocol (**TCP/IP**)



Local Area Connection Properties

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

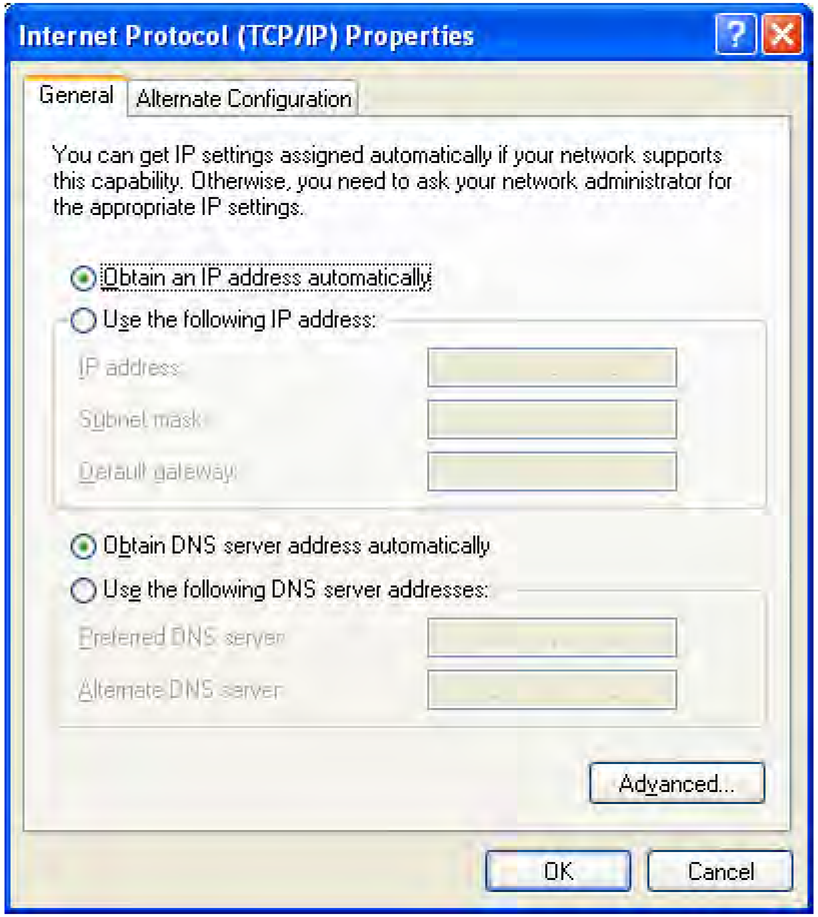
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

Figure 10-2 – Local Area Connection Status

- Please select **Obtain an IP address automatically** and O**btain DNS sever address automatically.**
- Click on OK to apply the changes.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

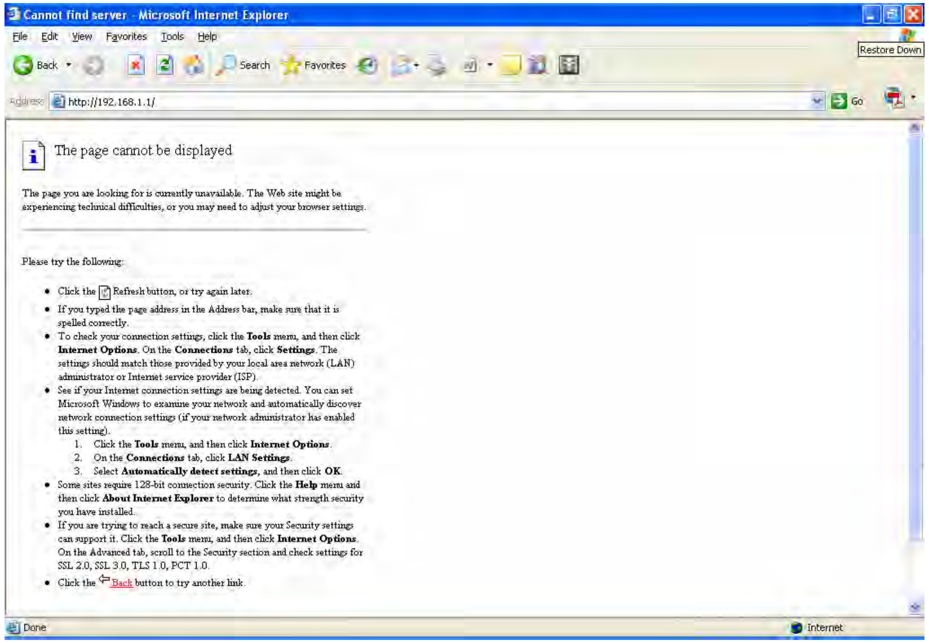
Preferred DNS server:

Alternate DNS server:

Figure 10-3 – Local Area Connection Status

- Connect the BW1230 with local network.
- Open the Web browser and enter the default IP address of the BW1230： http://192.168.1.1

  (check up the connection between your computer and any **LAN** Port of BW1230 with a RJ-45 network cable**)**



The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

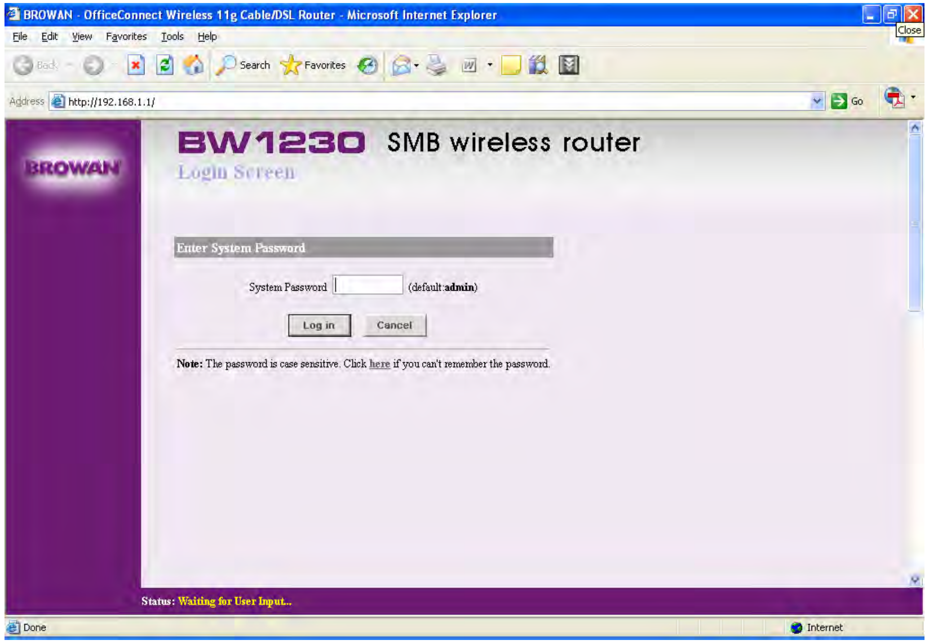
Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
  1. Click the **Tools** menu, and then click **Internet Options**.
  2. On the **Connections** tab, click **LAN Settings**.
  3. Select **Automatically detect settings**, and then click **OK**.
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.
- Click the Back button to try another link.

Figure 11 – Setup with Web browser

- Enter the BW1230 administrator login credential to access the Web management interface.

  The Default System Password is **admin**, and it is case sensitive.


BROWAN - OfficeConnect Wireless 11g Cable/DSL Router - Microsoft Internet Explorer
Close
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/
Go
BROWAN
Log in
Cancel
Done
Internet

BW1230 SMB wireless router

Login Screen

Enter System Password

System Password (default:**admin**)

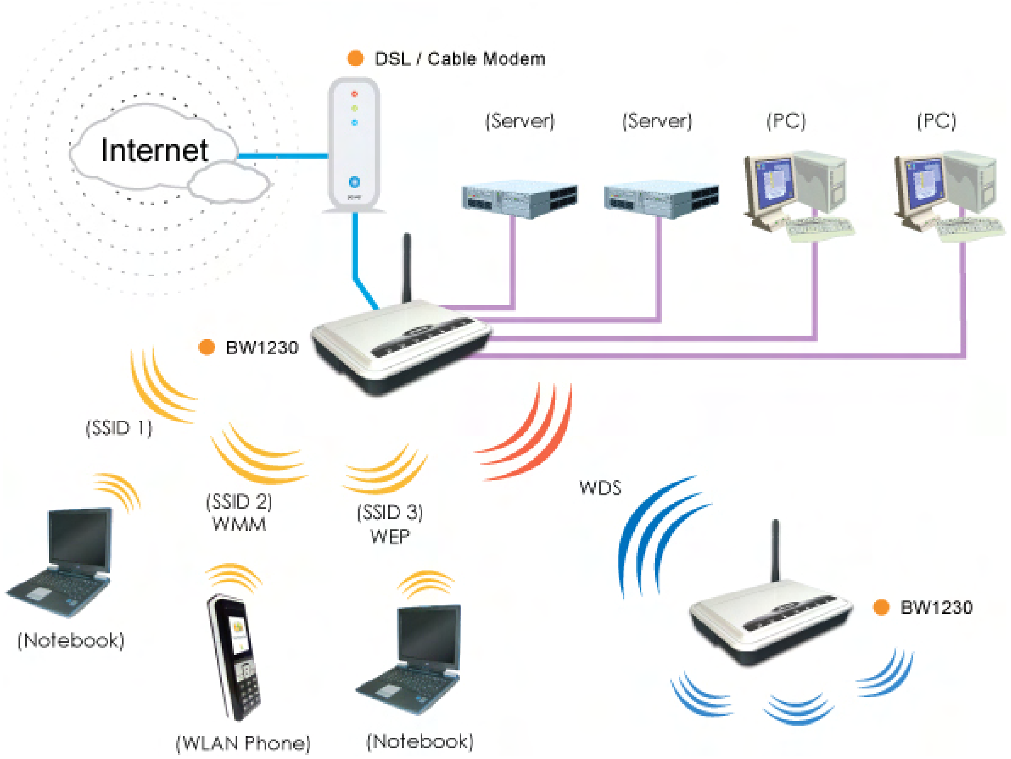
Note: The password is case sensitive. Click here if you can't remember the password.

Status: Waiting for User Input...

Figure 12 – Login page

Chapter 3 – Application Mode

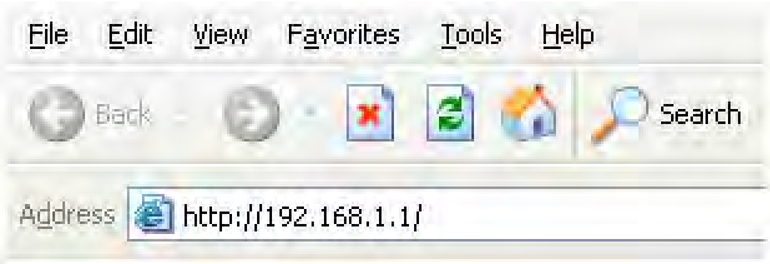
You could share the internet with everybody in anywhere.



Chapter 4 – Reference Manual

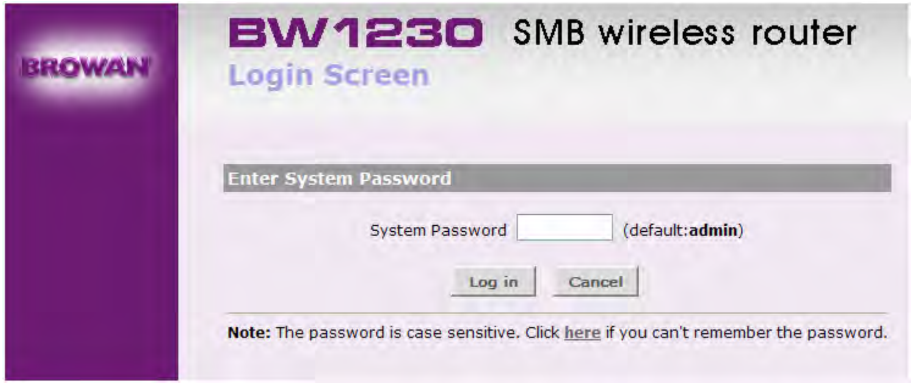
This chapter contains the illustration of the main functions in the configuration.

After the network connection setup (refer to **Accessing Your BW1230**), open the Web browser and enter the default IP address of the BW1230: **http://192.168.1.1**



http://192.168.1.1/

- Enter the System Password, **admin**.
- Click **Log in** button to **continue** the configuration, or click **Cancel** button to **quit** the configuration.

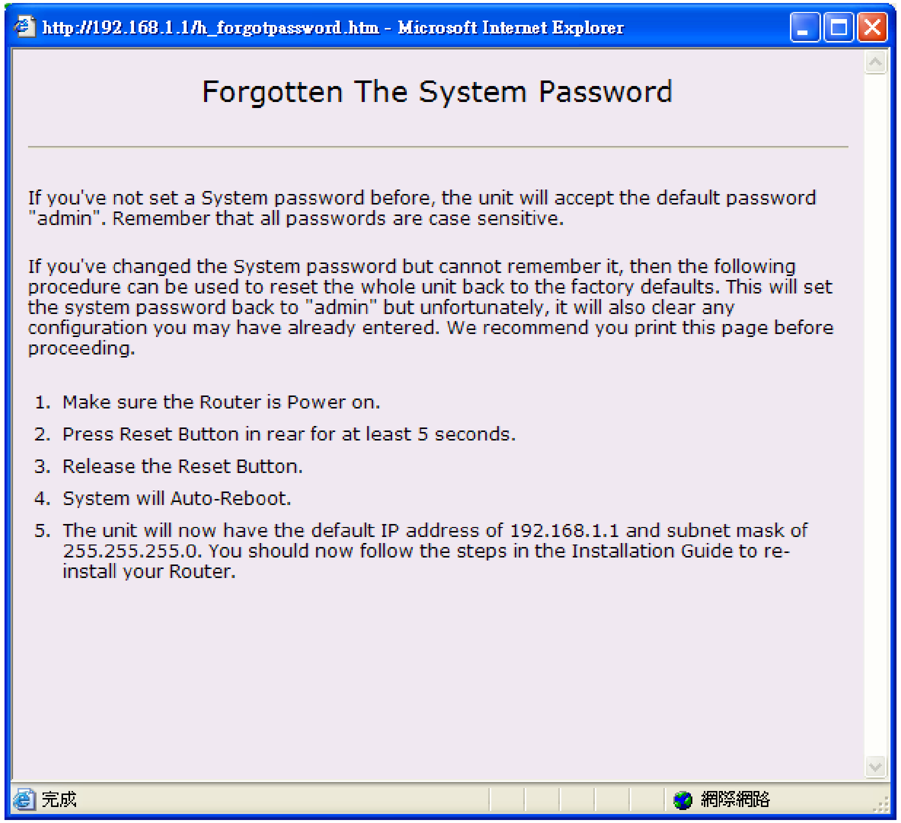


Enter System Password

System Password (default:**admin**)

Note: The password is case sensitive. Click here if you can't remember the password.

- If you forget your password, please click on the **here**. After you click on the **here**, there will be a popup window. And the popup window will show you what you should do.



http://192.168.1.1/h_forgotpassword.htm - Microsoft Internet Explorer

Forgotten The System Password

If you've not set a System password before, the unit will accept the default password "admin". Remember that all passwords are case sensitive.

If you've changed the System password but cannot remember it, then the following procedure can be used to reset the whole unit back to the factory defaults. This will set the system password back to "admin" but unfortunately, it will also clear any configuration you may have already entered. We recommend you print this page before proceeding.

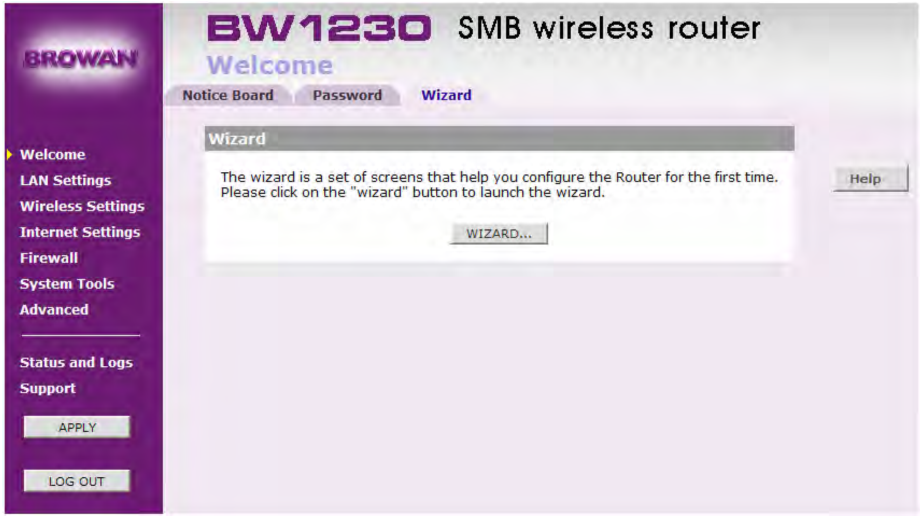
1. Make sure the Router is Power on.
2. Press Reset Button in rear for at least 5 seconds.
3. Release the Reset Button.
4. System will Auto-Reboot.
5. The unit will now have the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. You should now follow the steps in the Installation Guide to re-install your Router.

Welcome | Wizard

- The Wizard feature could help you to easily configure the router.

- The Wizard screen would display automatically for your preliminary configuration, or you could manually click on **Wizard tag**.

- Please click on the **WIZARD** button to launch the wizard feature.



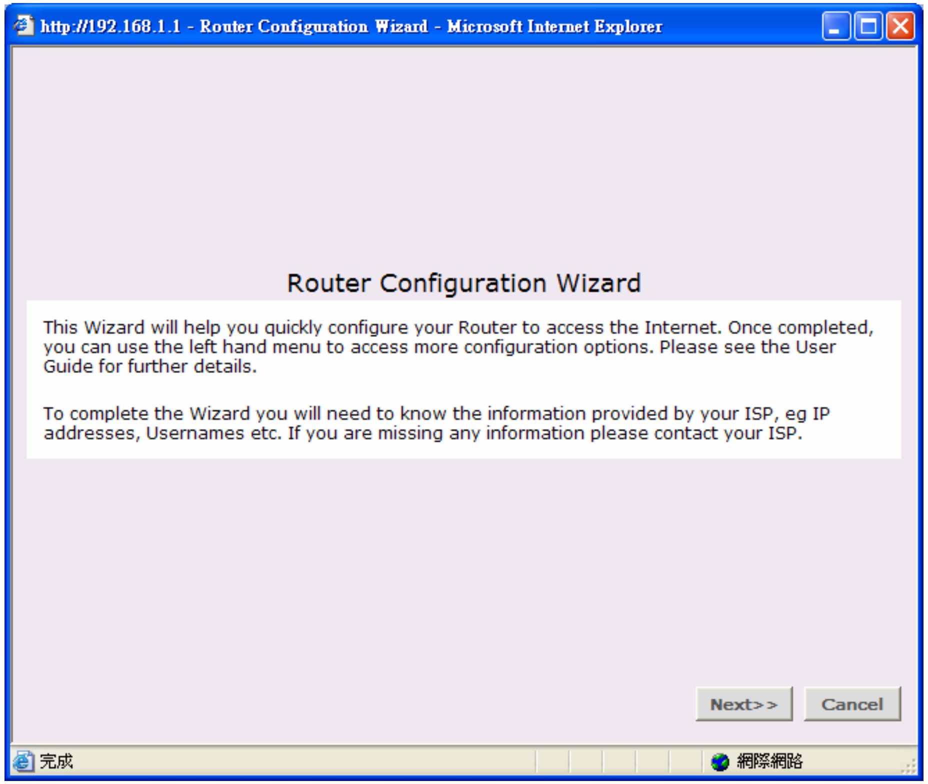
The wizard is a set of screens that help you configure the Router for the first time.
Please click on the "wizard" button to launch the wizard.

Welcome | Wizard | Setup Wizard

Router Configuration Wizard

- This screen is the first screen appears after you start the setup wizard.

- Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Router Configuration Wizard

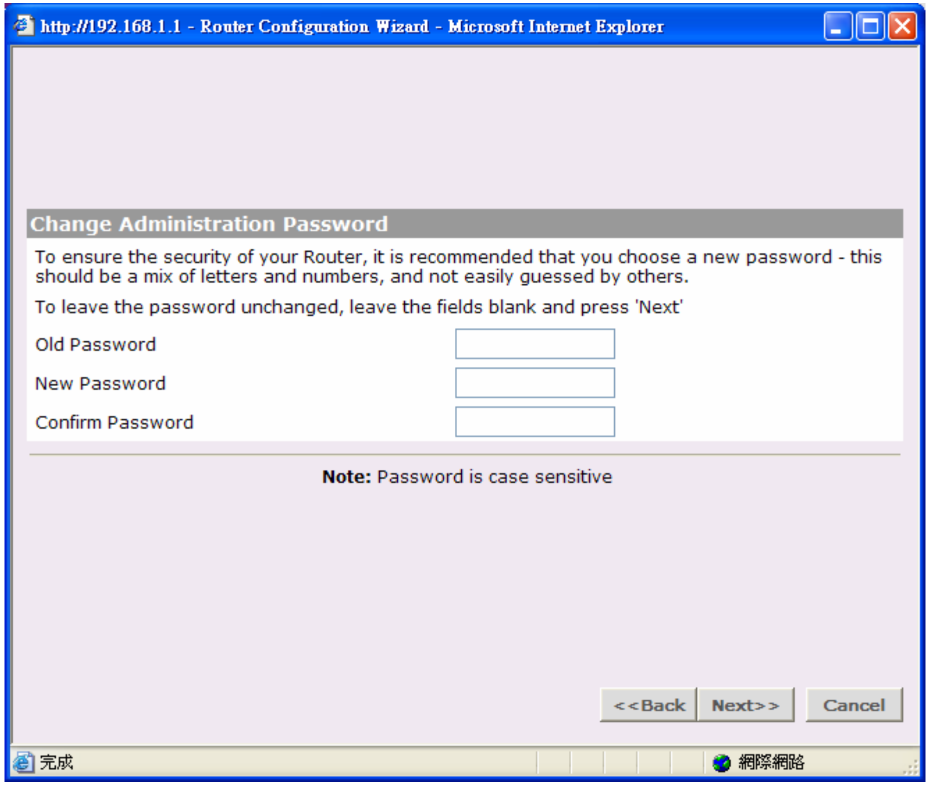
This Wizard will help you quickly configure your Router to access the Internet. Once completed, you can use the left hand menu to access more configuration options. Please see the User Guide for further details.

To complete the Wizard you will need to know the information provided by your ISP, eg IP addresses, Usernames etc. If you are missing any information please contact your ISP.

Change Administration Password

- You could leave fields blank to keep the default administrator password, or you could change a new password.
- If you would like to change a new password, please enter the old password in the first field. And enter the new password in the other two fields.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Change Administration Password

To ensure the security of your Router, it is recommended that you choose a new password - this should be a mix of letters and numbers, and not easily guessed by others.

To leave the password unchanged, leave the fields blank and press 'Next'

Old Password	
New Password	
Confirm Password	

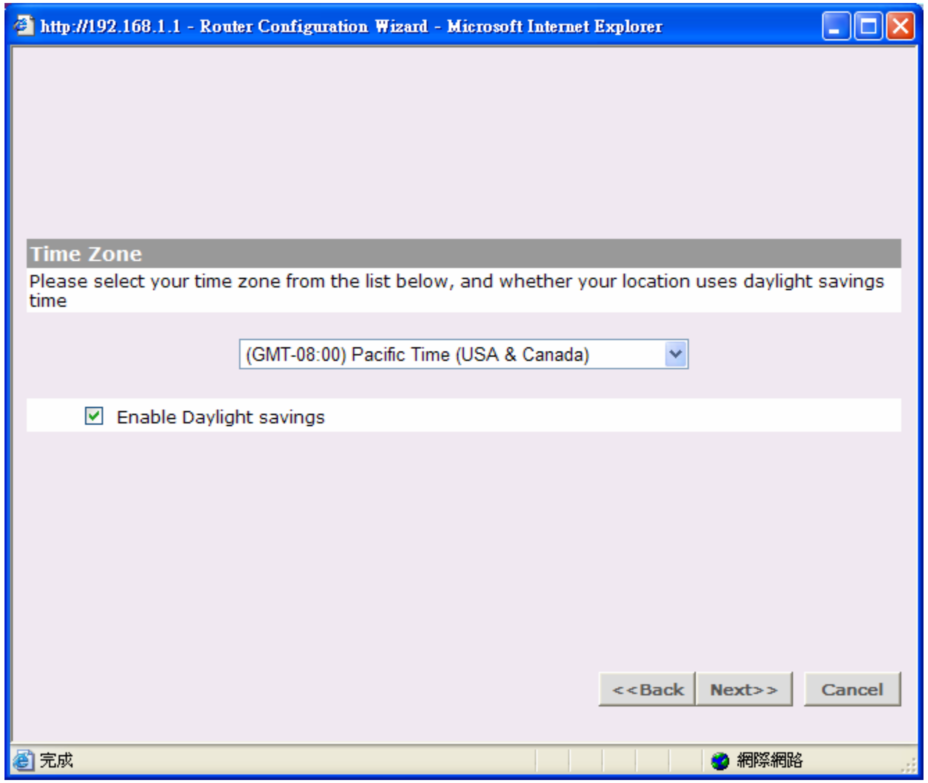
Note: Password is case sensitive

!	Browan recommand you to change a new password for your wireless network sercurity. And the **password is case sensitive.**

Time Zone

- Please select the time zone from the drop-down menu, and check the Enable Daylight saving selection if necessary

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Time Zone

Please select your time zone from the list below, and whether your location uses daylight savings time

(GMT-08:00) Pacific Time (USA & Canada)

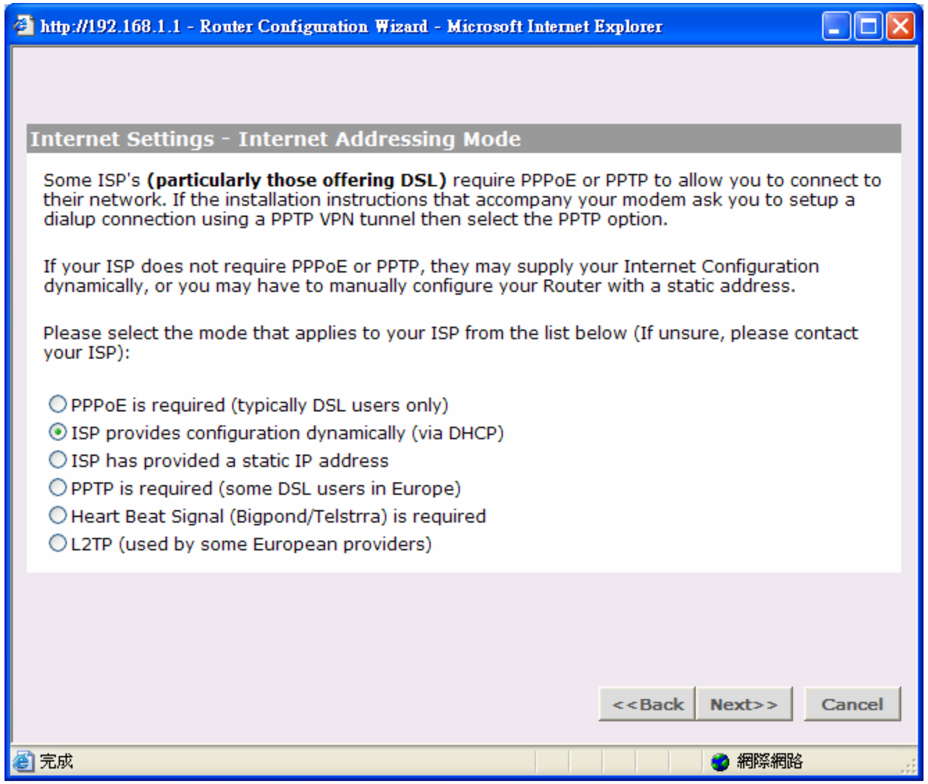
☑ Enable Daylight savings

<<Back
Next>>
Cancel
完成
網際網路

Internet Settings - Internet Addressing Mode

- Please select an internet connection mode you are using.
  - PPPoE is required (typically DSL users only)
  - ISP provides configuration dynamically (via DHCP)
  - ISP has provided a static IP address
  - PPTP is required (some DSL users in Europe)
  - Heart Beat Signal (Bigpond/Telstrra) is required
  - L2TP (used by some European providers)

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - Internet Addressing Mode

Some ISP's **(particularly those offering DSL)** require PPPoE or PPTP to allow you to connect to their network. If the installation instructions that accompany your modem ask you to setup a dialup connection using a PPTP VPN tunnel then select the PPTP option.

If your ISP does not require PPPoE or PPTP, they may supply your Internet Configuration dynamically, or you may have to manually configure your Router with a static address.

Please select the mode that applies to your ISP from the list below (If unsure, please contact your ISP):

○ PPPoE is required (typically DSL users only)
● ISP provides configuration dynamically (via DHCP)
○ ISP has provided a static IP address
○ PPTP is required (some DSL users in Europe)
○ Heart Beat Signal (Bigpond/Telstrra) is required
○ L2TP (used by some European providers)

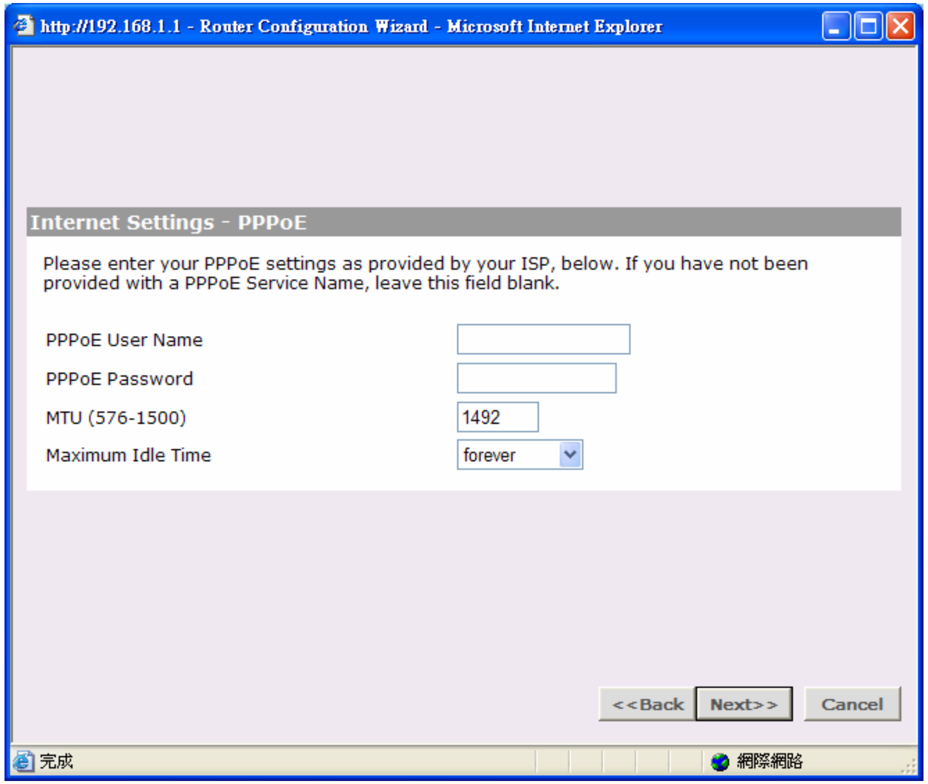
Internet Settings – PPPoE

- **PPPoE (Point-to-Point Protocol over Ethernet):**
Only ISP's providing DSL use PPPoE. If the installation instructions that accompany your modem ask you to install a PPPoE client on your PC then select this option. Note that you will not need to use PPPoE software on your PC once the Router is installed. If you are unsure, you should ask your ISP whether you need to use PPPoE.

  PPPoE User Name:
  Enter your User Name in this box. This field is required, and will be provided to you by your ISP.

  PPPoE Password:
  Enter your password in this box. This field is required, and will be provided to you by your ISP.

  PPPoE Service Name:
  If your ISP provided you with a Service Name, you should enter this here. If not, you should leave this blank.


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - PPPoE

Please enter your PPPoE settings as provided by your ISP, below. If you have not been provided with a PPPoE Service Name, leave this field blank.

PPPoE User Name	
PPPoE Password	
MTU (576-1500)	1492
Maximum Idle Time	forever

<<Back
Next>>
Cancel
完成
網際網路

Host Name:

Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is optional, and so if you have not been provided a host name, you may leave it blank.

MTU:

The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

Maximum Idle Time:

This is the amount of time that passes before your Internet Connection is dropped due to inactivity. If you want to keep your Internet Connection established at all times, you should select **Forever**; Otherwise, select the amount of time that you want to pass before your Router disconnects from your ISP.

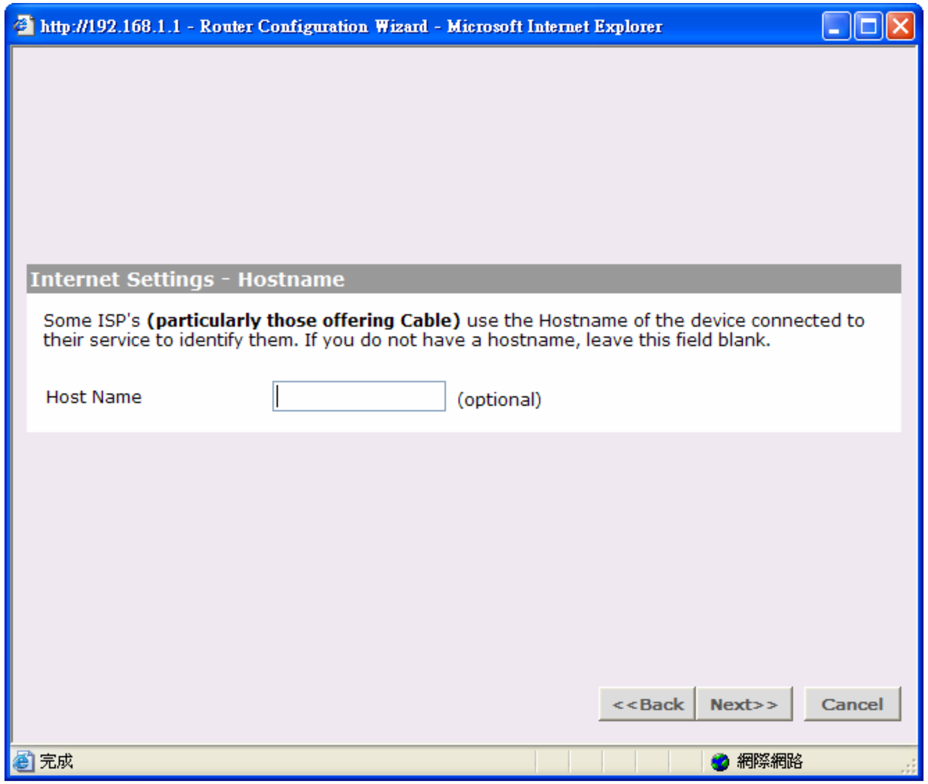
- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

Internet Settings – Hostname

- **Dynamic IP address (automatically allocated):**
  This allocation mode may be used by either Cable or DSL ISP's. It is popular with Cable providers, and may also be required if your modem has a built in DHCP server.
  If this mode is selected, your IP Address, Subnet Mask, and ISP Address will be obtained automatically from your ISP. They are not displayed on this screen, but may be viewed on the Status screen (click on **Status and Logs** on the left hand menu bar).

  Host Name:
  Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is optional, and so if you have not been provided a host name, you may leave it blank.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - Hostname

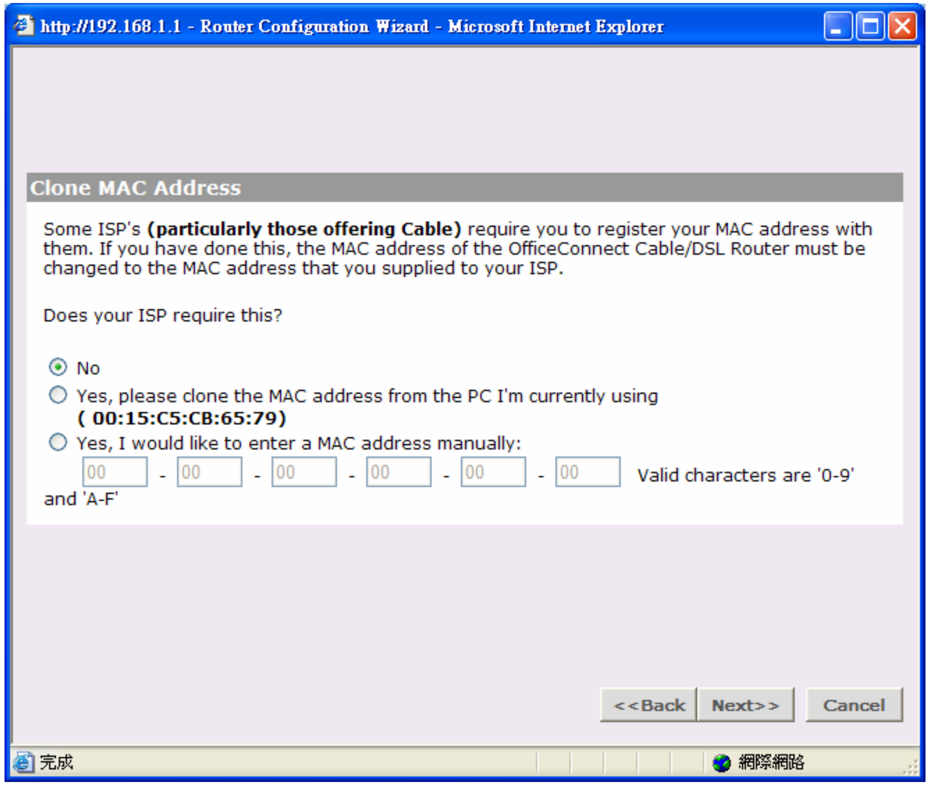
Some ISP's **(particularly those offering Cable)** use the Hostname of the device connected to their service to identify them. If you do not have a hostname, leave this field blank.

Host Name (optional)

- **Clone MAC address:**
  Some ISP's use the hardware (MAC) address of the device you connect to the Internet with to identify you. If you have previously used a different device with your current ISP, and they use your MAC address to identify you, then you can change the MAC address on the WAN side of your Router to be that of your old device. There are three options available for cloning the Router WAN port MAC address:

  Use the Router's original MAC address:
  This option is selected by default. When selected, the Router uses the WAN port MAC address that it was assigned at the factory.

  Use this PCs MAC address:
  This option will assign the MAC address of the PC you are using to manage the Router to the WAN port. If this is the PC that you used previously to connect to your ISP, then you should select this option.


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel
完成
網際網路

Clone MAC Address

Some ISP's **(particularly those offering Cable)** require you to register your MAC address with them. If you have done this, the MAC address of the OfficeConnect Cable/DSL Router must be changed to the MAC address that you supplied to your ISP.

Does your ISP require this?

● No
○ Yes, please clone the MAC address from the PC I'm currently using **(00:15:C5:CB:65:79)**
○ Yes, I would like to enter a MAC address manually:
00 - 00 - 00 - 00 - 00 - 00 Valid characters are '0-9' and 'A-F'

Enter a new MAC address manually

If the MAC addresses given by the previous two options are not correct, then you will need to find the MAC address of the previous device used with your ISP.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

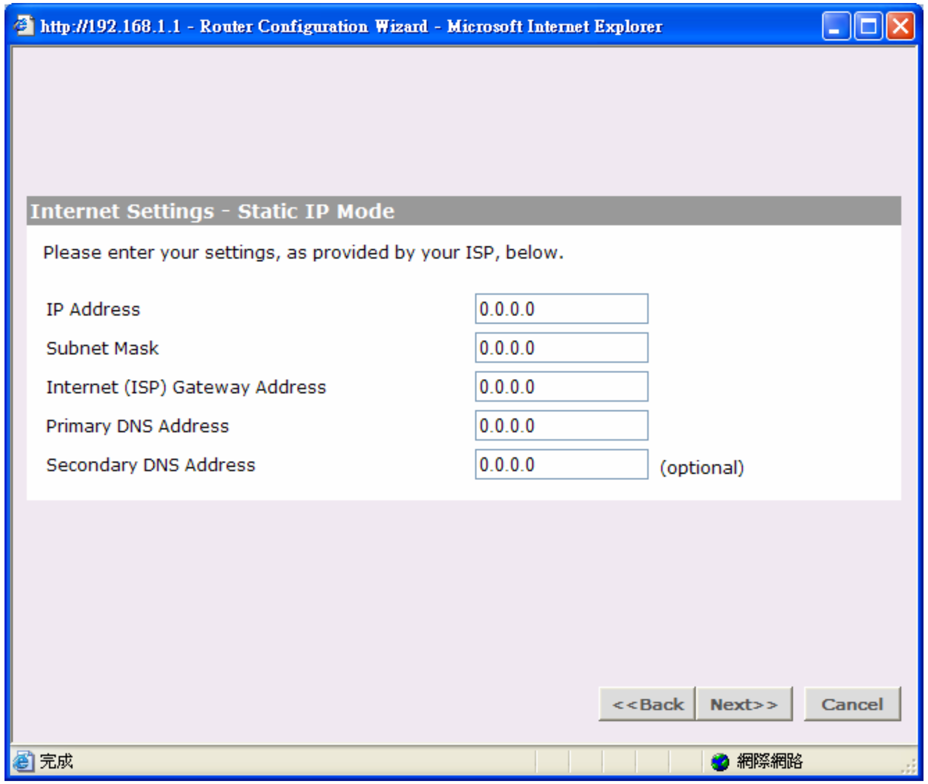
Internet Settings - Static IP Mode

- **Static IP address (to be specified manually):**
  This allocation mode may be used by either Cable or DSL ISP's.

  IP address:
  This is the IP address of your Router that will be seen from the WAN, or Internet. This setting is required, and will be provided to you by your ISP.

  Subnet mask:
  This is the Subnet Mask of your Router's WAN port. This setting is required, and will be provided to you by your ISP.

  ISP Gateway Address:
  This is sometimes referred to as **Default Gateway**. This setting is required, and will be provided to you by your ISP.


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - Static IP Mode

Please enter your settings, as provided by your ISP, below.

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Internet (ISP) Gateway Address	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0 (optional)

<<Back
Next>>
Cancel
完成
網際網路

Primary DNS Address:

Your ISP will normally provide you with at least one DNS (Domain Name Server) address, and you should enter the first here. A Domain Name Server performs the translation between user-friendly names (such as www.browan.com) and IP addresses. Note that this setting is optional, and can be left at 0.0.0.0 if it is not required.

Secondary DNS Address:

If your ISP has provided a second DNS address, you should enter it here. Otherwise, leave this setting at its default of 0.0.0.0. This setting is optional.

MTU:

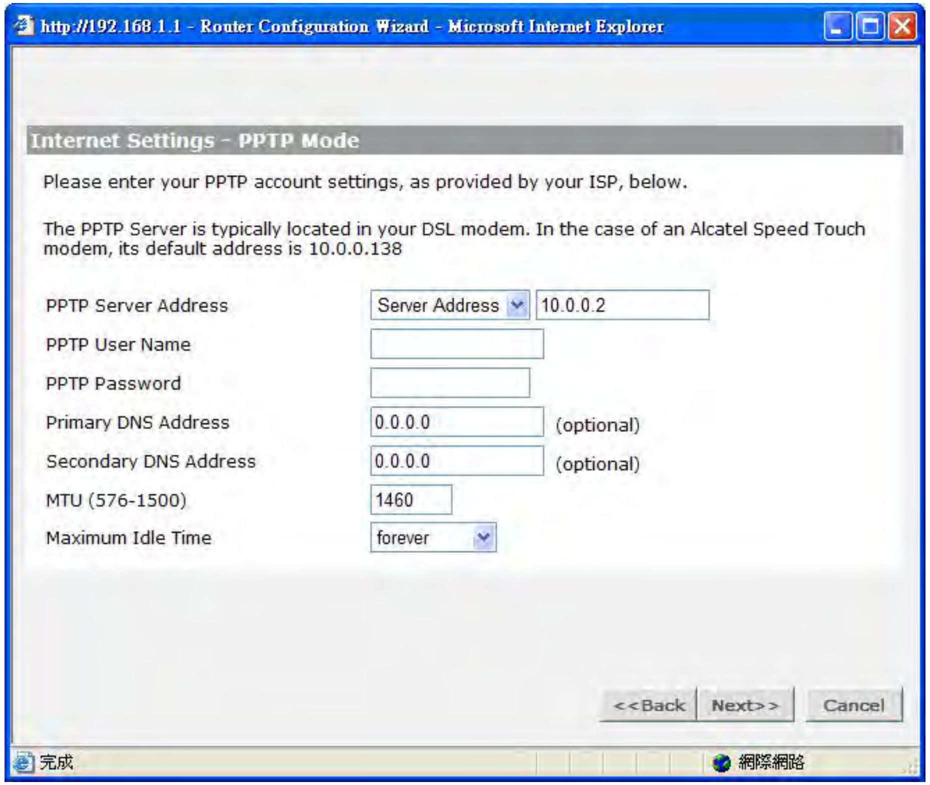
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

Internet Settings - PPTP Mode

- **PPTP (Point to Point Tunneling Protocol):**
  Some ISP's require the use of PPTP to establish connections to their networks. At present PPTP is only used by some European ISP's. If the installation instructions that accompany your modem ask you to set up a dialup connection using a PPTP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more.

  PPTP Server address:
  This is the IP address of the PPTP server you are connecting to. This setting is required, and will be provided to you by your ISP. The PPTP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.2


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - PPTP Mode

Please enter your PPTP account settings, as provided by your ISP, below.

The PPTP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.138

PPTP Server Address	Server Address 10.0.0.2
PPTP User Name	
PPTP Password	
Primary DNS Address	0.0.0.0 (optional)
Secondary DNS Address	0.0.0.0 (optional)
MTU (576-1500)	1460
Maximum Idle Time	forever

PPTP User Name:

Enter your User Name in this box. This field is required, and will be provided to you by your ISP.

PPTP Password:

Enter your password in this box. This field is required, and will be provided to you by your ISP.

DNS Addresses:

If your ISP has provided you with DNS addresses, you should enter them here. Otherwise, leave these setting at its default of 0.0.0.0. These settings are optional, and most ISP's will also provide you with DNS addresses automatically. When the addresses are obtained from your ISP, they will be displayed on the Status screen.

MTU:

The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

Maximum Idle Time:
This is the amount of time that passes before your Internet Connection is dropped due to inactivity. If you want to keep your Internet Connection established at all times, you should select **Forever**. Otherwise, select the amount of time that you want to pass before your Router disconnects from your ISP.

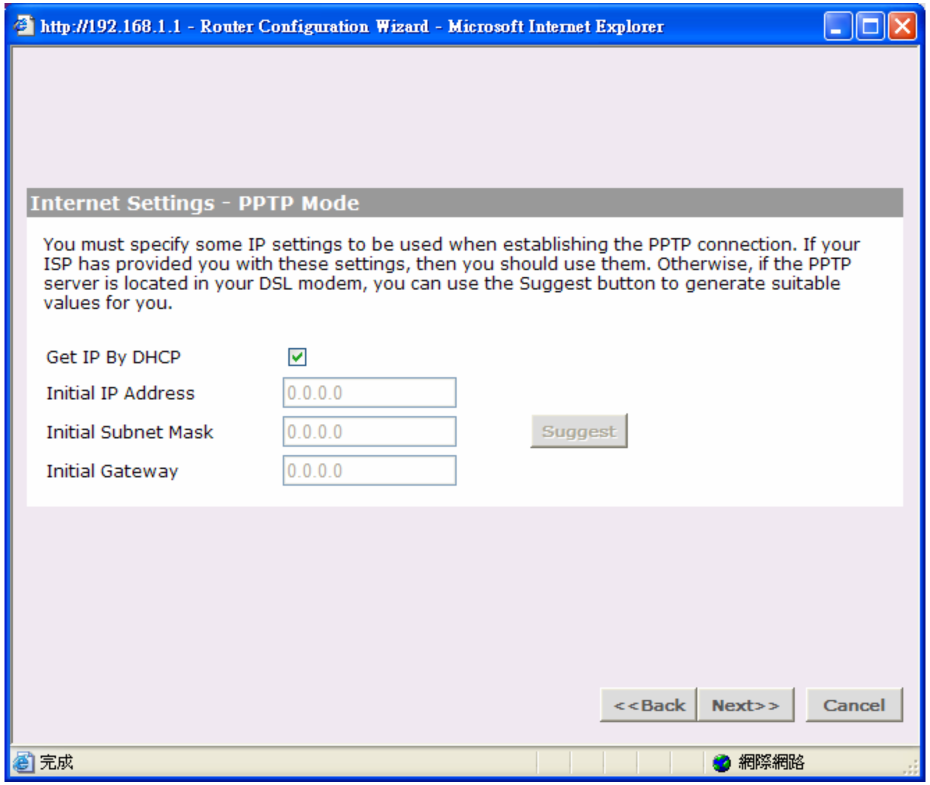
- Click Back to go to previous screen.
Or Click Next to continue the setup wizard.
Or click Cancel to quit the setup wizard.

Get IP By DHCP:

Some ISP may have the mechanism that automatically provides Initial IP Address, Subnet Mask and Default Gateway. If your ISP provides such mechanism, you should check this option. Otherwise, you should manually enter your initial IP Address, Subnet Mask and Default Gateway.

Initial IP address and Subnet Mask:

You must specify some IP settings to be used when establishing the PPTP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the PPTP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you. The **Suggest** button will select an IP address on the same subnet as the PPTP server.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - PPTP Mode

You must specify some IP settings to be used when establishing the PPTP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the PPTP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you.

Get IP By DHCP ☑

Initial IP Address 0.0.0.0

Initial Subnet Mask 0.0.0.0

Initial Gateway 0.0.0.0

Initial Default Gateway:

The PPTP Server address and the Initial IP Address that ISP provides sometimes may not be in the same Subnet. In this case, the Initial Default Gateway is necessarily to be provided to establish the PPTP connection. If the PPTP Server and Initial IP Address are in the same subnet, then you can set the Initial Default Gateway to 0.0.0.0 or 0.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

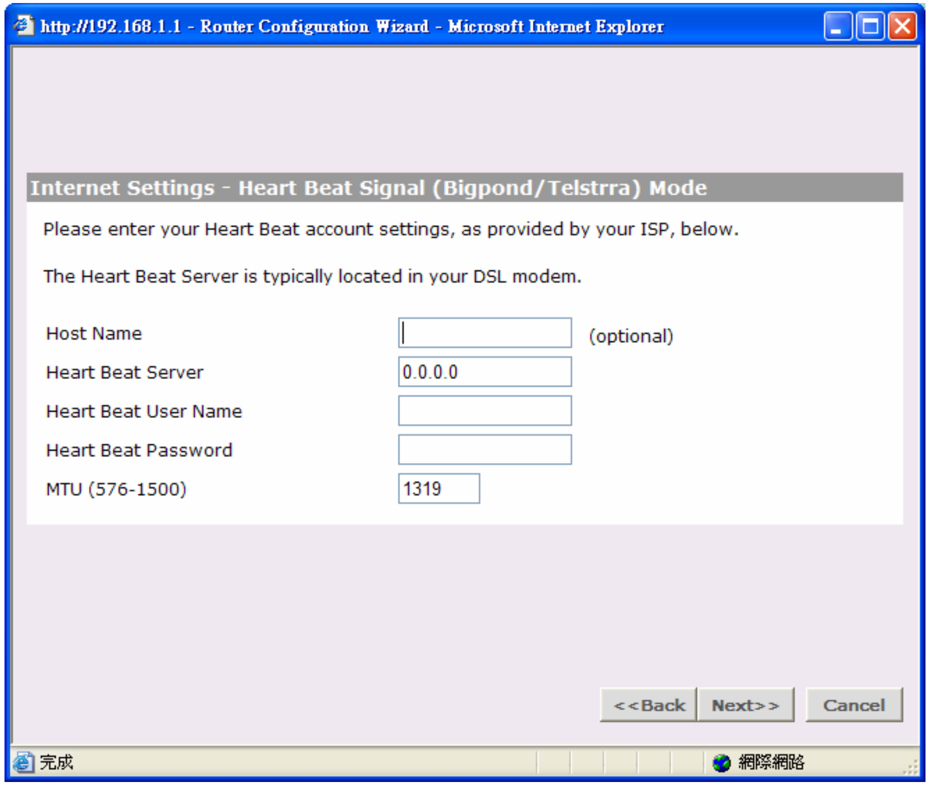
Internet Settings - Heart Beat Signal (Bigpond/Telstrra) Mode

- **Heart Beat Signal (For Australia only):**
  It is a service used in Australia only. If you are using Heart Beat Signal connection, check with your ISP for the necessary setup information.

  Host Name:
  Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is optional, and so if you have not been provided a host name, you may leave it blank.

  Heart Beat Server:
  Your ISP will provide you with the Heart Beat Server's IP Address.

  Heart Beat User Name:
  Enter the **User Name** you use when logging onto your ISP through a Heart Beat Signal connection


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer
<<Back
Next>>
Cancel
完成
網際網路

Internet Settings - Heart Beat Signal (Bigpond/Telstrra) Mode

Please enter your Heart Beat account settings, as provided by your ISP, below.

The Heart Beat Server is typically located in your DSL modem.

Host Name	(optional)
Heart Beat Server	0.0.0.0
Heart Beat User Name	
Heart Beat Password	
MTU (576-1500)	1319

Heart Beat Password:

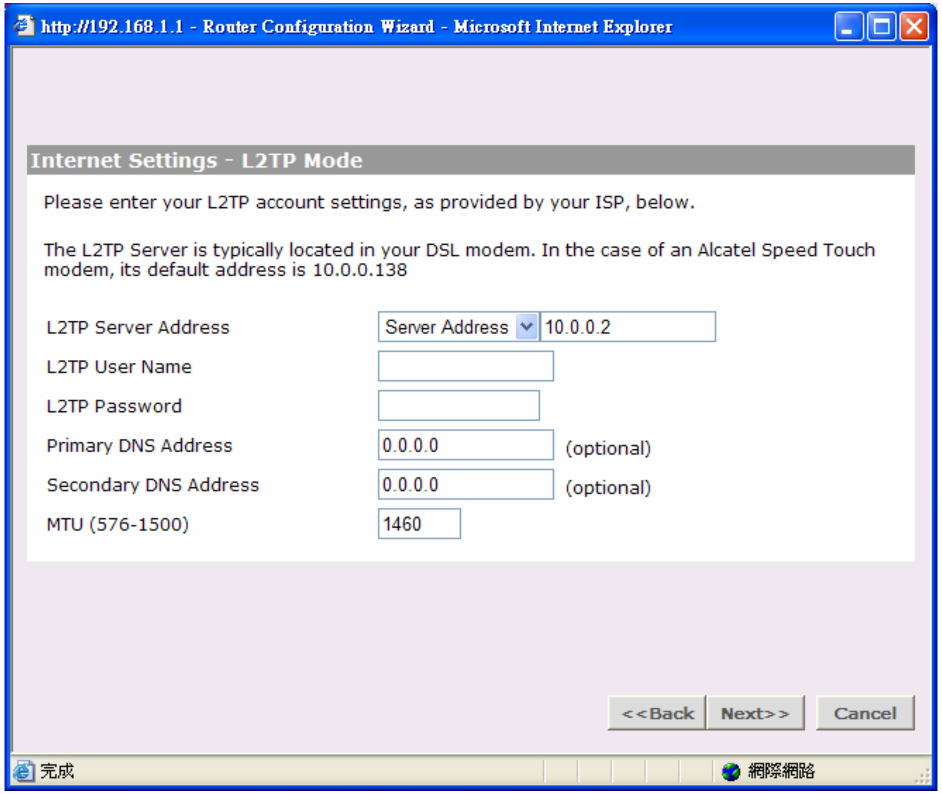
Enter the **Password** you use when logging onto your ISP through a Heart Beat Signal connection

MTU:

The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

Internet Settings - L2TP Mode


http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - L2TP Mode

Please enter your L2TP account settings, as provided by your ISP, below.

The L2TP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.138

L2TP Server Address	Server Address 10.0.0.2	
L2TP User Name		
L2TP Password		
Primary DNS Address	0.0.0.0	(optional)
Secondary DNS Address	0.0.0.0	(optional)
MTU (576-1500)	1460	

- **L2TP (Layer Two Tunneling Protocol):**
  Some ISP's require the use of L2TP to establish connections to their networks. If the installation instructions that accompany your modem ask you to set up a dialup connection using a L2TP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more.

  L2TP Server address:
  This is the IP address of the L2TP server you are connecting to. This setting is required, and will be provided to you by your ISP. The L2TP Server is typically located in your DSL modem.

  L2TP User Name:
  Enter your User Name in this box. This field is required, and will be provided to you by your ISP.

  L2TP Password:
  Enter your password in this box. This field is required,

and will be provided to you by your ISP.

DNS Addresses:
If your ISP has provided you with DNS addresses, you should enter them here. Otherwise, leave these setting at its default of 0.0.0.0. These settings are optional, and most ISP's will also provide you with DNS addresses automatically. When the addresses are obtained from your ISP, they will be displayed on the Status screen.

MTU:
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

Get IP By DHCP:

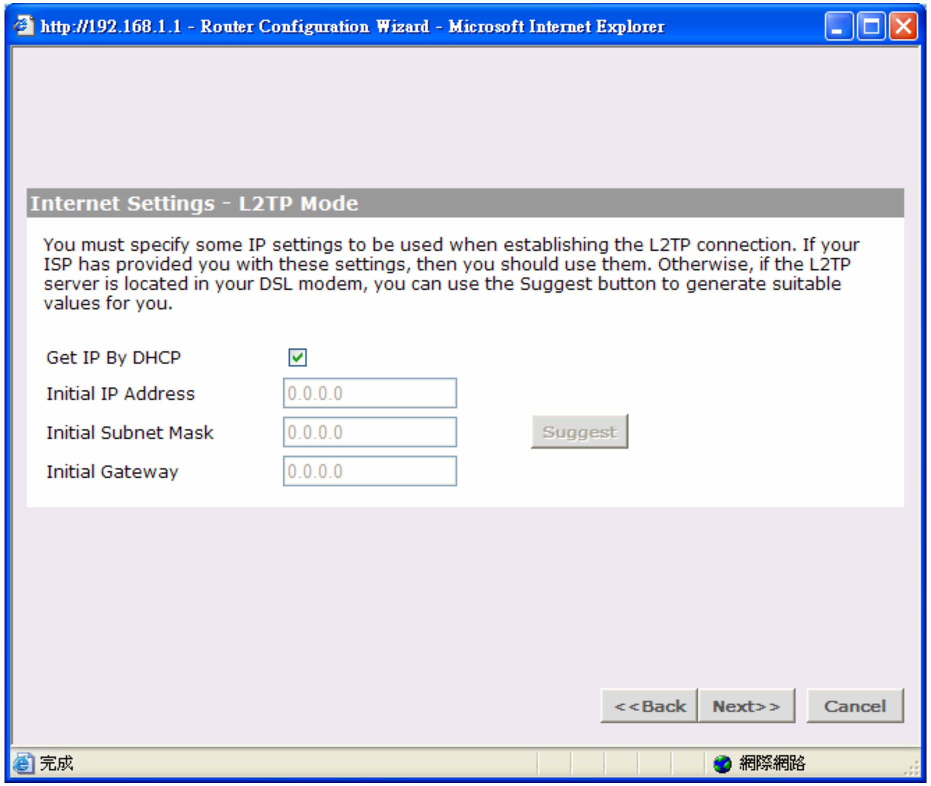
Some ISP may have the mechanism that automatically provides Initial IP Address, Subnet Mask and Default Gateway. If your ISP provides such mechanism, you should check this option. Otherwise, you should manually enter your initial IP Address, Subnet Mask and Default Gateway.

Initial IP address and Subnet Mask:

You must specify some IP settings to be used when establishing the L2TP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the L2TP server is located in your DSL modem, you can use the **Suggest** button to generate suitable values for you. The Suggest button will select an IP address on the same subnet as the L2TP server.

Initial Default Gateway:

The L2TP Server address and the Initial IP Address that ISP provides sometimes may not be in the same Subnet. In this case, the Initial Default Gateway is necessarily to be provided to establish the L2TP



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Internet Settings - L2TP Mode

You must specify some IP settings to be used when establishing the L2TP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the L2TP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you.

Get IP By DHCP ☑

Initial IP Address 0.0.0.0

Initial Subnet Mask 0.0.0.0

Initial Gateway 0.0.0.0

connection.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.

LAN Settings - LAN IP Address

The Router must be given a valid static IP address and subnet mask for the LAN interface.

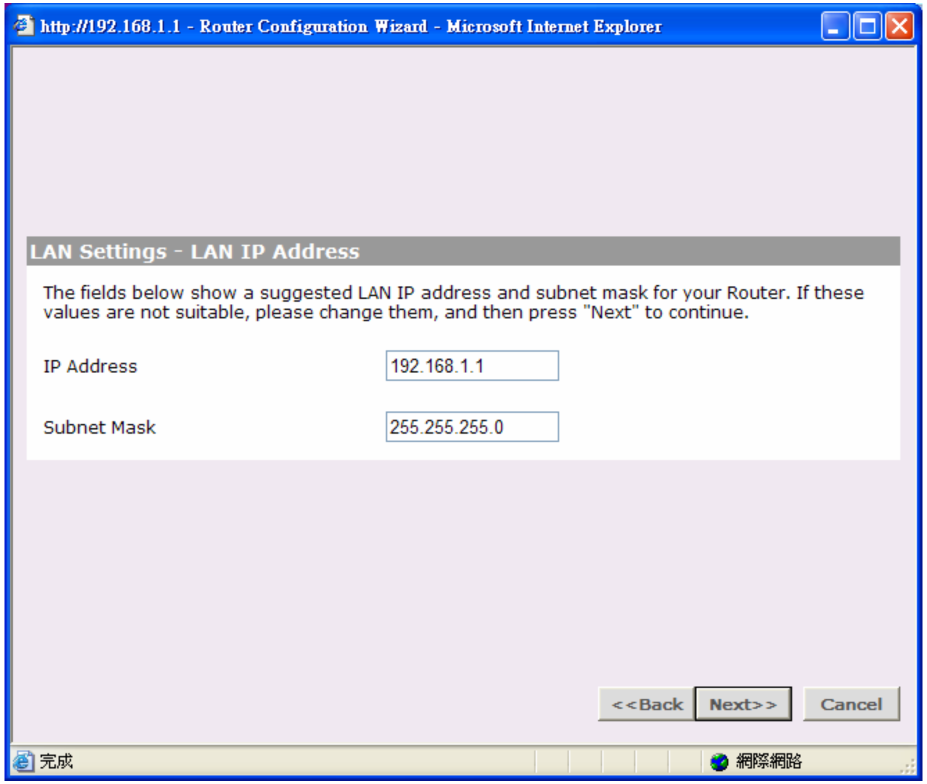
IP Address:

This is the IP address of the Router as seen by the devices on the LAN. The default value is 192.168.1.1.

Subnet Mask:

This is the Subnet Mask for the Router. For devices to be on the same subnet, they must have the same subnet mask. The default value is 255.255.255.0.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

LAN Settings - LAN IP Address

The fields below show a suggested LAN IP address and subnet mask for your Router. If these values are not suitable, please change them, and then press "Next" to continue.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

<<Back
Next>>
Cancel
完成
網際網路

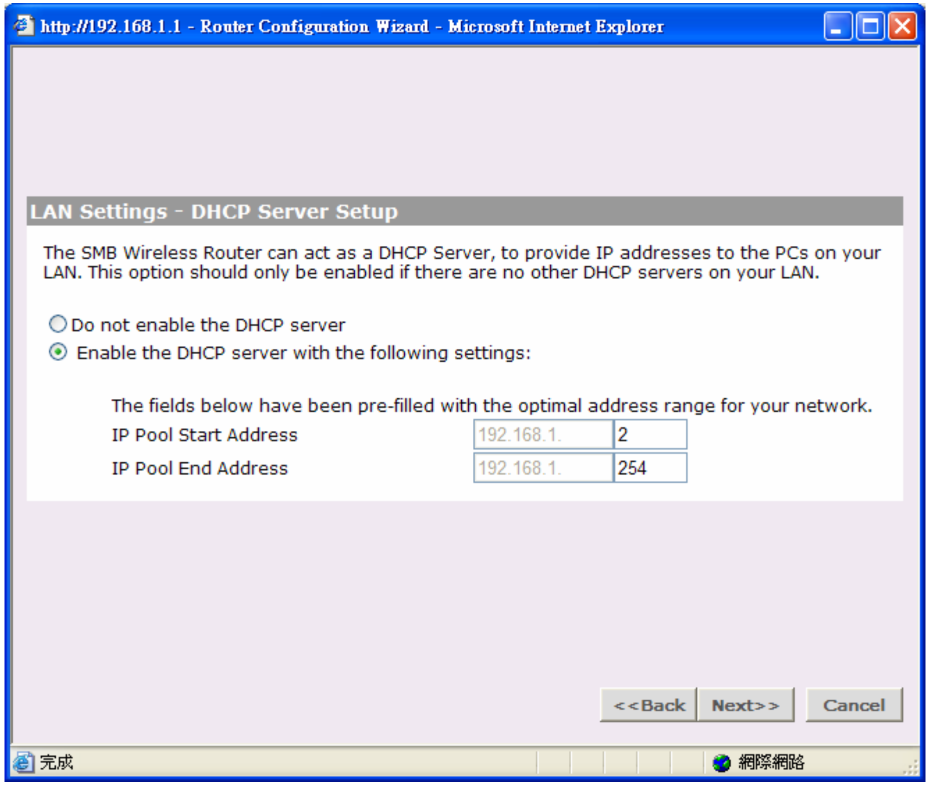
LAN Settings - DHCP Server Setup

- Please make selection if you would like to enable DHCP or disable DHCP.

  IP Pool Start Address:
  This defines the start address of the IP address range. The default value is 192.168.1.2.

  IP Pool End Address:
  This defines the end address of the IP address range. The default value is 192.168.1.254.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

LAN Settings - DHCP Server Setup

The SMB Wireless Router can act as a DHCP Server, to provide IP addresses to the PCs on your LAN. This option should only be enabled if there are no other DHCP servers on your LAN.

○ Do not enable the DHCP server
● Enable the DHCP server with the following settings:

The fields below have been pre-filled with the optimal address range for your network.

IP Pool Start Address 192.168.1. 2
IP Pool End Address 192.168.1. 254

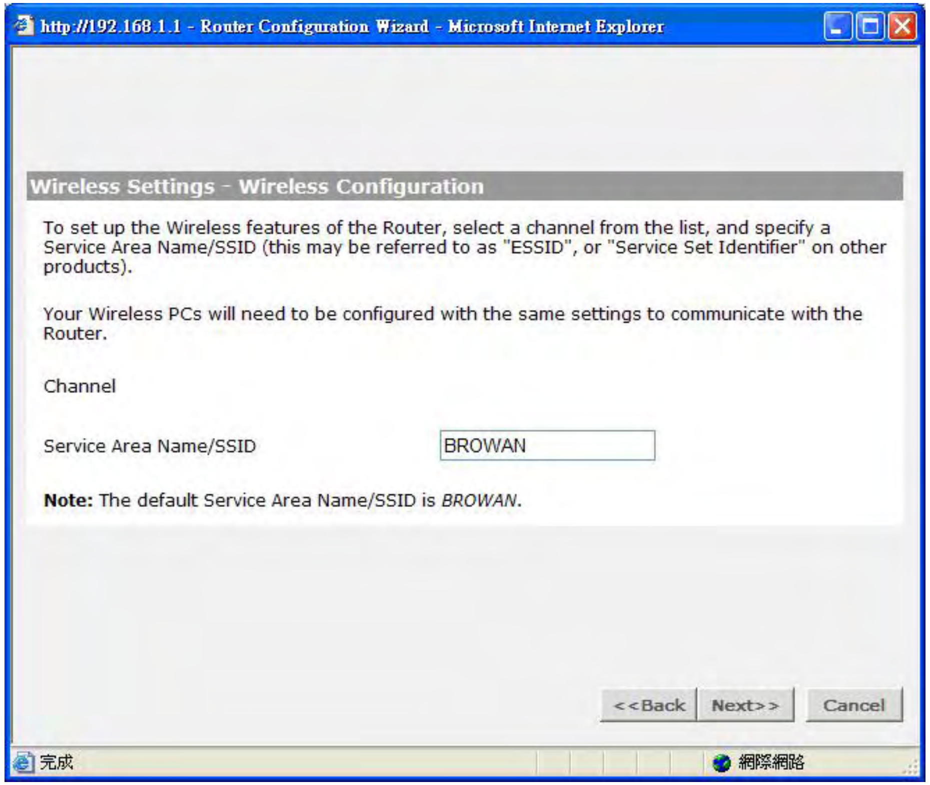
Wireless Settings - Wireless Configuration

Service Area Name/SSID:

This allows you to name your Wireless network. The field will accept any alphanumeric string but not spaces and has a maximum length of 32 characters. Your Wireless PCs must be configured with exactly the same name or you will not establish a connection.

The Service Area Name may also be referred to as **ESSID** depending on your networking vendor. By default the Router uses the name **BROWAN**.

- Click Back to go to previous screen.
  Or Click Next to continue the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Wireless Settings - Wireless Configuration

To set up the Wireless features of the Router, select a channel from the list, and specify a Service Area Name/SSID (this may be referred to as "ESSID", or "Service Set Identifier" on other products).

Your Wireless PCs will need to be configured with the same settings to communicate with the Router.

Channel

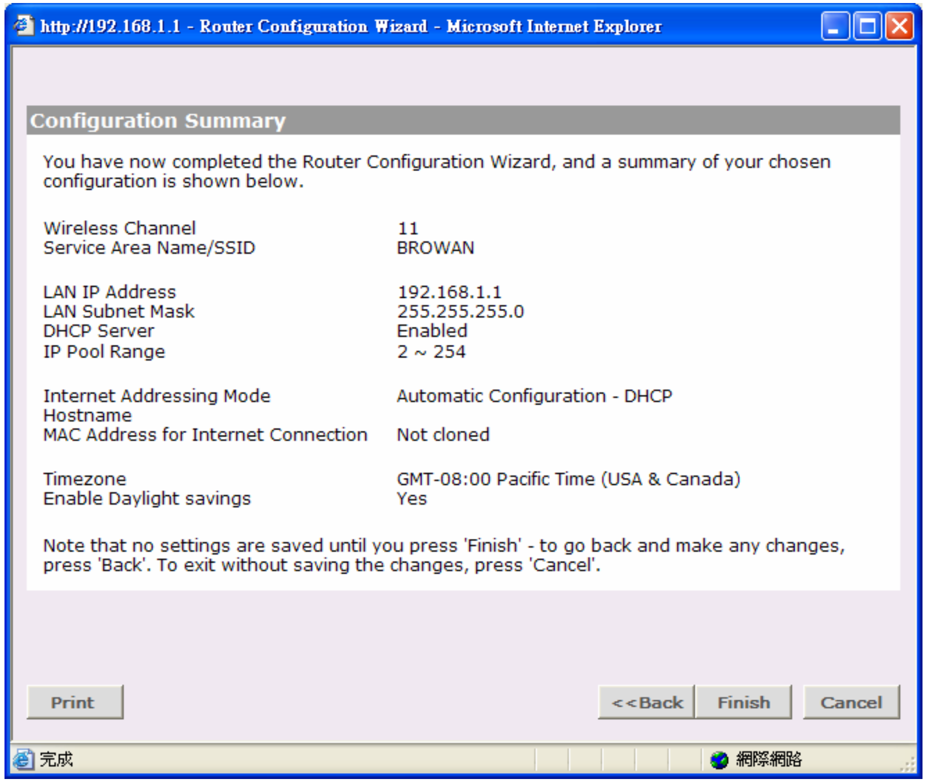
Service Area Name/SSID: BROWAN

Note: The default Service Area Name/SSID is *BROWAN*.

Configuration Summary

This screen will show the configuration of your BW1230.

- Click Print to print out the configuration.
  And click Back to go to previous screen.
  Or Click Finish to complete the setup wizard.
  Or click Cancel to quit the setup wizard.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Configuration Summary

You have now completed the Router Configuration Wizard, and a summary of your chosen configuration is shown below.

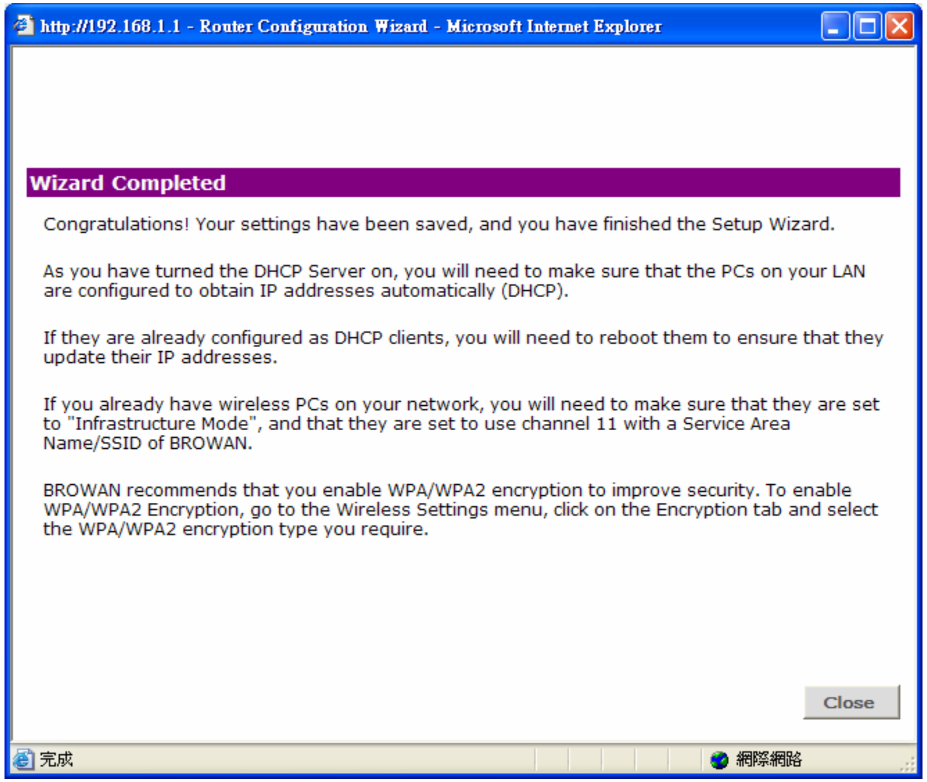
Wireless Channel	11
Service Area Name/SSID	BROWAN
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	Enabled
IP Pool Range	2 ~ 254
Internet Addressing Mode	Automatic Configuration - DHCP
Hostname	
MAC Address for Internet Connection	Not cloned
Timezone	GMT-08:00 Pacific Time (USA & Canada)
Enable Daylight savings	Yes

Note that no settings are saved until you press 'Finish' - to go back and make any changes, press 'Back'. To exit without saving the changes, press 'Cancel'.

Wizard Completed

Your BW1230 settings have been completely saved.

Now you are ready to enjoy your wire and wireless network.



http://192.168.1.1 - Router Configuration Wizard - Microsoft Internet Explorer

Wizard Completed

Congratulations! Your settings have been saved, and you have finished the Setup Wizard.

As you have turned the DHCP Server on, you will need to make sure that the PCs on your LAN are configured to obtain IP addresses automatically (DHCP).

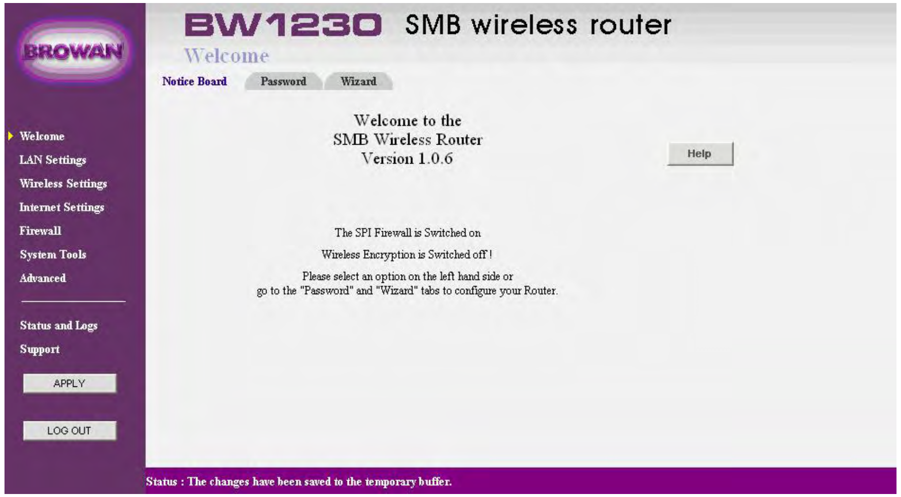
If they are already configured as DHCP clients, you will need to reboot them to ensure that they update their IP addresses.

If you already have wireless PCs on your network, you will need to make sure that they are set to "Infrastructure Mode", and that they are set to use channel 11 with a Service Area Name/SSID of BROWAN.

BROWAN recommends that you enable WPA/WPA2 encryption to improve security. To enable WPA/WPA2 Encryption, go to the Wireless Settings menu, click on the Encryption tab and select the WPA/WPA2 encryption type you require.

Welcome | Notice Board

The Notice Board is used to display warning messages if you've configured the Router in a non standard manner. For example, you would be warned if you had disabled the Firewall.



Welcome to the
SMB Wireless Router
Version 1.0.6

The SPI Firewall is Switched on

Wireless Encryption is Switched off !

Please select an option on the left hand side or
go to the "Password" and "Wizard" tabs to configure your Router.

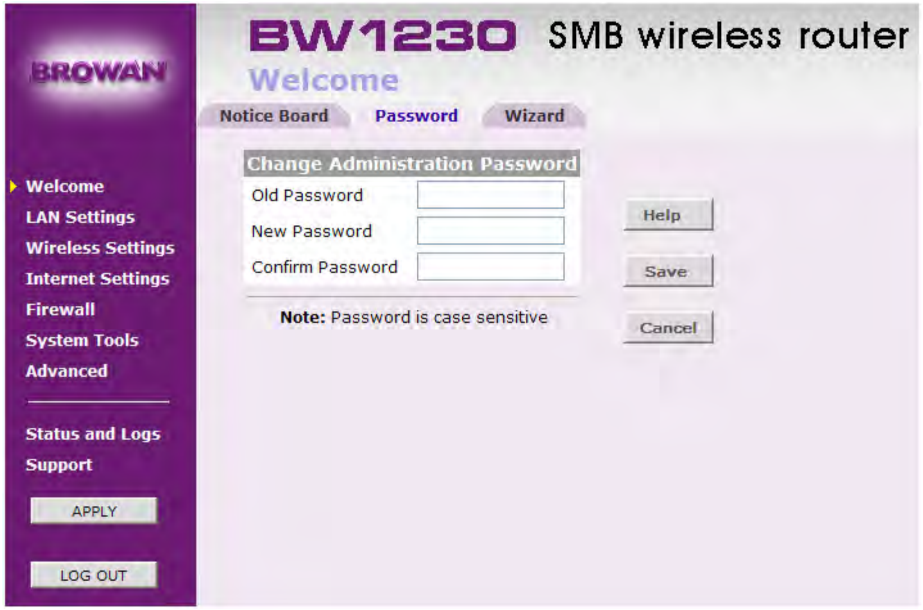
Status : The changes have been saved to the temporary buffer.

Welcome | Password

Changing the Administration Password

You can change the password to prevent unauthorized access to the Administration System. To do this:

1. Enter the current password in the Old Password field.
2. Enter the new password in the New Password field.
3. Enter the new password again in the Confirm Password field.
4. Click Apply to save the new password.



Change Administration Password

Old Password

New Password

Confirm Password

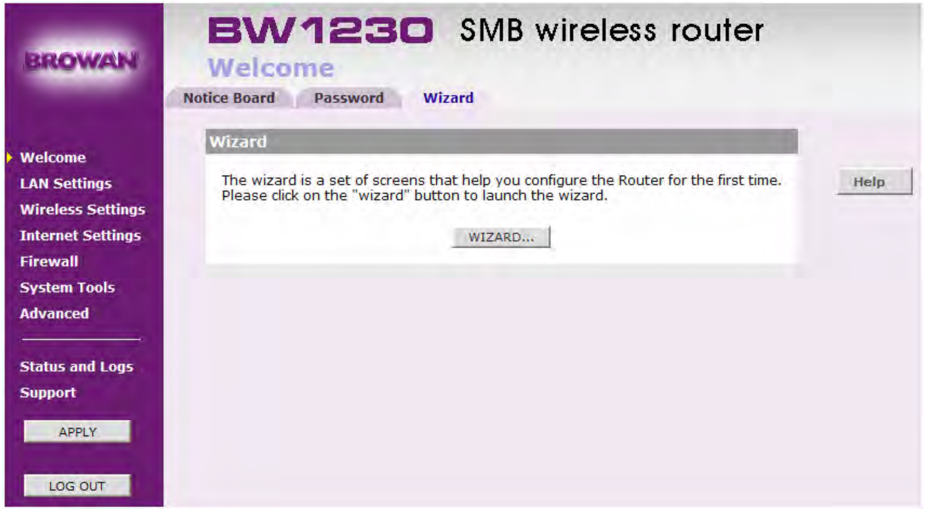
Note: Password is case sensitive

!	Browan recommand you to change a new password for your wireless network sercurity. And the **password is case sensitive.**

Welcome | Wizard

- This option allows you to run the Setup Wizard to change the configuration settings of the Router.

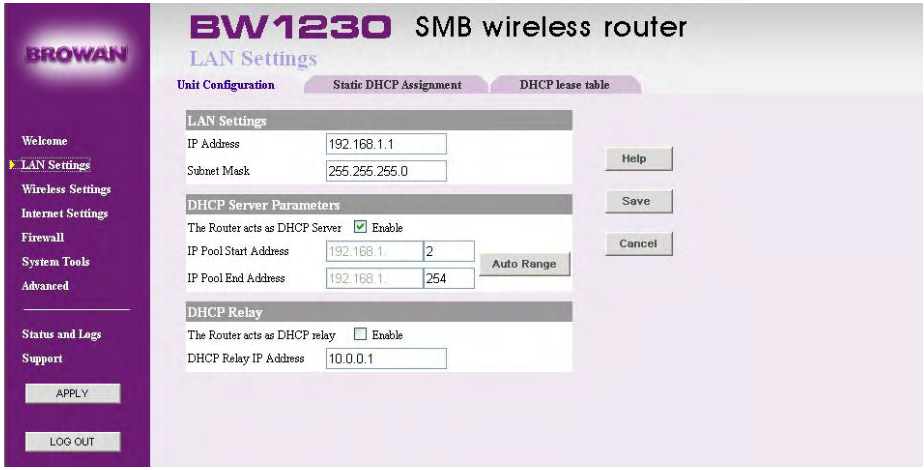
  - You could click WIZARD bottom to start the wizard setup.



Wizard

The wizard is a set of screens that help you configure the Router for the first time. Please click on the "wizard" button to launch the wizard.

LAN Settings | Unit Configuration



LAN Settings

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

DHCP Server Parameters

The Router acts as DHCP Server ☑ Enable

IP Pool Start Address 192.168.1. 2

IP Pool End Address 192.168.1. 254

DHCP Relay

The Router acts as DHCP relay □ Enable

DHCP Relay IP Address 10.0.0.1

- **LAN Settings:**

  The Router must be given a valid static IP address and subnet mask for the LAN interface.

  IP Address:

  This is the IP address for PC accessing the Router on the LAN. The default value is 192.168.1.1.

  Subnet Mask:

  This is the Subnet Mask for the Router. For devices to be on the same subnet, they must have the same subnet mask. The default value is 255.255.255.0.

- **DHCP Server Parameters:**

  The Router can act as a DHCP (Dynamic Host Control Protocol) Server for your LAN and can automatically allocate IP addresses to the other devices on the LAN. To use the Router as a DHCP Server, you must tick the **The Router acts as a DHCP Server**.

IP Pool Start Address

This defines the start address of the IP address range. When the Router is acting as a DHCP server, it will issue IP addresses to the devices on the LAN from within the IP address range. The default value is 192.168.1.2.

IP Pool End Address

This defines the end address of the IP address range. The default value is 192.168.1.254.

- **DHCP Relay:**

  The DHCP Relay Agent can deliver the IP address from the DHCP Server and allows you to place DHCP Clients and DHCP Servers on the same network. Deploying DHCP in a single segment network is easy.

  All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond through the DHCP relay to these broadcasts. A single scope on a solitary DHCP server is all that is required.

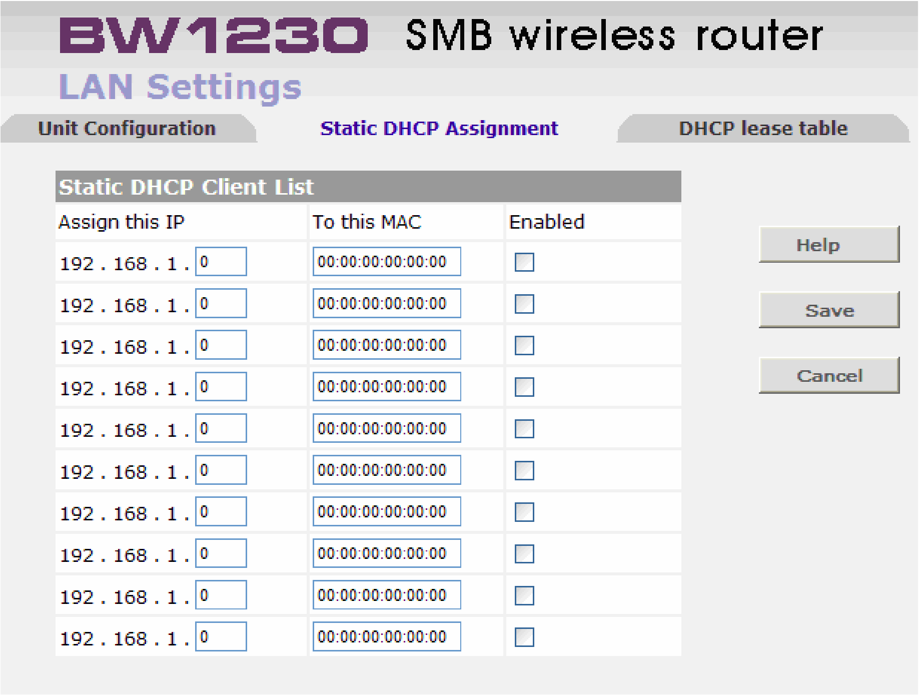
LAN Settings | Static DHCP Assignment

Static DHCP Client List

This feature is for users would like a PC to be assigned the same IP address when every time it reboots.

On the Static DHCP Client List , enter the static local IP address in the Assign this IP field, and enter the MAC address of the PC in the To this MAC field. Then click the **Enabled** checkbox.

When you have finished your entries, click the Save button to save your changes.



BW1230 SMB wireless router

LAN Settings

Static DHCP Client List

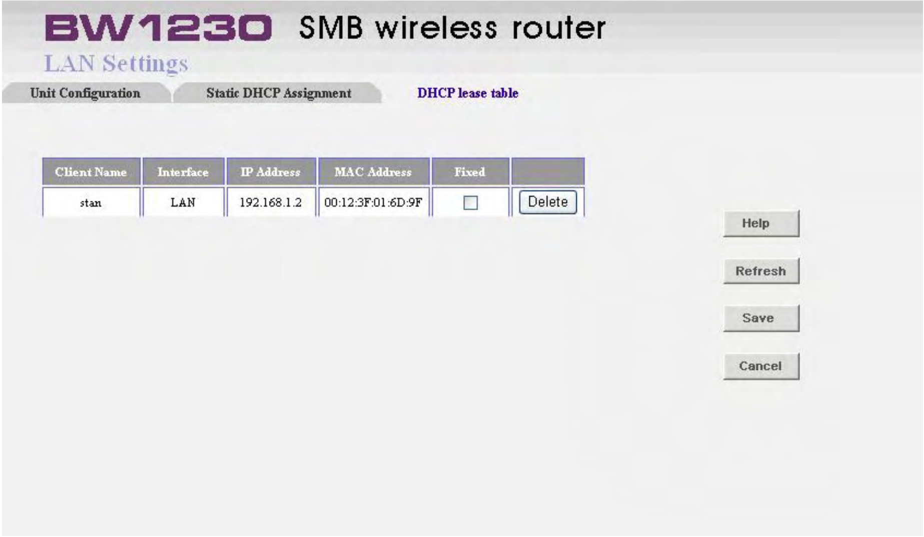
Assign this IP	To this MAC	Enabled
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□
192 . 168 . 1 . 0	00:00:00:00:00:00	□

LAN Settings | DHCP lease table

DHCP Lease Table

On the DHCP Lease Table, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, and MAC Addresses. If you want to add any of the DHCP clients to the Static DHCP Client List, just click the **Fixed** checkbox. Then click the Save button.

To view the most up-to-date information, click the Refresh button.



Client Name	Interface	IP Address	MAC Address	Fixed	
stan	LAN	192.168.1.2	00:12:3F:01:6D:9F	□	Delete

Wireless Settings | Configuration

- **Enable Wireless Networking**

  It allows you to enable/disable the wireless section of your LAN. When disabled, the router will close all the wireless connection and no wireless PCs can get the access to either the Internet in wired LAN of the router.

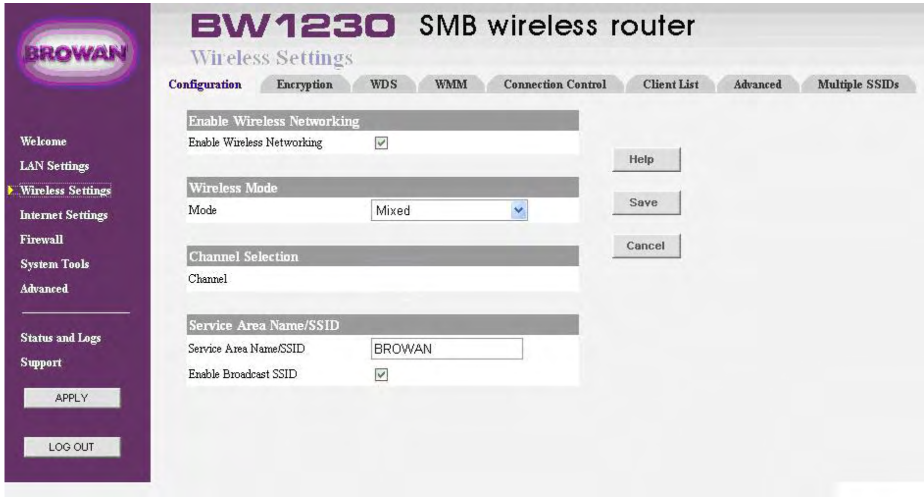
- **Wireless Mode**

  From this drop-down menu, you could see the selection which including mixed, wireless-B only, wireless-G only, Dynamic SuperG and SuperG without turbo. You could choose the proper wireless standards running on your network. The default setting is mixed mode.

- **Service Area Name/SSID**

  This allows you to name your Wireless network. The field will accept any alphanumeric string but not spaces and has a maximum length of 32 characters. Your Wireless PCs must be configured with exactly the same name or you will not establish a connection.

  The Service Area Name may also be referred to as **ESSID**



Enable Wireless Networking

Enable Wireless Networking ☑

Wireless Mode

Mode: Mixed

Channel Selection

Channel

Service Area Name/SSID

Service Area Name/SSID: BROWAN

Enable Broadcast SSID ☑

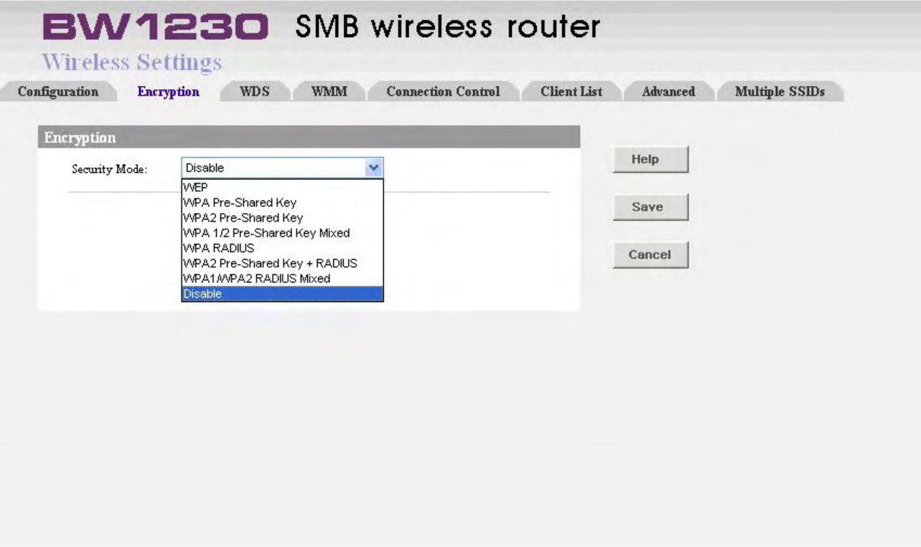
depending on your networking vendor. By default the Router uses the name **BROWAN**.

Wireless Settings | Encryption

- The Router offers two methods of encryption for greater wireless network security：

  - **WPA — Wi-Fi Protected Access.**
    WPA is an enhancement over WEP and will strongly increase the level of data protection and access control on your wireless network.
    WPA allows you to encrypt the switched packet in network between your Wireless PC and the Router.
    The default value of security mode is disable.
    WPA allows you to configure：

1. Type
There are three types of WPA methods available：
Manual Pre-Shared Key, Pre-Shared Passphrase and



Security Mode: Disable

Enterprise Mode. Use the **WPA Type** box to select the desired type.

2. Manual Pre-Shared Key

A Key is a hexadecimal (0-9, A-F) number used to encrypt and decrypt the data. There is only one key available, which are 63 digits long. Each wireless PC client using WPA must be configured to have the exact same Key; otherwise the client will be unable to connect. Manual Pre-Shared Keys provide the greatest combination of possible Keys, which provides greater security to the wireless network.

3. Pre-Shared Passphrase

The Router also offers a method for converting plain text into hex keys. The Passphrase is much easier to remember than the hex key but it relies on your wireless adapters also supporting this feature. The Passphrase limits the possible number of key combinations and it is recommended that users enter text containing 20 characters or more. The text entered must be greater than 8 characters and shorter than 64 characters.

4. Enterprise Mode

Allows Enterprise-level User Authentication via 802.1x and EAP (Extensible Authentication Protocol). This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it.

This option features a WPA used in coordination with a RADIUS server that uses either EAP-TLS or PEAP as its authentication method. (This should only be used when a RADIUS server is connected to the Router.)

First, select the type of encryption method you want to use, TKIP or AES. Enter the RADIUS servers IP address and port number, along with the authentication key shared by the Router and the server. Last, enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

- **WEP — Wired Equivalent Privacy.**

  Wired Equivalent Privacy or WEP allows you to encrypt the traffic between your Wireless PC and the Router.

WEP Encryption allows you to configure：

- **Wireless Encryption Type**
  There are two levels of encryption available, 64 bit (sometimes referred to as 40 bit) and 128 bit (sometimes referred to as 104 bit). 128 bit WEP is more secure than 64 bit. Use the **Wireless Encryption Type** box to select the desired level.

- **Key Generation Method**
  A Key is a hexadecimal (0-9, A-F) number used to encrypt and decrypt the data. There can be up to 4 keys and each key can be as long as 26 digits. The Router also offers a number of methods for converting plain text into hex keys. The text is much easier to remember than hex keys but it relies on your wireless adapters also supporting this feature. Different manufacturers have developed different ways of converting plain text and so interoperability is not guaranteed. If you are experiencing difficulty, the Manual Hex Key method is supported by most vendors.

The Router supports 4 methods to specify the WEP Keys：

① Manual Hex Key — This method allows you to manually enter hex keys. Virtually all manufacturers support this scheme.

② BROWAN Encryption String — This method is only supported by BROWAN Wireless products. The string can contain any alpha numeric characters and must be between 6 and 30 characters long. A single string will automatically generate 4 unique keys for 64 or 128 bit WEP.

③ ASCII — This method is supported by some adapter cards running under Windows XP. The string must be exactly 5 characters for 64 bit WEP and 13 characters for 128 bit WEP. You must enter a separate string for each of the 4 Keys. You can leave a string blank so long as this Key is not selected as the Active Transmit Key.

④ Passphrase — This is another common method and similar to the BROWAN Encryption string. In 64 bit WEP, the Passphrase will generate 4 different keys. However, in 128 bit WEP, this method only generates 1 key which is replicated for all 4 keys.

- **Active Transmit Key**

  The **Active Transmit Key** selects which of the 4 Keys the Router uses when it transmits. You can change the selected key every now and then to increase the security of your network.

When you apply the Mutiple SSIDs in Wireless Settings, you can operate different SSID in different security mode. And you must enter the correct key forward intto the SSID that you connect. It means that WPA and WEP encryption modes are enabled allowing wireless client PCs to be configured to run with either WPA or the original WEP encryption.

Maximum security can be obtained by configuring your wireless network to WPA encryption only. It is important to remember that with encryption disabled anyone with a

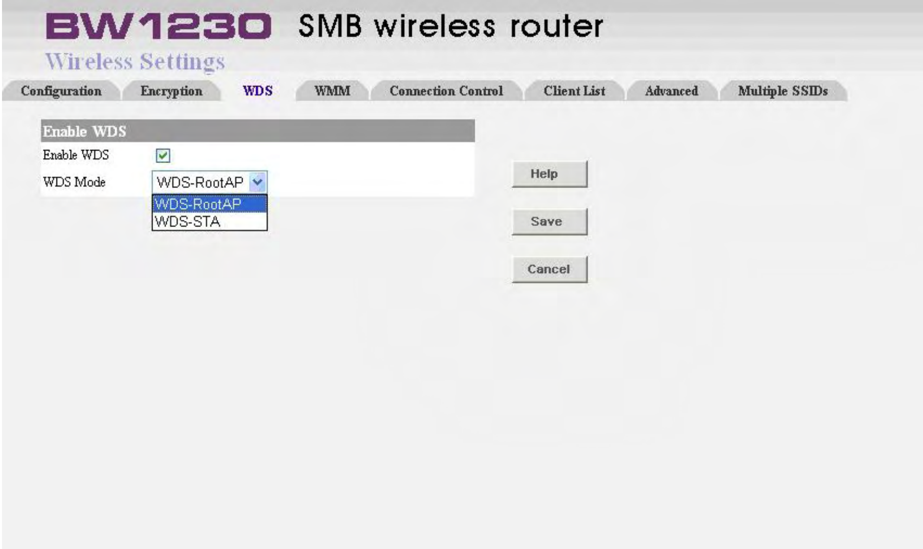
Wireless PC can eavesdrop on your network.

!	If you enable WPA or WEP on the Router, you must reconfigure your wireless PCs to use exactly the same Encryption Type and Keys otherwise the devices will not understand each other.

Wireless Settings | WDS

- WDS (Wireless Distribution System) is comprised of a bridging and/or a repeater mode. Wireless bridging is where the WDS APs communicate only with each other to bridge together 2 separate networks (without allowing for wireless clients or stations to access them). Wireless repeating is where the WDS APs rebroadcasts the received signals to extend reach and range (at the expense of half or more of the throughput).

- Enabling the WDS will enable wireless repeating.



Enable WDS

Enable WDS ☑

WDS Mode WDS-RootAP

WDS-RootAP
WDS-STA

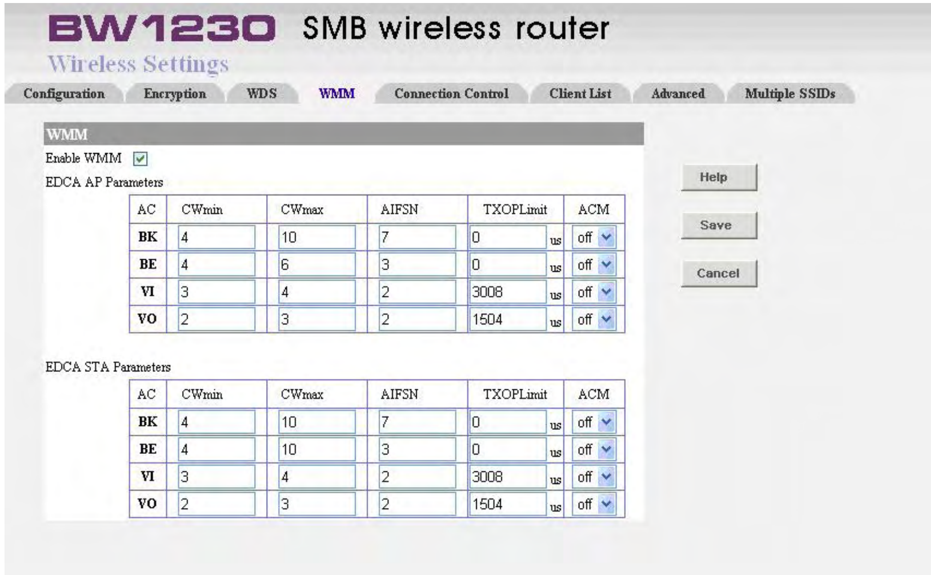
If you choose WDS-STA for the router, you have specified the router to act as a **Repeater** of your wireless distributed system (WDS); whereas if you choose WDA-ROOTA for your router, you have specified this router to act as a **Base** of your wireless distributed system.

Wireless Settings | WMM

- You can enable Wi-Fi Multimedia (WMM) support to help improve the Quality of Service (QoS) for audio, video, and voice applications over the wireless network. When WMM support is enabled, multimedia traffic is given higher priority over other types of traffic.

  - **EDCA Parameter**

    The IEEE 802.11e standard improves the Medium Access Control (MAC) of the legacy 802.11 with regard to Quality of Service (QoS) by introducing the Enhanced Distributed Channel Access (EDCA).The 802.11e MAC is based on both centrally-controlled and contention-based channel accesses. The EDCA



WMM

Enable WMM ☑

EDCA AP Parameters

AC	CWmin	CWmax	AIFSN	TXOPLimit	ACM
BK	4	10	7	0 us	off
BE	4	6	3	0 us	off
VI	3	4	2	3008 us	off
VO	2	3	2	1504 us	off

EDCA STA Parameters

AC	CWmin	CWmax	AIFSN	TXOPLimit	ACM
BK	4	10	7	0 us	off
BE	4	10	3	0 us	off
VI	3	4	2	3008 us	off
VO	2	3	2	1504 us	off

provides differentiated channel access to frames with different priorities. Typically, voice and video traffic types are delay-sensitive, but are tolerant of some frame losses. On the other hand, data traffic type is delay-tolerable, but requires loss-free transmission. So you may adjust theses parameters with regard to the characteristics of these types of data to better manage your network flow.

- **AC (Access Category):**
  Using 4 different ACs: From high to low: VO: Voice, VI: Video, BE: Best Effort, BK: Background.
- **AIFS (Arbitrary Inter-frame Space):**
  An Inter-frame Space for different Access Category

- **TXOP (Transmission Opportunity):**
  WMM (Wireless Multimedia) Transmission Opportunity: defined by IEEE 802.11e, the TXOP is the interval of time when a particular STA (station) has the right to initiate transmissions.

- **ACM (Admission Mandatory):**
  Advertised in the EDCA parameter set element to

indicate the admission control is required for each of the ACs.

- **Access Point**
  Theses values of AIFS, CWmin, and CWmax are announced by the AP via beacon frames. The AP can adapt these parameters dynamically depending on the network conditions. Basically, the smaller AIFS and CWmin, the shorter the channel access delay for the corresponding priority, and hence the more capacity share for a given traffic condition. However, the probability of collisions increases when operating with smaller CWmin. Theses parameters can be used in order to differentiate the channel access among different priority traffic.

- **STA**
  Each station maintains a Contention Window (CW), which is used to select the random back off counter. The BC is determined as a random integer drawn from a uniform distribution over the interval (0, CW).The CW size is initially assigned CWmin, and increases when a transmission fails, i.e., the transmitted data frame has

not been acknowledged. After any unsuccessful transmission attempt, another back off timer is performed, with an upper bound of CWmax. This reduces the collision probability in case there are multiple stations attempting to access the channel.

- **CW min:**
  should be smaller for delay-sensitive data

- **CW max:**
  should be smaller for delay-sensitive data

- **AIFSN:**
  should be smaller for delay-sensitive data

- **TXOPLimit:**
  These will allow multiple MAC frames consecutively as long as the whole transmission time does not exceed the TXOP limit. So keep it larger for delay-sensitive data.

- **ACM:**

Admission Mandatory; could be turned on to mandatory execution of the contention control.

Wireless Settings | Connection Control

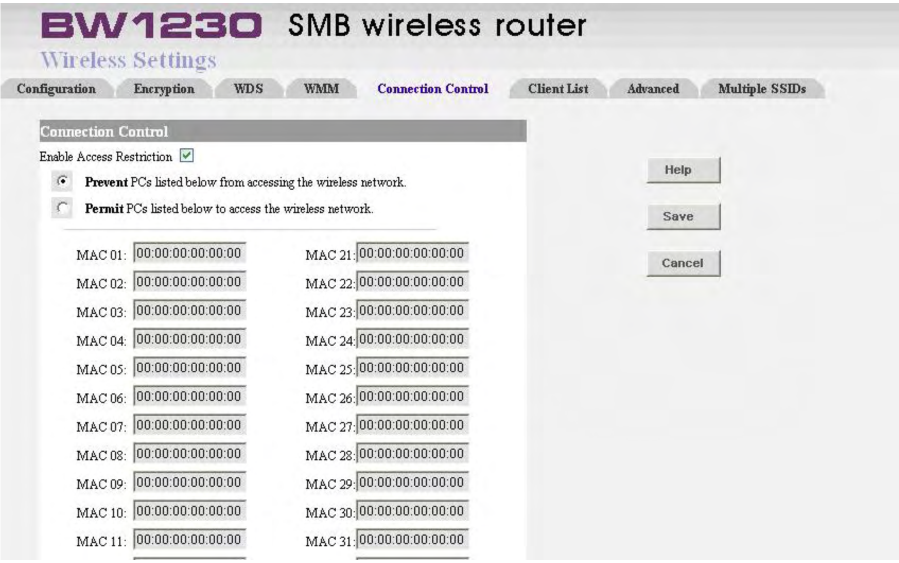
- Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your networks radius.

  - **Access Restrictions**

    - **Prevent** PC listed below from accessing the wireless network. Clicking this radio button will block wireless access by MAC Address.

    - **Permit** PC listed below to access the wireless network. Clicking this radio button will allow wireless access by MAC Address.

  - **Wireless MAC Filter List**
    Click the Enable Access Restriction checkbox to display a list of network users by MAC Address. If you want to add any of the wireless clients to the Wireless MAC Filter List, just fill in wireless clients' Mac to to the Wireless MAC Filter List.



Connection Control

Enable Access Restriction ☑

● **Prevent** PCs listed below from accessing the wireless network.

○ **Permit** PCs listed below to access the wireless network.

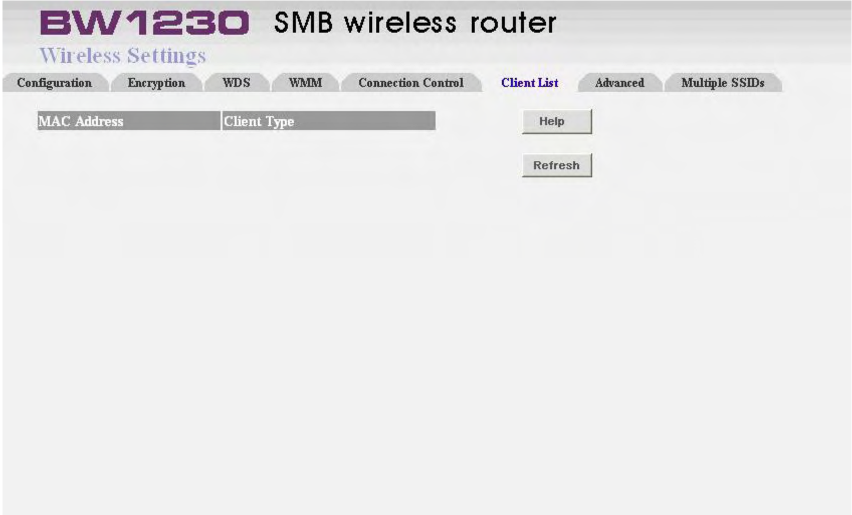
MAC 01:	00:00:00:00:00:00	MAC 21:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 23:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 25:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00

Wireless Settings | Client List

- The Wireless Clients List provides details on the devices that are connected to the Wireless LAN. The list is only created when Wireless Networking is enabled.

- For each device that is connected to the Wireless LAN: the MAC address, Connection Speed and Client Type of that device is displayed.

- As you connect more devices to the Wireless LAN, the client list will grow to a maximum of 32 (the maximum number of wireless devices that the Router can support).



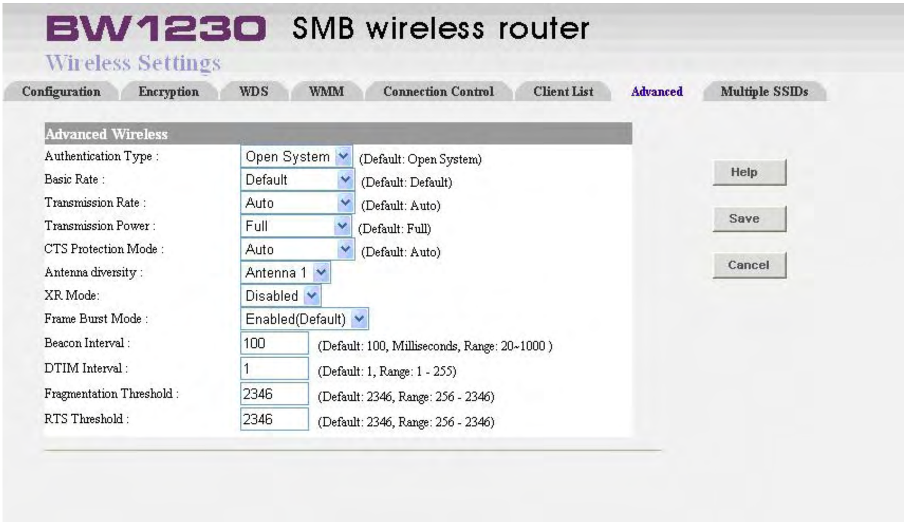
Wireless Settings | Advanced

- **Authentication Type**

  The default is set to open system (Default), allows choosing Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication.

- **Basic Rate**

  The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are 1-2Mbps, for use with older wireless technology, and All, when the Router can transmit at all wireless rates. The Basic Rate is not the



Advanced Wireless

Authentication Type :	Open System	(Default: Open System)
Basic Rate :	Default	(Default: Default)
Transmission Rate :	Auto	(Default: Auto)
Transmission Power :	Full	(Default: Full)
CTS Protection Mode :	Auto	(Default: Auto)
Antenna diversity :	Antenna 1	
XR Mode:	Disabled	
Frame Burst Mode :	Enabled(Default)	
Beacon Interval :	100	(Default: 100, Milliseconds, Range: 20~1000)
DTIM Interval :	1	(Default: 1, Range: 1 - 255)
Fragmentation Threshold :	2346	(Default: 2346, Range: 256 - 2346)
RTS Threshold :	2346	(Default: 2346, Range: 256 - 2346)

actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

- **Transmission Rate**
  The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto (Default) to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto (Default).

- **CTS Protection Mode**

  CTS (Clear-To-Send) Protection Mode should be set to Auto (Default). The Router will automatically use CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance. If you do not want to use CTS Protection Mode at all, select Disabled.

- **Frame Burst Mode**

  Frame burst is a term in wireless technology supported by the 802.11e QoS specification. Suggesting to enable this option on point to point should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, Enabled.

- **Beacon Interval**

  A beacon is a packet broadcast by the wireless router to make the client scan the wireless signal. The Beacon Interval value indicates the time interval of the beacon. The default value is 100.

- **DTIM Interval**

  This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has stored in buffer with broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.

- **Fragmentation Threshold**

  This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation

Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.

RTS Threshold
Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.

Wireless Settings | Multiple SSIDs

- **Enable Multiple SSID**

  Allows you to enable/disable the Multiple SSID. When disabled, only one SSID on your Wireless LAN.

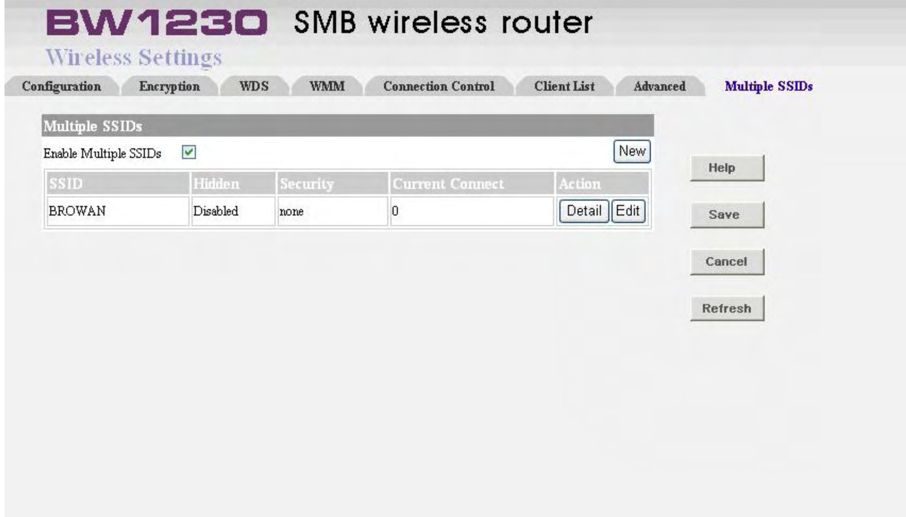
  The default setting is BROWAN.

- **Service Area Name/SSID**

  This allows you to name your Wireless network. The field will accept any alphanumeric string but not spaces and has a maximum length of 32 characters. Your Wireless PCs must be configured with exactly the same name or you will not establish a connection.

  The Service Area Name may also be referred to as **ESSID** depending on your networking vendor. By default the Router uses the name **BROWAN**.

  You may specify up to 3 SSIDs. (1 Main SSID , 2 Multiple SSIDs)



Multiple SSIDs

Enable Multiple SSIDs ☑

SSID	Hidden	Security	Current Connect	Action
BROWAN	Disabled	none	0	Detail Edit

- **Enable Broadcast SSID**
  This feature can be used to improve the security of your wireless network. When the checkbox is unchecked, the Router will not broadcast the Service Area Name / SSID of your wireless network. It will prevent unauthorized clients from detecting your SSID and attempting to connect to your network.

  If you have a wireless client that can detect all the available SSIDs in your area, your client will not list the Router SSID when this feature is enabled.

  We recommend that you install your wireless network with this feature unchecked and then enable it once your have set up the Router and wireless clients.

Internet Settings | Connection to ISP

Connection Parameters

IP Allocation Mode: To establish a connection with your ISP's network, select the IP Allocation Mode that they use.

There are four different options available：

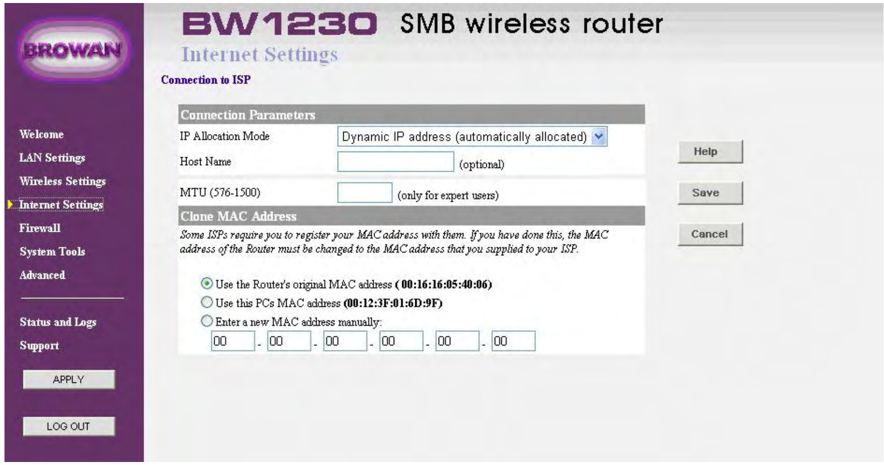
- **Dynamic IP address (automatically allocated):**

  This allocation mode may be used by either Cable or DSL ISP's. It is popular with Cable providers, and may also be required if your modem has a built in DHCP server.

  If this mode is selected, your IP Address, Subnet Mask, and ISP Address will be obtained automatically from your ISP. They are not displayed on this screen, but may be viewed on the Status screen (click on **Status and Logs** on the left hand menu bar).

  Host Name:

  Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is



Connection Parameters

IP Allocation Mode: Dynamic IP address (automatically allocated)

Host Name: (optional)

MTU (576-1500): (only for expert users)

Clone MAC Address

Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Router must be changed to the MAC address that you supplied to your ISP.

● Use the Router's original MAC address **(00:16:16:05:40:06)**

○ Use this PCs MAC address **(00:12:3F:01:6D:9F)**

○ Enter a new MAC address manually:

00 - 00 - 00 - 00 - 00 - 00

optional, and so if you have not been provided a host name, you may leave it blank.

- **Clone MAC address:**
  Some ISP's use the hardware (MAC) address of the device you connect to the Internet with to identify you. If you have previously used a different device with your current ISP, and they use your MAC address to identify you, then you can change the MAC address on the WAN side of your Router to be that of your old device. There are three options available for cloning the Router WAN port MAC address:

  Use the Router's original MAC address:
  This option is selected by default. When selected, the Router uses the WAN port MAC address that it was assigned at the factory.

  Use this PCs MAC address:
  This option will assign the MAC address of the PC you are using to manage the Router to the WAN port. If this is the PC that you used previously to connect to your ISP, then you should select this option.

Enter a new MAC address manually

If the MAC addresses given by the previous two options are not correct, then you will need to find the MAC address of the previous device used with your ISP.

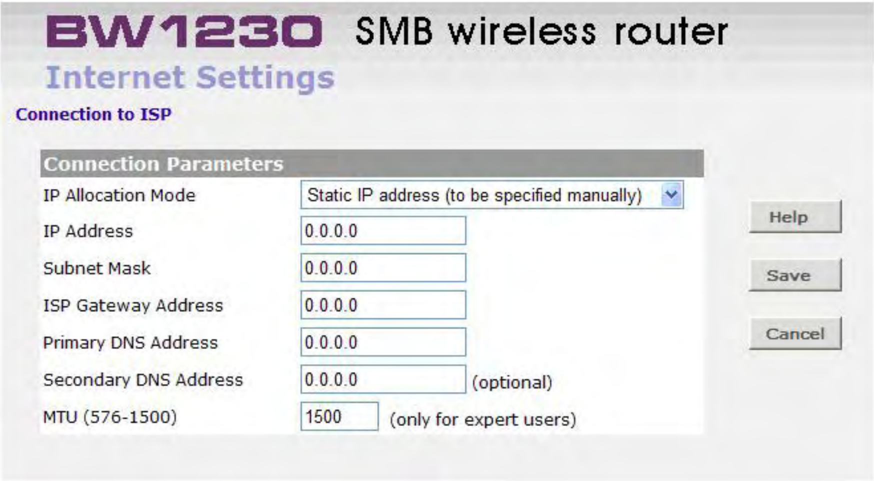
- **Static IP address (to be specified manually):**
  This allocation mode may be used by either Cable or DSL ISP's.

IP address:
This is the IP address of your Router that will be seen from the WAN, or Internet. This setting is required, and will be provided to you by your ISP.

Subnet mask:
This is the Subnet Mask of your Router's WAN port. This setting is required, and will be provided to you by your ISP.

ISP Gateway Address:
This is sometimes referred to as **Default Gateway**. This setting is required, and will be provided to you by your ISP.

Primary DNS Address:
Your ISP will normally provide you with at least one DNS (Domain Name Server) address, and you should enter the first here. A Domain Name Server performs



BW1230 SMB wireless router

Internet Settings

Connection to ISP

Connection Parameters	
IP Allocation Mode	Static IP address (to be specified manually)
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
ISP Gateway Address	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0 (optional)
MTU (576-1500)	1500 (only for expert users)

the translation between domain name (such as www.browan.com) and IP addresses. Note that this setting is optional, and can be left at 0.0.0.0 if it is not required.

Secondary DNS Address:
If your ISP has provided a second DNS address, you should enter it here. Otherwise, leave this setting at its default of 0.0.0.0. This setting is optional.

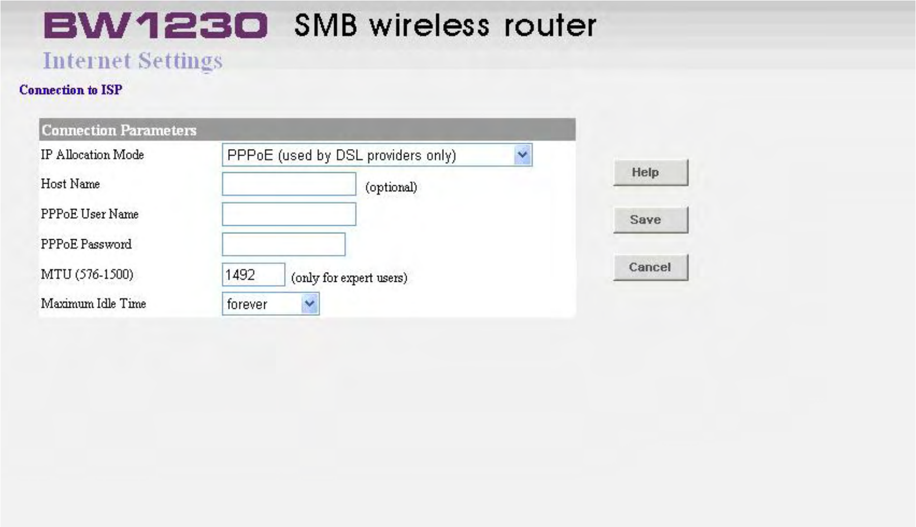
MTU:
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

- **PPPoE (Point-to-Point Protocol over Ethernet):** Only ISP's providing DSL use PPPoE. If the installation instructions that accompany your modem ask you to install a PPPoE client on your PC then select this option. Note that you will not need to use PPPoE software on your PC once the Router is installed. If you are unsure, you should ask your ISP whether you need to use PPPoE.

  PPPoE User Name:
  Enter your User Name in this box. This field is required, and will be provided to you by your ISP.

  PPPoE Password:
  Enter your password in this box. This field is required, and will be provided to you by your ISP.

  PPPoE Service Name:
  If your ISP provided you with a Service Name, you should enter this here. If not, you should leave this blank.



BW1230 SMB wireless router

Internet Settings

Connection to ISP

Connection Parameters

IP Allocation Mode	PPPoE (used by DSL providers only)
Host Name	(optional)
PPPoE User Name	
PPPoE Password	
MTU (576-1500)	1492 (only for expert users)
Maximum Idle Time	forever

Host Name:
Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is optional, and so if you have not been provided a host name, you may leave it blank.

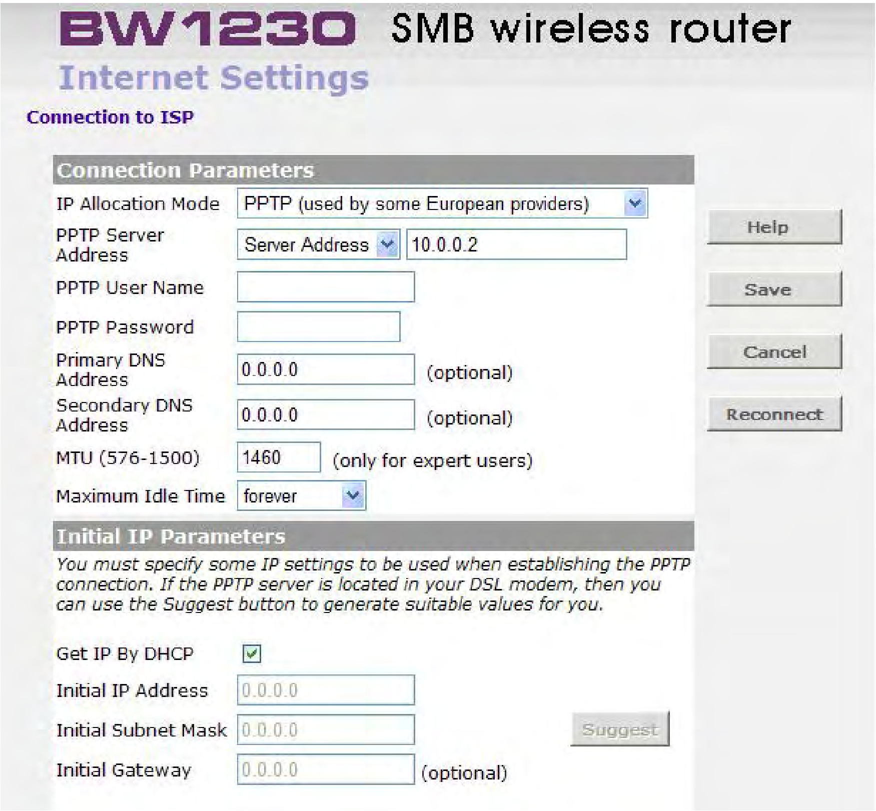
MTU:
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

Maximum Idle Time:
This is the amount of time that passes before your Internet Connection is dropped due to inactivity. If you want to keep your Internet Connection established at all times, you should select **Forever**; Otherwise, select the amount of time that you want to pass before your Router disconnects from your ISP.

- **PPTP (Point to Point Tunneling Protocol):** Some ISP's require the use of PPTP to establish connections to their networks. At present PPTP is only used by some European ISP's. If the installation instructions that accompany your modem ask you to set up a dialup connection using a PPTP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more.

  PPTP Server address:
  This is the IP address of the PPTP server you are connecting to. This setting is required, and will be provided to you by your ISP. The PPTP Server is typically located in your DSL modem. In the case of an Alcatel Speed Touch modem, its default address is 10.0.0.2

  PPTP User Name:
  Enter your User Name in this box. This field is required, and will be provided to you by your ISP.



BW1230 SMB wireless router

Internet Settings

Connection to ISP

Connection Parameters

IP Allocation Mode	PPTP (used by some European providers)	
PPTP Server Address	Server Address	10.0.0.2
PPTP User Name		
PPTP Password		
Primary DNS Address	0.0.0.0	(optional)
Secondary DNS Address	0.0.0.0	(optional)
MTU (576-1500)	1460	(only for expert users)
Maximum Idle Time	forever	

Initial IP Parameters

You must specify some IP settings to be used when establishing the PPTP connection. If the PPTP server is located in your DSL modem, then you can use the Suggest button to generate suitable values for you.

Get IP By DHCP	☑	
Initial IP Address	0.0.0.0	
Initial Subnet Mask	0.0.0.0	
Initial Gateway	0.0.0.0	(optional)

PPTP Password:
Enter your password in this box. This field is required, and will be provided to you by your ISP.

DNS Addresses:
If your ISP has provided you with DNS addresses, you should enter them here. Otherwise, leave these setting at its default of 0.0.0.0. These settings are optional, and most ISP's will also provide you with DNS addresses automatically. When the addresses are obtained from your ISP, they will be displayed on the Status screen.

MTU:
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

Maximum Idle Time:
This is the amount of time that passes before your Internet Connection is dropped due to inactivity. If you want to keep your Internet Connection established at all times, you should select **Forever**; Otherwise, select

the amount of time that you want to pass before your Router disconnects from your ISP.

Get IP By DHCP:

Some ISP may have the mechanism that automatically provides Initial IP Address, Subnet Mask and Default Gateway. If your ISP provides such mechanism, you should check this option. Otherwise, you should manually enter your initial IP Address, Subnet Mask and Default Gateway.

Initial IP address and Subnet Mask:

You must specify some IP settings to be used when establishing the PPTP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the PPTP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you. The **Suggest** button will select an IP address on the same subnet as the PPTP server.

Initial Default Gateway:

The PPTP Server address and the Initial IP Address that ISP provides sometimes may not be in the same Subnet. In this case, the Initial Default Gateway is necessarily to be provided to establish the PPTP connection. If the PPTP Server and Initial IP Address are in the same subnet, then you can set the Initial Default Gateway to 0.0.0.0 or 0.

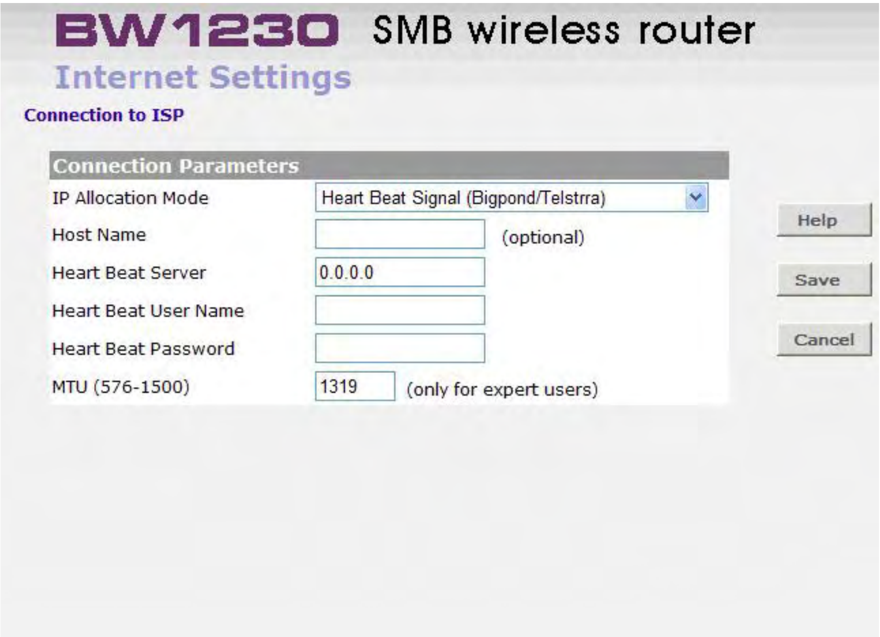
- **Heart Beat Signal (For Australia only):**
  It is a service used in Australia only. If you are using Heart Beat Signal connection, check with your ISP for the necessary setup information.

  Host Name:
  Some ISP's require a host name to identify you when you connect. If you have been provided a Host Name by your ISP, you should enter it here. This field is optional, and so if you have not been provided a host name, you may leave it blank.

  Heart Beat Server:
  Your ISP will provide you with the Heart Beat Server's IP Address.

  Heart Beat User Name:
  Enter the **User Name** you use when logging onto your ISP through a Heart Beat Signal connection

  Heart Beat Password:
  Enter the **Password** you use when logging onto your ISP through a Heart Beat Signal connection



Connection Parameters

IP Allocation Mode	Heart Beat Signal (Bigpond/Telstrra)	
Host Name		(optional)
Heart Beat Server	0.0.0.0	
Heart Beat User Name		
Heart Beat Password		
MTU (576-1500)	1319	(only for expert users)

MTU:

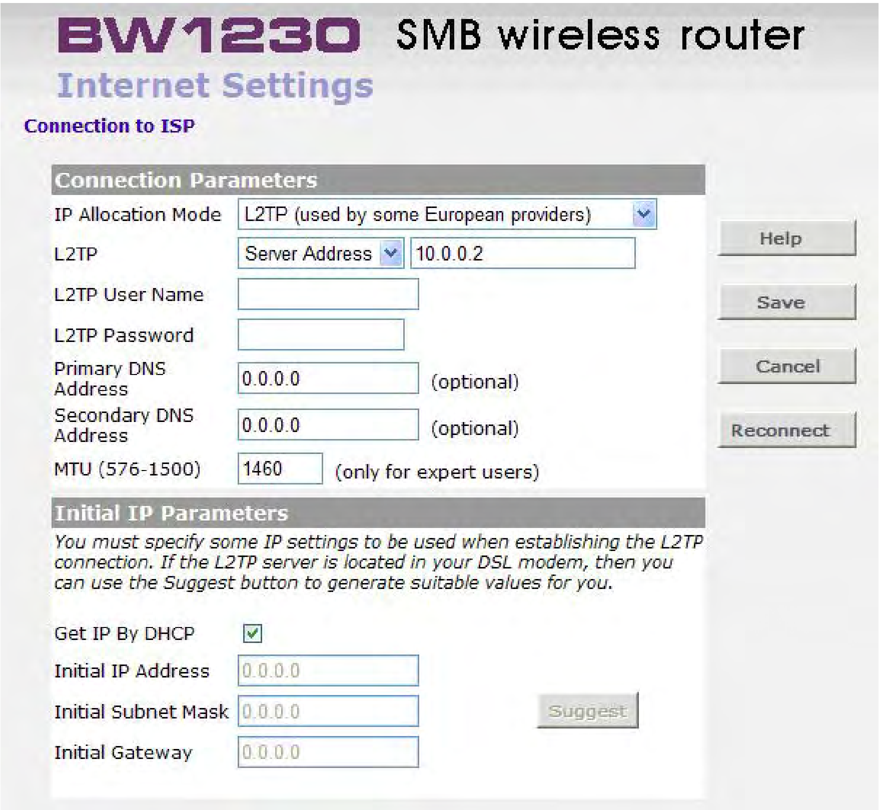
The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

- **L2TP (Layer Two Tunneling Protocol):**
  Some ISP's require the use of L2TP to establish connections to their networks. If the installation instructions that accompany your modem ask you to set up a dialup connection using a L2TP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more.

  L2TP Server address:
  This is the IP address of the L2TP server you are connecting to. This setting is required, and will be provided to you by your ISP. The L2TP Server is typically located in your DSL modem.

  L2TP User Name:
  Enter your User Name in this box. This field is required, and will be provided to you by your ISP.

  L2TP Password:
  Enter your password in this box. This field is required, and will be provided to you by your ISP.



BW1230 SMB wireless router

Internet Settings

Connection to ISP

Connection Parameters

IP Allocation Mode	L2TP (used by some European providers)	
L2TP	Server Address 10.0.0.2	
L2TP User Name		
L2TP Password		
Primary DNS Address	0.0.0.0	(optional)
Secondary DNS Address	0.0.0.0	(optional)
MTU (576-1500)	1460	(only for expert users)

Initial IP Parameters

You must specify some IP settings to be used when establishing the L2TP connection. If the L2TP server is located in your DSL modem, then you can use the Suggest button to generate suitable values for you.

Get IP By DHCP	☑
Initial IP Address	0.0.0.0
Initial Subnet Mask	0.0.0.0
Initial Gateway	0.0.0.0

DNS Addresses:

If your ISP has provided you with DNS addresses, you should enter them here. Otherwise, leave these setting at its default of 0.0.0.0. These settings are optional, and most ISP's will also provide you with DNS addresses automatically. When the addresses are obtained from your ISP, they will be displayed on the Status screen.

MTU:

The MTU settings should be obtained from your Internet Service Provider. If you do not know this value, just leave it at the default value.

Get IP By DHCP:

Some ISP may have the mechanism that automatically provides Initial IP Address, Subnet Mask and Default Gateway. If your ISP provides such mechanism, you should check this option. Otherwise, you should manually enter your initial IP Address, Subnet Mask and Default Gateway.

Initial IP address and Subnet Mask:

You must specify some IP settings to be used when establishing the L2TP connection. If your ISP has provided you with these settings, then you should use them. Otherwise, if the L2TP server is located in your DSL modem, you can use the Suggest button to generate suitable values for you. The Suggest button will select an IP address on the same subnet as the L2TP server.

Initial Default Gateway:

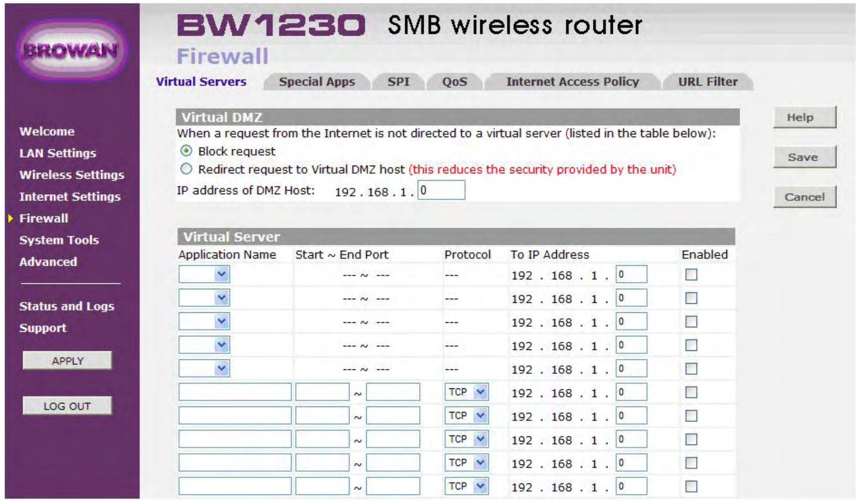
The L2TP Server address and the Initial IP Address that ISP provides sometimes may not be in the same Subnet. In this case, the Initial Default Gateway is necessarily to be provided to establish the L2TP connection.

Firewall | Virtual Servers

Virtual DMZ

The default operation of the Router is to block any requests from the Internet. This maximizes the security of your network. However, if you want to host a server on your LAN and make it accessible from the internet, you will need to configure a Virtual Server.

A Virtual DMZ is a special case of a Virtual Server which can intercept all unsolicited incoming traffic not already assigned to a Virtual Server, and redirects it to a specified PC on the LAN.



Virtual DMZ

When a request from the Internet is not directed to a virtual server (listed in the table below):

● Block request

○ Redirect request to Virtual DMZ host (this reduces the security provided by the unit)

IP address of DMZ Host: 192 . 168 . 1 . 0

Virtual Server

Application Name	Start ~ End Port	Protocol	To IP Address	Enabled
	--- ~ ---	---	192 . 168 . 1 . 0	□
	--- ~ ---	---	192 . 168 . 1 . 0	□
	--- ~ ---	---	192 . 168 . 1 . 0	□
	--- ~ ---	---	192 . 168 . 1 . 0	□
	--- ~ ---	---	192 . 168 . 1 . 0	□
	~	TCP	192 . 168 . 1 . 0	□
	~	TCP	192 . 168 . 1 . 0	□
	~	TCP	192 . 168 . 1 . 0	□
	~	TCP	192 . 168 . 1 . 0	□
	~	TCP	192 . 168 . 1 . 0	□

Blocking Service Requests

Select the Block Request radio button, in the Virtual DMZ box.

Redirecting to a Virtual DMZ Host

1. Select the Redirect Request radio button, in the Virtual DMZ box.
2. Enter the IP address of the Host.
3. Press the Apply button.

Virtual Servers

A Virtual Server is used to enable hosting of Internet Services, for example a web site or email server, by opening one or more incoming ports in the Router and redirecting the unsolicited requests from the Internet to a specified PC on the LAN.

- **Application Name**

  Each drop-down menu offers a choice of ten preset applications (select None if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields. The preset applications are among the most widely used Internet applications. They include the following：

  1. **FTP (File Transfer Protocol)**

     A protocol used to transfer files from PC to another across the network.(Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

2. **Telnet**
   A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or host computer to log on to a remote device and run a program.

3. **SMTP (Simple Mail Transfer Protocol)**
   The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

4. **DNS (Domain Name System)**
   The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember handle for an Internet address.

5. **TFTP (Trivial File Transfer Protocol)**
   A version of the TCP/IP FTP protocol that has no directory or password capability.

6. **Finger**
   A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being fingered must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

7. **HTTP (HyperText Transport Protocol)**
   The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

8. **POP3 (Post Office Protocol 3)**
   A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are

downloaded at the same time. POP3 uses the SMTP messaging protocol.

9. **NNTP (Network News Transfer Protocol)**
   The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

10. **SNMP (Simple Network Management Protocol)**
    A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

- **Start/End**
  This is the port range. Enter the port number or range of external ports used by the server or Internet

application. Check with the software documentation of the Internet application for more information.

- **Protocol**
  Select the protocol(s) used for this application, TCP and/or UDP.

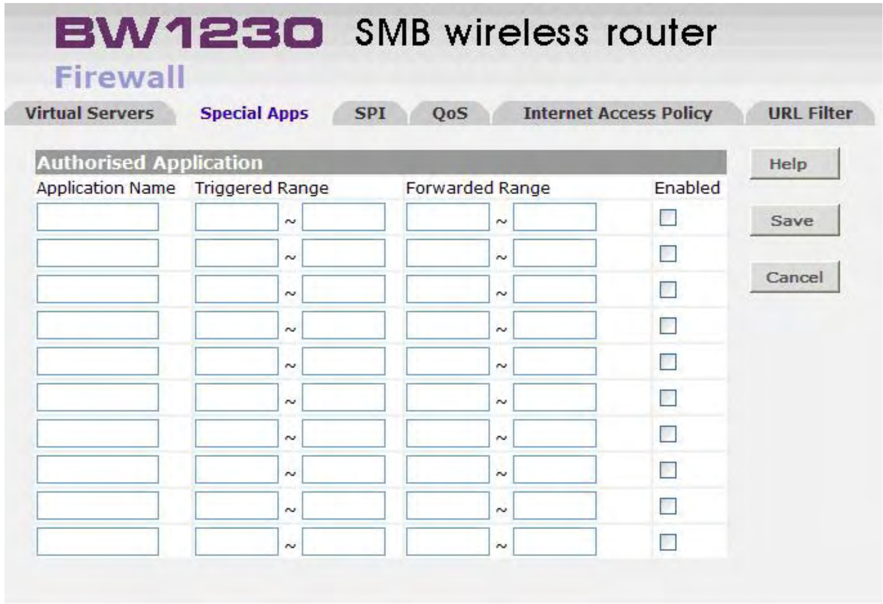
- **To IP Address**
  For each application, enter the IP address of the PC running the specific application.

- **Enabled**
  Click the **Enabled** checkbox to enable port forwarding for the relevant application.

Firewall | Special Apps

Some software applications require special or multiple connections to the Internet and these would normally be blocked by the Firewall. For example Internet Telephony or Video conferencing require multiple connections.

So that these special applications can work properly and are not blocked, the firewall needs to be told about them. In each instance there will be a trigger port and incoming port(s), where traffic on the trigger port tells the Firewall to open the incoming ports.



Authorised Application

Application Name	Triggered Range	Forwarded Range	Enabled
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐
	~	~	☐

- **Authorized Application**
  - **Application Name**

    Enter the application name of the trigger.

  - **Triggered Range**

    For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the

Triggered Range. In the second field, enter the ending port number of the Triggered Range.

- **Forwarded Range**
  For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

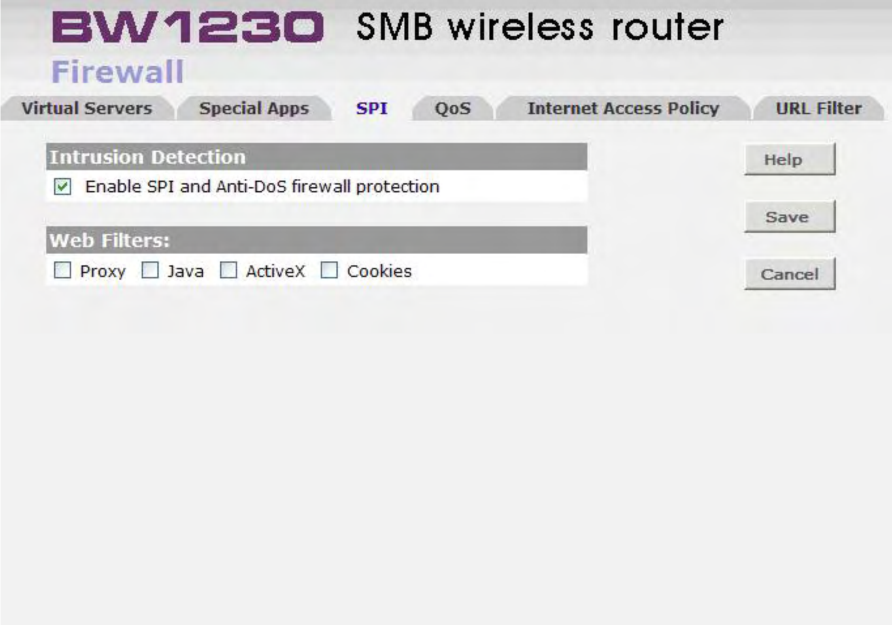
- **Enabled**
  Click the Enabled checkbox to enable port range triggering for the relevant application.

!	Each defined Special Application only supports a single PC user and up to 10 Special Applications can be defined.

Firewall | SPI

- The Router inspects packets at the application layer, and maintains TCP and UDP session information, including timeouts and the number of active sessions. The Router also provides the ability to detect and prevent certain types of network attacks such as DOS attacks. Network attacks that deny access to a network device are called denial-of-service (DOS) attacks. Denials of Service (DOS) attacks are aimed at devices and networks with a connection to the Internet. The goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

- By using above inspected information and timeout/threshold criteria, the Router provide following DOS attacks prevention: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attach), UDP port loopback, Stork Attack etc.



Intrusion Detection

☑ Enable SPI and Anti-DoS firewall protection

Web Filters:

□ Proxy □ Java □ ActiveX □ Cookies

- **Intrusion Detection**
  Enable this feature to employ Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment
- **Web Filters**
  Using the Web Filters feature, you may enable up to four specific filtering methods.

1. **Proxy**
   Use of WAN proxy servers may compromise the Router's security. Denying Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the Proxy box.

2. **Java**
   Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the Java box.

3. **ActiveX**
   ActiveX is a programming language for websites. If

you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the ActiveX box.

4. **Cookies**

   A cookie is the data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click the Cookies box.

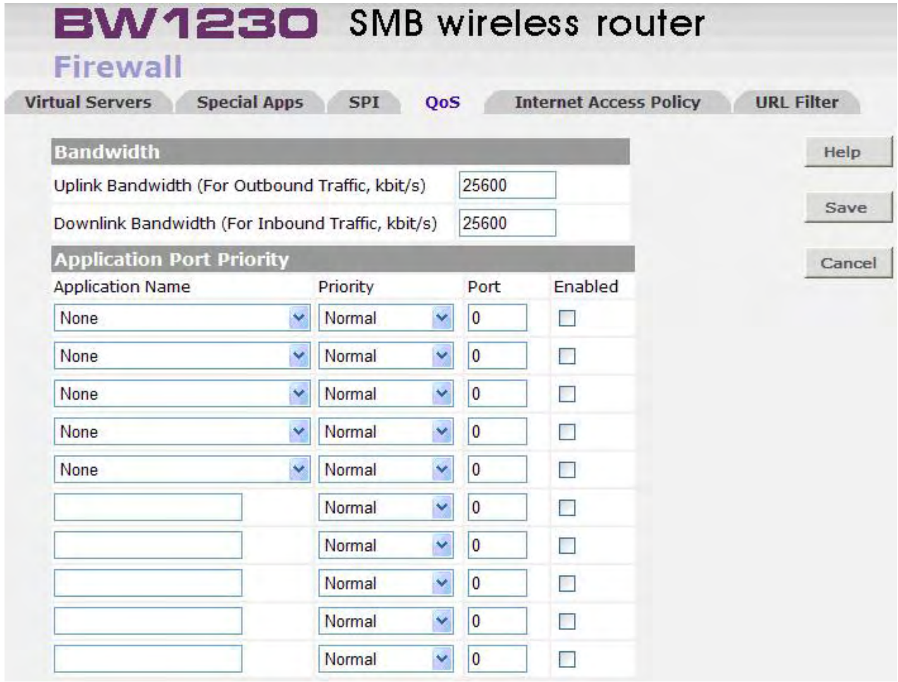
Firewall | QoS

- **QoS (Quality of Service)** manages information as it is transmitted and received. It ensures better service to high priority types of Internet traffic, which may involve demanding, real-time applications, such as videoconferencing. QoS can also prioritize traffic for a specific device or the Routers LAN ports.

  You may give a comparative metric for your selected application with High, Low, or Normal to prioritize bandwidth of your services.

- **Bandwidth**
  Specify the limit for your uplink and downlink connection bandwidth in kilobit per second. Remember that if you specify a speed exceeding your current broadband service capabilities, you will still only be able to achieve the maximum speed provided by your broadband service.

  - **If NAT is enabled:**
    Maximum Uplink/Downlink Bandwidth: 25 Mbps



Bandwidth

Uplink Bandwidth (For Outbound Traffic, kbit/s): 25600

Downlink Bandwidth (For Inbound Traffic, kbit/s): 25600

Application Port Priority

Application Name	Priority	Port	Enabled
None	Normal	0	☐
None	Normal	0	☐
None	Normal	0	☐
None	Normal	0	☐
None	Normal	0	☐
	Normal	0	☐
	Normal	0	☐
	Normal	0	☐
	Normal	0	☐
	Normal	0	☐

Minimum Uplink/Downlink Bandwidth: 1 kbit/s

- **If NAT is disabled:**
  Maximum Uplink/Downlink Bandwidth: 30 Mbps
  Minimum Uplink/Downlink Bandwidth: 1 kbit/s

Application Port Priority

- **Application Name:**

1. **FTP (File Transfer Protocol)**
   A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP.

2. **Telnet**
   A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

3. **SMTP (Simple Mail Transfer Protocol)**
   The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.
4. **DNS (Domain Name System)**
   The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember handle for an Internet address.

5. **TFTP (Trivial File Transfer Protocol)**
   A version of the TCP/IP FTP protocol that has no directory or password capability.

6. **Finger**
   A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being fingered must have placed his or her profile on the system in order for the

information to be available. Fingering requires entering the full user@domain address.

7. **HTTP (HyperText Transport Protocol)**
   The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

8. **POP3 (Post Office Protocol 3)**
   A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

9. **NNTP (Network News Transfer Protocol)**
   The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

10. **SNMP (Simple Network Management Protocol)**
A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.)

11. **Kazaa**
Kazaa uses peer-to-peer technology. The means that individual users connect to each other directly, without need for a central point of management.

12. **DC++**
DC++ is an open source client for the Direct Connect network. Direct Connect allows you to share files over the Internet without restrictions or limits. The client is completely free of

advertisements and has a nice, easy to use interface. Firewall and router support is integrated and it is easy and convenient to use functionality like multi-hub connections, auto-connections and resuming of downloads.

13. **RSVP**

The RSVP protocol is part of a larger effort to enhance the current Internet architecture with support for Quality of Service flows. The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service.

RSVP requests will generally result in resources being reserved in each node along the data path.

14. **H.323**

H.323 is the international standard for multimedia communication over packet-switched networks, including LANs, WANs, and the Internet. It was first defined by the ITU in 1996 and has been updated regularly.

The scope of H.323 covers real-time voice, video, and data communication over packet-switched networks. It was designed from the outset to operate over IP networks, primarily, though H.323 may also operate over other packet-switched networks. It was designed with multipoint voice and video conferencing capabilities, though most users do not take advantage of the multipoint capabilities specified in the protocol.

15. L2TP

L2TP, Layer 2 Tunneling Protocol, is used to provide IP security at the network layer.

L2TP uses UDP to transport the PPP data; this is often encapsulated in IPSec for encryption instead of using MPP.

16. PPTP

PPP (Point-to-Point Protocol) is a standard for transporting datagram over point-to-point links. It is used to encapsulate IP packets for transport between two peers.

To establish a PPP tunnel, both sides send LCP frames to negotiate parameters and test the data link. If authentication is used, at least one of the peers has to authenticate itself before the network layer protocol parameters can be negotiated using NCP. During the LCP and NCP negotiation optional parameters such as encryption, can be negotiated. When LCP and NCP negotiation is done, IP datagram can be sent over the link.

17. IPSec

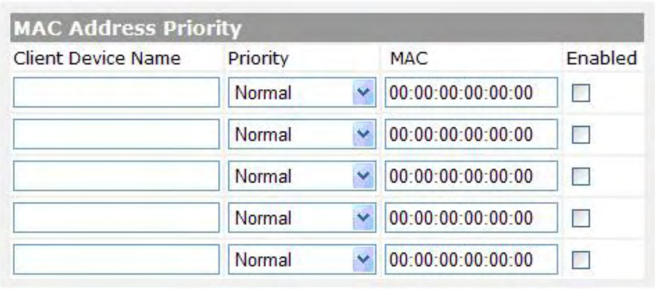
Internet Protocol Security (IPSec) is a collection of standards that was designed specifically to create secure end-to-end secure connections. The standards were developed by the Internet Engineering Task For (IETF) to secure communications over both public and private networks, though it is particularly beneficial to public networks. In this article I'll explain to you some of the fundamentals of IPSec, how it is used, and what products use it.

IPSec is framework that is built into various security products to provide end-to-end security in wide area networking communications. Using strong encryption, and public key cryptography, IPSec can secure data links that would otherwise be insecure and susceptible to exploitation.

- **Priority**
  Select one of these priority levels: Highest, High, Above Normal, or Normal.

- **Port**
  For preset applications, the port number is automatically displayed. For custom applications, enter the appropriate port number in the Port field.

MAC Address Priority



MAC Address Priority

Client Device Name	Priority	MAC	Enabled
	Normal	00:00:00:00:00:00	☐
	Normal	00:00:00:00:00:00	☐
	Normal	00:00:00:00:00:00	☐
	Normal	00:00:00:00:00:00	☐
	Normal	00:00:00:00:00:00	☐

- **Client Device Name**
  Enter the name of your network device.

- **Priority**

Select one of these priority levels: Highest, High, Above Normal, or Normal

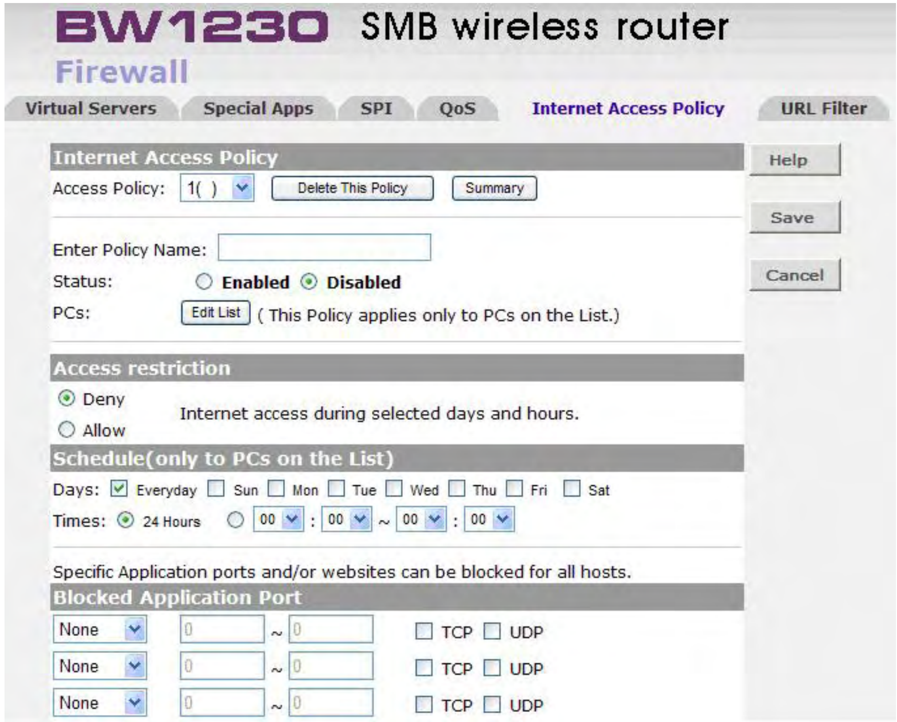
- **MAC**
  Enter the MAC address of the device.

- **Enabled**
  Click the Enabled checkbox to enable QoS for the appropriate MAC address.

Firewall | Internet Access Policy

- The Internet Access Policy screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated applications, websites, and inbound traffic during specific days and times.

- **Internet Access Policy**
  - Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the Save Settings button is clicked).
  - Selecting a policy from the drop-down menu will display those policies settings.
  - To delete a policy, select policies number and click the Delete This Policy button.
  - To view all the policies, click the Summary button.
  - On the Summary screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). You can change the type of access, days, and times of a policy.
  - To activate a policy, click the Enabled checkbox.
  - To delete a policy, click its Delete button.



Internet Access Policy

Access Policy: 1( )

Enter Policy Name:

Status: ○ Enabled ● Disabled

PCs: (This Policy applies only to PCs on the List.)

Access restriction

● Deny
○ Allow

Internet access during selected days and hours.

Schedule(only to PCs on the List)

Days: ☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times: ● 24 Hours ○ 00 : 00 ~ 00 : 00

Specific Application ports and/or websites can be blocked for all hosts.

Blocked Application Port

None	0	~	0	□ TCP	□ UDP
None	0	~	0	□ TCP	□ UDP
None	0	~	0	□ TCP	□ UDP

- Click the Save Settings button to save your changes.
- To view the list of PCs for a specific policy, click the Edit List button.
- On the List of PCs screen, you can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs.
- After making your changes, click the Save Settings button to apply your changes.

To create an Internet Access policy

1. Select a number from the Access Policy drop-down menu.
2. Enter a Policy Name in the field provided.

3. To enable this policy, select **Enabled** from the Status drop-down menu.

4. Click the **Edit** List button to select which PCs will be affected by the policy. The List of PCs screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if

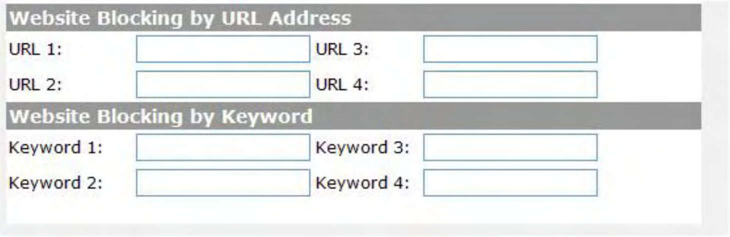
you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes.

5. Click the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.

6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. You can filter access to various applications accessed over the Internet, such as FTP or telnet by selecting up to three applications from the drop-down menus next to Blocked Application Port. Each drop-down menu offers a choice of ten preset applications (select **None** if you do not want to use any of the applications). For the preset applications you select, the appropriate ranges of ports will automatically be displayed. If the application you want to block is not listed or you want to edit

applications settings, then select **Custom** from the drop-down menu. Enter the port range you want to block. Then select its protocol(s), **TCP** and/or **UDP**.



Website Blocking by URL Address

URL 1:		URL 3:	
URL 2:		URL 4:	

Website Blocking by Keyword

Keyword 1:		Keyword 3:	
Keyword 2:		Keyword 4:	

8. Internet Access can also be filtered by URL Address, the address entered to access Internet sites, by entering the address in one of the **Website Blocking by URL Address** fields. If you do not know the URL Address, filtering can be done by Keyword by entering a keyword in one of the Website Blocking by Keyword fields.

9. Click the **Save** button to save the policy settings.

!	By pressing the **Cancel** button all changes will be discarded.

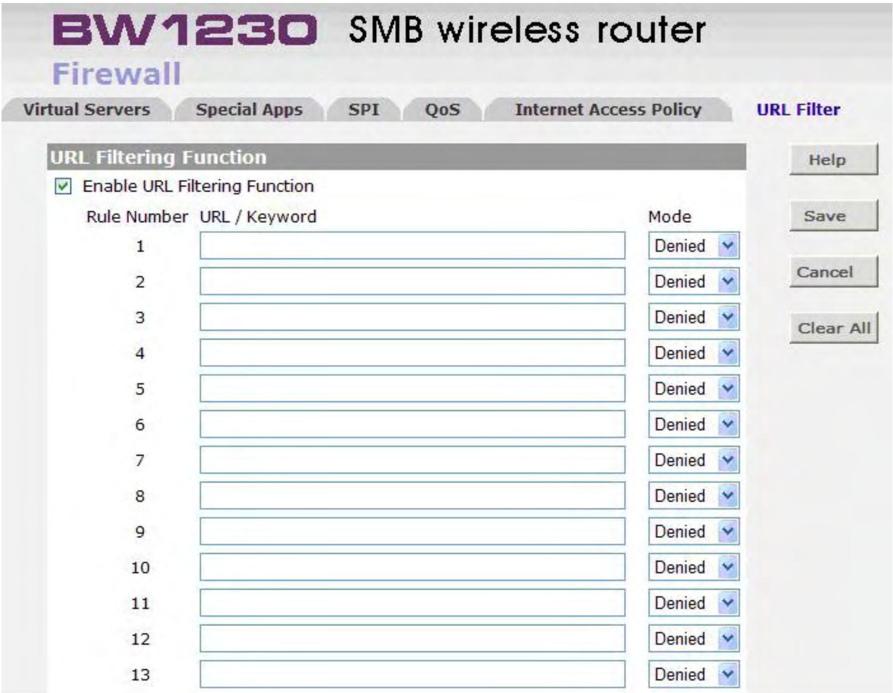
Firewall | URL Filter

- This feature allows you to block or allow access to specified Websites. The feature is used in conjunction with PC Privileges. PC Privileges allow the administrator to control Internet access.
  There are two types of URL Filter available:
  Deny List and **Allow List**. In both cases the Router will only check the URL and not the content of the site.

  - The **Deny List** will compare entries in the Filter Table to that of a requested Website URL and block the user from viewing the Website if a match is found.

  - The **Allow List** will compare entries in the Filter Table to that of a requested Website URL and allow the Website to be viewed if a match is found. All other URL requests are blocked.

- If a user attempts to access a blocked website, they will be presented with a warning message in their Internet Browser informing them that this website is blocked and to contact



URL Filtering Function

☑ Enable URL Filtering Function

Rule Number	URL / Keyword	Mode
1		Denied
2		Denied
3		Denied
4		Denied
5		Denied
6		Denied
7		Denied
8		Denied
9		Denied
10		Denied
11		Denied
12		Denied
13		Denied

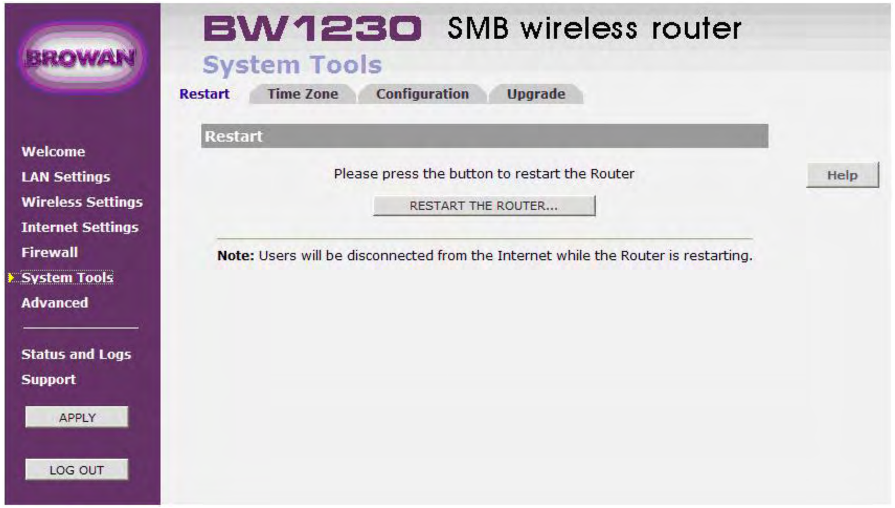
their system administrator.

- The Filter Table allows the entry of either URLs or keywords.
  For example, a URL would typically look take the form: www.examplesite.com, www.another-site.org, www.eg_website.net. Whereas a Keyword would typically be a word or letters that should be blocked, for example: adult, xxx, excite.

System Tools | Restart

- Pressing the **Restart the Router** button will cause the Router to restart, simulating the effect of power cycling the unit. No configuration information will be lost. This function may be of use if you are experiencing problems and you wish to re-establish your Internet connection.

- Any network users who are currently accessing the Internet will have their access interrupted whilst the restart takes place, and they may need to reboot their computers when the restart has completed and the Router is operational again.



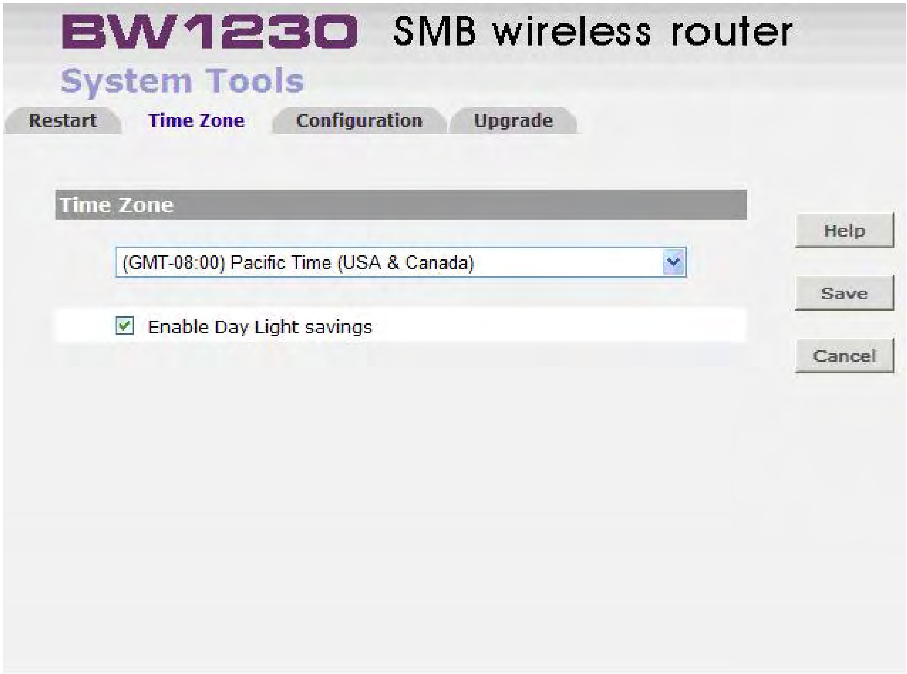
Please press the button to restart the Router

Note: Users will be disconnected from the Internet while the Router is restarting.

System Tools | Time Zone

- Choose the **Time Zone** that is closest to your actual location. The time zone setting is used by the system clock when displaying the correct time in the log files.

- The system time is automatically updated from Time Servers on the Internet. The **Daylight saving feature** allows you to manually add 1 hour to the Internet time. This is not automatically updated when the Daylight saving time ends.



Time Zone

(GMT-08:00) Pacific Time (USA & Canada)

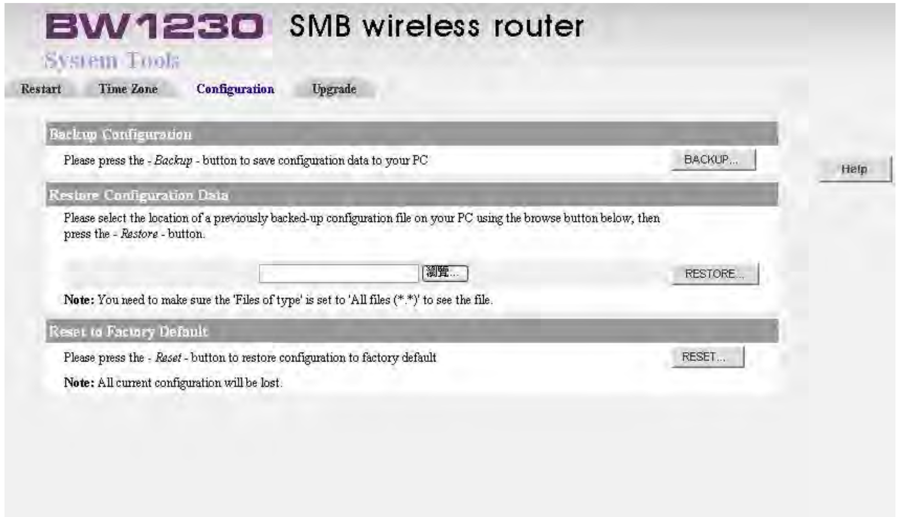
☑ Enable Day Light savings

System Tools | Configuration

- **Backup Configuration**
  Use the **Backup** button to save the Router's current configuration settings in a file on your computer. When you select this function, your browser will prompt you to enter a file name and folder location in which to save the data. Note that a file saved in this way cannot be viewed or modified with a word processor or spreadsheet program.

- **Restore Configuration Data**
  The Restore Configuration Data function is used to reinstate the configuration data previously saved to a file using the Backup Configuration function. Use the Browse button to locate the backup file on your computer, and then click the **Restore** button to copy the data into the Router's memory.
  Note that the system password is **NOT** changed when a new configure file is loaded.

- **Reset to Factory Default**
  The Reset to Factory Default function will clear all the



Backup Configuration

Please press the - *Backup* - button to save configuration data to your PC

Restore Configuration Data

Please select the location of a previously backed-up configuration file on your PC using the browse button below, then press the - *Restore* - button.

Note: You need to make sure the 'Files of type' is set to 'All files (*.*)' to see the file.

Reset to Factory Default

Please press the - *Reset* - button to restore configuration to factory default

Note: All current configuration will be lost.

configuration information from the Router and return it to the state it was in when it was shipped from BROWAN. The unit will then restart. This function might be useful if, for instance, a Router is moved from one network to another and you wish to start the configuration process from a known **clean** state.

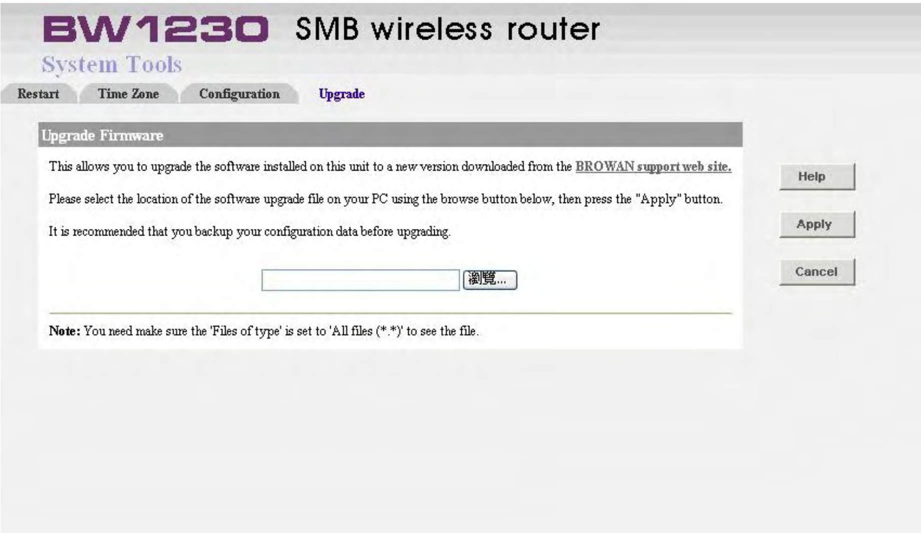
This function should be used with caution, as once a unit has been reset to its factory default state, then the current configuration settings are irrevocably lost. It is strongly recommended that you backup the current configuration with the Backup Configuration facility before using the Reset to Factory Defaults function unless you are certain that the current settings are no longer needed.

System Tools | Upgrade

- The Upgrade facility allows you to install on the Router any new releases of system software that BROWAN may make available.

- To install new software, you first need to **download** the software from the BROWAN support web site. Once you have done this, use the **Browse** button to tell your web browser where this file is on your computer, and then click on **Apply**.

- The file will be copied to the Router, and when this has completed, the Router will restart. Although the upgrade process has been designed to preserve your configuration settings, it is recommended that you make a backup of the configuration beforehand, in case the upgrade process fails for any reason (for example, the connection between the computer and the Router is lost while the new software is being copied to the Router).



Upgrade Firmware

This allows you to upgrade the software installed on this unit to a new version downloaded from the BROWAN support web site.

Please select the location of the software upgrade file on your PC using the browse button below, then press the "Apply" button.

It is recommended that you backup your configuration data before upgrading.

Note: You need make sure the 'Files of type' is set to 'All files (*.*)' to see the file.

Advanced | Static Route

- The device supports static route functionality.

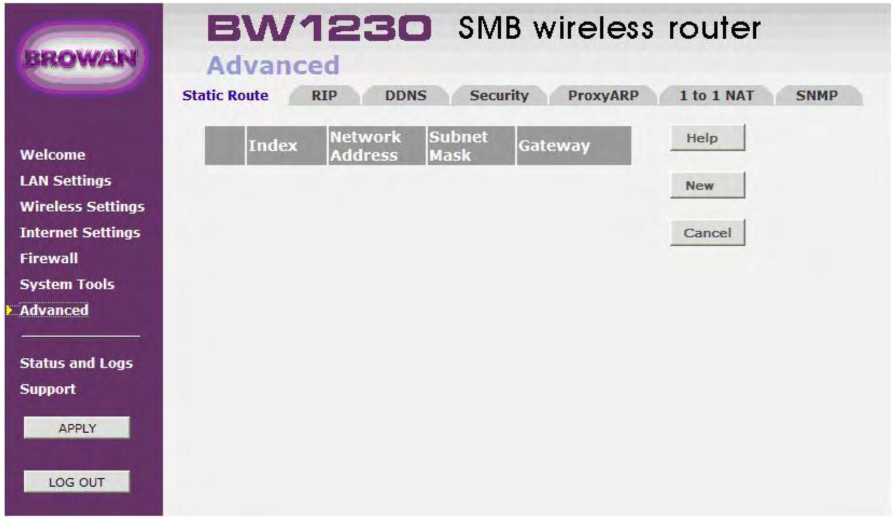
  - **Index**
    The index of the entry for the static route.

  - **Network Address**
    The network address of the static route.

  - **Subnet Mask**
    The subnet mask of the static route.

  - **Gateway**
    Gateways are most commonly used to transfer data between private networks and the internet.

- Click **New** button below the table to add the static route entries. After adding any entry in the static routing table, you could click **Delete** button to delete the entries you have made. Click **Apply** button to save the changes, otherwise click **Cancel** button to quit the setup.

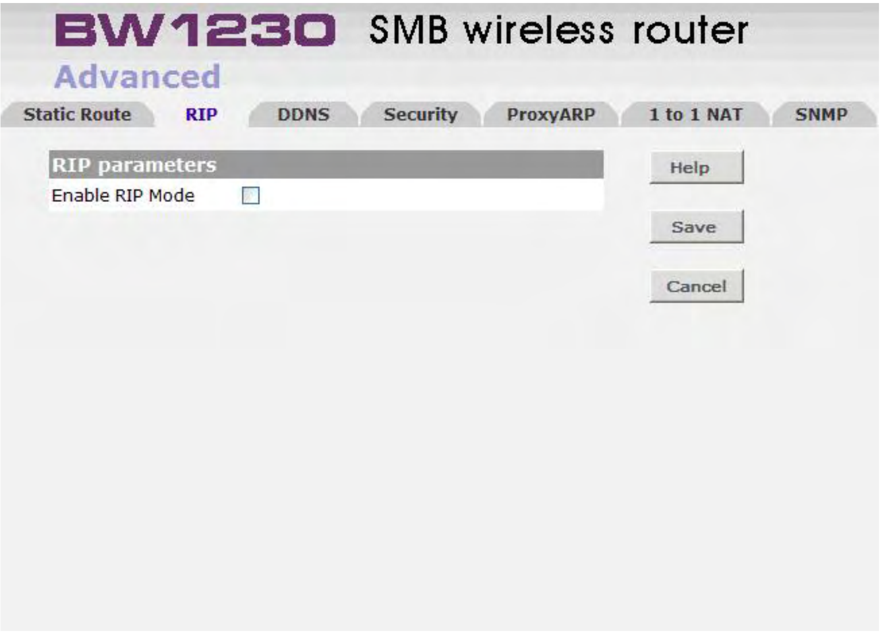


	Index	Network Address	Subnet Mask	Gateway

Advanced | RIP

- **RIP (Routing Information Protocol)** is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs.

- Check the check box to enable RIP Mode, or uncheck the check box for disable RIP Mode.



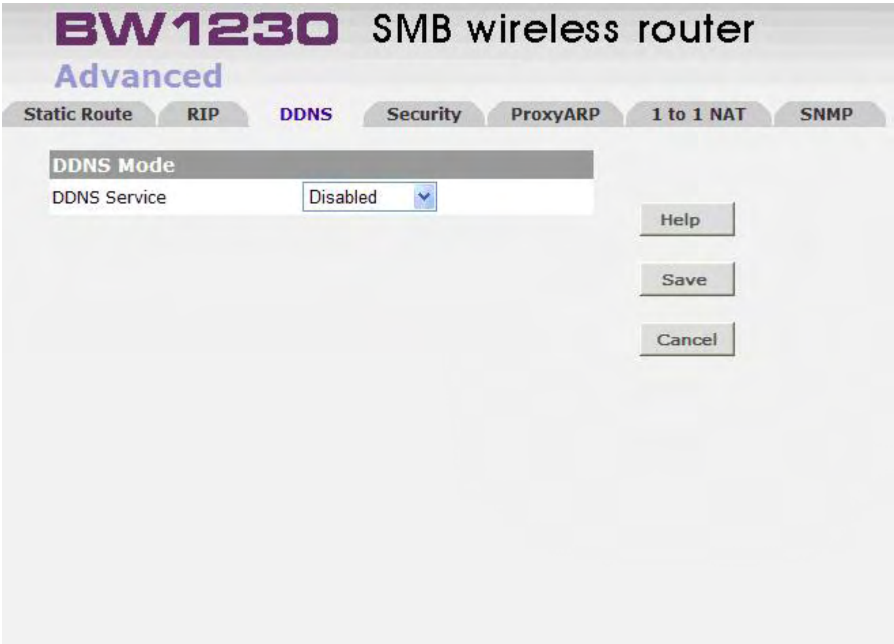
RIP parameters

Enable RIP Mode □

Advanced | DDNS

- **Dynamic Domain Name System (DDNS)** is a system which allows the domain name data held in a name server to be updated in real time. The most common use for this is in allowing an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. This makes it possible for other sites on the Internet to establish connections to the machine without needing to track the IP address themselves. A common use is for running server software on a computer that has a dynamic IP address, as is the case with many consumer Internet service providers.

- The DDNS is **disabled** by default selection.

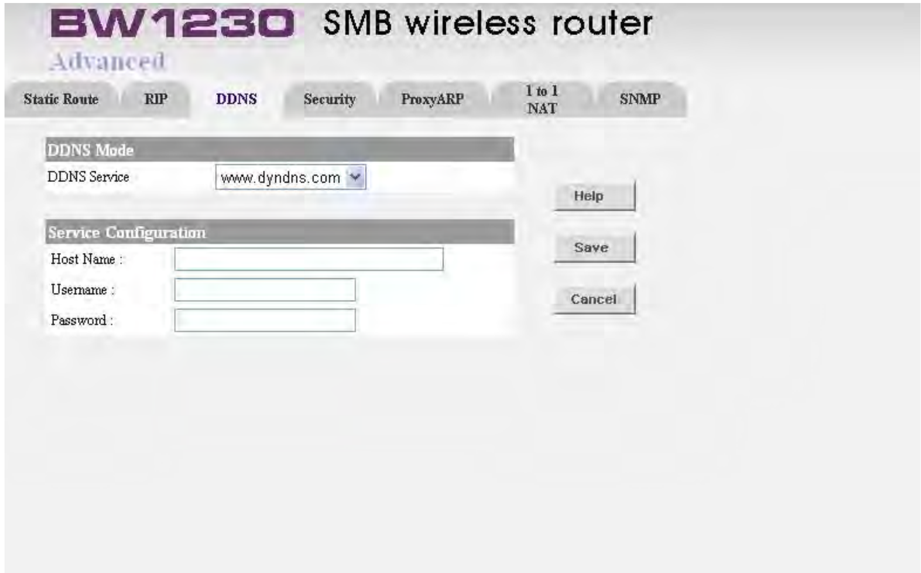


DDNS Mode

DDNS Service: Disabled

- You could select DynDNS.org to Enable the DDNS.

- Please enter the **Host Name, Username and Password** you acquired form your DDNS provider (http://www.dyndns.com/)..



DDNS Mode

DDNS Service: www.dyndns.com

Service Configuration

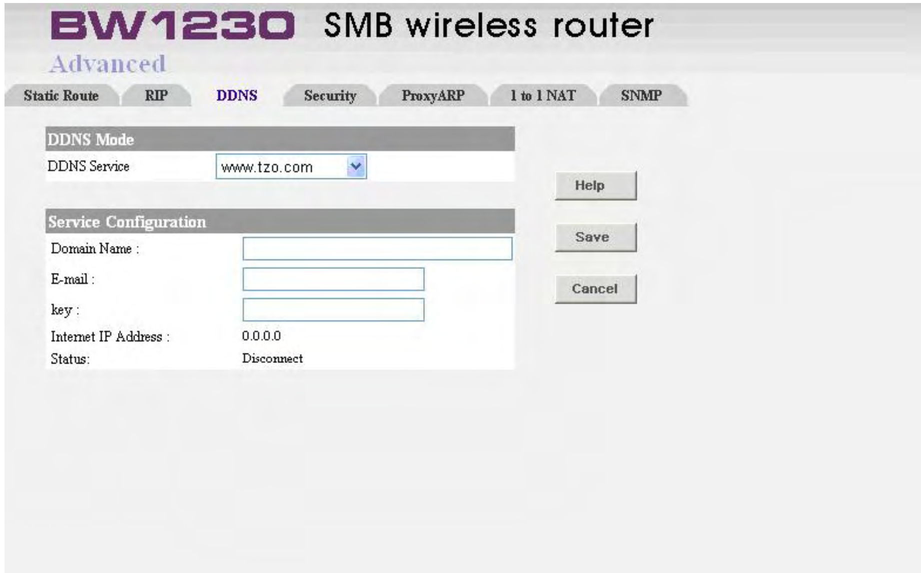
Host Name :

Username :

Password :

- You could select TZO.com to Enable the DDNS.

- Please enter the **Host Name, Username and Password** you acquired form your DDNS provider (http://www.tzo.com/).



DDNS Mode

DDNS Service: www.tzo.com

Service Configuration

Domain Name :

E-mail :

key :

Internet IP Address : 0.0.0.0

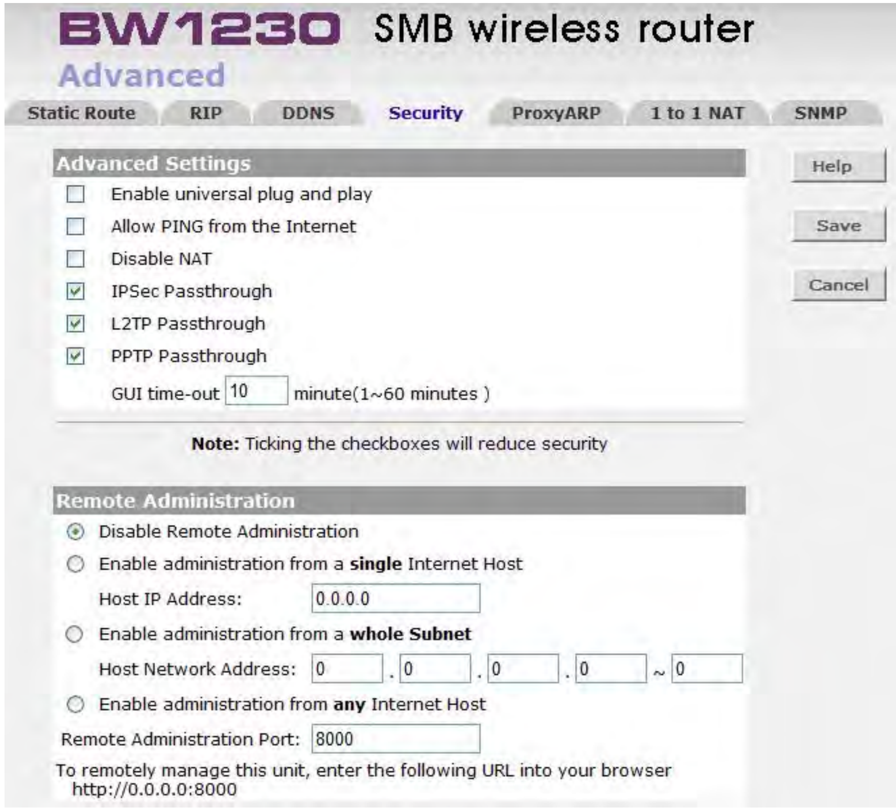
Status: Disconnect

Advanced | Security

- The security setup could help you to protect your network.

- The Router contains both an Advanced Firewall and a Basic Firewall. The Basic Firewall detects the common attack patterns used by people on the Internet and once detected will block their access to your network. The Advanced Firewall uses Stateful Packet Inspection (SPI), which is a more secure method of protection against attacks to your network. When an attack is detected a log entry will be generated and the Alert LED will be lit for 2 seconds.

  - **Enable universal plug and play**
    The universal plug and play architecture enables discovery and control between devices on a network. Enabling this feature will make the Router less secure, as you no longer have control on which ports in the Firewall are opened.
    Universal plug and play is enabled by:
    - Checking on the Enable universal plug and play



Advanced Settings

□ Enable universal plug and play
□ Allow PING from the Internet
□ Disable NAT
☑ IPSec Passthrough
☑ L2TP Passthrough
☑ PPTP Passthrough

GUI time-out 10 minute(1~60 minutes)

Note: Ticking the checkboxes will reduce security

Remote Administration

● Disable Remote Administration
○ Enable administration from a **single** Internet Host
Host IP Address: 0.0.0.0
○ Enable administration from a **whole Subnet**
Host Network Address: 0 . 0 . 0 . 0 ~ 0
○ Enable administration from **any** Internet Host

Remote Administration Port: 8000

To remotely manage this unit, enter the following URL into your browser
http://0.0.0.0:8000

check box so that a tick can be seen.

- Clicking the Apply button.

- **Allow PING from the Internet**

  Ping is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending **ICMP echo request packets** to the target host and listening for **ICMP echo response replies**. Using interval timing and response rate, ping estimates the round-trip time and rate of packet loss (if any) between hosts.

  Allow PING is enabled by：

  - Checking on the Allow PING from the Internet check box so that a tick can be seen.
  - Click the Apply button.

- **Disable NAT**

  When NAT is Disabled, the Router does not perform IP address and port translation. The related features, such as Virtual Server, Special Applications, PC Privileges, Virtual DMZ, do not work after NAT Disabled.

Disable NAT is enabled by：

- Checking on the Disable NAT check box so that a tick can be seen.
- Clicking he Apply button.

- **IPSec Pass-through**

  Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default.

- **L2TP Pass-through**

  Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default.

- **PPTP Pass-through**

  Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default.

- **GUI timeout**

If you do not access the GUI for the specified time span (Default is 10 minutes), the system will ask you to login again.

- **Enabling Remote Administration**

It is possible to administer the Router from the Internet. You can enable remote administration for a single PC, all PCs in a subnet, or for any PC. The more PCs you enable access for, the less secure your Router will be. To do this :

1. Select the remote administration mode you require.

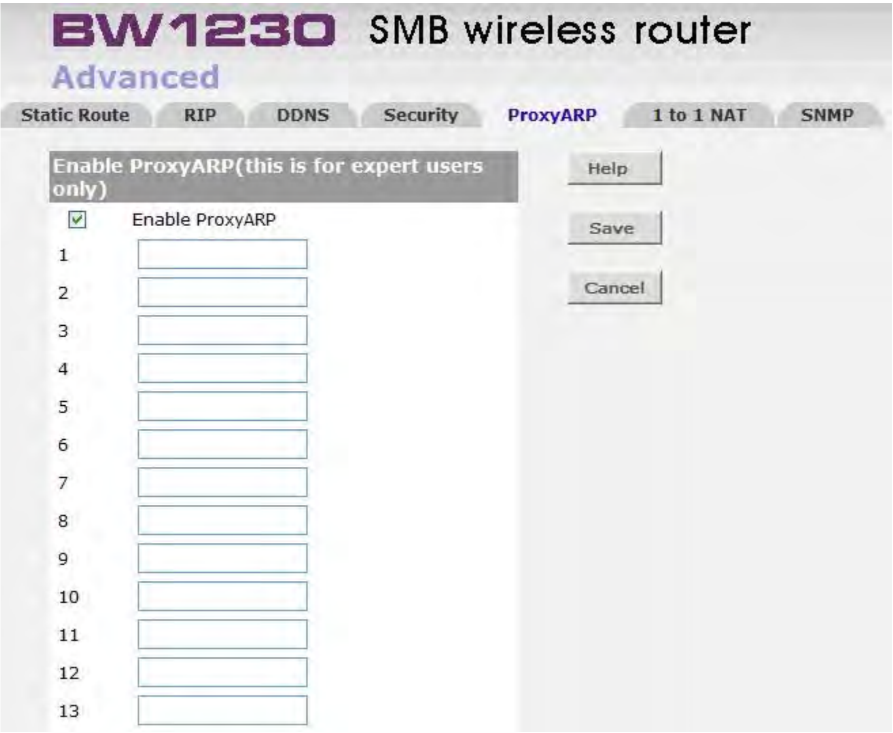
2. In the case of a single PC, specify its IP address. In the case of a subnet, specify the address of a PC in the subnet, and the subnet mask.

3. The Remote PC can now administer the Router by entering http：//<Router_Internet_IP_Address>：8000 into a web browser.

Advanced | Proxy ARP

- Proxy ARP is the technique in which one machine, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP allows a site to use a single IP address with two physical networks.

- Following is the setting procedures on Proxy ARP function
  1. Set the GW wan IP in static ip mode, such as IP：10.0.0.2, submask：255.255.0.0, route：10.0.0.1
  2. Enable Proxy ARP on WEB UI and set the Public IP range you want to set on PC in your LAN network such as from 10.0.0.3 to 10.0.0.14
  3. Set PC in your LAN network with one of those Public IP, such as IP：10.0.0.3, submask：255.255.0.0, route：10.0.0.1



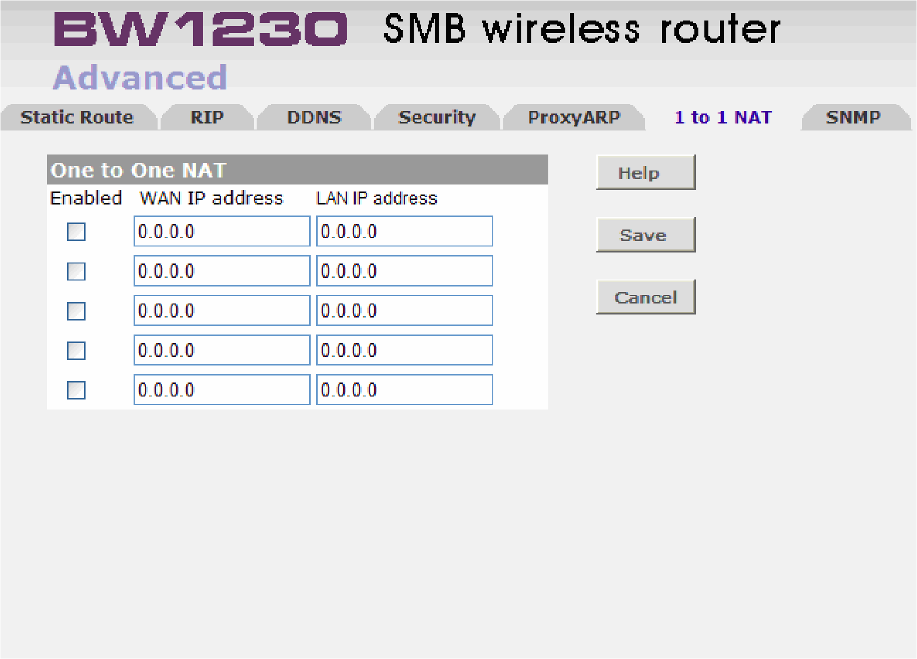
Enable ProxyARP(this is for expert users only)

☑ Enable ProxyARP

Advanced | 1 to 1 NAT

The following criteria must be met to be able to use One-to-One NAT：

- You must have a static Internet IP address for every computer on your network plus one for the Router itself.
- The addresses must be in one continuous block in the same subnet
- You must have selected Static IP Address as your IP Allocation Mode and have given your VPN Firewall the first of the Internet addresses allocated by your ISP.
- To set up One-to-One NAT：
- Enable the entry of One-to-One NAT.
- Enter the Internet addresses in ISP Pool field. (WAN IP address).
- Enter the IP address in your LAN side to which you want to map it in LAN Pool field.

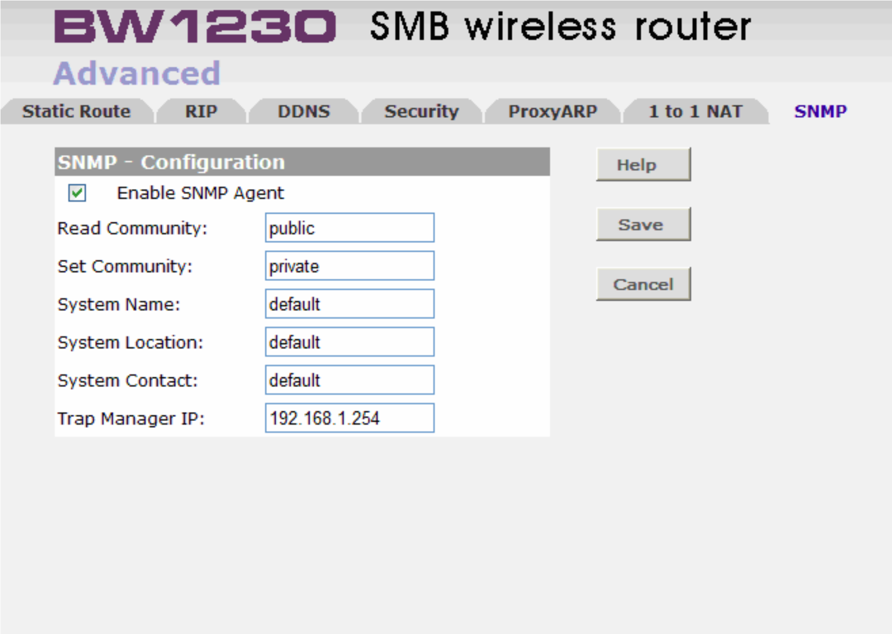


One to One NAT

Enabled	WAN IP address	LAN IP address
☐	0.0.0.0	0.0.0.0
☐	0.0.0.0	0.0.0.0
☐	0.0.0.0	0.0.0.0
☐	0.0.0.0	0.0.0.0
☐	0.0.0.0	0.0.0.0

Advanced | SNMP

- **Simple Network Management Protocol (SNMP)** allows a management application to retrieve statistics and status from the SNMP agent in this device.



SNMP - Configuration

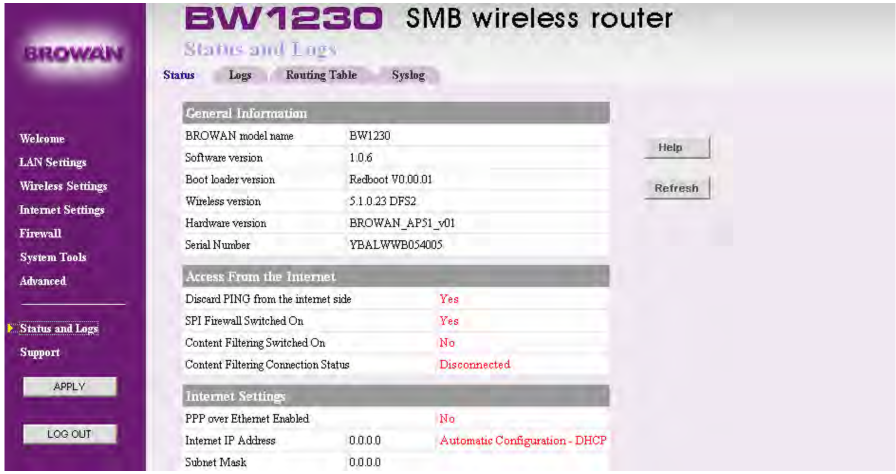
☑ Enable SNMP Agent

Read Community:	public
Set Community:	private
System Name:	default
System Location:	default
System Contact:	default
Trap Manager IP:	192.168.1.254

Status and Logs | Status

- This page summarizes most of the unit's configuration in one place. You may be asked to print this page out if you call **BROWAN Support**.

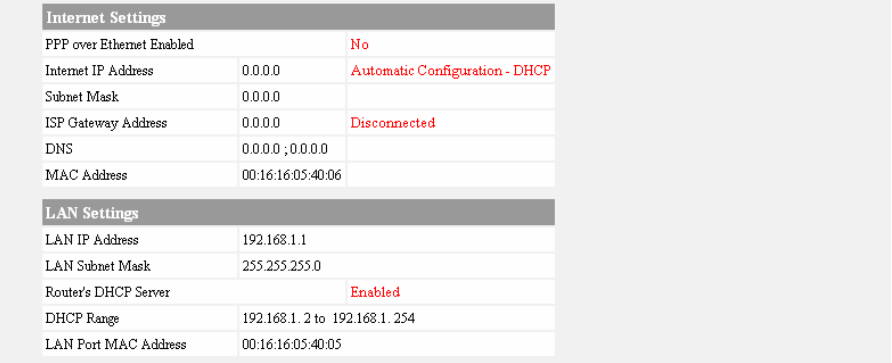
- You can refresh the information by clicking on the **Refresh** button.



General Information	
BROWAN model name	BW1230
Software version	1.0.6
Boot loader version	Redboot V0.00.01
Wireless version	5.1.0.23 DFS2
Hardware version	BROWAN_AP51_v01
Serial Number	YBALWWB054005

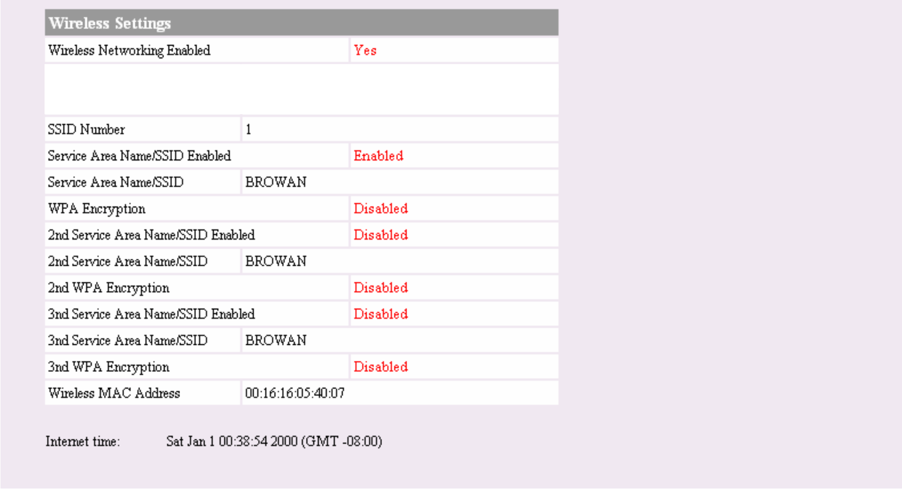
Access From the Internet	
Discard PING from the internet side	Yes
SPI Firewall Switched On	Yes
Content Filtering Switched On	No
Content Filtering Connection Status	Disconnected

Internet Settings		
PPP over Ethernet Enabled		No
Internet IP Address	0.0.0.0	Automatic Configuration - DHCP
Subnet Mask	0.0.0.0	



Internet Settings		
PPP over Ethernet Enabled		No
Internet IP Address	0.0.0.0	Automatic Configuration - DHCP
Subnet Mask	0.0.0.0	
ISP Gateway Address	0.0.0.0	Disconnected
DNS	0.0.0.0 ; 0.0.0.0	
MAC Address	00:16:16:05:40:06	

LAN Settings		
LAN IP Address	192.168.1.1	
LAN Subnet Mask	255.255.255.0	
Router's DHCP Server		Enabled
DHCP Range	192.168.1. 2 to 192.168.1. 254	
LAN Port MAC Address	00:16:16:05:40:05	



Wireless Settings

Wireless Networking Enabled	Yes
SSID Number	1
Service Area Name/SSID Enabled	Enabled
Service Area Name/SSID	BROWAN
WPA Encryption	Disabled
2nd Service Area Name/SSID Enabled	Disabled
2nd Service Area Name/SSID	BROWAN
2nd WPA Encryption	Disabled
3nd Service Area Name/SSID Enabled	Disabled
3nd Service Area Name/SSID	BROWAN
3nd WPA Encryption	Disabled
Wireless MAC Address	00:16:16:05:40:07

Internet time: Sat Jan 1 00:38:54 2000 (GMT -08:00)

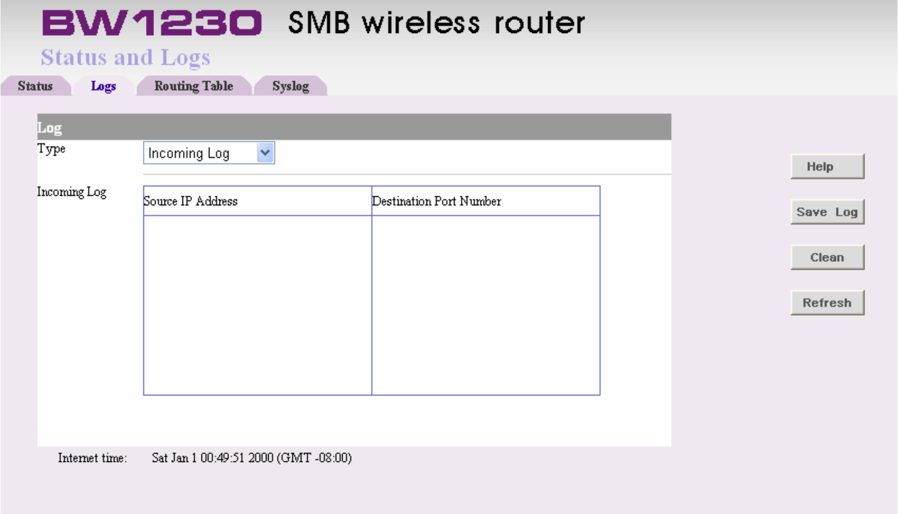
Status and Logs | Logs

- This page allows the user to view or download the System Log files. These files record the date and time of a variety of events that took place when using the Router. Most of them are normal events for example issuing DHCP addresses to requesting PCs. However, this is also where the Router would record security threats like：

  - Hacker Attacks detected.
    - Attempts to login to the admin interface from the LAN side.
    - Attempts to login to the admin interface from the Internet.

  - **View Log**
    Select I**ncoming Log, Outgoing Log,Security Log, Security Log, or DHCP Client Log** from the Type drop-down menu.

    - The **Incoming Log** will display a temporary log of the Source IP Addresses and Destination Port



Log

Type: Incoming Log

Incoming Log

Source IP Address	Destination Port Number

Internet time: Sat Jan 1 00:49:51 2000 (GMT -08:00)

Numbers for the incoming Internet traffic

- The **Outgoing Log** will display a temporary log of the LAN IP Addresses, Destination URLs or IP Addresses, and Service or Port Numbers for the outgoing Internet traffic.
- The **Security Log** will display the login information for the WEB Utility.
- The **DHCP Client Log** will display the LAN DHCP server status information.

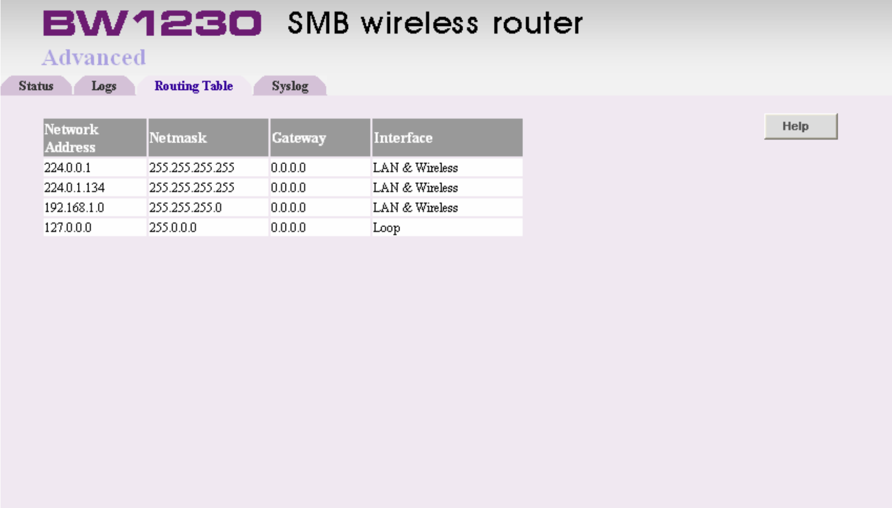
- The files can be downloaded and saved as a text file on your PC. To do this:
  1. Click on the **Save Log** button.
  2. Specify a location to save the file and click **OK.**

- Click the **Refresh** button to update the log

- The **Clean** button deletes all of the log contents.

Status and Logs | Routing Table

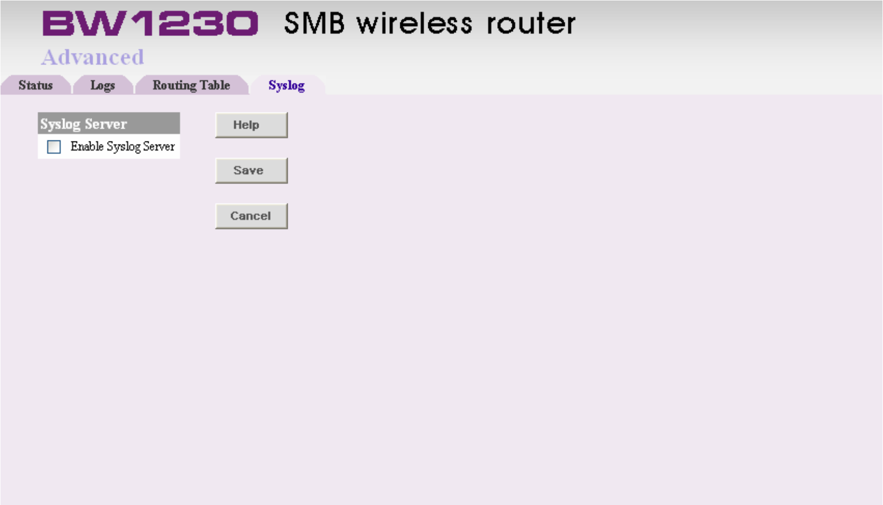
- The routing table details the default routing used by the router and any routing created using Static routing or RIP.



Network Address	Netmask	Gateway	Interface
224.0.0.1	255.255.255.255	0.0.0.0	LAN & Wireless
224.0.1.134	255.255.255.255	0.0.0.0	LAN & Wireless
192.168.1.0	255.255.255.0	0.0.0.0	LAN & Wireless
127.0.0.0	255.0.0.0	0.0.0.0	Loop

Status and Logs | Syslog

- Syslog allows the user to to log system information to a remote server.



□ Enable Syslog Server

!	You may need to modify your remote syslog server settings to accept remote logs.

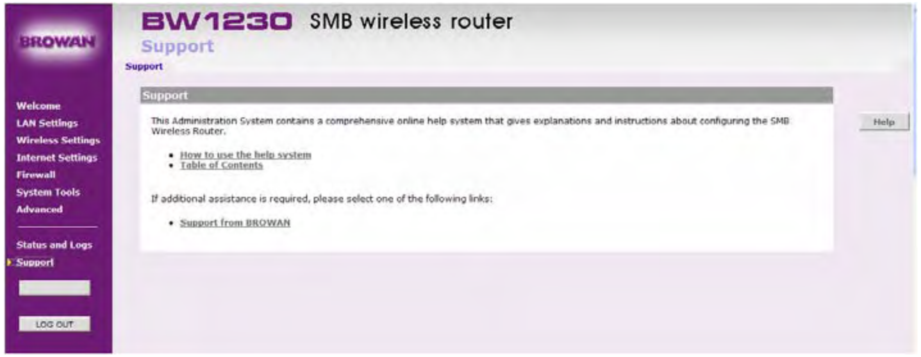
Support | Support

- To access help for the Administration System, Click **Help** button o. The help pop-up window will appear after you click Help button.
- How to use the help system:

<< BACK	Works exactly like a browser's back button.
FORWARD >>	Works exactly like a browser's forward button
INDEX	Opens the Help Table of Contents.

- Table of Contents：
  This link will help you to find the keyword in help system quickly.

- Support from BROWAN：
  You could visit our support web page with is link.



Support

This Administration System contains a comprehensive online help system that gives explanations and instructions about configuring the SMB Wireless Router.

- How to use the help system
- Table of Contents

If additional assistance is required, please select one of the following links:

- Support from BROWAN

Appendix

Wireless specification	
Data rate supported	IEEE 802.11 b ： 1, 2, 5.5, 11 Mbps 802.11 g ： 6, 9, 12, 18, 24 , 36 , 48, 54, and 108 Mbps
Frequency Band	802.11b/g 2.400 ~ 2.483GHz
Channel	FCC： 11 , EU ： 13
Modulation	802.11b：DBPSK(1Mbps), DQPSK(2Mbps), CCK(5.5Mbps, 11Mbps) 802.11g：OFDM with BPSK, QPSK, 16QAM, 64QAM

Transmit Power	18dBm(+/-2dBm)@ 11Mbps (not including Antenna gain)
	16dBm(+/-2dBm)@ 54Mbps (not including Antenna gain)

Receive Sensitivity	-83dBm@11Mbps (IEEE 802.11b) -65dBm@54Mbps (IEEE 802.11g)
Antenna	One R-SMA connector for external antenna 1 detachable antenna, peak: 2.0dBi
Radio	2.4GHz ISM band

Product specification	
Interface	WAN ：1 port 100BASE-T, auto-sensing LAN ：4 ports 100BASE-T, auto-sensing
Physical characteristics	Dimension： 173mm(L) x 128mm(W) x 33mm(H) Weight： 256 g
Environment	Operation temperature：0 ~ 55°C (Operating) Storage temperature： -20~85°C (Storing) Humidity：5~95% (Non-condensing)
Power supply	PoE：IEEE 802.3af compliance (option) Power adapter：100 ~ 240 V AC, 50 ~60 Hz input and 12V / 500mA output
LEDs	Power, WLAN, WAN, LAN

Network Management	
Firewall	Access control, Authorized application, Application port priority, URL filtering, Stateful packet inspection(SPI), Website blocking, Virtual Server, Virtual DMZ
Internet connection	Static IP, DHCP, PPPoE, PPTP, Heart Beat Signal, L2TP
Remote management	HTTPS, SNMP, back up and restore configuration files
Firmware upgradeable	Web firmware upgrade

Regulation	
Certification	FCC, CE
Compliance	RoHS, WEEE
Warranty	Two years.