SMC Networks

USER GUIDE

EZ Connect™ N
Wireless N Universal Repeater

SMCWEB-N2

Wireless Broadband Router
User Guide

SMC®
Networks
No. 1, Creation Road III,
Hsinchu Science Park,
30077, Taiwan, R.O.C.
TEL: +886 3 5770270
Fax: +886 3 5780764

October 2012
SMC-UG-1012-02

Warranty and Product Registration

To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http://www.smc.com.

COMPLIANCES

CE MARK WARNING

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NATIONAL RESTRICTIONS

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/Remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

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 60950-1:2006 + A11: 2009Safety of Information Technology Equipment.
- EN 300 328 V1.7.1: 2006-10Electromagnetic 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 301 489-17 V1.8.1/ 2008-04EN 301 489-17 V2.1.1/ 2009-05Electromagnetic 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.
- EN 55022: 2006 + A1: 2007Limits and methods of measurement of radio disturbance characteristics of information technology equipment.
- EN 55024: 1998 + A1: 2001 + A2: 2003Information technology equipment immunity characteristics limits and methods of measurement.
- EN 62311: 2008Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz).

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.

This equipment may be operated in:

AT	DK	DE	IE	LU	PL	ES	LI
BE	EE	GR	IT	MT	PT	SE	BG
CY	FI	HU	LV	NL	SI	CH	RO
CZ	FR	IS	LT	NO	SK	GB	TR

The official CE certificate of conformity can be downloaded by selecting the relevant model/ part number from www.smc.com -> support -> download.

Bulgarian Български	С настоящето, SMC Networks декларира, че това безжично устройство е в съответствие със съществените изисквания и другите приложими разпоредби на Директива 1999/5/EC.
Czech Česky	SMC Networks tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish Dansk	Undertegnede SMC Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Dutch Nederlands	Hierbij verklaart SMC Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze SMC Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, SMC Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian Eesti	Käesolevaga kinnitab SMC Networks seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish Suomi	Valmistaja SMC Networks vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French Français	Par la présente SMC Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
German Deutsch	Hiermit erklärt SMC Networks, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt SMC Networks die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek Ελληνική	με την παρουσα SMC Networks δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ.
Hungarian Magyar	Alulírott, SMC Networks nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Italian Italiano	Con la presente SMC Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian Latviski	Ar šo SMC Networks deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo SMC Networks deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Maltese Malti	Hawnhekk, SMC Networks, jiddikjara li dan Radio LAN device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Polish Polski	Niniejszym SMC Networks oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	SMC Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Romanian Română	SMC Networks declară că acest dispozitiv fără fir respectă cerințele esențiale precum şi alte dispoziții relevante ale Directivei 1999/5/EC.
Slovak Slovensky	SMC Networks týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	SMC Networks izjavlja, da je ta radio LAN device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Spanish Español	Por medio de la presente SMC Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Swedish Svenska	Härmed intygar SMC Networks att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Turkish Turk	SMC Networks bu kablosuz cihazın temel gereksinimleri ve 1999/5/EC yonergesindeki ilgili koşulları karşıladığını beyan eder.

SAFETY PRECAUTIONS

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use the power adapter that is included with the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet or damaged cords and plugs may cause electric shock or fire. Check the power cords regularly, if you find any damage, replace it at once.
- Proper space for heat dissipation is necessary to avoid any damage caused by device overheating. The ventilation holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these ventilation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid placing the device in direct sunshine.
- Do not put this device close to a place which is damp or wet. Do not spill any fluid on this device.

- Please follow the instructions in the user manual/quick install guide carefully to connect the device to your PC or other electronic product. Any invalid connection may cause a power or fire risk.

- Do not place this device on an unstable surface or support.

PRÉCAUTIONS DE SÉCURITÉ

Lisez attentivement les informations suivantes avant d'utiliser votre appareil. Respectez toutes les précautions afin de protéger l'appareil des risques et dégâts provoqués par un incendie et l'alimentation électrique :

- Utilisez exclusivement l'adaptateur d'alimentation fourni avec cet appareil.

- Faites attention à la puissance de charge de la prise de courant ou des rallonges électriques. Une prise surchargée ou des cordons et des fiches endommagés peuvent provoquer une électrocution ou un incendie. Vérifiez régulièrement votre câble électrique. Si vous constatiez le moindre défaut, remplacez-le immédiatement.

- Il est primordial de laisser suffisamment d'espace autour de l'appareil pour permettre la dissipation de la chaleur et éviter les dégâts provoqués par une surchauffe de l'appareil. Les orifices de ventilation de l'appareil sont conçus pour permettre la dissipation thermique et garantir le bon fonctionnement de l'appareil. Ne couvrez jamais ces orifices.

- Ne placez pas cet appareil à proximité d'une source de chaleur ou dans un endroit exposé à des températures élevées. Evitez également de l'exposer à la lumière directe du soleil.

- Ne placez pas cet appareil à proximité d'un lieu humide ou mouillé. Prenez garde à ne renverser aucun liquide sur cet appareil.

- Merci de suivre les instructions du manuel d'utilisateur / guide d'installation rapide attentivement pour connecter l'appareil à votre PC ou à tout autre produit électronique. Toute connexion non valide peut provoquer un problème électrique ou un risque d'incendie.

- Ne placez pas cet appareil sur une surface ou un support instable.

SICHERHEITSMAßNAHMEN

Lesen Sie vor der Inbetriebnahme des Gerätes aufmerksam die nachstehenden Informationen. Bitte befolgen Sie die nachstehenden Sicherheitsmaßnahmen, damit das Gerät nicht beschädigt wird oder Gefahren durch Brand oder elektrische Energie entstehen:

- Verwenden Sie nur das beim Gerät mitgelieferte Netzteil.

- Achten Sie auf die Last der Steckdose oder des Verlängerungskabels. Eine überlastete Steckdose oder beschädigte Kabel und Stecker können Stromschläge und Brand verursachen. Prüfen Sie die Netzkabel regelmäßig. Ersetzen Sie sie umgehend, falls sie beschädigt sind.

- Achten Sie zur Vermeidung von Geräteschäden aufgrund von Überhitzung darauf, dass genügend Freiraum zur Wärmeabfuhr vorhanden ist. Die Belüftungsöffnungen am Gerät dienen der Wärmeabfuhr und damit der Gewährleistung eines normalen Gerätebetriebs. Decken Sie diese Belüftungsöffnungen nicht ab.

- Stellen Sie dieses Gerät nicht in der Nähe von Wärmequellen oder an Orten mit hohen Temperaturen auf. Platzieren Sie das Gerät nicht im direkten Sonnenlicht.

- Stellen Sie dieses Gerät nicht an feuchten oder nassen Orten auf. Achten Sie darauf, keine Flüssigkeiten über dem Gerät zu verschütten.

- Befolgen Sie die Hinweise im Benutzerhandbuch (bzw. in der Kurzanleitung) zum Anschluß des Gerätes an einen PC oder ein anderes Elektrogerät. Jegliche unzulässige Verbindung birgt die Gefahr von Stromschlägen und Brandgefahr.

- Platzieren Sie dieses Gerät nicht auf einer instabilen Oberfläche oder Halterung.

PRECAUCIONES DE SEGURIDAD

Lea la siguiente información detenidamente antes de utilizar el dispositivo. Siga las indicaciones de precaución que se mencionan a continuación para proteger el dispositivo contra riesgos y daños causados por el fuego y la energía eléctrica:

- Utilice el adaptador de alimentación incluido en el paquete del dispositivo.

- Preste atención a la carga de potencia de la toma de corriente o de los alargadores. Una toma de corriente sobrecargada o líneas y enchufes dañados pueden provocar descargas eléctricas o un incendio. Compruebe los cables de alimentación con cierta frecuencia. Si detecta algún daño, reemplácelos inmediatamente.

- Deje un espacio adecuado para que se disipe el calor y evitar así cualquier daño en el dispositivo causado por sobrecalentamiento. Los orificios de ventilación del dispositivo están diseñados para disipar el calor y garantizar que dicho dispositivo funciona con normalidad. No tape estos orificios de ventilación.

- No coloque este dispositivo cerca de un lugar donde haya una fuente de calor o temperaturas elevadas. Evite exponer el dispositivo a la luz solar directa.

- No coloque este dispositivo junto a un lugar húmedo o mojado. No derrame ningún fluido sobre el dispositivo.
- Por favor, siga cuidadosamente las instrucciones que figuran en el manual/ guía de instalación rápida para conectar el dispositivo a su PC o a cualquier otro producto electrónico. Cualquier conexión no válida podría causar riesgo de descarga o de incendio.
- No coloque este dispositivo en una superficie o soporte inestable.

PRECAUÇÕES DE SEGURANÇA

Leia atentamente as seguintes informações antes de utilizar o dispositivo. Respeite as seguintes indicações de segurança para proteger o dispositivo contra riscos e danos causados por fogo e energia eléctrica:

- Utilize o transformador incluído na embalagem do dispositivo.
- Respeite a potência da tomada eléctrica e das extensões. Uma tomada eléctrica sobrecarregada ou cabos e fichas danificadas podem causar choques eléctricos ou fogo. Verifique regularmente os cabos de alimentação. Caso algum se encontre danificado, substitua-o imediatamente.
- É necessário deixar algum espaço livre em volta do dispositivo para dissipação de calor, de forma a evitar danos causados pelo sobreaquecimento do dispositivo. Os orifícios de ventilação do dispositivo foram concebidos para dissipar o calor e assegurar que o mesmo funciona normalmente. Não bloqueie esses orifícios de ventilação.
- Não coloque este dispositivo junto a fontes de calor ou em locais com temperaturas elevadas. Evite colocar o dispositivo sob luz solar directa.
- Não coloque este dispositivo junto a locais molhados ou com humidade. Não derrame líquidos sobre o dispositivo.
- Por favor siga atentamente as instruções do manual / guia de instalação rápida para conectar o dispositivo ao seu PC ou a qualquer outro dispositivo electrónico. Atenção que qualquer tipo de ligação inválida pode originar risco de choque eléctrico ou de incêndio.
- Não coloque este dispositivo numa superfície ou suporte instáveis.

Contents

About User Manual

This user manual describes how to install and configure SMCWEB-N2.

Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1.: Safety Precautions	Provides safety precaution information.
Chapter 2.: Overview	Provides a general overview of SMCWEB-N2, and the packing list.
Chapter 3.: Mode Introduction	Introduce network topologies and basic wireless connection settings for the Bridge, Router, Wireless Universal Repeater/WDS, and Client modes.
Chapter 4.: Hardware Description and Installation	Describes the front and rear panels of SMCWEB-N2 and hardware installation.
Chapter 5.: Configuring Your Computer and Wireless Connection	Describes how to set the TCP/IP for your computer and how to connect to SMCWEB-N2 wirelessly.
Chapter 6.: Configuring SMCWEB-N2	Describes how to configure SMCWEB-N2 for the Bridge, Router, Wireless Universal Repeater, WDS, and Client modes in a quick and basic way.
Chapter 7.: Web Configuration for the Bridge Mode	Describes how to use to Web page to configure parameters for the Bridge mode.
Chapter 8.: Web Configuration for the Router Mode	Describes how to use to Web page to configure parameters for the Router mode.
Chapter 9.: Web Configuration for the Wireless Universal Repeater Mode	Describes how to use to Web page to configure parameters for the Wireless Universal Repeater mode (URM).

Chapter 10.: Web Configuration for the WDS Mode	Describes how to use to Web page to configure parameters for the WDS mode.
Chapter 11.: Web Configuration for the Client Mode	Describes how to use to Web page to configure parameters for the Client mode.

Features

- Support IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i, and IEEE802.11e
- Provide wireless transmission rate up to 300 Mbps
- Support WEP and WPA for secure data transmission
- Support DHCP server
- Support manually configuring static routing
- Support software upgrade through Web pages
- Support restoring factory default settings
- Support demilitarized zone (DMZ)
- Support DNS proxy and forwarding
- Support UPnP
- Support WPS
- Support port forwarding
- Support port triggering
- Support wireless repeater
- Support guest network
- Support filtering by keyword and domain name
- Support wireless security authentication
- Support 5 types of WAN connection modes, including static IP, dynamic IP, PPPoE, PPTP and L2TP
- Support remote access control
- Support firewall
- Support system status display
- Support backing up and restoring configuration files

1 Safety Precautions

Before operating SMCWEB-N2, read the following precaution information carefully:

- Leave proper space for heat dissipation to avoid damage caused by device overheating. Heat dissipation holes enable the device to work normally. Do not cover heat dissipation holes.
- Keep the device away from heat outlets or high temperature places. Prevent the device from direct sunlight.
- Keep the device in dry places. Do not spill any liquid on this device.
- Do not connect the device to any PC or electronic product unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risks.
- Do not place this device on an unstable surface.

2 Overview

2.1 Product Introduction

Thank you for choosing the SMCWEB-N2 Wireless N Universal Repeater. SMCWEB-N2, a pocket router, is case-shaped, easy to carry, and easy to install. Its wireless transmission rate is up to 300 Mbps. It is a high-performance and IEEE802.11b/g/n-compatible network access device that can provide reliable and convenient network access service for individual users and SOHO (Small Office, Home Office). It features Web-based GUI, allowing users to easily modify settings to connect the device to ISP (Internet Service Provider) and conveniently perform upgrade using the WEB page.

In addition, SMCWEB-N2 has a three-way switch on the side panel that enables users to change the device's working mode among AP, Repeater, and Client. In the AP mode, the device functions as a wireless router to achieve wireless connection for the wired LAN. In the Repeater mode, the device provides the URM (Universal Repeater Mode) function for users to expand wireless coverage of the existing AP in a quick and easy way. In the Client mode, the device functions as a wireless network adapter but it can provide a better transmission and connection performance.

2.2 Packing List

Please check whether your packing list includes the following items:

- Wireless N Universal Repeater
- 1 RJ-45 Cable
- CD with user manual, Source code, GPL license(s), GPL disclaimer
- Quick Installation Guide
- Warranty/Support card
- GPL Disclaimer

3 Mode Introduction

3.1 Bridge Mode

In the Bridge mode, SMCWEB-N2 works as a wireless router to achieve wireless connection for the wired LAN.

3.2 Router Mode

In the Router mode, SMCWEB-N2 works as a domestic gateway.

3.3 Wireless Universal Repeater/WDS Mode

In the Wireless Universal Repeater/WDS mode, SMCWEB-N2 expands wireless coverage of the existing AP. Computers can connect to SMCWEB-N2 in either a wired or wireless way.

3.4 Client Mode

In the Client mode, SMCWEB-N2 provides Internet access for a set-top box or a computer with a network adapter.

4 Hardware Description and Installation

4.1 Hardware Description

4.1.1 Front Panel and LED Status

There are 4 LED indicators on the front panel of SMCWEB-N2. By observing their status, you can check whether the device runs normally.

Table 4.1 SMCWEB-N2 indicator status

Indicator	Color	Status	Description
Power	Green	On	The device is working normally.
	Red	On	The system is in the process of self-inspection or fails the self-inspection. Or it is in the process of software upgrade.
WPS	Green	Off	The WPS session is down.
		On	The **WPS** indicator keeps on for 5 minutes after WPS (Wi-Fi Protected Setup) connection succeeds.
		Quick	A terminal is attempting to connect to the

		blink	SMCWEB-N2 through WPS but fails.
		Quick blink with a certain interval	Multiple terminals are connecting to the SMCWEB-N2 through WPS at the same time. WPS sessions conflict.
		Slow blink	The WPS session is up.
Ethernet	Green	Off	The Ethernet port is in the non-communication state.
		On	The Ethernet port is in the communication state.
		Blink	The Ethernet port is transmitting and receiving data.
WLAN	Green	Off	The WLAN connection is in the non-communication state.
		On	The WLAN connection is in the communication state.
		Blink	Data is being transmitted and received in the WLAN.

4.1.2 Side Panel and Interface Description

Side Panel

Table 4.2 SMCWEB-N2 interface and button status

Interface/Button	Description
WAN/LAN	If SMCWEB-N2 is set to the AP mode, the interface is a WAN interface which connects SMCWEB-N2 to WAN or uplink network devices. If SMCWEB-N2 is set to the Repeater/Client mode, the interface is an LAN interface.
Reset	Press the **Reset** button gently for 3-6 seconds and then release it. The system restores to the factory default settings.
AP/Repeater/Client	It is used for setting SMCWEB-N2 to the AP, Repeater, or Client mode. AP mode—including the Bridge and router modes Repeater mode—to expand wireless network coverage Client mode—equivalent to a wireless network adapter
WPS	For enabling WPS PBC mode. For more information, refer to WPS descriptions for each mode.

4.2 Hardware Installation

4.2.1 System Requirements

Before installing the device, please ensure that the following items are available:

- At least one Ethernet RJ45 cable (10BASE-T/100BASE-T)
- One SMCWEB-N2 Wireless N Universal Repeater
- A PC is already installed with the TCP/IP protocol and the PC can access the Internet.

4.2.2 Before You Begin

Before you install the device, please pay attention to the following items:

- The Ethernet cables that are used to connect the device to a computer, hub, router, or switch should be less than 100 meters.
- Do not place this device on an uneven or unstable surface. Do not put this device on the ground.
- Keep the device clean. Prevent the device from direct sunlight. Avoid any metal in the device.
- Place the device in the center of the area to optimize the wireless coverage.

4.3 Operation Range

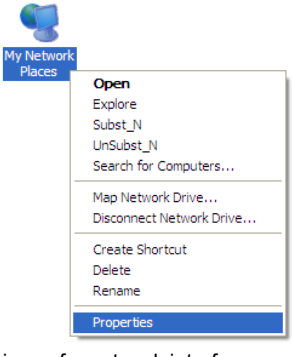
The operation range of SMCWEB-N2 depends on the actual environment. The path and effect of signal transmission vary with the deployment in a house or an office. For example, the outdoor straight transmission distance for a certain device can reach 300 meters and the indoor transmission distance can reach 100 meters.

5 Configuring Your Computer and Wireless Connection

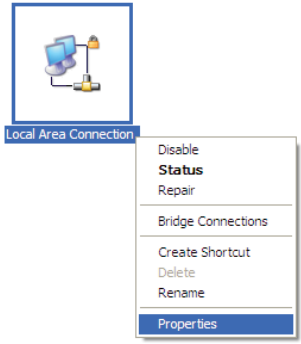
5.1 Configuring Your Computer

The following takes Windows XP as an example. Do as follows to manually set the network adapter:

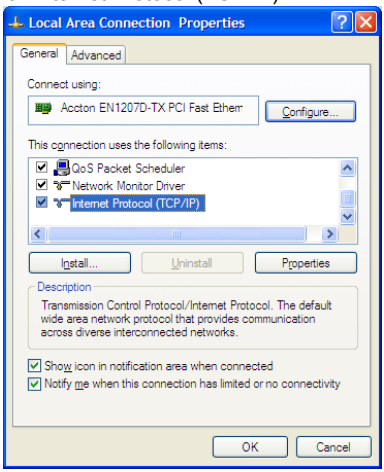
Step 1 Right-click the icon of **My Network Places** and choose **Properties** to display the **Network Connections** window.



Step 2 Right-click the icon of a network interface card or wireless network adapter and choose **Properties**. (Note: In the Client mode, computers can connect to SMCWEB-N2 through an Ethernet cable only.)

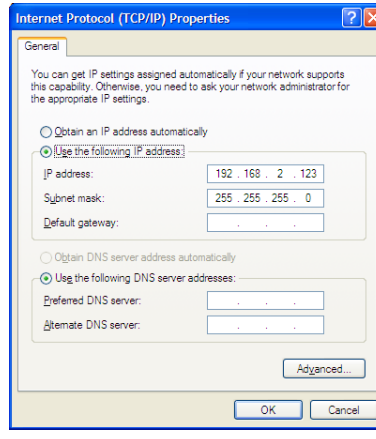


Step 3 Double-click Internet Protocol (TCP/IP).



Step 4 (1) When SMCWEB-N2 is set to the Router mode, select **Obtain an IP address automatically**.

(2) When SMCWEB-N2 is set to other modes, set the IP address of your computer to **192.168.2.X** (X is an integer in the range of 2 to 253), and the MAC address to 255.255.255.0. Set the gateway and the IP address of the DNS server. You can leave them blank if you do not know information about the gateway and DNS server. Click **OK**.



Note:

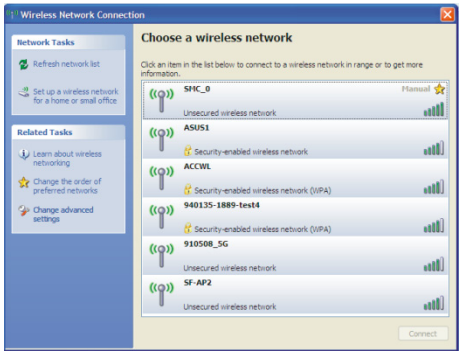
After you finish configuring SMCWEB-N2, the domestic gateway can set the Internet protocol for the PC's network adapter. Set the IP address and DNS server to Obtain an IP address automatically as shown in the figure above.

5.2 Configuring Wireless Configuration

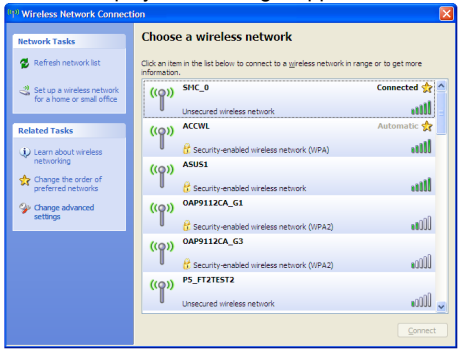
The following takes Windows XP as an example. Do as follows to connect the wireless network adapter of your PC to SMCWEB-N2:

Step 1 Click the icon displayed at the right bottom corner of the desktop (Note: Ensure that your PC is installed with a wireless network adapter).

Step 2 In the **Wireless Network Connection** page, double-click the desired wireless network.



Step 3 Your computer successfully connects to the wireless network when **Connected** is displayed on the right upper corner.



Note:

The default SSID of SMCWEB-N2 is SMC_0.

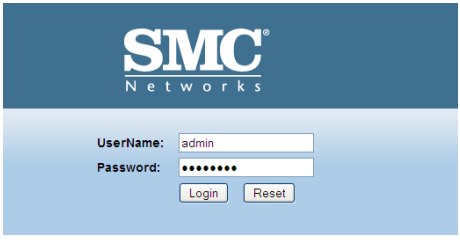
6 Configuring SMCWEB-N2

Table 6.1 IP information of AP/Repeater/Client modes of SMCWEB-N2

Mode On the Case	Mode Available In the Web	Management IP Address	Subnet MAC Address	DHCP	Way of connecting to PC
AP	Bridge (default)	192.168.2.1	255.255.255.0	Disable	Ethernet cable /Wireless
	Router			Enable	Wireless only
Repeater	Wireless Universal Repeater (default)	192.168.2.1	255.255.255.0	Disable	Ethernet cable /Wireless
	WDS				
Client	Client (default)	192.168.2.1	255.255.255.0	Disable	Ethernet cable only

Step 1 Set the three-way switch on the case of SMCWEB-N2 to the mode you want.

Run the Internet Explorer (IE). Enter the management IP address of **192.168.2.1** and press **Enter**. In the login window that is displayed, enter the user name **admin** and password **smcadmin**, and click **Login**.

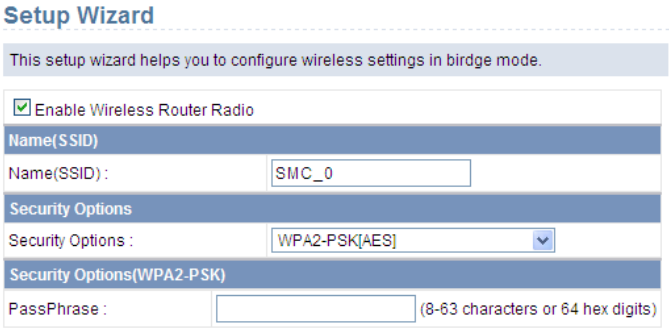


Step 2 Configure parameters for the mode you selected. Terminal devices can access the network through SMCWEB-N2 after you finish configuration by following procedures in the sections below.

6.1 Bridge Mode Configuration

Step 1 Set the three-way switch on the side panel to **AP** after SMCWEB-N2 is powered on. Log in to the configuration page after the system is started.

Step 2 Click **Setup Wizard** in the navigation bar on the left pane of the page. Set the SSID and encryption password and note them down. Click **Finish** to complete the settings.



6.2 Router Mode Configuration

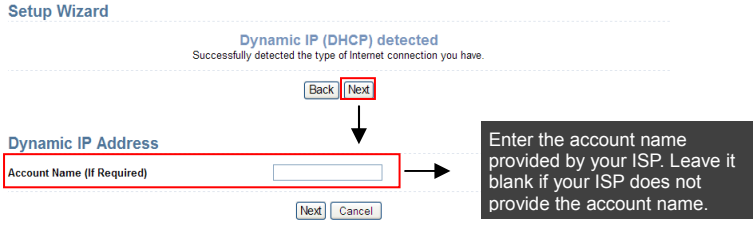
Step 1 Set the three-way switch on the side panel to AP after SMCWEB-N2 is powered on. Log in to the configuration page after the system is started.

Step 2 Click **Mode Settings** and select **Router Mode**. (The default mode is **Bridge Mode**.)

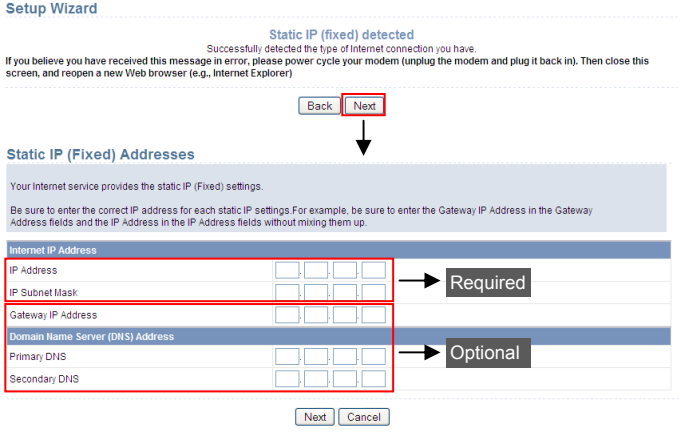
Step 3 Connect your PC to SMCWEB-N2 using a wireless network adapter after SMCWEB-N2 is restarted successfully. Log in to the configuration page. Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **Yes** and click **Next**. SMCWEB-N2 will automatically detect the broadband type.

Step 4 SMCWEB-N2 can detect three types of broadband: DHCP, Static IP, and PPPoE. Perform configurations according to the broadband type you are using.

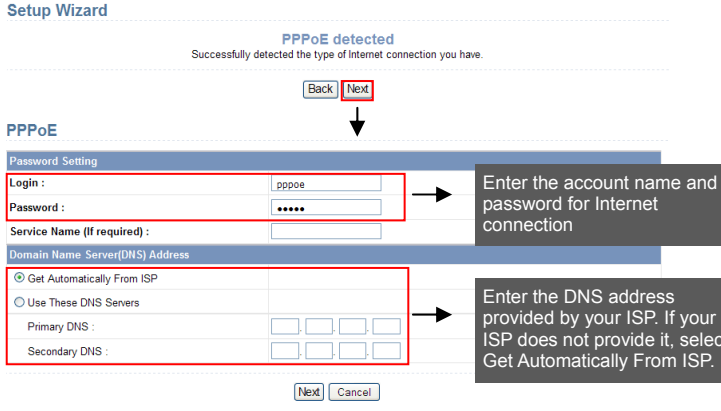
Parameter configuration for DHCP



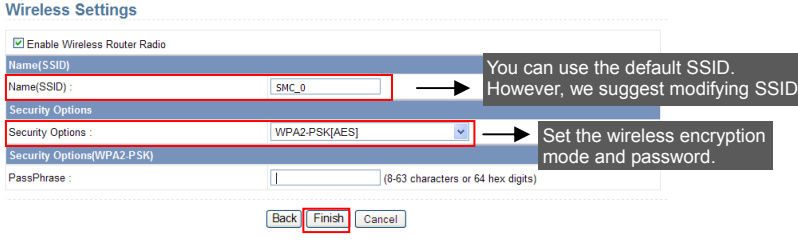
Parameter configuration for static IP



Parameter configuration for PPPoE



Step 5 CliCk **Next**. Set the SSID and password and note them down. Click **Finish** to complete the settings.



6.3 Repeater Mode Configuration

Step 1 Set the three-way switch on the side panel to **Repeater** after SMCWEB-N2 is powered on. Log in to the configuration page after the system is started.

Step 2 Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **Wireless Universal Repeater Mode** and click **Next**.

Setup Wizard

Step1: There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or Wireless Universal Repeater Mode.

Please choose your repeater mode as follows:

- ○ WDS Mode
- ◉ Wireless Universal Repeater Mode

Next

Step 3 Click **Site Survey** to search for the wireless network you want to connect. Select a desired network. Click **Next**.

Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

Site Survey

Number of Sites Scaned :17

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	SF-AP2	00:13:F7:DC:EB:98	6	76%	None	◉
2	ASUS1	00:1E:8C:4A:C4:66	1	70%	WEP	○
3	ACCWL	D8:C7:C8:CD:03:CA	6	70%	WPA-1X(TKIP)	○
4	950079-3389-V0	00:11:88:06:36:10	11	65%	WPA2-1X(AES)	○

Next

Step 4 Configure the repeater with the same security option as its uplink network. (The following figure takes the security option of **None** as an example.) Set the encryption password and note it down. Click **Next**.

Wireless Client Function

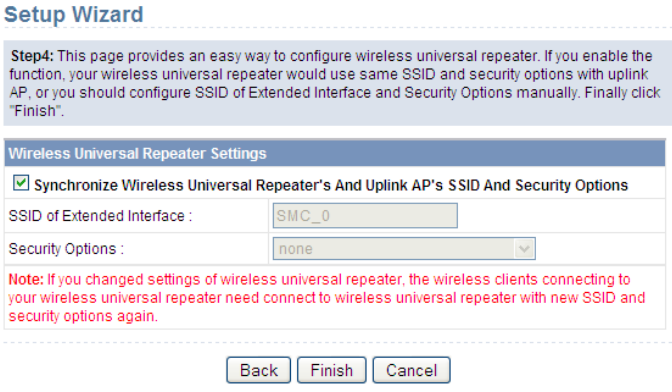
Step2: You should configure your wireless client manually so it has the same wireless security settings as the network which you selected. Then click "Next".

Security Options

Security Options : None

Back Next

Step 5 SMCWEB-N2 provides the wireless roaming function if you select **Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options**. Otherwise, manually configure the SSID and security options for the repeater. Click **Finish** to complete setup wizard.

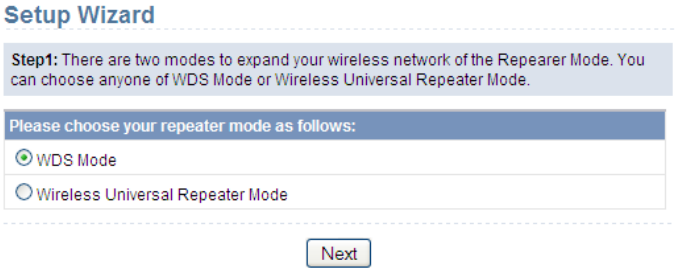


6.4 WDS Mode Configuration

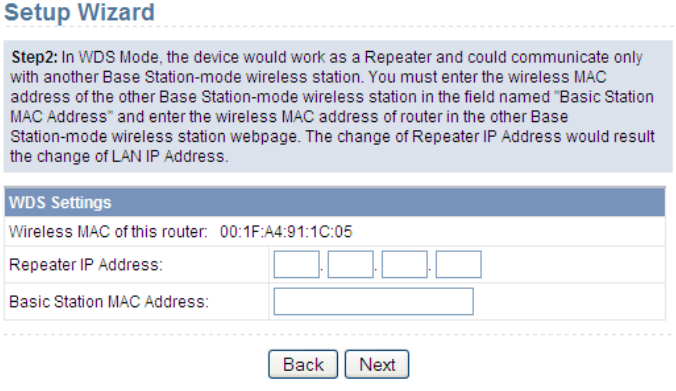
6.4.1 Repeater Configuration in the WDS Mode

Step 1 Set the three-way switch on the side panel to **Repeater** after SMCWEB-N2 is powered on. Log in to the configuration page after the system is started.

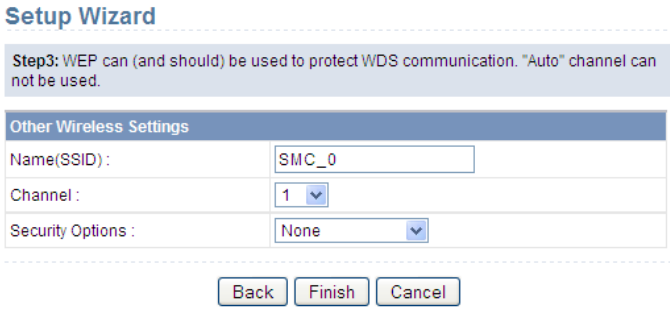
Step 2 Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **WDS Mode** and click **Next**. (Note: The WDS function cannot be used if the channel is set to **Auto**) Manually set all WDS devices to the same channel.



Step 3 Set the IP address of the LAN port of the repeater and enter the MAC address of the basic station. Click **Next**.



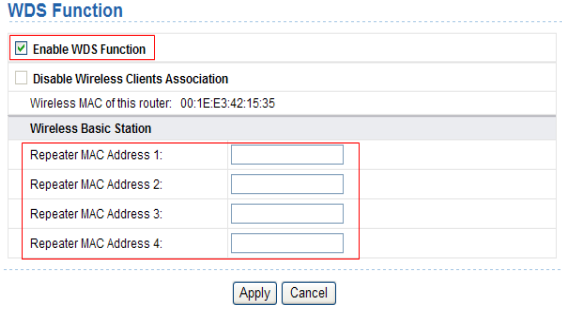
Step 4 Set the SSID, channel, and security encryption for the repeater. The channel cannot be set to **Auto**. It is recommended to configure the repeater with the same security option as its base station. Set the encryption password and note it down. Click **Finish** to complete the settings.



6.4.2 Central Base Station Configuration in the WDS Mode

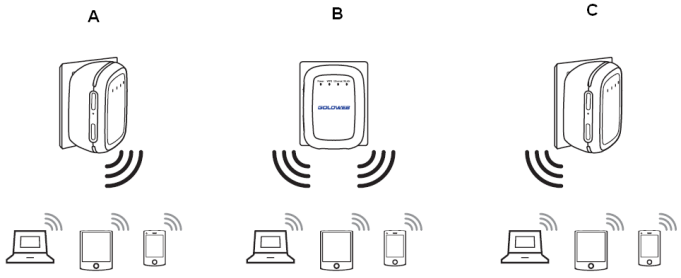
Step 1 Set SMCWEB-N2 to the Router mode.

Step 2 Choose **Wireless Settings** > **WDS Function**, select **Enable WDS Function**, and enter the MAC address of the Repeater (Note: One basic station can connect to a maximum of 4 repeaters).



6.4.3 WDS Application

The following figure shows a wireless network for Humans Resource Department (marked as A in the figure), Finance Department (marked as B), and Marketing Department (marked as C) in an enterprise. If the three departments share one Wireless N Universal Repeater, signals searched by computers may be rather weak or even no signals are available. However, if each of the three departments uses a Wireless N Universal Repeater, we can use WDS to connect the three routers to provide perfect wireless coverage for the whole areas.



Configure the three routers in this way:
Wireless N Universal Repeater B functions as the wireless basic station; Wireless N Universal Repeaters A and C connect to Wireless N Universal Repeater B by using WDS.

(1) Configuring Wireless N Universal Repeater B as the wireless basic station

Step 1 Log in to the Web management page of Wireless N Universal Repeater B. Choose **Wireless Settings** > **Wireless Basic Settings** and set the SSID, channel, and wireless encryption information. Write down the SSID, channel, and wireless encryption information that are required when you are configuring wirelss router A and C.

Step 2 Choose **Wireless Settings** > **WDS Function** and enable the WDS function. Enter MAC addresses of repeaters (that is, Wireless N Universal Repeaters A and C in this example). Click **Apply** to save the settings.

(2) Configuring Wireless N Universal Repeater A

Do as follows to establish WDS connection between Wireless N Universal Repeaters A and B:

Step 1 Set Wireless N Universal Repeater A with the same channel and encryption information as Wireless N Universal Repeater B.

Step 2 Choose **Wireless Settings** > **WDS Function** and enable the WDS function. Set the IP address of Wireless N Universal Repeater B different from that of Wireless N Universal Repeater B to avoid IP address conflict (for example, change the IP address to 192.168.2.20 in the **LAN**

Interface Settings page and log in to the Web management page again). Enter the MAC address of the wireless basic station.

Step 3 Click **Apply** to save the settings.

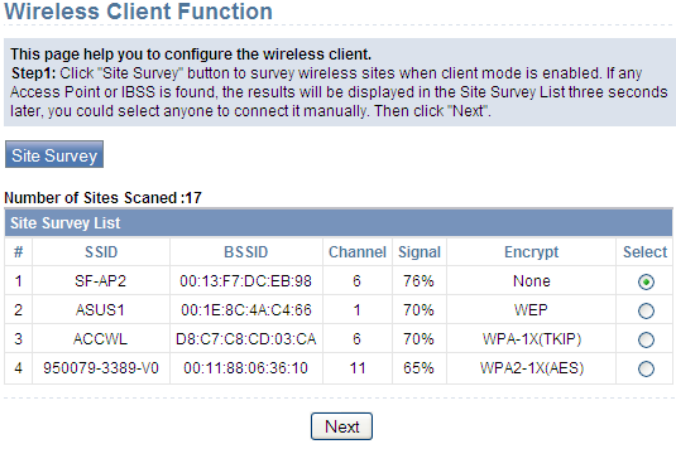
Then, WDS connection is established between Wireless N Universal Repeaters A and B.

(3) Configuring Wireless N Universal Repeater C

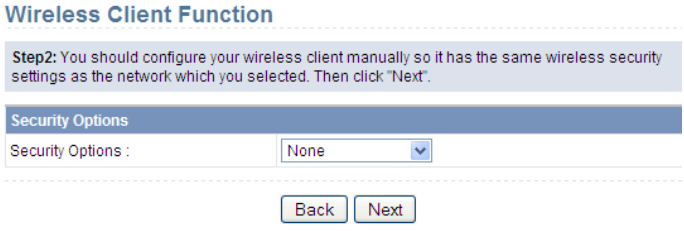
Configure Wireless N Universal Repeater C in the same way as Wireless N Universal Repeater A. Note that the IP address of the LAN interface must be changed to an IP address that does not conflict with IP addresses of existing computers or devices in the network.

6.5 Client Mode Configuration

Step 1 Click **Setup Wizard** in the navigation bar on the left pane of the page. Click **Site Survey** to search for the wireless network you want to connect.



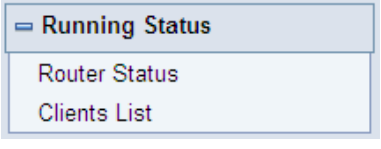
Step 2 Enter encryption information of the selected wireless network. Click **Finish** to complete the settings.



7 Web Configuration for the Bridge Mode

7.1 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:



Click the submenu to enter a specific configuration page.

7.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

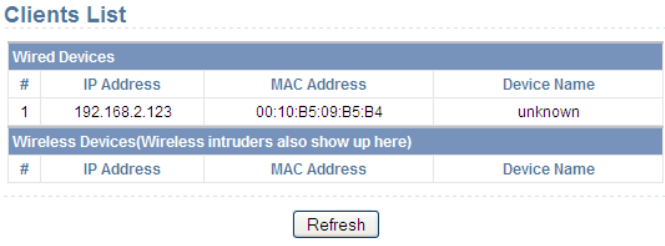
Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	SMCWEB-N2
Work Mode	Bridge Mode
Time and Date	1971-01-01 10:14:14
LAN Port	
MAC Address	00:1F:A4:91:1C:03
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	SMC_0
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

In this page, you can view information about the current running status of SMCWEB-N2, including system information, LAN port status, and wireless network status.

7.1.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.



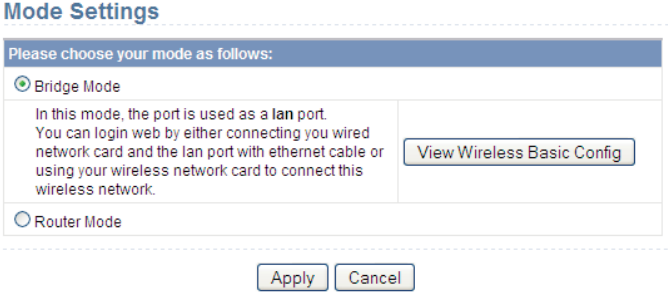
This page displays information of computers connected to the router, including the IP adress, and MAC address of each computer.

7.2 Setup Wizard

For settings, refer to section 6.1 “Bridge Mode Configuration”.

7.3 Mode Setting

Click **Mode Settings** and the **Mode Settings** page is displayed.

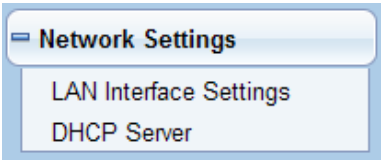


- **Bridge Mode**: The interface on its case is an LAN interface. Users can connect SMCWEB-N2 and the PC using an RJ45 cable or a wireless network card.

- **Router Mode**: Computers can connect to SMCWEB-N2 in a wireless way only.

7.4 Network Settings

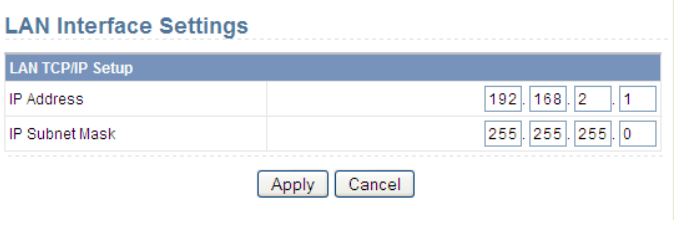
Click **LAN Interface Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

7.4.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.



You can modify the IP address and IP subnet mask of the LAN port as required.

Note:

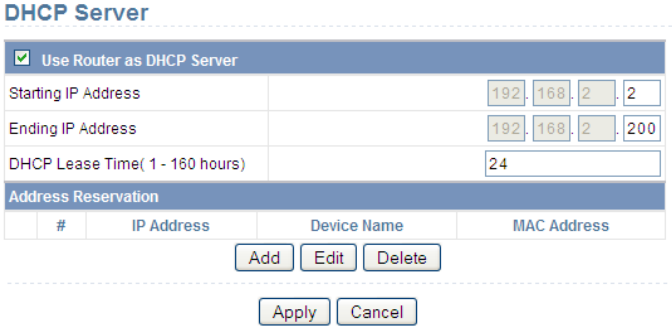
If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

7.4.2 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, SMCWEB-N2 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

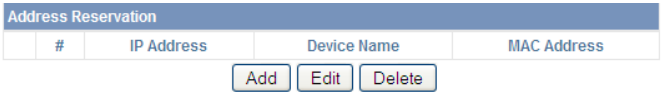


7.4.2.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server**: If you select the **Use Router as DHCP Server** check box, SMCWEB-N2 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address**/**Ending IP Address**: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address**/**Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

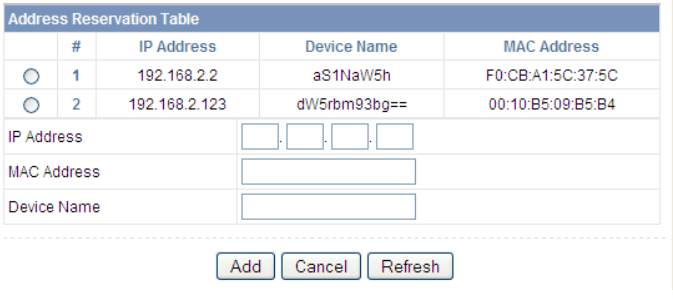
7.4.2.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.



To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.



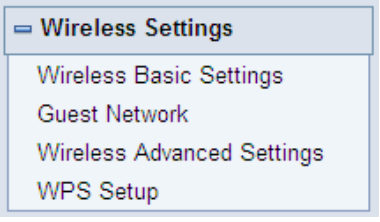
Step 2 Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.2.x). Enter the MAC address and device name of the computer or server.

Step 3 Click **Add** to add a new item into **Address Reservation**.

Step 4 Click **Apply** to save the settings.

7.5 Wireless Settings

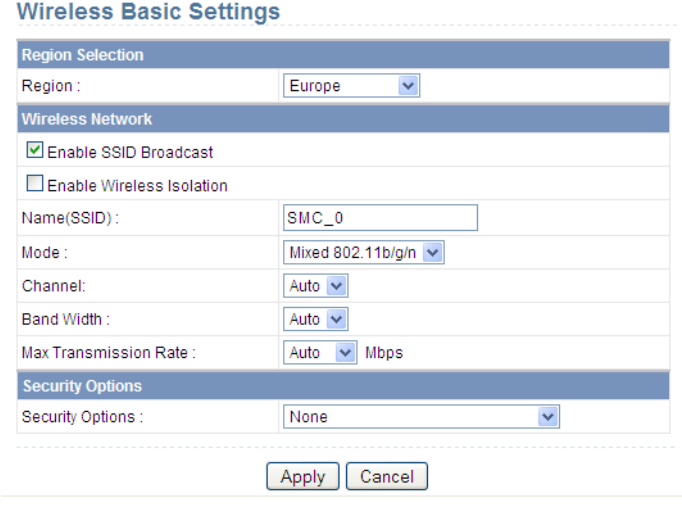
Click **Wireless Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

7.5.1 Wireless Basic Settings

Choose **Wireless Settings** > **Wireless Basic Settings** and the **Wireless Basic Settings** page is displayed.



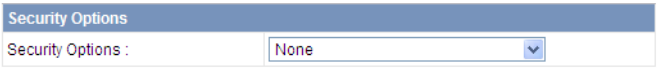
- **Region**: Select the region where you are located.
- **Enable SSID Broadcast**: If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.

- **Enable Wireless Isolation**: If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Name (SSID)**: Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive.
- **Mode**: Select the wireless mode. **Mixed 802.11b/g/n** is recommended.
- **Channel**: The channel for transmitting wireless signals. The default channel is **Auto**. When you select **Auto**, SMCWEB-N2 automatically selects the best channel from the available channels according to actual situations.
- **Band Width**: The bandwidth occupied for wireless signal transmission.
- **Max Transmission Rate**: The maximum transmission rate of SMCWEB-N2.
- **Security Options**: Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

– None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.



– **WEP**

Wired equivalent privacy. You can use WEP 64- or 128-bit encryption.

Security Options	
Security Options :	WEP
Security Encryption(WEP)	
Authentication Type :	Automatic
Encryption Type :	ASCII
Encryption Strength :	64 bits
Security Encryption(WEP) Key	
Key 1:	(5 ASCII characters)
Key 2:	(5 ASCII characters)
Key 3:	(5 ASCII characters)
Key 4:	(5 ASCII characters)

Apply Cancel

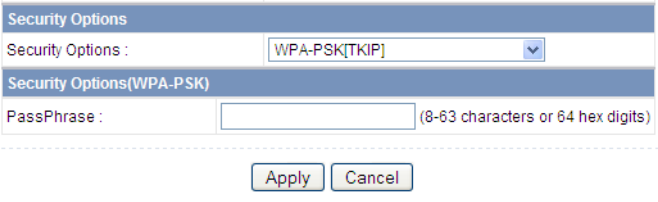
- **Authentication Type**: Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and Shared keys.
  - **Automatic**: If selected, the router uses an authentication type of **Open** or **Shared keys** according to the request of the host.
  - **Open**: If selected, hosts in the wireless network can pass the authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.
  - **Shared keys**: If selected, hosts in the wireless network can pass authentication only when the correct password is entered. Otherwise, the hosts cannot connect to the wireless network.
- **Encryption Type**: The type of the key to be set. Hexadecimal and ASCII code are available.
  - **Hex**: Valid characters for keys contain 0–9 and A–F.
  - **ASCII**: Valid characters for keys contain all characters of the key board.
- **Encryption Strength**: The encryption strength determines the length of the key.
  - If **Encryption Strength** is set to **64 bits**, set the key to 10 hexadecimal digits or 5 ASCII characters.

– If **Encryption Strength** is set to **128 bits**, set the key to 26 hexadecimal digits or 13 ASCII characters.

- **Key 1/2/3/4**: Set the key based on the selected encryption type and encryption strength.

– WPA-PSK[TKIP] or WPA2-PSK[TKIP]

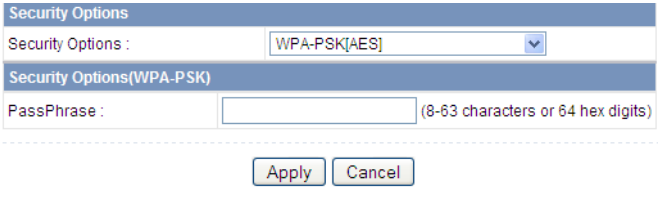
WPA-PSK: Preshared key Wi-Fi protection access
WPA2-PSK: Preshared key Wi-Fi protection access version 2
TKIP: Temporal Key Integrity Protocol
Note that the 802.11n mode does not support the TKIP algorithm.



- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

– WPA-PSK[AES] or WPA2-PSK[AES]

WPA-PSK: Preshared key Wi-Fi protection access.
WPA2-PSK: Preshared key Wi-Fi protection access version 2.
AES: Advanced Encryption Standard



- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

– WPA-PSK/WPA2-PSK+[TKIP]/[AES]

It allows the client to use either WPA-PSK[TKIP]/[AES] or WPA2-PSK [TKIP]/[AES].

- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

Note:

After you complete configuring wireless settings for SMCWEB-N2, only hosts that have the same wireless settings (for example, the SSID) as SMCWEB-N2 can connect to it. If you configure security settings for SMCWEB-N2, hosts must have the same security settings (for example, the password) as SMCWEB-N2 in order to connect to SMCWEB-N2.

7.5.2 Guest Network

If you do not want visitors to know your wireless security key, you can use the guest network to allow them to use your Internet without knowing your wireless connection password.

Choose **Wireless Settings** > **Guest Network** and the **Guest Network** page is displayed.

Guest Network

Network Profiles

	Scheme	SSID	Security	Apply	SSID Broadcast
◉	1	SMC_02	None	NO	YES
○	2	SMC_03	None	NO	YES
○	3	SMC_04	None	NO	YES
○	4	SMC_05	None	NO	YES

Wireless Settings--Profile 1

☐ Enable Guest Network

☑ Enable SSID Broadcast

☐ Allow Guest to access My Local Network

☐ Enable Wireless Isolation

Guest Wireless Network Name(SSID) : SMC_02

Security Options--Profile 1

Security Options : None

Apply Cancel

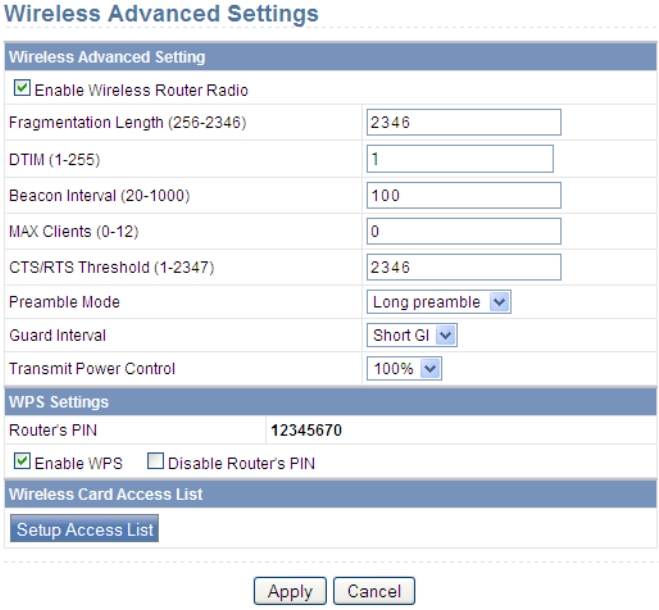
- **Network Profiles**: Brief description of the created guest network. You can create up to four guest networks. A network profile contains the SSID and encryption mode, whether to use the guest network, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.
- **Enable Guest Network**: If enabled, both you and visitors can connect to the network by using the SSID of the guest network.
- **Enable SSID Broadcast**: If enabled, SMCWEB-N2 broadcasts its SSID to all wireless stations.
- **Allow Guest to access My Local Network**: If enabled, visitors using the SSID of a guest network can access not only the Internet but also the LAN of SMCWEB-N2, like users using the primary SSID of the network. If disabled, visitors using the SSID of a guest network cannot access the LAN of SMCWEB-N2.
- **Enable Wireless Isolation**: If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Guest Wireless Network Name (SSID)**: Set the name of the guest network.

- **Security Options**: Refer to security option descriptions in section 8.5.2 “Wireless Basic Settings”.

After finishing settings, click **Apply** to save the settings.

7.5.3 Wireless Advanced Settings

Choose **Wireless Settings** > **Wireless Advanced Settings** and the **Wireless Advanced Settings** page is displayed.



- **Enable Wireless Router Radio**: If you disable the wireless router radio, wireless devices cannot connect to the SMCWEB-N2 router. If you do not use your wireless network for a period of time, you can clear this check box and disable all wireless connectivity.
- **Fragmentation Length (256-2346)**: Set the threshold of fragmentation length. If the length of a packet exceeds the set value, the packet is automatically fragmented into several packets. The value of **Fragmentation Length** cannot be too small because excessive packets reduce wireless network performance. The default value is 2346.
- **DTIM (1-255)**: Set the interval for sending DTIM frames.

- **Beacon Interval (20-1000)**: The beacon interval is the frequency of sending Beacon frames. Set the interval for sending Beacon frames. The unit is millisecond (ms). The default value is 100 ms.
- **MAX Clients (0-12)**: Set the maximum number of clients. 0 indicates the number of connected clients is not limited.
- **CTS/RTS Threshold (1-2347)**: Set the CTS/RTS threshold. If the length of a packet is greater than the specified RTS value, SMCWEB-N2 sends an RTS frame to the destination station to negotiate. After receiving an RTS frame, the wireless station responds with a Clear to Send (CTS) frame to SMCWEB-N2, notifying that they can communicate with each other.
- **Preamble Mode**: A preamble (especially the **802.11b High Rate/DSSS PHY** field; 56 digits synchronized field for short preamble) defines the length of the CRC correction block for communication between wireless devices. Short preamble should be applied in a network with intense traffics. It helps improve the efficiency of a wireless network responding to applications that have high requirement of real-time, such as streaming video and voice-over-IP telephony.
- **Guard Interval**:
  - Short GI: The interval is 400 ns. When short GI is enabled, SMCWEB-N2 can receive and send short-frame-interval packets. This helps improve the transmission rate of SMCWEB-N2.
  - Long GI: The interval is 800 ns.
- **Transmit Power Control**: Set the transmit power of the wireless network. It is recommended to use the default setting of **100%**.
- **Router's PIN**: Display the PIN to be used for the wireless client when wireless settings of the router are configured through WPS.
- **Enable WPS**: Functions in the **WPS Setup** page are available only after the **Enable WPS** check box is selected. If the check box is not selected, the **WPS Setup** menu item is greyed out.
- **Disable Router's PIN**: The PIN mode function in the **WPS Setup** page is available only when the **Disable Router's PIN** check box is not selected. If the check box is selected, the PIN mode option is unavailable.

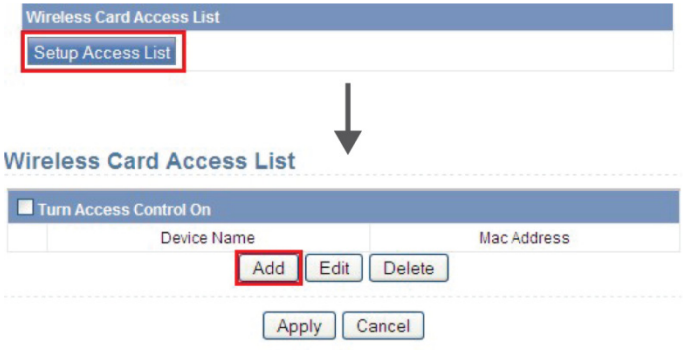
Restricting wireless access by MAC address

When a wireless card access list is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computer list.

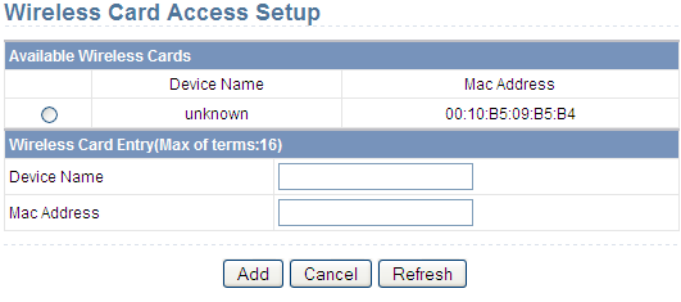
The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only. The MAC address is in the format of XX:XX:XX:XX:XX:XX.

To restrict wireless access by MAC address:

Step 1 Click **Setup Access List** button in the **Wireless Advanced Settings** page to display the **Wireless Card Access List** page.



Step 2 Click **Add** to add a wireless device to the wireless access control list. The **Wireless Card Access Setup** page is displayed.



Step 3 If the computer you want appears in the **Available Wireless Cards** list, you can select the radio button of that computer to obtain its MAC address. Otherwise, you can manually enter a name and MAC address of the computer to be authorized. Generally, the MAC address is labeled on the bottom of the wireless device.

Step 4 Click **Add** to add this wireless device to the wireless card access list. The page jumps to the list page.

Step 5 Select **Turn Access Control On**. If selected, you can restrict PCs' access to the wireless network, only allowing specified PCs to access your network according to their MAC addresses.

Step 6 Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the SMCWEB-N2 router.

7.5.4 WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

The following describes how to configure WPS for the AP mode.

7.5.4.1 Using the WPS Button

In the AP mode with WDS disabled, press the **WPS** button on the side panel of SMCWEB-N2 and the **WPS** button on the client device. SMCWEB-N2 can perform WPS encrypted connection to the downlink client device.

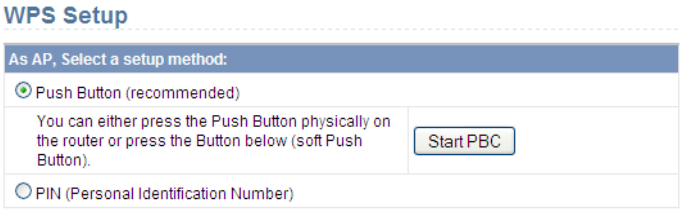
7.5.4.2 Using the Web Page

You can perform WPS settings using the Web page for configuration.

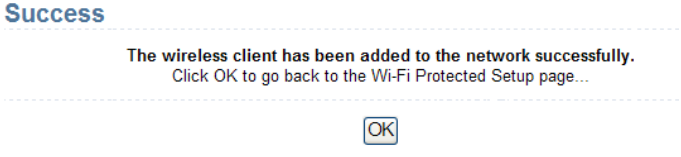
Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

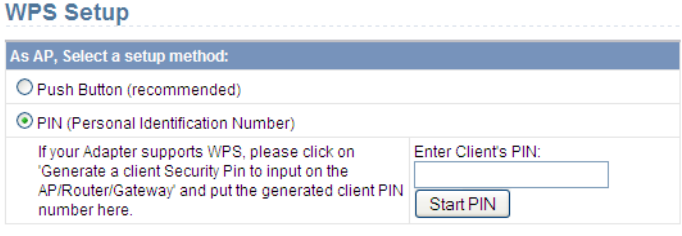


Step 2 Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

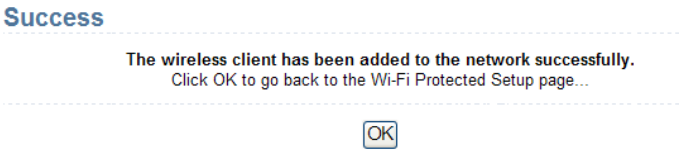


- PIN mode

Step 1 Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.

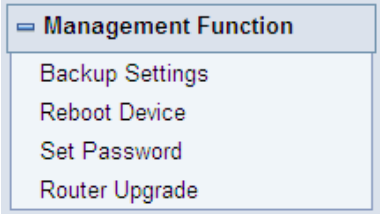


Step 2 Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



7.6 Management Function

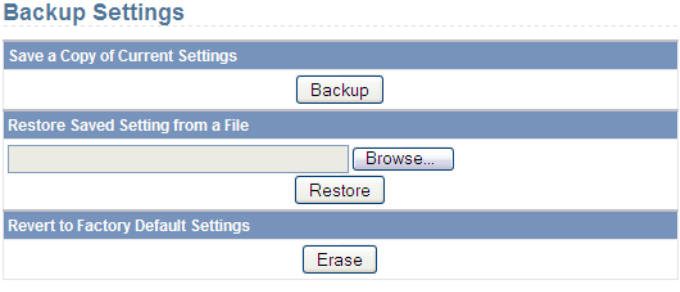
Click **Management Function** and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

7.6.1 Backup Settings

Choose **Management Function** > **Backup Settings** and the **Backup Settings** page is displayed.



In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.

Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.

Click **Browse…** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

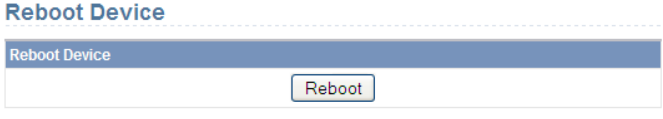
- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

7.6.2 Reboot Router

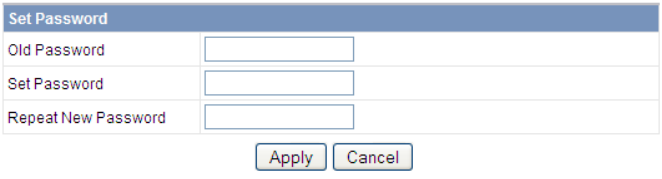
Choose **Management Function** > **Reboot Router** and the **Reboot Router** page is displayed.



Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

7.6.3 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.



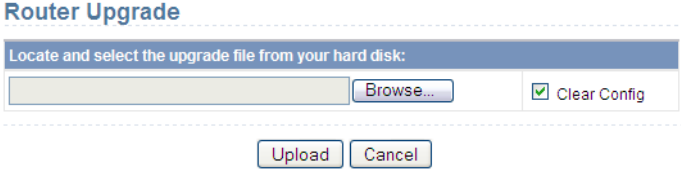
In this page, you can change the login password.

Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

7.6.4 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.



To upgrade the software of the router:

Step 1 Click **Browse…** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade is finished. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.

Note:

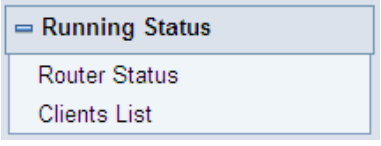
After the software upgrade, SMCWEB-N2 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software.

Do not power off the router during the upgrade.

8 Web Configuration for the Router Mode

8.1 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:



Click the submenu to enter a specific configuration page.

8.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	SMCWEB-N2
Work Mode	Router Mode
Time and Date	1971-01-01 08:21:12
Internet Port	
MAC Address	00:1F:A4:91:1C:03
Internet Access Mode	Connected(DHCP)
IP address	10.2.78.155
IP Subnet mask	255.255.254.0
Default Gateway	10.2.78.254
Domain Name Server	10.2.3.5,10.2.3.1,10.2.3.4
LAN Port	
MAC Address	00:1F:A4:91:1C:05
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	SMC_0
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

Show Statistics Connection Status

In this page, you can view information about the current running status of SMCWEB-N2, including system information, connection status of the Internet port, LAN port status, and wireless network status.

Click **Show Statistics** and the **Statistic Information** page as shown in the following figure is displayed:

Statistic Information

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	10728	19090	0	1194466	2467114	00:22:57
WLAN	Auto	18522	27740	0	9027136	3544186	00:23:39
System Up Time		00:23:56					

Poll Interval

5 (1~86400 secs) Set Interval Stop

In this page, you can view performance statistics information of SMCWEB-N2, including the numbers of sent and received packets at each port.

- **Set Interval**: Set the interval for traffic statistics.
- **Stop**: If you click this button, this page always displays statistics information that was refreshed for the last time and it is not refreshed any more.

Click **Connection Status** in the **Router Status** page, and the **Connection Status** page is displayed. This page displays current connection information of SMCWEB-N2.

The following takes WAN connection of **DHCP** as an example.

Connection Status

IP Address	10.2.78.155
Subnet Mask	255.255.254.0
Default Gateway	10.2.78.254
DHCP Server	10.2.3.4
DNS Server	10.2.3.5,10.2.3.1,10.2.3.4
Lease Obtained	3Day,0Hour,0Minute
Lease Expires	2Day,23Hour,36Minute

Release Renew

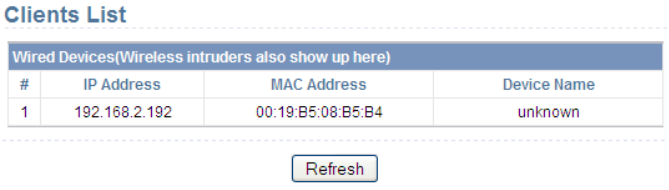
Close Window

- **Release**: Click the button and SMCWEB-N2 sends a request to the ISP for releasing the IP address, the subnet mask, the default gateway, and DNS server settings.
- **Renew**: Click the button and SMCWEB-N2 dynamically obtains an IP address, a subnet mask, the default gateway, and DNS server settings from the ISP. The information will be displayed in this page.

For details of WAN connection modes, refer to section 8.4.2 “WAN Interface Settings”.

8.1.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.



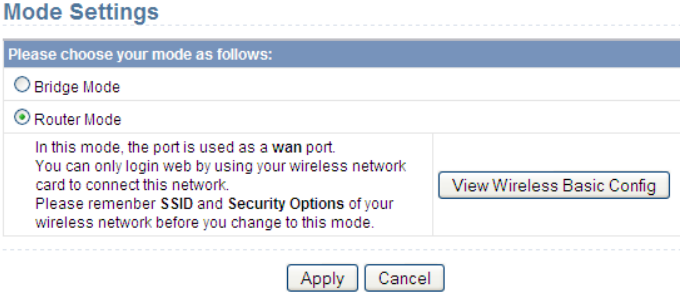
This page displays information of computers connected to SMCWEB-N2, including the IP adress and MAC address of each computer.

8.2 Setup Wizard

For settings, refer to section 6.2 “Router Mode Configuration”.

8.3 Mode Setting

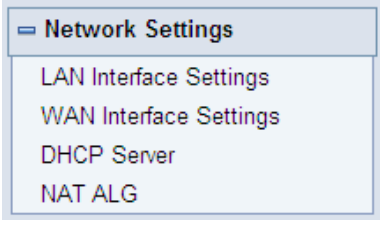
Click **Mode Settings** and the **Mode Settings** page is displayed.



- **Bridge Mode**: The interface on its case is an LAN interface. Users can connect SMCWEB-N2 and the PC using an RJ45 cable or a wireless network card.
- **Router Mode**: Computers can connect to SMCWEB-N2 in a wireless way only.

8.4 Network Settings

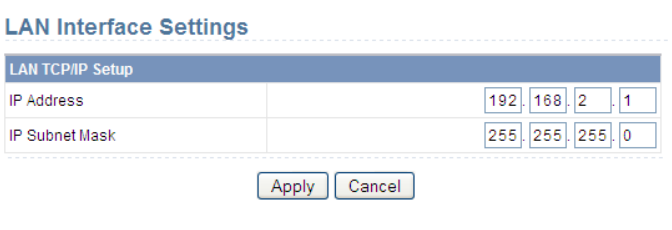
Click **Wired Network Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

8.4.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.



You can modify the IP address and IP subnet mask of the LAN port as required.

Note:

If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access. The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

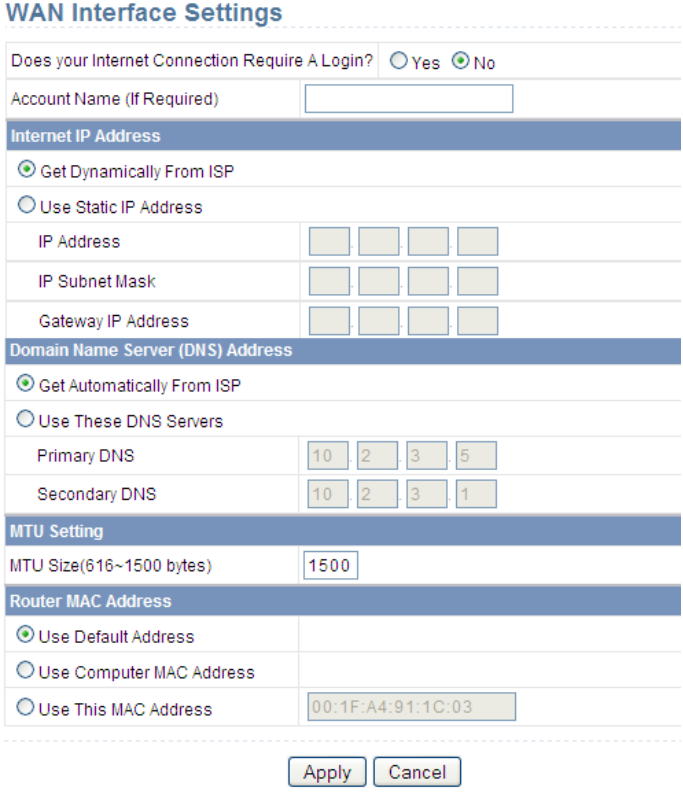
8.4.2 WAN Interface Settings

Choose **Network Settings** > **WAN Interface Settings** and the **WAN Interface Settings** page is displayed.

The router supports 5 modes of WAN connection, including **Dynamic IP (DHCP)**, **Static IP**, **PPPoE, PPTP, and L2TP**. Select the WAN connection you use. Contact your ISP if you do not know your WAN connection mode.

(1) Dynamic IP (DHCP)

If you select dynamic IP (DHCP), SMCWEB-N2 automatically obtains the IP address from the ISP automatically. Select DHCP when the ISP does not provide any IP network parameters. See the following figure:



- **Account Name**: The account name is provided by your ISP. If the ISP does not provide it, you can leave the item blank.
- **Domain Name Service (DNS) Address**: Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.
- **MTU Size**: Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address**: Physical address of the router.
  - Generally, select **Use Default Address**.
  - If the ISP requires MAC address authentication, Select **Use Computer MAC Address** or **Use This MAC Address**. If you select **Use Computer MAC Address**, the MAC address of the current computer serves as the MAC address of the router. If you select **Use This MAC Address**, you need to enter the MAC address of another computer. The format of an MAC address is XX:XX:XX:XX:XX:XX.

After finishing settings, click **Apply** to save the settings.

(2) Static IP

If the ISP provides the IP address, subnet mask, and information about the gateway and DNS server, select Static IP. Contact your ISP if you do not know the information.

WAN Interface Settings

Does your Internet Connection Require A Login?	○ Yes ◉ No
Account Name (If Required)	
Internet IP Address	
○ Get Dynamically From ISP	
◉ Use Static IP Address	
IP Address	. . .
IP Subnet Mask	. . .
Gateway IP Address	. . .
Domain Name Server (DNS) Address	
○ Get Automatically From ISP	
◉ Use These DNS Servers	
Primary DNS	. . .
Secondary DNS	. . .
MTU Setting	
MTU Size(616~1500 bytes)	1500
Router MAC Address	
◉ Use Default Address	
○ Use Computer MAC Address	
○ Use This MAC Address	00:1F:A4:91:1C:03

Apply Cancel

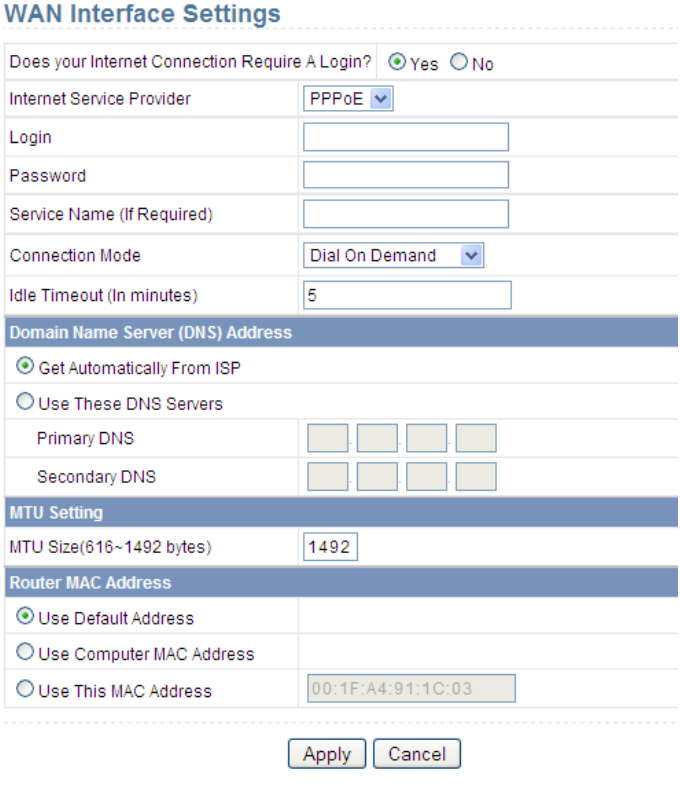
- **Account Name**: The account name is provided by your ISP. If the ISP does not provide it, you can leave the item blank.
- **IP Address**: Enter the WAN IP address provided by the ISP. The parameter must be entered.
- **IP Subnet Mask**: Enter the WAN subnet mask provided by the ISP. It varies with the network type. It is usually 255.255.255.0 (Class C).
- **Gateway IP Address**: Enter the IP address of the gateway provided by the ISP. It is the IP address used for connecting to the ISP.
- **Primary DNS**: Enter the IP address of the primary DNS server if necessary.
- **Secondary DNS**: Enter the IP address of that DNS server if the ISP provides another DNS server.

- **MTU Size**: Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address**: See descriptions on setting **Router MAC Address** for DHCP.

After finishing settings, click **Apply** to save the settings.

(3) PPPoE

If the ISP provides the user name and password for PPPoE (Point-to-Point Protocol over Ethernet) dialup, select **PPPoE**.



- **Login**: Enter the user name for PPPoE dialup provided by the ISP.
- **Password**: Enter the password for PPPoE dialup provided by the ISP.

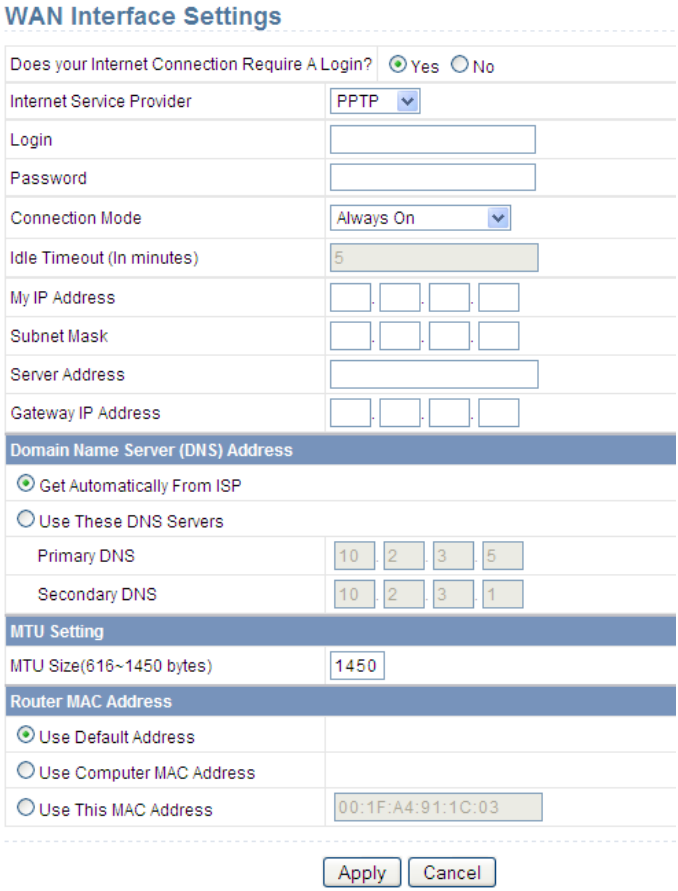
- **Service Name**: If several PPPoE servers are available, specify one in this field.

- **Connection Mode**:
  - **Always On**: If you select it, the system automatically establishes a connection. If SMCWEB-N2 is disconnected from the network because of external factors when you are using the Internet access service, the system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we recommend you to use this connection mode.
  - **Dial On Demand**: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of **Idle Timeout**, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.
  - **Manually Connect**: If you select it, you need to manually set dialup connection after startup.
- **Idle Timeout**: If the system does not detect any Internet access behavior within the specified time of **Idle Timeout**, the system interrupts the Internet connection.
- **Domain Name Server (DNS) Address**: Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.
- **MTU Size**: Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address**: See descriptions on setting **Router MAC Address** for DHCP.

After finishing settings, click **Apply** to save the settings.

(4) PPTP

If the ISP provides the user name and password for PPTP dialup, select **PPTP**.



- **Login**: Enter the user name for PPTP dialup provided by the ISP.
- **Password**: Enter the password for PPTP dialup provided by the ISP.
- **Connection Mode**:
  - **Always On**: If you select it, the system automatically establishes a connection. If SMCWEB-N2 is disconnected from the network because of external factors when you are using the Internet access service, the

system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we recommend you to use this connection mode.

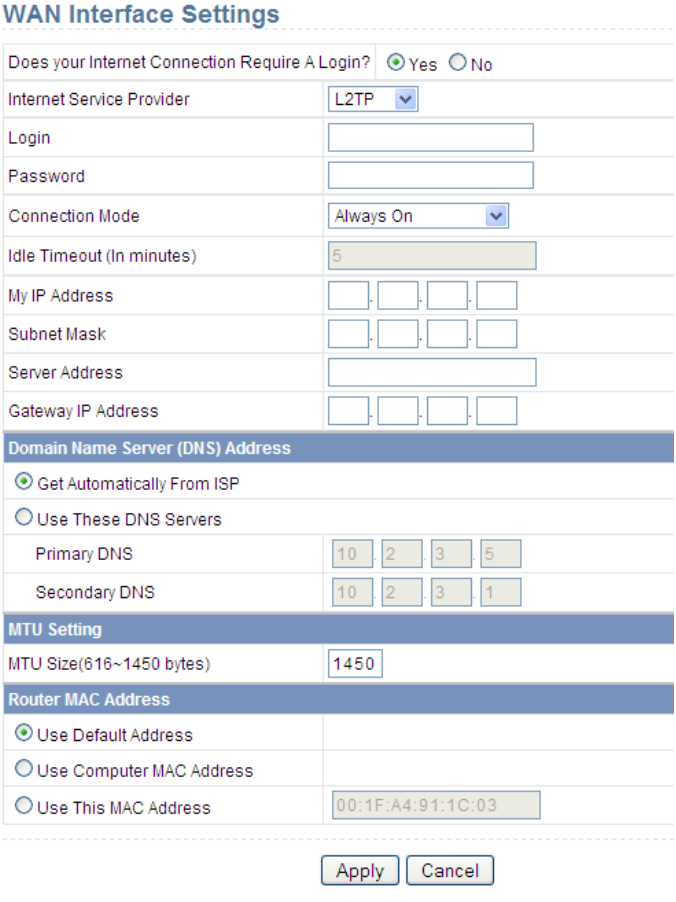
- **Dial On Demand**: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of **Idle Timeout**, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.
- **Manually Connect**: If you select it, you need to manually set dialup connection after startup.

- **Idle Timeout**: If the system does not detect any Internet access behavior within the specified time of **Idle Timeout**, the system interrupts the Internet connection.
- **My IP Address**: Enter your IP address. You can also leave this field blank.
- **Subnet Mask**: Enter the subnet mask. You can also leave this field blank.
- **Sever Address**: Enter the IP address of the server. You can also leave this field blank.
- **Gateway IP Address**: Enter the IP address of the gateway. You can also leave this field blank.
- **Domain Name Server (DNS) Address**: Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.
- **MTU Size**: Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address**: See descriptions on setting **Router MAC Address** for DHCP.

After finishing settings, click **Apply** to save the settings.

(5) L2TP

If the ISP provides the user name and password for L2TP dialup, select **L2TP**.

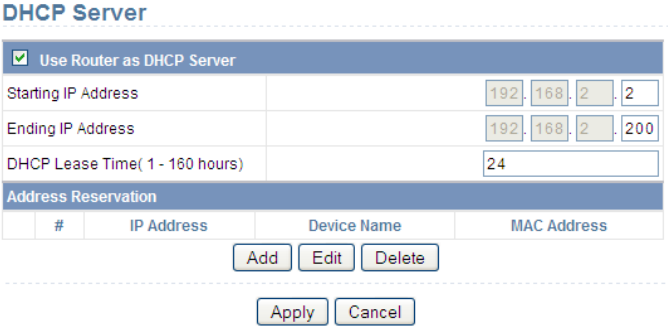


For details of parameter settings for this page, refer to previous parameter descriptions for **PPTP**.

8.4.3 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, SMCWEB-N2 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

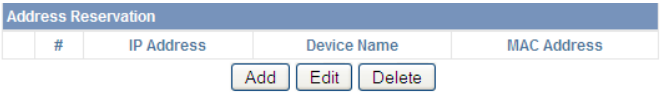


8.4.3.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server**: If you select the **Use Router as DHCP Server** check box, SMCWEB-N2 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address**/**Ending IP Address**: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address**/**Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

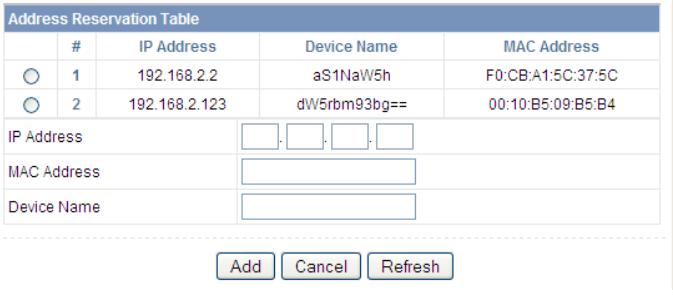
8.4.3.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.



To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.



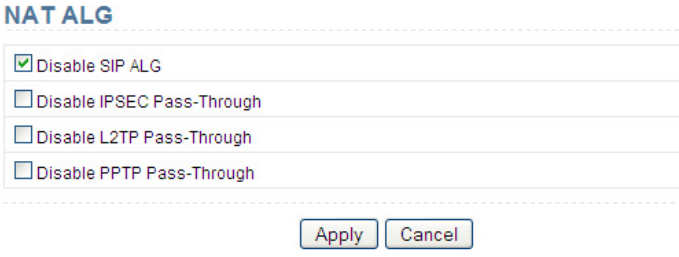
Step 2 Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.2.x). Enter the MAC address and device name of the computer or server.

Step 3 Click **Add** to add a new item into **Address Reservation**.

Step 4 Click **Apply** to save the settings.

8.4.4 NAT ALG

Choose **Network Settings** > **NAT ALG** and the **NAT ALG** page is displayed.

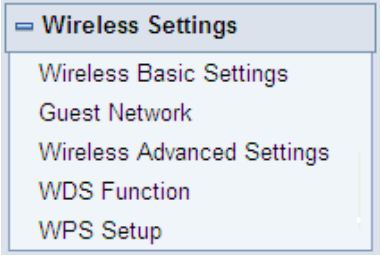


- **Disable SIP ALG**: Certain SIP applications have special mechanisms for passing through the NAT firewall and SIP ALG may have conflicts with these mechanisms. In most cases, please disable SIP ALG.
- **Disable IPSEC/L2TP/PPTP Pass-Through**: IPSEC/PPTP/L2TP Pass-Through provides a secure communication method for remote computers in the wide area network (WAN) (for example, the Internet). Enable the corresponding VPN pass-through function if an intra-network host needs to use a VPN protocol (such as the PPTP, L2TP, IPSEC) to connect to a remote VPN network through the router.

After finishing settings, click **Apply** to save the settings.

8.5 Wireless Settings

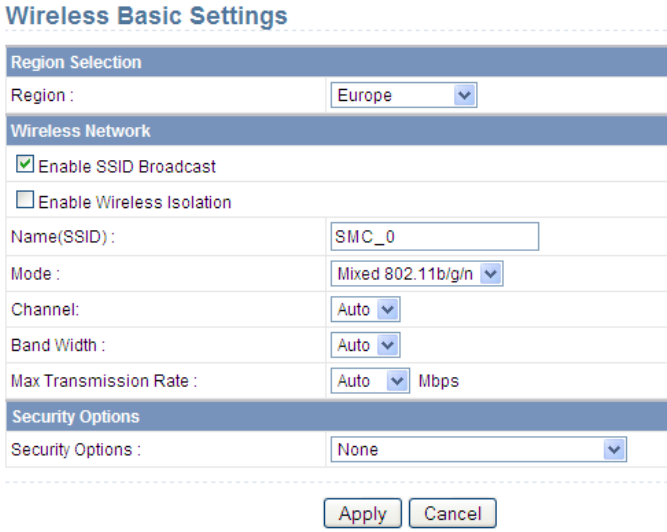
Click **Wireless Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

8.5.1 Wireless Basic Settings

Choose **Wireless Settings** > **Wireless Basic Settings** and the **Wireless Basic Settings** page is displayed.



- **Region**: Select the region where you are located.
- **Enable SSID Broadcast**: If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.
- **Enable Wireless Isolation**: If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Name (SSID)**: Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive.
- **Mode**: Select the wireless mode. **Mixed 802.11b/g/n** is recommended.
- **Channel**: The channel for transmitting wireless signals. The default channel is **Auto**. When you select **Auto**, SMCWEB-N2 automatically selects the best channel from the available channels according to actual situations.
- **Band Width**: The bandwidth occupied for wireless signal transmission.

- **Max Transmission Rate**: The maximum transmission rate of SMCWEB-N2.
- **Security Options**: Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

– None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	None

– WEP

Wired equivalent privacy. You can use WEP 64- or 128-bit encryption.

Security Options	
Security Options :	WEP
Security Encryption(WEP)	
Authentication Type :	Automatic
Encryption Type :	ASCII
Encryption Strength :	64 bits
Security Encryption(WEP) Key	
Key 1:	(5 ASCII characters)
Key 2:	(5 ASCII characters)
Key 3:	(5 ASCII characters)
Key 4:	(5 ASCII characters)

Apply Cancel

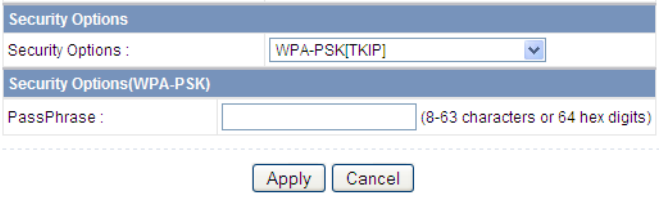
- **Authentication Type**: Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and Shared keys.
  - **Automatic**: If selected, the router uses an authentication type of **Open** or **Shared keys** according to the request of the host.

- **Open**: If selected, hosts in the wireless network can pass the authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.
- **Shared keys**: If selected, hosts in the wireless network can pass authentication only when the correct password is entered. Otherwise, the hosts cannot connect to the wireless network.

- **Encryption Type**: The type of the key to be set. Hexadecimal and ASCII code are available.
  - **Hex**: Valid characters for keys contain 0–9 and A–F.
  - **ASCII**: Valid characters for keys contain all characters of the key board.
- **Encryption Strength**: The encryption strength determines the length of the key.
  - If **Encryption Strength** is set to **64 bits**, set the key to 10 hexadecimal digits or 5 ASCII characters.
  - If **Encryption Strength** is set to **128 bits**, set the key to 26 hexadecimal digits or 13 ASCII characters.
- **Key 1/2/3/4**: Set the key based on the selected encryption type and encryption strength.

– WPA-PSK[TKIP] or WPA2-PSK[TKIP]

WPA-PSK: Preshared key Wi-Fi protection access
WPA2-PSK: Preshared key Wi-Fi protection access version 2
TKIP: Temporal Key Integrity Protocol
Note that the 802.11n mode does not support the TKIP algorithm.

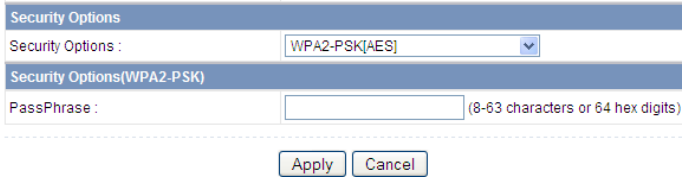


- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

– WPA-PSK[AES] or WPA2-PSK[AES]

WPA-PSK: Preshared key Wi-Fi protection access.
WPA2-PSK: Preshared key Wi-Fi protection access version 2.

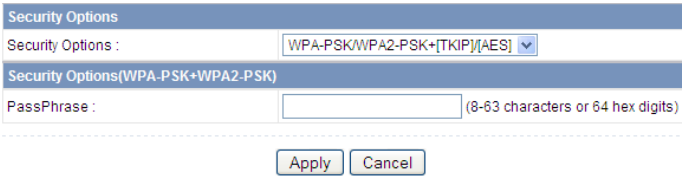
AES: Advanced Encryption Standard



- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

– **WPA-PSK/WPA2-PSK+[TKIP]/[AES]**

It allows the client to use either WPA-PSK[TKIP]/[AES] or WPA2-PSK[TKIP]/[AES].



- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

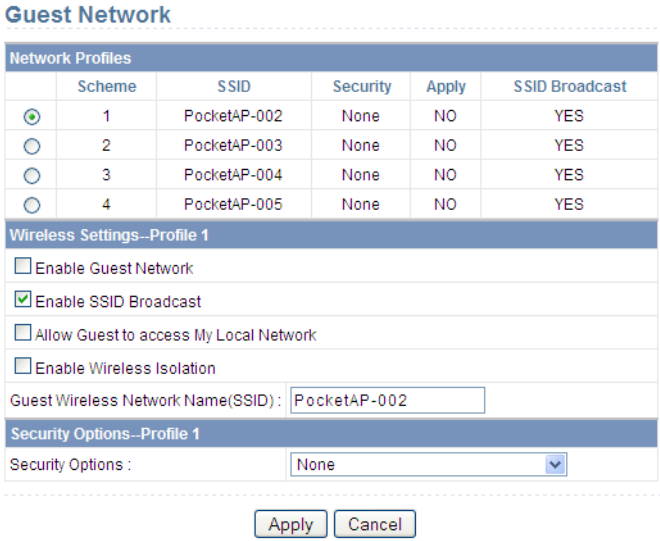
Note:

After you complete configuring wireless settings for SMCWEB-N2, only hosts that have the same wireless settings (for example, the SSID) as SMCWEB-N2 can connect to SMCWEB-N2. If you configure security settings for SMCWEB-N2, hosts must have the same security settings (for example, the password) as SMCWEB-N2 in order to connect to SMCWEB-N2.

8.5.2 Guest Network

If you do not want visitors to know your wireless security key, you can use the guest network to allow them to use your Internet without knowing your wireless connection password.

Choose **Wireless Settings** > **Guest Network** and the **Guest Network** page is displayed.



- **Network Profiles**: Brief description of the created guest network. You can create up to four guest networks. A network profile contains the SSID and encryption mode, whether to use the guest network, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.
- **Enable Guest Network**: If enabled, both you and visitors can connect to the network by using the SSID of the guest network.
- **Enable SSID Broadcast**: If enabled, SMCWEB-N2 broadcasts its SSID to all wireless stations.
- **Allow Guest to access My Local Network**: If enabled, visitors using the SSID of a guest network can access not only the Internet but also the LAN of SMCWEB-N2, like users using the primary SSID of the network. If disabled,

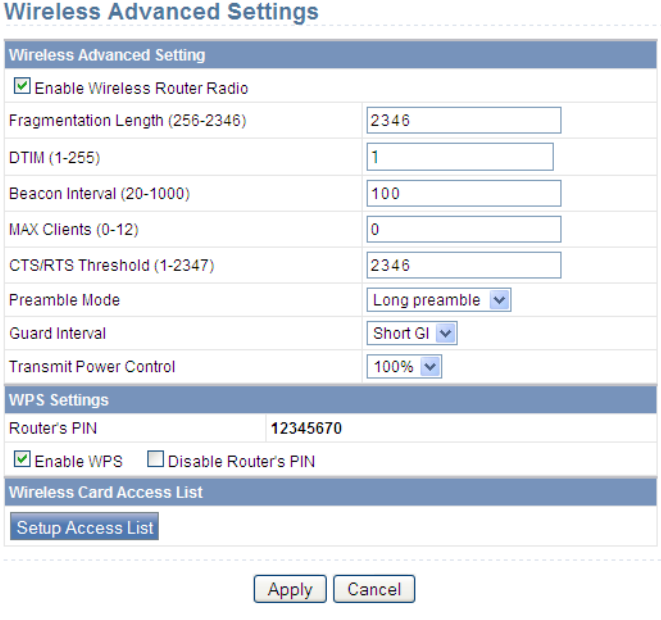
visitors using the SSID of a guest network cannot access the LAN of SMCWEB-N2.

- **Enable Wireless Isolation**: If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Guest Wireless Network Name (SSID)**: Set the name of the guest network.
- **Security Options**: Refer to security option descriptions in section 8.5.1 “Wireless Basic Settings”.

After finishing settings, click **Apply** to save the settings.

8.5.3 Wireless Advanced Settings

Choose **Wireless Settings** > **Wireless Advanced Settings** and the **Wireless Advanced Settings** page is displayed.



- **Fragmentation Length (256-2346)**: Set the threshold of fragmentation length. If the length of a packet exceeds the set value, the packet is automatically fragmented into several packets. The value of **Fragmentation Length** cannot be too small because excessive packets reduce wireless network performance. The default value is 2346.
- **DTIM (1-255)**: Set the interval for sending DTIM frames.
- **Beacon Interval (20-1000)**: The beacon interval is the frequency of sending Beacon frames. Set the interval for sending Beacon frames. The unit is millisecond (ms). The default value is 100 ms.
- **MAX Clients (0-12)**: Set the maximum number of clients. 0 indicates the number of connected clients is not limited.
- **CTS/RTS Threshold (1-2347)**: Set the CTS/RTS threshold. If the length of a packet is greater than the specified RTS value, SMCWEB-N2 sends an RTS frame to the destination station to negotiate. After receiving an RTS frame, the wireless station responds with a Clear to Send (CTS) frame to SMCWEB-N2, notifying that they can communicate with each other.
- **Preamble Mode**: A preamble (especially the **802.11b High Rate/DSSS PHY** field; 56 digits synchronized field for short preamble) defines the length of the CRC correction block for communication between wireless devices. Short preamble should be applied in a network with intense traffics. It helps improve the efficiency of a wireless network responding to applications that have high requirement of real-time, such as streaming video and voice-over-IP telephony.
- **Guard Interval**:
  - Short GI: The interval is 400 ns. When short GI is enabled, SMCWEB-N2 can receive and send short-frame-interval packets. This helps improve the transmission rate of SMCWEB-N2.
  - Long GI: The interval is 800 ns.
- **Transmit Power Control**: Set the transmit power of the wireless network. It is recommended to use the default setting of **100%**.
- **Router's PIN**: Display the PIN to be used for the wireless client when wireless settings of the router are configured through WPS.
- **Enable WPS**: Functions in the **WPS Setup** page are available only after the **Enable WPS** check box is selected. If the check box is not selected, the **WPS Setup** menu item is greyed out.

- **Disable Router's PIN**: The PIN mode function in the **WPS Setup** page is available only when the **Disable Router's PIN** check box is not selected. If the check box is selected, the PIN mode option is unavailable.

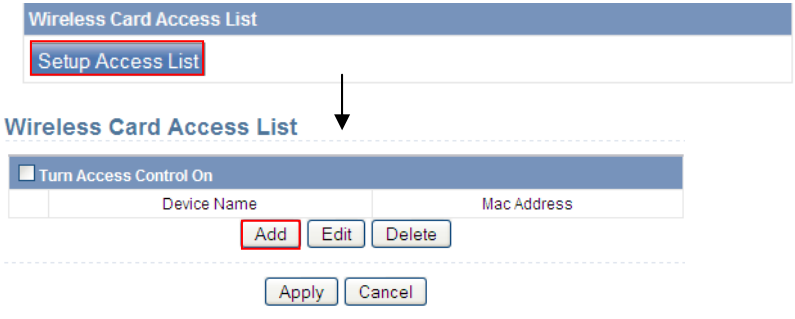
Restricting wireless access by MAC address

When a wireless card access list is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computer list.

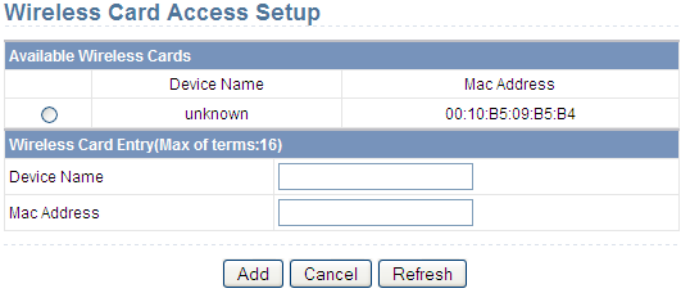
The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only. The MAC address is in the format of XX:XX:XX:XX:XX:XX.

To restrict wireless access by MAC address:

Step 1 Click **Setup Access List** button in the **Wireless Advanced Settings** page to display the **Wireless Card Access List** page.



Step 2 Click **Add** to add a wireless device to the wireless access control list. The **Wireless Card Access Setup** page is displayed.



Step 3 If the computer you want appears in the **Available Wireless Cards** list, you can select the radio button of that computer to obtain its MAC address. Otherwise, you can manually enter a name and MAC address of the computer to be authorized. Generally, the MAC address is labeled on the bottom of the wireless device.

Step 4 Click **Add** to add this wireless device to the wireless card access list. The page jumps to the list page.

Step 5 Select **Turn Access Control On**. If selected, you can restrict PCs' access to the wireless network, only allowing specified PCs to access your network according to their MAC addresses.

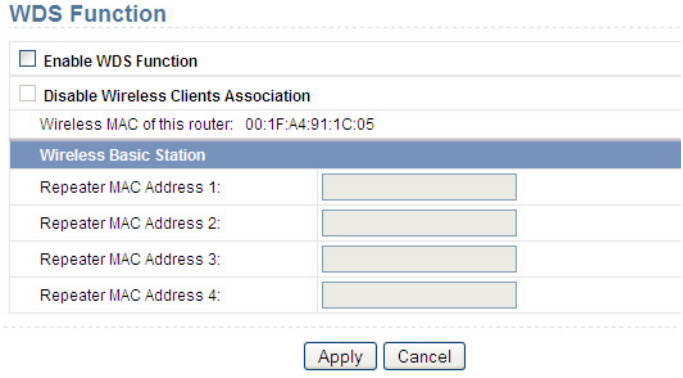
Step 6 Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the SMCWEB-N2 router.

8.5.4 WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. If you want to use WDS to achieve wireless repeating or bridging, enable WDS.

Choose **Wireless Settings** > **WDS Function** and the **WDS Function** page is displayed.



- **Enable WDS Function**: Enable the WDS function if you want to use this function. Note that the WDS function cannot be enabled if the channel is set to **Auto**.

- **Enable Wireless Clients Association**: If not selected, the wireless basic station does not transmit any signals to clients that are directly connected to it.
- **Central Base Station**: In this mode, the router serves as a basic station to communicate with repeaters. The basic station forwards the data of communication between repeaters to the destination repeaters. Repeaters should be configured accordingly. Note that a wireless basic station can be configured with up to four repeaters.
- **Repeater MAC Address 1/2/3/4**: Enter the MAC address of the repeater.

After finishing settings, click **Apply** to save the settings.

For WDS application description, refer to section 6.4.3 “WDS Application”.

8.5.5 WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

The following describes how to configure WPS for the router mode.

8.5.5.1 Using the WPS Button

In the Router mode with WDS disabled, press the **WPS** button on the side panel of SMCWEB-N2 and the **WPS** button on the client device. SMCWEB-N2 can perform WPS encrypted connection to the downlink client device.

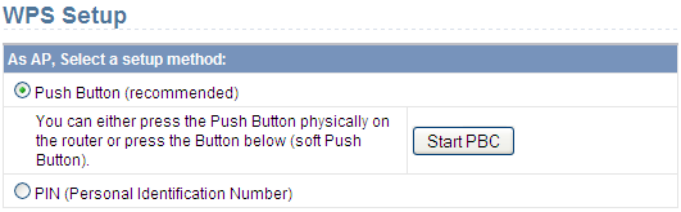
8.5.5.2 Using the Web Page

You can perform WPS settings using the Web page for configuration.

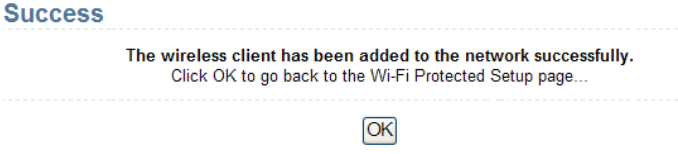
Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

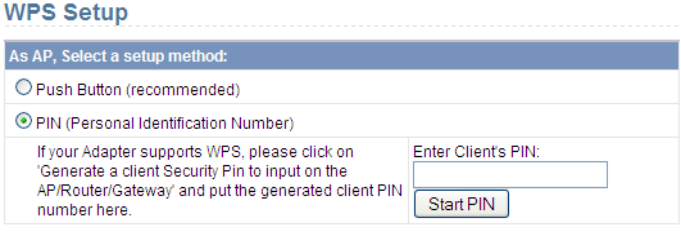


Step 2 Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

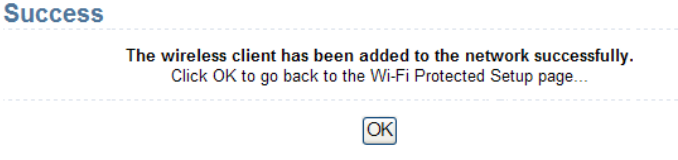


- PIN mode

Step 1 Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.

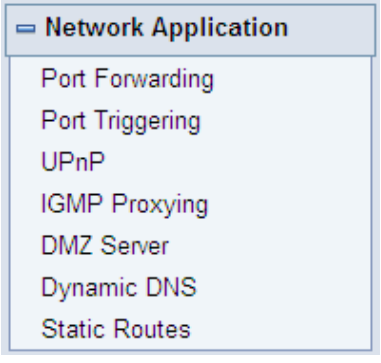


Step 2 Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



8.6 Network Application

Click **Network Application** and the extended navigation menu is shown as follows:

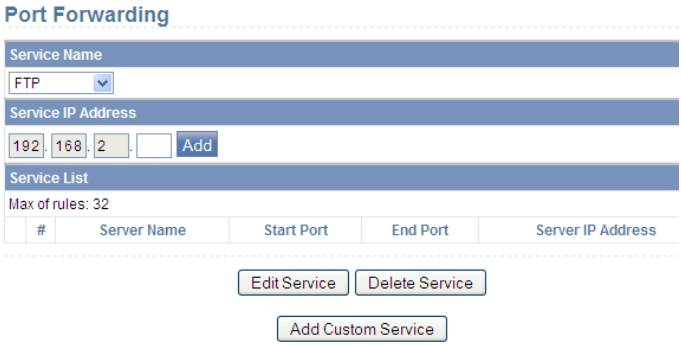


Click a submenu to perform specific parameter configurations.

8.6.1 Port Forwarding

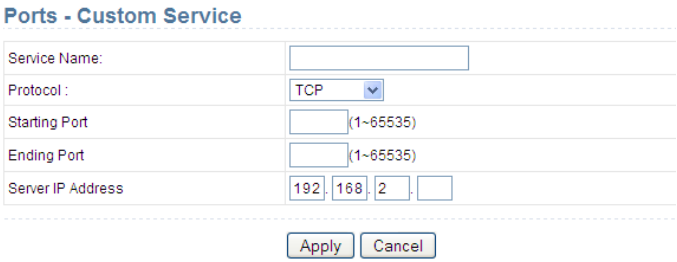
By default, the firewall function of the router hides your LAN. As a result, other users on the Internet can detect only the router, but cannot access a certain PC in the LAN directly. If you want to access a PC in an LAN, you need to configure port forwarding for the router and map the desired port to the corresponding PC in the LAN. The router forwards packets to the PC according to the port mapping rule after receiving an access request from the Internet. In this way, communication is successfully established between the Internet and the PC in the LAN.

Choose **Network Application** > **Port Forwarding** and the **Port Forwarding** page is displayed.



- **Service Name**: Select a service type.
- **Service IP Address**: Enter the IP address of the computer that provides services.

Click the **Add Custom Service** button and the **Ports - Custom Service** page is displayed:



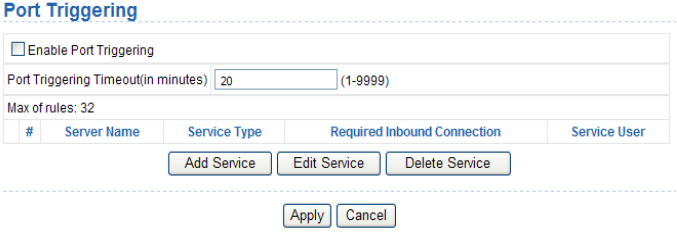
- **Service Name**: Select a service type.
- **Protocol**: The protocol used at the mapping port. You can select **TCP/UDP**, **TCP**, or **UDP**. It is recommended to use **TCP/UDP** if you do not know which protocol should be used.
- **Starting Port**: After the connection to the mapping port is established, the corresponding port is open and the application can initiate subsequent connection requests to the open port.
- **Ending Port**: Set the end port of the mapping port range.
- **Service IP Address**: Enter the IP address of the computer that provides services.

After finishing settings, click **Apply** to save the settings.

8.6.2 Port Triggering

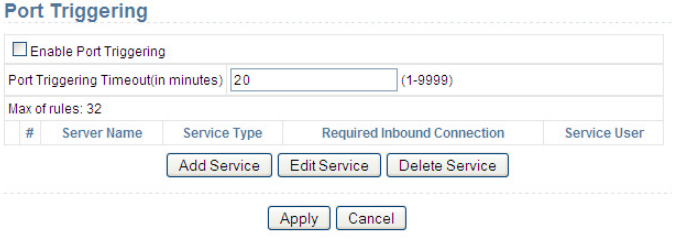
Certain applications, such as WAN network games, video conferences, and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on an NAT router. When an application sends a connection request to a trigger port, the corresponding ports are open for later connection and service provision.

Choose **Network Application** > **Port Triggering** and the **Port Triggering** page is displayed.



- **Enable Port Triggering**: If Enable Port Triggering box is not checked, all port triggering function will be disabled.
- **Port Triggering Timeout**: The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled.

Click the **Add Service** button and the **Port Triggering – Services** page is displayed:



- **Service Name**: Enter a service name.
- **Service User**:
  - **Any**: Allow everybody in the user network to use the service.

- **Single address**: Enter the IP address of the network adapter on the PC. Then, the service is applied only on the specific network adapter of the PC.

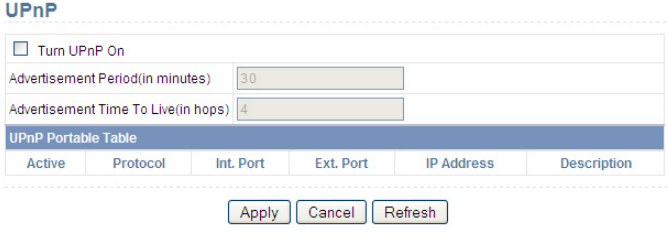
- **Service Type**: The protocol used at the triggering port. You can select **TCP/UDP**, **TCP**, or **UDP**.
- **Triggering Starting Port**: The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
- **Triggering Ending Port**: Set the end port of the triggering port range.
- **Starting Port**: The starting port of the port range.
- **Ending Port**: The ending port of the port range.

After finishing settings, click **Apply** to add a port triggering rule.

8.6.3 UPnP

By using the Universal Plug and Play (UPnP) protocol, a host in the LAN can ask the router to perform specific port conversion, to enable an external host to access resources on the internal host when necessary. For example, if MSN Messenger is installed on Windows ME and Windows XP operating systems, UPnP can be used for audio and video conversations. In this way, functions restricted by NAT can work properly.

Choose **Network Application** > **UPnP** and the **UPnP** page is displayed.



- **Turn UPnP On**: If selected, UPnP is enabled.
- **Advertisement Period (in minutes)**: Set the broadcast interval. It indicates the interval for the router broadcasting its UPnP information. The value should be in the range of 1 to 1440 minutes and the default is 30 minutes.
- **Advertisement Time To Live (in hops)**: The time for the broadcast to live. It is the number of hops after each UPnP packet is sent. The number of hops is the times that each packet can be broadcast before it vanishes. The value is in the range of 1 to 255 hops and the default is 4 hops.

- **UPnP Portable Table**: This table shows the IP addresses of UPnP devices that are connected to the router and open (internal and external) ports on the devices. It also lists the types and status of the open ports.

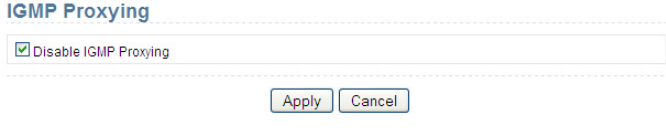
Note:

Only applications that support UPnP can use the UPnP function.

The functionality of UPnP requires support by the application and operating systems such as Windows ME, Windows XP, and Windows Vista.

8.6.4 IGMP Proxying

Click **Network Application** > **IGMP Proxying** and the **IGMP Proxying** page is displayed.



- **Enable IGMP proxying**: IGMP proxying enables a PC in the LAN to receive desired multicast traffic from the Internet. Disable IGMP proxying if you do not need this function.

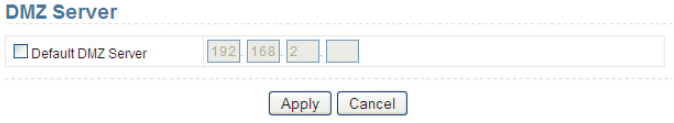
After finishing the setting, click **Apply** to apply the setting.

8.6.5 DMZ Server

DMZ (Demilitarized Zone), a special network zone that is different from the external network or the internal network. Servers that are allowed to access the external network, such as Web and e-mail, connect to the DMZ. The internal network is protected behind the Trust Zone interface, and is not allowed any user to access. Therefore, the internal and external networks are separated, which can meet user's secrecy demand. Usually, there are some public servers in DMZ, such as Web, Mail, and FTP. Users from the external network can access services in DMZ, but they cannot obtain the company's secret information or personal information that is

stored on the internal network. Even though servers in the DMZ are damaged, it does not cause secret information loss on the internal network.

Choose **Network Application** > **DMZ Server** and the **DMZ Server** page is displayed.



- **Default DMZ Server**: Enter the IP address of a PC that serves as the DMZ server.

Note:

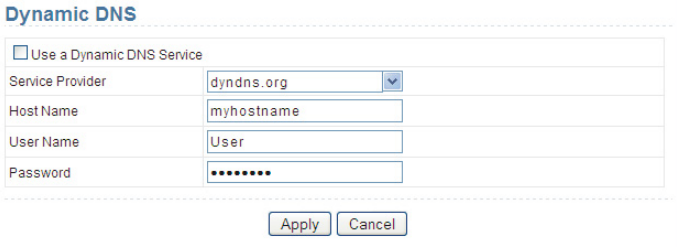
When PC on the internal network is set to be the DMZ host, all interfaces of the PC will be exposed to the Internet and the PC will risk great security. Unless necessary, please do not set the DMZ casually.

After the DMZ host is set, mappings of all the interfaces will point to the DMZ host and the port mappings that point to other hosts will be invalid.

8.6.6 Dynamic DNS

Dynamic domain name resolution (DDNS) is mainly used to achieve resolution between fixed domain names and dynamic IP addresses. For a user that uses a dynamic IP address, after the user obtains a new IP address in the Internet access, the dynamic domain name software installed in the host sends the IP address to the DDNS server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Choose **Network Application** > **Dynamic DNS** and the **Dynamic DNS** page is displayed.



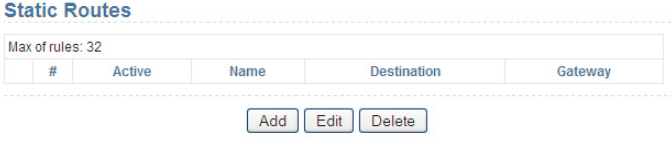
- **Use a Dynamic DNS Service**: If you have registered with a DDNS service provider, select **Use a Dynamic DNS Service**.
- **Service Provider**: Select your DDNS service provider.
- **Host Name**: Enter the host name or domain name provided by your DDNS service provider.
- **User Name**: Enter the name of your DDNS account.
- **Password**: Enter the password of the DDNS account.

After finishing the settings, click **Apply** to apply the settings.

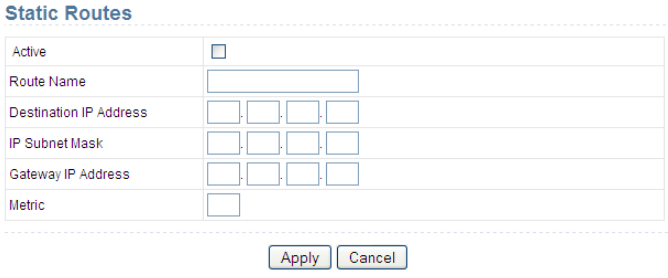
8.6.7 Static Routes

Static routing is a special type of routing that can be applied in a network to reduce the problem of routing selection and data flow overload caused by routing selection so as to improve the packets forwarding speed. You can set the destination IP address, subnet mask, and gateway to specify a routing rule. The destination IP address and subnet mask determine a destination network or host to which the router sends packets through the gateway.

Choose **Network Application** > **Static Routes** and the **Static Routes** page is displayed.



Click **Add** to add a static routing rule.

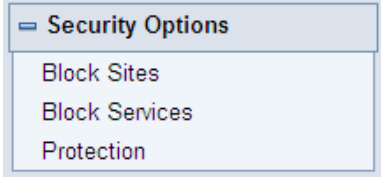


- **Active**: The static routing rule can take effect only if the **Active** check box is selected.
- **Route Name**: Enter the name of the static route.
- **Destination IP Address**: The destination address or network that you want to access. This IP address cannot be in the same network segment as the IP address of the WAN or LAN interface of SMCWEB-N2.
- **IP Subnet Mask**: This IP subnet mask together with the destination IP address identify the target network.
- **Gateway IP Address**: The IP address of the next node to which packets are sent. The gateway IP address must be in the same network segment as the IP address of the WAN or LAN interface of SMCWEB-N2.
- **Metric**: The number of other routers in the user network. The value ranges from 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direct connection, set **Metric** to 2.

After finishing settings, click **Apply** to save the settings.

8.7 Security Options

Click **Security Options** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

8.7.1 Block Sites

SMCWEB-N2 allows you to restrict access based on WEB addresses and WEB address keywords. When a user tries accessing a restricted website, a message is displayed, indicating that the firewall restricts access to the website.

Choose **Security Options** > **Block Sites** and the **Block Sites** page is displayed.

To block access to Internet sites:

Step 1 Select **Per Schedule** or **Always** to enable keyword blocking.

To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section 8.8.3 “Schedules”.

Step 2 Enter keywords or domain names that you want to block in the keyword field and click **Add Keyword**. The keyword or domain name then appears in the **Block Sites Containing these Keywords or Domain Names** list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL www.aabbcc.com/xxx.html is blocked.
- If the keyword **.com** is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be accessed.

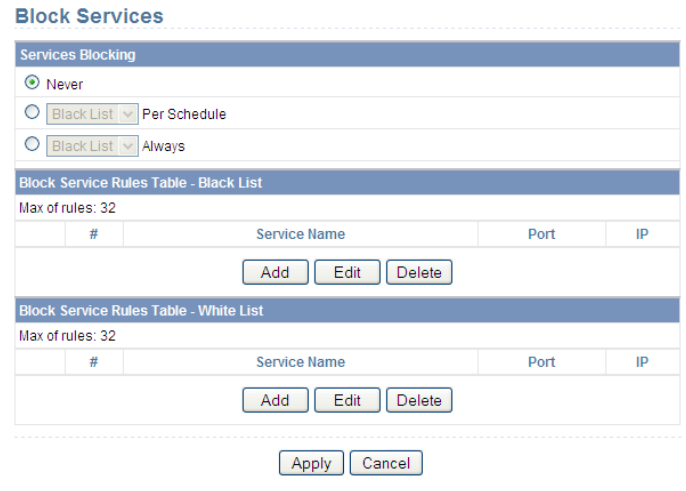
Step 3 You can specify one trusted user, which is a computer that has no restriction in network access. To specify a trusted user, enter the computer's IP address in the **Trusted IP Address** field and select the **Allow Trusted IP Address To Visit Blocked Sites** check box. Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

Step 4 Click **Apply** to save the settings.

8.7.2 Block Services

SMCWEB-N2 allows you to block the use of certain Internet services by computers on your network.

Choose **Security Options** > **Block Services** and the **Block Services** page is displayed.

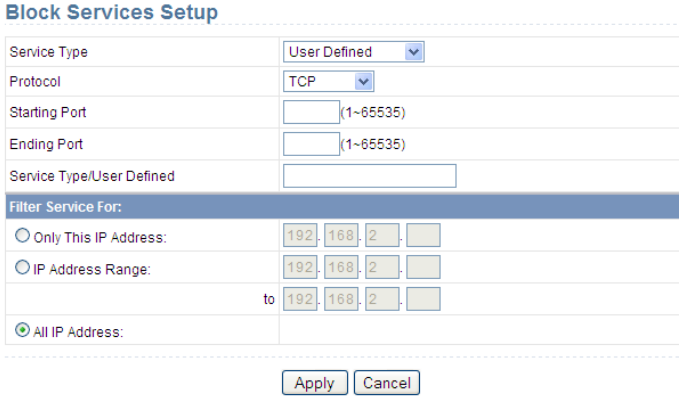


To specify a service for blocking:

Step 1 Select **Per Schedule** or **Always** to enable keyword blocking. To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section 8.8.3 "Schedules".

- **Black List**: Indicates to prevent service that complies with the rule in the **Block Service Rules Table-Black List** area from being used.
- **White List**: Indicates to allow only service that complies with the rule in the **Block Service Rules Table-White List** area to be available for use.

Step 2 Click **Add** to specify a service for blocking. The **Block Services Setup** page is displayed:



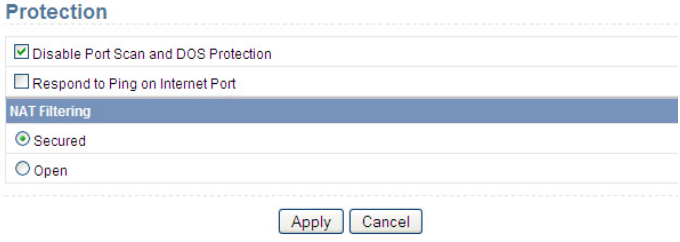
Step 3 Set the parameters in this page.

- **Service Type**: Select a service type. If your desired type is not in the list, select **User defined**. Then, you need to select the protocol, enter the service name, and specify the port range. For services that exist in the drop-down list, the corresponding information is already preset.
- **Protocol**: Set the protocol used at service ports. If you are not sure about the protocol that the application uses, select **TCP/UDP**.
- **Starting Port/Ending Port**: The starting and ending ports of the port range where the specified service is blocked. If the application uses a single port number, enter the number in both fields.
- **Service Type/User Defined**: Enter the service name.
- **Filter Service For:** You can block the specified service for a single computer, computers within an IP address range, or all computers.

After finishing settings, click **Add** to add a new rule. Then, click **Apply** to save the settings.

8.7.3 Protection

Choose **Security Options** > **Protection** and the **Protection** page is displayed.

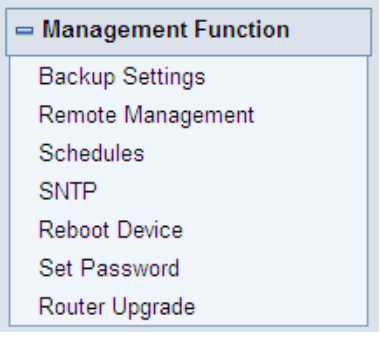


- **Disable port scan and DoS protection**: Denial of service (DoS) protection protects your LAN against DOS attacks. Generally, please enable the port scanning and DOS protection function.
- **Respond to Ping on Internet Port**: If enabled, the router responds to ping commands from the Internet. However, like the DMZ server, enabling this function can bring about security risks. Generally, please disable this function.
- **NAT Filtering**: NAT filtering determines the way that the router deals with incoming traffic.
  - **Secured**: This option provides a secured firewall to protect PCs on LAN from attacks from the Internet, but it may not allow some Internet games, point-to-point applications, or multimedia applications to work.
  - **Open**: This option provides a less secure firewall that allows almost all Internet applications to work.

After finishing the settings, click **Apply** to apply the settings.

8.8 Management Function

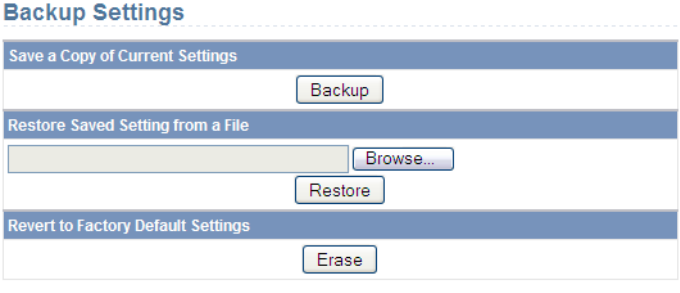
Click **Management Function** and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

8.8.1 Backup Settings

Choose **Management Function** > **Backup Settings** and the **Backup Settings** page is displayed.



In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.

Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

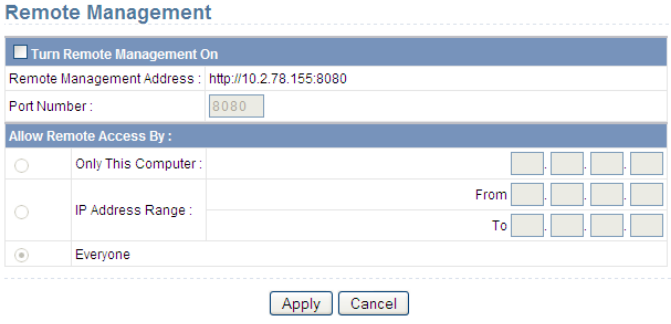
The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.
Click **Browse…** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.
Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

8.8.2 Remote Management

The remote management function allows you to configure the router from the WAN through the Web browser. In this way, you can manage the router on a remote host.
Choose **Management Function** > **Remote Management** and the **Remote Management** page is displayed.

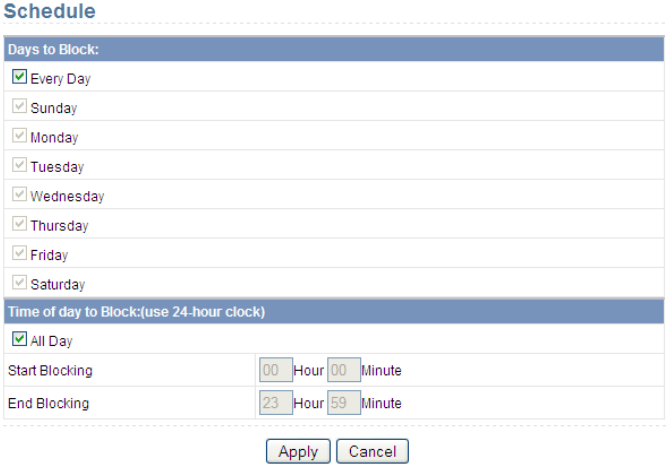


- **Turn Remote Management On**: If selected, you can perform remote Web management for the router from the WAN.
- **Remote Management Address**: IP address that is used to access the router from the Internet. The default is http://0.0.0.0:8080. When accessing the router, you need to enter an address in the form of "**the WAN IP address of the router**"+ "**:**" + "**the port number**" in the IE address bar. For example, if your external address is **10.0.0.123** and the used port number is **8080**, enter **10.0.0.123:8080** in your browser.
- **Port Number**: The port number for accessing the router through remote Web management.
- **Allow Remote Access By**: Set the IP address of the computer on which remote Web management is carried out to access the router.
  - **Only This Computer**: Only the specified IP address can access the router.
  - **IP Address Range**: A range of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify a range.
  - **Everyone**: Everyone on the Internet can access the router.

After finishing settings, click **Apply** to save the settings.

8.8.3 Schedules

Choose **Management Function** > **Schedules** and the **Schedule** page is displayed.



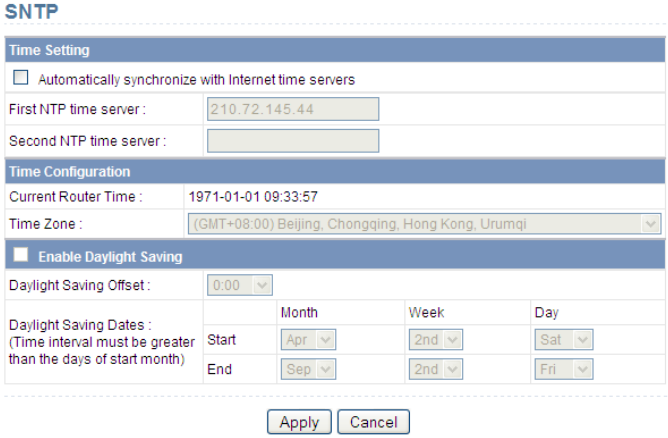
If you already set site filtering in the **Block Sites** page or set sevice filtering in the **Block Services** page, you can set a schedule to specify the time and mode of restricting Internet access.

- Days to Block: Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days.
- Time of Day to Block:
  - **All Day**: To perform 24-hour blocking.
  - **Start Blocking/End Blocking**: If you want to restrict access in a fixed period during the days you specify, enter the start and end time in 24-hour format.

After finishing settings, click **Apply** to save the settings.

8.8.4 SNTP

Choose **Management Function** > **SNTP** and the **SNTP** page is displayed.



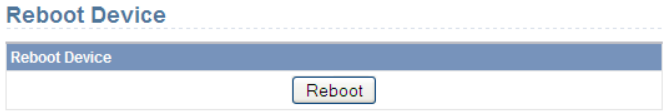
SNTP refers to Simple Network Time Protocol. In this page, you can set time information of your router. It is strongly recommended to set the correct time on the router first. This ensures proper functioning of log, site blocking, and schedule because their time settings are based on time information in this page.

- **Automatically synchronize with Internet time servers**: If selected automatic synchronization with the network time server is enabled.
- **First NTP time server**: Enter the IP address of the primary NTP server. The NTP server is a network time server that is used to synchronize the time of computers on the Internet. When you set the first NTP time server, the router obtains GMT time from the specified NTP server with priority after it is connected to the Internet.
- **Second NTP time server**: Enter the IP address of the secondary NTP server if available.
- **Current Router Time**: Display the current system time of the router.
- **Time Zone**: Select the time zone where you are located.
- **Enable Daylight Saving**: Enable or disable daylight saving time (DST).
- **Daylight Saving Offset**: Select a proper offset. If it is set to +1:00, 10:00 in the morning in standard time becomes 11:00 in the morning in DST.
- **Daylight Saving Dates**: Set the starting time and ending time of DST.

After finishing settings, click **Apply** to save the settings.

8.8.5 Reboot Router

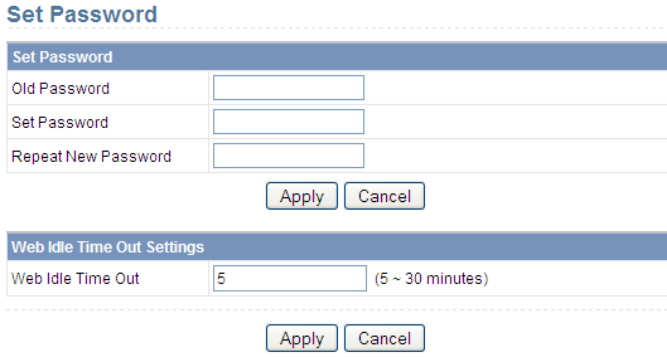
Choose **Management Function** > **Reboot Router** and the **Reboot Router** page is displayed.



Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

8.8.6 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.



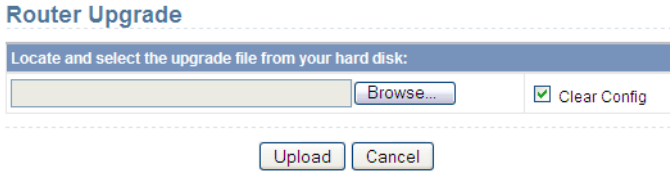
In this page, you can change the login password and set the page timeout time.

Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

8.8.7 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.



Upgrade the software of the router in the following steps:

Step 1 Click **Browse…** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.

Note:

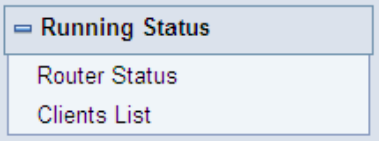
After the software upgrade, SMCWEB-N2 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software.

Do not power off the router during the upgrade.

9 Web Configuration for the Wireless Universal Repeater Mode

9.1 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:



Click the submenu to enter a specific configuration page.

9.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

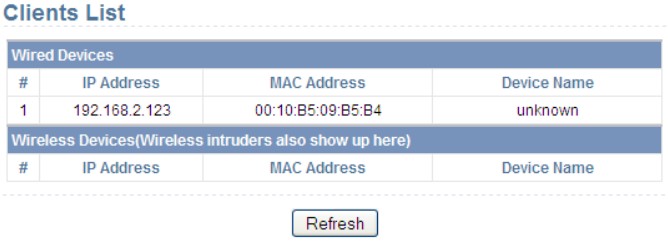
Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	SMCWEB-N2
Work Mode	Repeater Mode
Time and Date	1971-01-01 08:01:49
LAN Port	
MAC Address	00:1F:A4:91:1C:04
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
Wireless Client	
Wireless Network Selected Name (SSID)	
Wireless Channel	Auto
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None
Connect Status	Disconnected
Wireless Universal Repeater	
SSID of Extended Interface	SMC_0
Wireless Security Mode	None

In this page, you can view information about the current running status of SMCWEB-N2, including system information, LAN port status, wireless client information, and wireless universal repeater status.

9.1.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.



Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.2.123	00:10:B5:09:B5:B4	unknown
Wireless Devices(Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name

Refresh

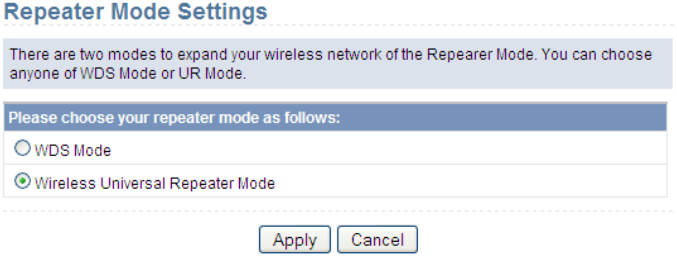
This page displays information of devices connected to SMCWEB-N2, including the IP adress, device name, and MAC address of each device.

9.2 Setup Wizard

For settings, refer to section 6.1 “Repeater Mode Configuration”.

9.3 Repeater Mode Setting

Click **Repeater Mode Settings** and the **Repeater Mode Settings** page is displayed. Select **Wireless Universal Repeater Mode**.



Repeater Mode Settings

There are two modes to expand your wireless network of the Repearer Mode. You can choose anyone of WDS Mode or UR Mode.

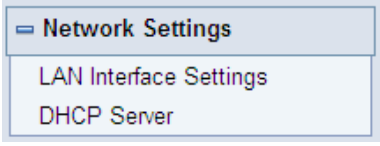
Please choose your repeater mode as follows:

- ○ WDS Mode
- ◉ Wireless Universal Repeater Mode

Apply Cancel

9.4 Network Settings

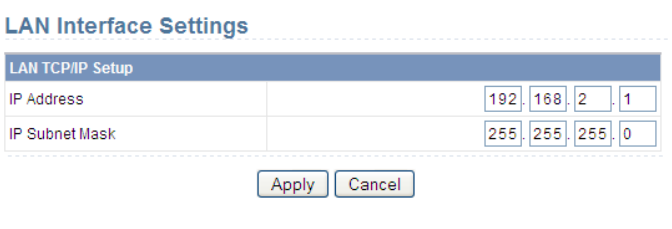
Click **Network Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

9.4.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.



You can modify the IP address and IP subnet mask of the LAN port as required.

Note:

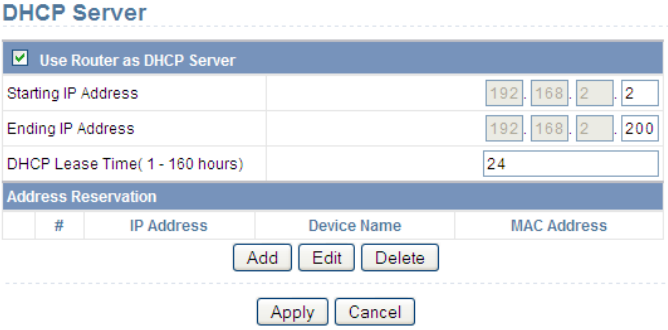
If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

9.4.2 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, SMCWEB-N2 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

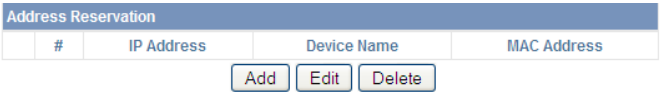


9.4.2.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server**: If you select the **Use Router as DHCP Server** check box, SMCWEB-N2 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address**/**Ending IP Address**: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address**/**Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

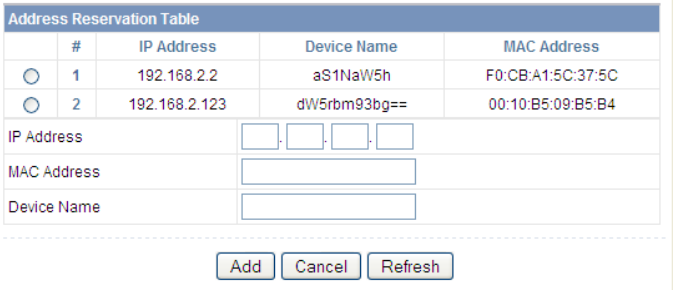
9.4.2.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.



To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.



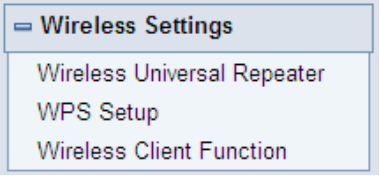
Step 2 Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.2.x). Enter the MAC address and device name of the computer or server.

Step 3 Click **Add** to add a new item into **Address Reservation**.

Step 4 Click **Apply** to save the settings.

9.5 Wireless Settings

Click **Wireless Settings** and the extended navigation menu is shown as follows:

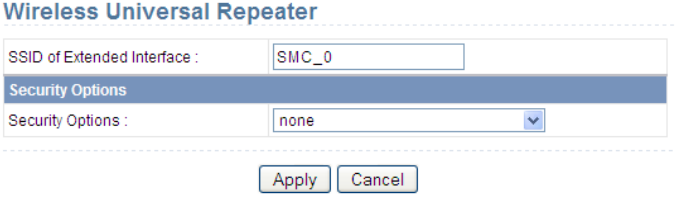


Click a submenu to perform specific parameter configurations.

9.5.1 Wireless Universal Repeater

In universal repeater mode, SMCWEB-N2 acts as the AP and client simultaneously.

Choose **Wireless Settings** > **Wireless Universal Repeater** and the **Wireless Universal Repeater** page is displayed.



- **SSID of Extended Interface**: Set the SSID of the repeater.
- **Security Options**: Set the security encryption mode for the repeater. It is recommended to configure the repeater with the same encryption mode as that of its uplink AP.

After finishing settings, click **Apply** to save the settings.

9.5.2 WPS Setup

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

In the Repeater mode with WDS disabled, SMCWEB-N2 can perform WPS encrypted connection to both the uplink AP and the downlink client device.

The following describes how to configure WPS for the Repeater mode.

9.5.2.1 Using the WPS Button

- WPS connection to the uplink AP

In the Repeater mode with WDS disabled, press the **WPS** button on the side panel of SMCWEB-N2 in 3 seconds and release it. And press the **WPS** button on the uplink AP. Then they can start WPS session.

- WPS connection to the downlink client device

In the Repeater mode with WDS disabled, press the **WPS** button on the side panel of SMCWEB-N2 for 3-10 seconds and release it. And press the **WPS** button on the client device. Then they can start WPS session.

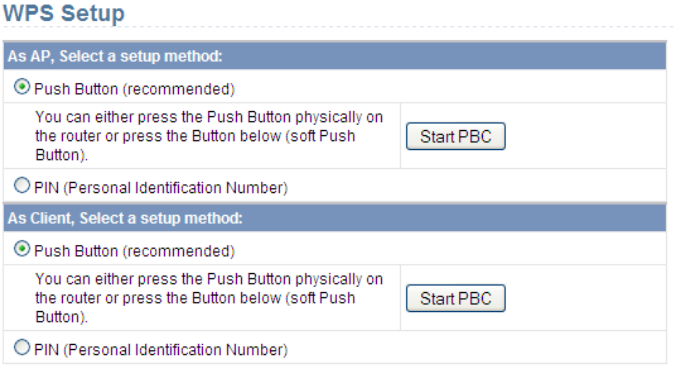
Note:

The SSID, authentication and pre-shared key for SMCWEB-N2 will automatically change to the same as those of its uplink AP after SMCWEB-N2 succeeds in connecting to the uplink AP through the WPS button mode.

9.5.2.2 Using the Web Page

You can perform WPS settings using the Web page for configuration.

Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.



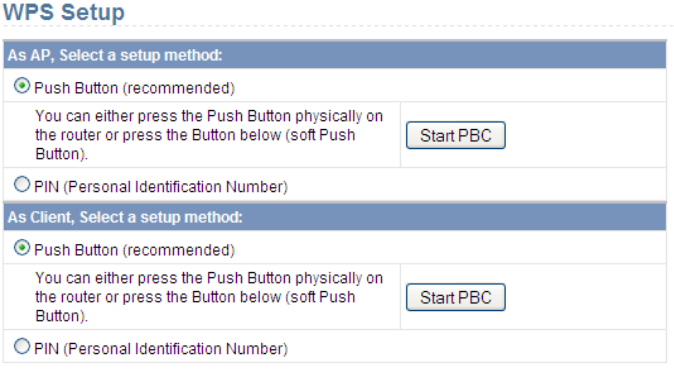
– **As an AP**

You can perform WPS settings using the Web page for configuration.

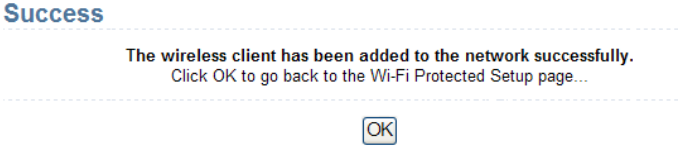
Choose **Wireless Settings** > **WPS Setup** to display the WPS page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

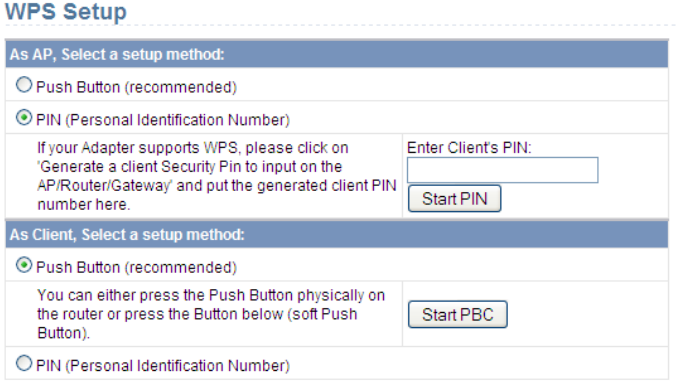


Step 2 Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

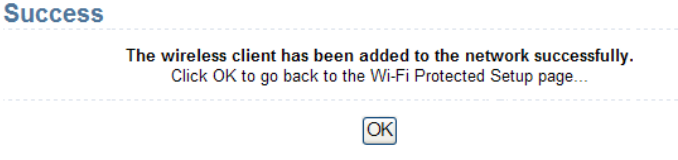


- PIN mode

Step 1 Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.



Step 2 Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



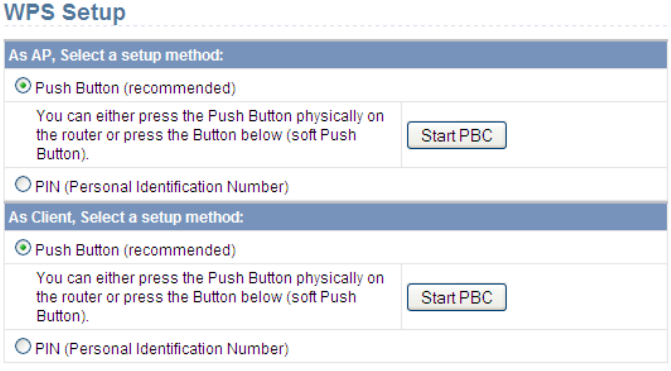
– As a client

You can perform WPS settings using the Web page for configuration.

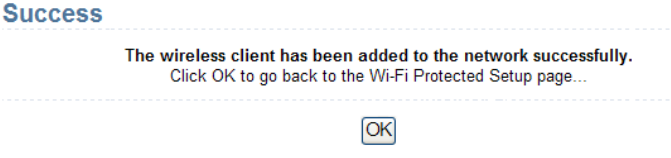
Choose **Wireless Settings** > **WPS** to display the WPS page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

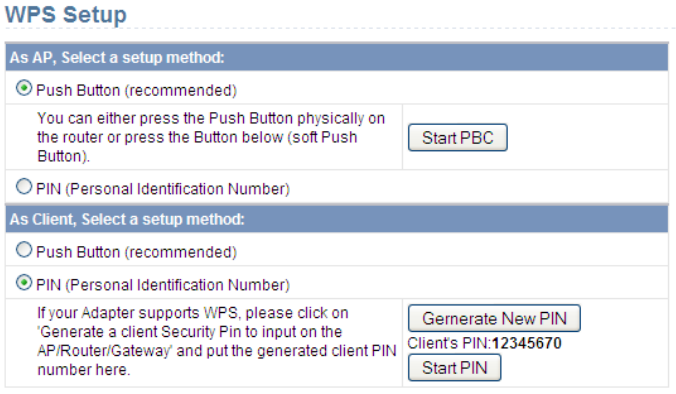


Step 2 Start the WPS PBC process. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

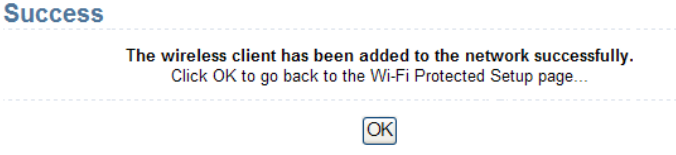


- PIN mode

Step 1 Select **PIN**, click **Generate New PIN**, and click **Start PIN** to start WPS connection.

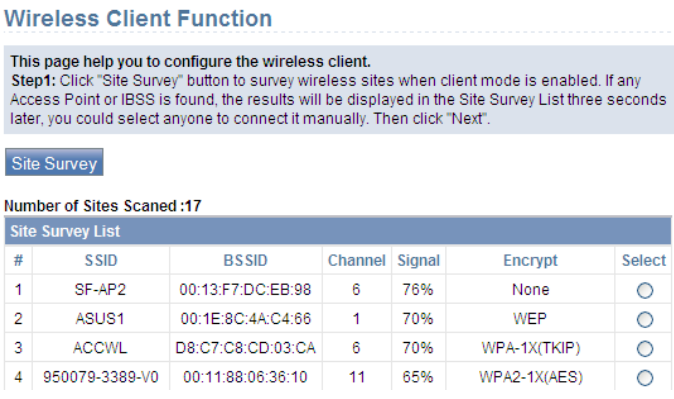


Step 2 Start the WPS PBC process within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



9.5.3 Wireless Client Function

Choose **Wireless Settings** > **Wireless Client Function** and the **Wireless Client Function** page is displayed.



Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

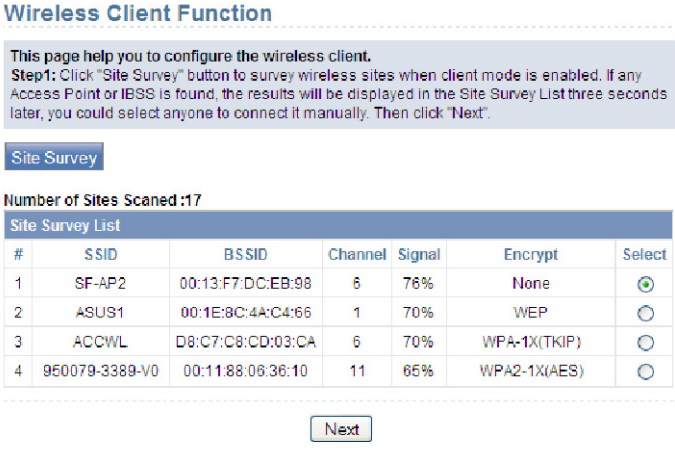
Site Survey

Number of Sites Scaned :17

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	SF-AP2	00:13:F7:DC:EB:98	6	76%	None	○
2	ASUS1	00:1E:8C:4A:C4:66	1	70%	WEP	○
3	ACCWL	D8:C7:C8:CD:03:CA	6	70%	WPA-1X(TKIP)	○
4	950079-3389-V0	00:11:88:06:36:10	11	65%	WPA2-1X(AES)	○

Step 1 Click **Site Survey** to search for the wireless network you want to connect.



Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

Site Survey

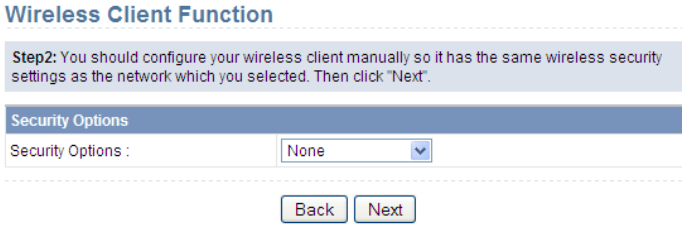
Number of Sites Scaned :17

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	SF-AP2	00:13:F7:DC:EB:98	6	76%	None	◉
2	ASUS1	00:1E:8C:4A:C4:66	1	70%	WEP	○
3	ACCWL	D8:C7:C8:CD:03:CA	6	70%	WPA-1X(TKIP)	○
4	950079-3389-V0	00:11:88:06:36:10	11	65%	WPA2-1X(AES)	○

Next

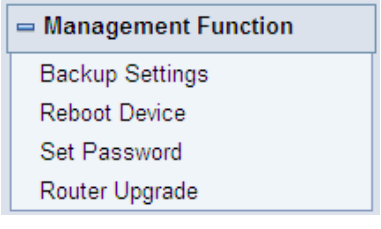
Step 2 Enter encryption information of the selected wireless network. Configure the client with the same security settings as the selected network. Click **Next**.



Step 3 SMCWEB-N2 provides the wireless roaming function if you select **Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options**. Click **Finish**. Then, the client can communicate with the selected network.

9.6 Management Function

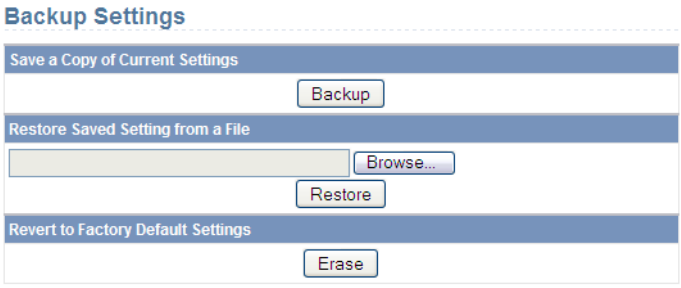
Click **Management Function** and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

9.6.1 Backup Settings

Choose **Management Function** > **Backup Settings** and the **Backup Settings** page is displayed.



In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.

Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.

Click **Browse…** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

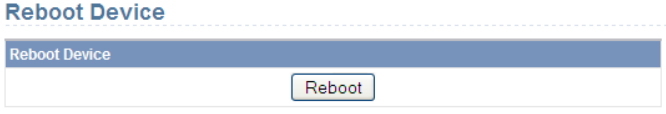
- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

9.6.2 Reboot Router

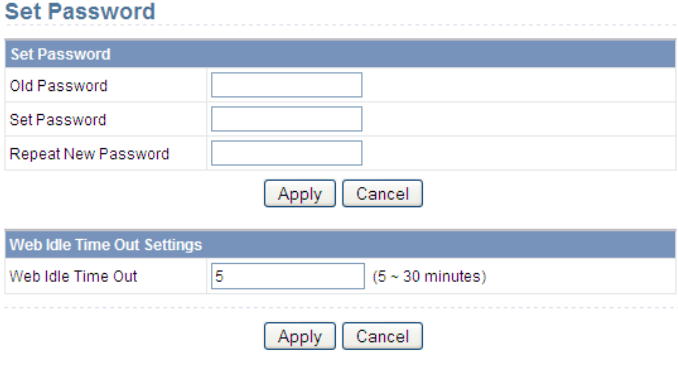
Choose **Management Function** > **Reboot Router** and the **Reboot Router** page is displayed.



Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

9.6.3 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.



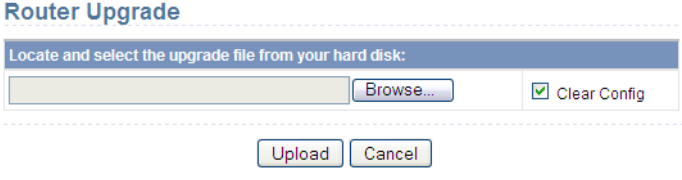
In this page, you can change the password of the administrator and set the page timeout time.

Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

9.6.4 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.



Upgrade the software of the router in the following steps:

Step 1 Click **Browse…** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.

Note:

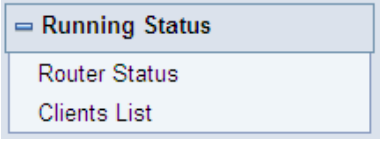
After the software upgrade, SMCWEB-N2 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software.

Do not power off the router during the upgrade.

10 Web Configuration for the WDS Mode

10.1 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:



Click the submenu to enter a specific configuration page.

10.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	SMCWEB-N2
Work Mode	Repeater Mode
Time and Date	1971-01-01 08:38:14
LAN Port	
MAC Address	00:1F:A4:91:1C:04
IP Address	192.168.2.1
IP Subnet Mask	255.255.255.0
Wireless Repeating	
Base Station Address	
Connect Status	Disconnected

In this page, you can view information about the current running status of SMCWEB-N2, including system information, LAN port status, and wireless repeating information.

10.1.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.2.123	00:10:B5:09:B5:B4	unknown
Wireless Devices(Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name

Refresh

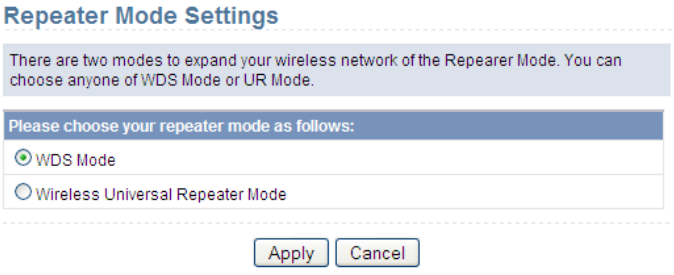
This page displays information of devices connected to SMCWEB-N2, including the IP adress and MAC address of each device.

10.2 Setup Wizard

For settings, refer to section 6.4 “WDS Mode Configuration”.

10.3 Mode Setting

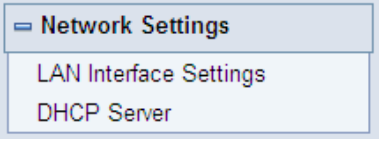
Click **Mode Settings** and the **Mode Settings** page is displayed.



Select **WDS Mode**. Note that WDS function cannot be used if the channel is set to **Auto**.

10.4 Network Settings

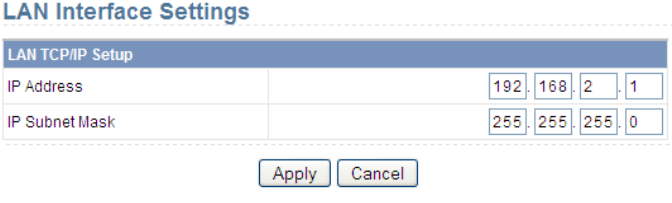
Click **Wired Network Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

10.4.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.



You can modify the IP address and IP subnet mask of the LAN port as required.

Note:

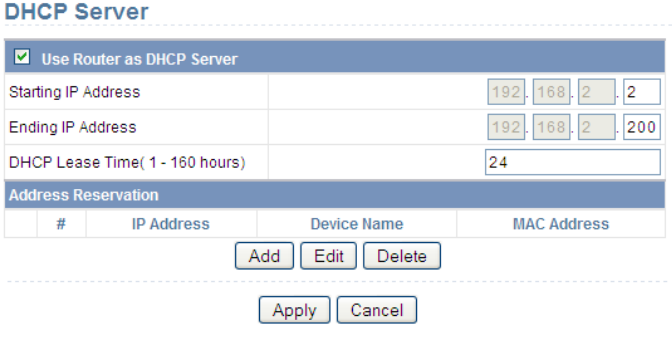
If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

10.4.2 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, SMCWEB-N2 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

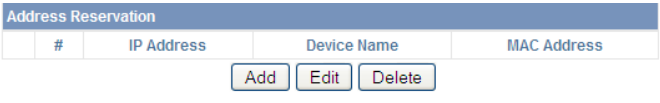


10.4.2.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server**: If you select the **Use Router as DHCP Server** check box, SMCWEB-N2 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address/Ending IP Address**: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address/Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

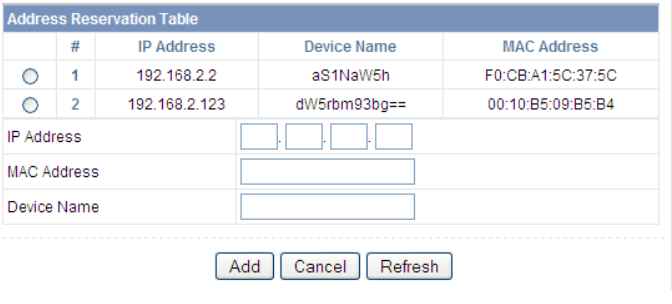
10.4.2.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.



To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.



Step 2 Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server

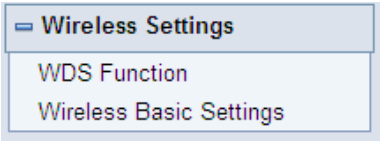
(Choose an IP address from the IP address pool that you have specified, for example 192.168.2.x). Enter the MAC address and device name of the computer or server.

Step 3 Click **Add** to add a new item into **Address Reservation**.

Step 4 Click **Apply** to save the settings.

10.5 Wireless Settings

Click **Wireless Settings** and the extended navigation menu is shown as follows:

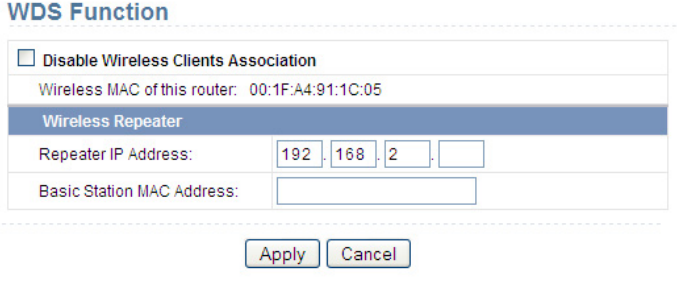


Click a submenu to perform specific parameter configurations.

10.5.1 WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. Enable WDS if you want to use WDS to achieve wireless repeating or bridging.

Choose **Wireless Settings** > **WDS Function** and the **WDS Function** page is displayed.



- **Disable Wireless Clients Association**: If selected, the repeater does not transmit any signals to clients that are connected to it. Generally, clear this check box. Generally, select this check box.

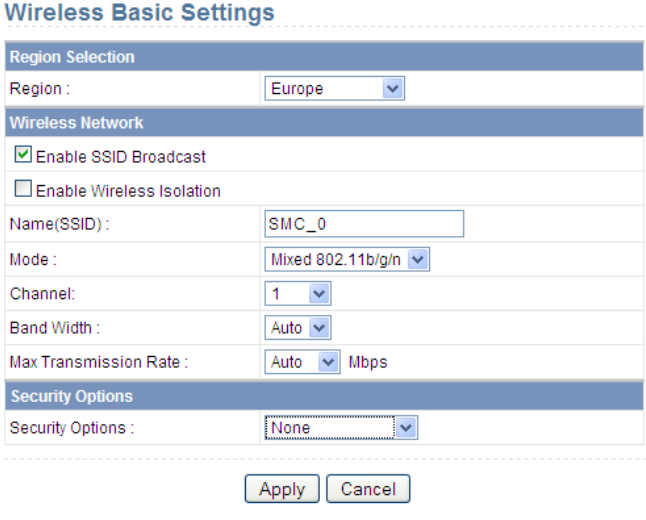
- **Repeater IP Address**: Set the repeater's IP address different from the wireless basic station and other repeaters to avoid IP address conflict. We suggest setting IP addresses of the same network segment for the wireless basic station and repeaters.
- **Basic Station MAC Address**: Enter the MAC address of the wireless basic station.

After finishing settings, click **Apply** to save the settings.

For WDS application description, refer to section 6.4.3 "WDS Application".

10.5.2 Wireless Basic Settings

Choose **Wireless Settings** > **Wireless Basic Settings** and the **Wireless Basic Settings** page is displayed.



- **Region**: Select the region where you are located.
- **Enable SSID Broadcast**: If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.
- **Enable Wireless Isolation**: If enabled, wireless clients using the SSID can access the Internet only, but cannot communicate with other wireless clients.

- **Name (SSID)**: Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive.
- **Mode**: Select the wireless mode. **Mixed 802.11b/g/n** is recommended.
- **Channel**: The channel for transmitting wireless signals. Note that WDS function cannot be used if the channel is set to **Auto**.
- **Band Width**: The bandwidth occupied for wireless signal transmission.
- **Max Transmission Rate**: The maximum transmission rate of SMCWEB-N2.
- **Security Options**: Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

– None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	None

– WEP

Wired equivalent privacy. You can use WEP 64- or 128-bit encryption.

Security Options	
Security Options :	WEP
Security Encryption(WEP)	
Authentication Type :	Automatic
Encryption Type :	ASCII
Encryption Strength :	64 bits
Security Encryption(WEP) Key	
Key 1:	(5 ASCII characters)
Key 2:	(5 ASCII characters)
Key 3:	(5 ASCII characters)
Key 4:	(5 ASCII characters)

Apply Cancel

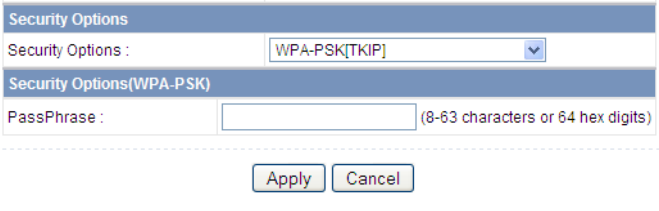
- **Authentication Type**: Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and Shared keys.
  - **Automatic**: If selected, the router uses an authentication type of **Open** or **Shared keys** according to the request of the host.
  - **Open**: If selected, hosts in the wireless network can pass the authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.
  - **Shared keys**: If selected, hosts in the wireless network can pass authentication only when the correct password is entered. Otherwise, the hosts cannot connect to the wireless network.
- **Encryption Type**: The type of the key to be set. Hexadecimal and ASCII code are available.
  - **Hex**: Valid characters for keys contain 0–9 and A–F.
  - **ASCII**: Valid characters for keys contain all characters of the key board.
- **Encryption Strength**: The encryption strength determines the length of the key.
  - If **Encryption Strength** is set to **64 bits**, set the key to 10 hexadecimal digits or 5 ASCII characters.
  - If **Encryption Strength** is set to **128 bits**, set the key to 26 hexadecimal digits or 13 ASCII characters.
- **Key 1/2/3/4**: Set the key based on the selected encryption type and encryption strength.

– WPA-PSK[TKIP]

WPA-PSK: Preshared key Wi-Fi protection access

TKIP: Temporal Key Integrity Protocol

Note that the 802.11n mode does not support the TKIP algorithm.

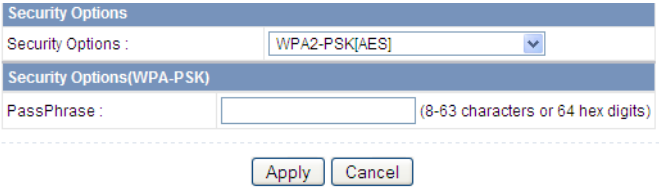


- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

– **WPA2-PSK[AES]**

WPA2-PSK: Preshared key Wi-Fi protection access version 2.

AES: Advanced Encryption Standard



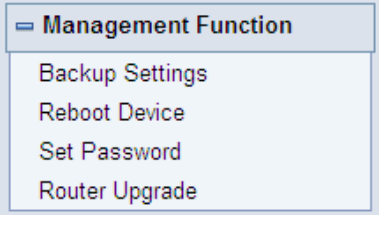
- **PassPhrase**: Enter 8-63 ASCII characters or 64 hexadecimal digits.

Note:

After you complete configuring wireless settings for SMCWEB-N2, only hosts that have the same wireless settings (for example, the SSID) as SMCWEB-N2 can connect to SMCWEB-N2. If you configure security settings for SMCWEB-N2, hosts must have the same security settings (for example, the password) as SMCWEB-N2 in order to connect to SMCWEB-N2.

10.6 Management Function

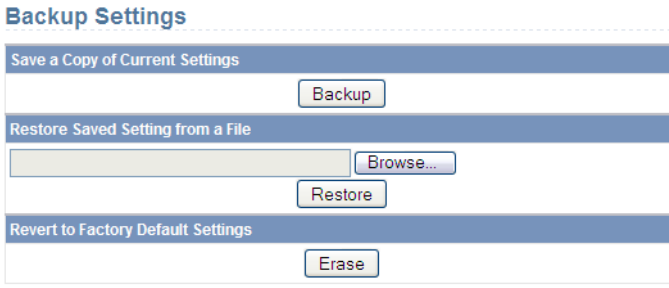
Click **Management Function** and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

10.6.1 Backup Settings

Choose **Management Function** > **Backup Settings** and the **Backup Settings** page is displayed.



In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.

Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.

Click **Browse…** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

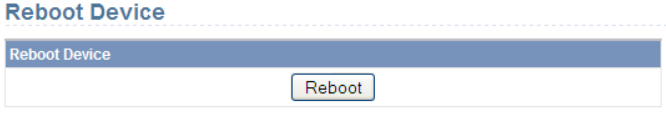
- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

10.6.2 Reboot Router

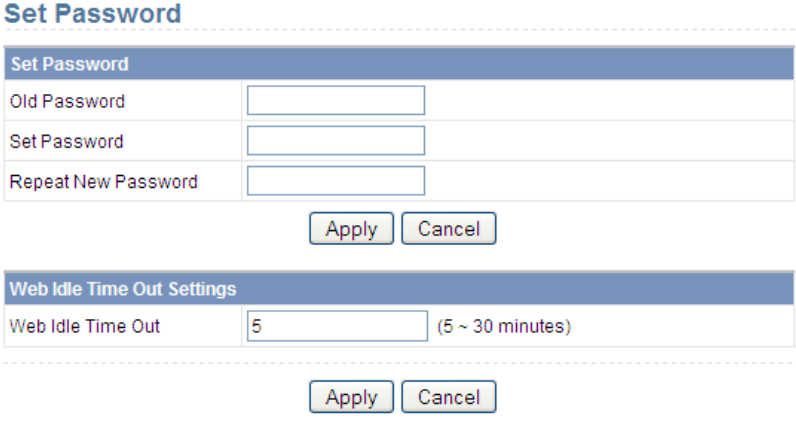
Choose **Management Function** > **Reboot Router** and the **Reboot Router** page is displayed.



Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

10.6.3 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.



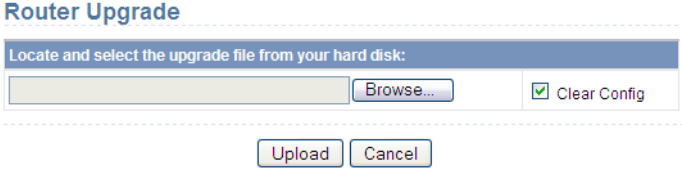
In this page, you can change the password of the administrator and set the page timeout time.

Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

10.6.4 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.



Upgrade the software of the router in the following steps:

Step 1 Click **Browse…** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.

Note:

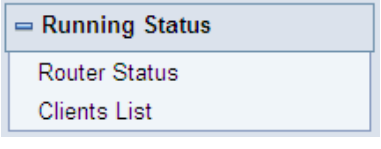
After the software upgrade, SMCWEB-N2 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software.

Do not power off the router during the upgrade.

11 Web Configuration for the Client Mode

11.1 Running Status

Click **Running Status** and the extended navigation menu is shown as follows:



Click the submenu to enter a specific configuration page.

11.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Client Mode
Time and Date	1971-01-01 08:05:11
LAN Port	
MAC Address	00:1E:E3:5B:DE:22
IP Address	192.168.100.254
IP Subnet Mask	255.255.255.0
Wireless Client	
Wireless Network Selected Name (SSID)	
Wireless Channel	Auto
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None
Connect Status	Disconnected

In this page, you can view information about the current running status of SMCWEB-N2, including system information, LAN port status, and wireless client status.

11.1.2 Clients List

Choose **Running Status** > **Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices(Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name
1	192.168.2.192	00:19:B5:08:B5:B4	unknown

Refresh

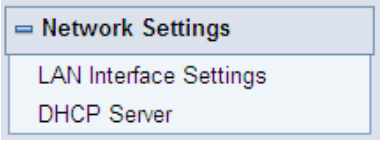
This page displays information of wireless devices connected to SMCWEB-N2, including the IP adress and MAC address of each device.

11.2 Setup Wizard

For settings, refer to section 6.5 “Client Mode Configuration”.

11.3 Network Settings

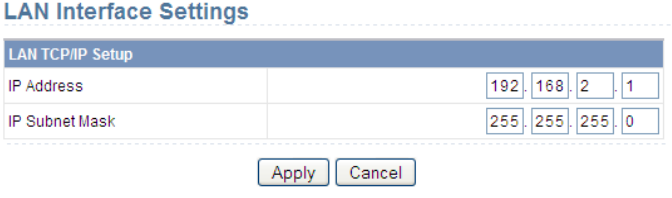
Click **Wired Network Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

11.3.1 LAN Interface Settings

Choose **Network Settings** > **LAN Interface Settings** and the **LAN Interface Settings** page is displayed.



You can modify the IP address and IP subnet mask of the LAN port as required.

Note:

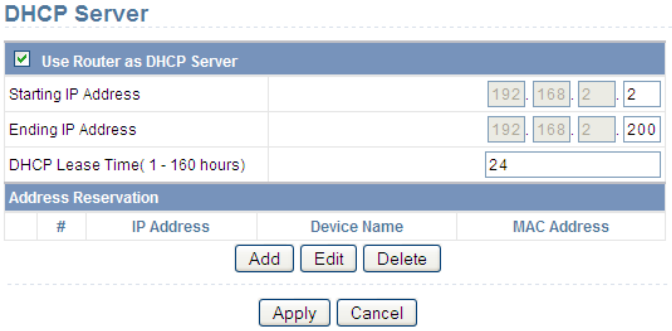
If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

11.3.2 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, SMCWEB-N2 automatically assigns IP addresses to comupters in the LAN. Users do not need to configure TCP/IP protocol paramters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

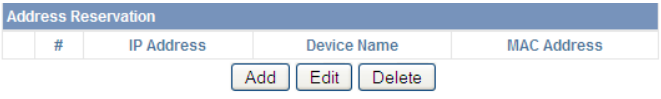


11.3.2.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server**: If you select the **Use Router as DHCP Server** check box, SMCWEB-N2 serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address**/**Ending IP Address**: Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address**/**Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time**: The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

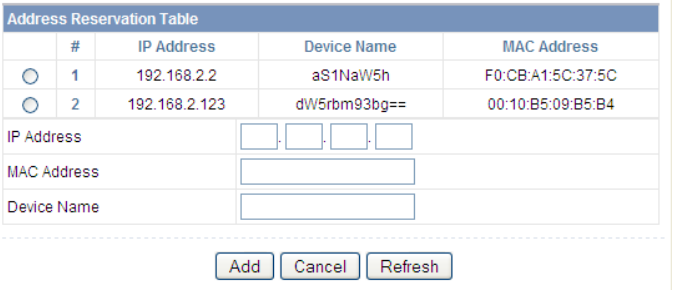
11.3.2.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.



To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.



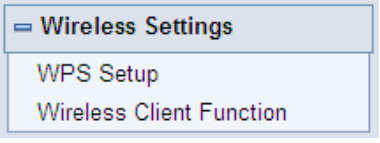
Step 2 Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.2.x). Enter the MAC address and device name of the computer or server.

Step 3 Click **Add** to add a new item into **Address Reservation**.

Step 4 Click **Apply** to save the settings.

11.4 Wireless Settings

Click **Wireless Settings** and the extended navigation menu is shown as follows:



Click a submenu to perform specific parameter configurations.

11.4.1 WPS Setup

WPS refers to Wi-Fi Protected Setup.
You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.
The following describes how to configure WPS for the Client mode.

– Using the WPS Button

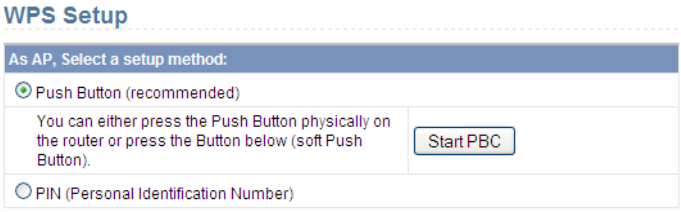
In the Client mode, SMCWEB-N2 can perform WPS encrypted connection to either the uplink AP or the repeater.

– Using the Web Page

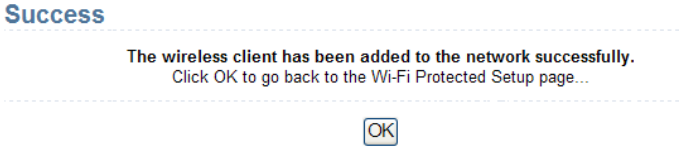
You can perform WPS settings using the Web page for configuration.
Choose **Wireless Settings** > **WPS Setup** to display the **WPS Setup** page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

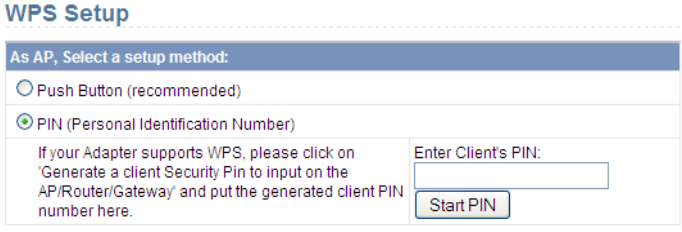


Step 2 Start the WPS PBC process. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

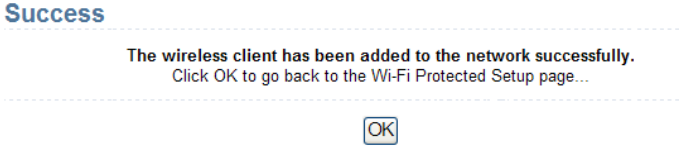


- PIN mode

Step 1 Select **PIN**, click **Generate New PIN**, and click **Start PIN** to start WPS connection.

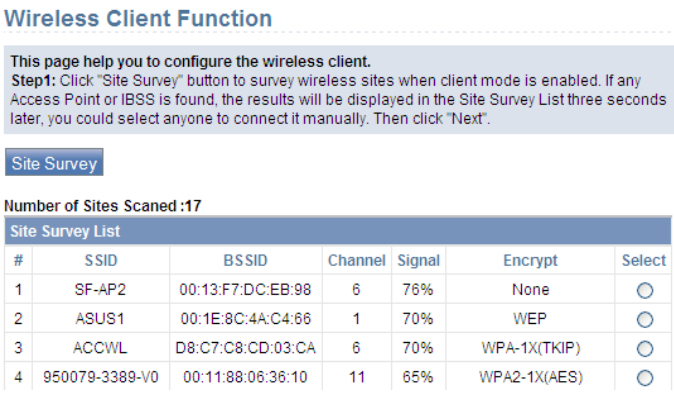


Step 2 Start the WPS PBC process within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.



11.4.2 Wireless Client Function

Choose **Wireless Settings** > **Wireless Client Function** and the **Wireless Client Function** page is displayed.



Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

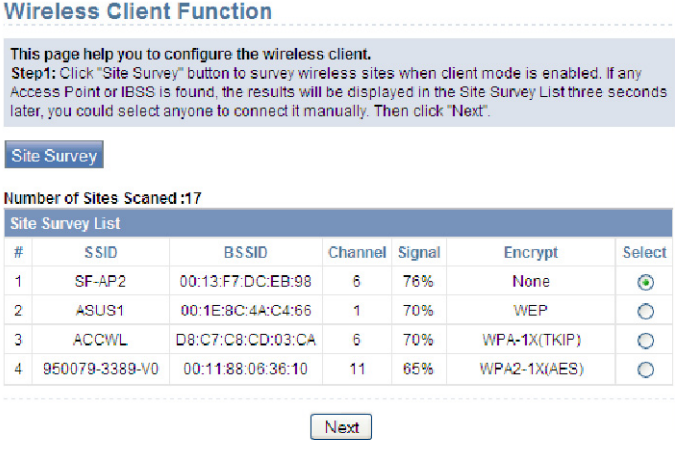
Site Survey

Number of Sites Scaned :17

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	SF-AP2	00:13:F7:DC:EB:98	6	76%	None	○
2	ASUS1	00:1E:8C:4A:C4:66	1	70%	WEP	○
3	ACCWL	D8:C7:C8:CD:03:CA	6	70%	WPA-1X(TKIP)	○
4	950079-3389-V0	00:11:88:06:36:10	11	65%	WPA2-1X(AES)	○

Step 1 Click **Site Survey** to search for the wireless network you want to connect.



Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

Site Survey

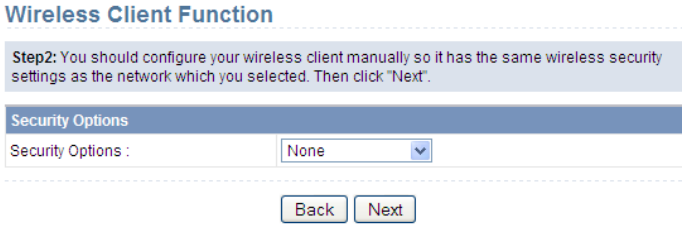
Number of Sites Scaned :17

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	SF-AP2	00:13:F7:DC:EB:98	6	76%	None	◉
2	ASUS1	00:1E:8C:4A:C4:66	1	70%	WEP	○
3	ACCWL	D8:C7:C8:CD:03:CA	6	70%	WPA-1X(TKIP)	○
4	950079-3389-V0	00:11:88:06:36:10	11	65%	WPA2-1X(AES)	○

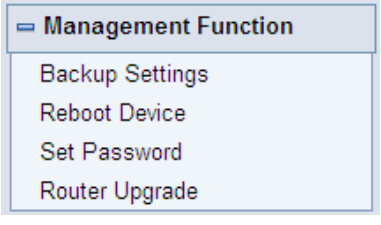
Next

Step 2 Enter encryption information of the selected wireless network. Configure the client with the same security settings as the selected network. Click **Finish**. Then, the client can communicate with the selected network.



11.5 Management Function

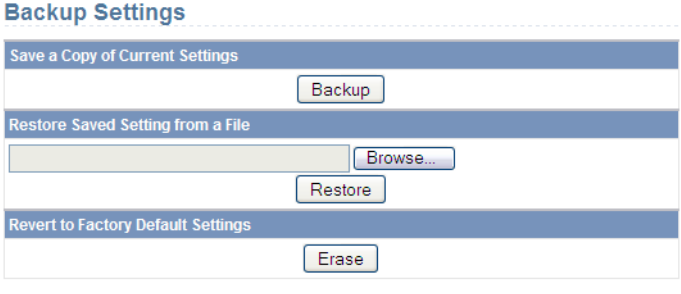
Click **Management Function** and the extended navigation menu is shown as follows.



Click a submenu to perform specific parameter configurations.

11.5.1 Backup Settings

Choose **Management Function** > **Backup Settings** and the **Backup Settings** page is displayed.



In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.

Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.

Click **Browse…** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

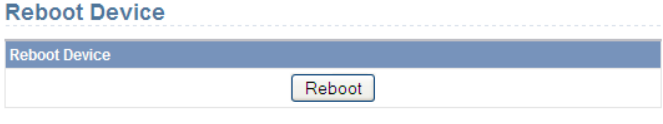
- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

11.5.2 Reboot Router

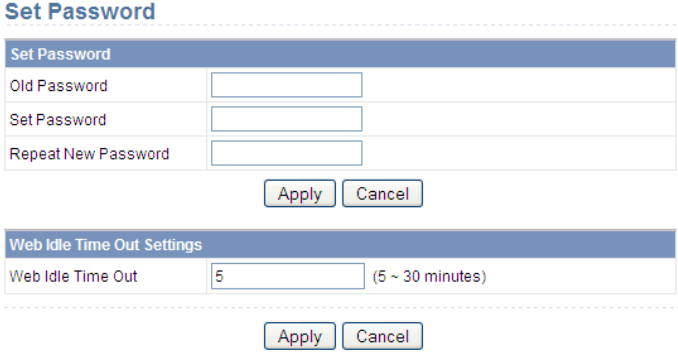
Choose **Management Function** > **Reboot Router** and the **Reboot Router** page is displayed.



Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

11.5.3 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.



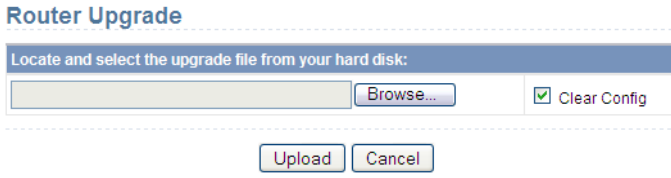
In this page, you can change the password of the administrator and set the page timeout time.

Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

11.5.4 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.



Upgrade the software of the router in the following steps:

Step 1 Click **Browse…** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.

Note:

After the software upgrade, SMCWEB-N2 returns to the factory default settings. In case of losing the previous configuration information, please save settings before updating the software.

Do not power off the router during the upgrade.

Appendix A FAQ

1	**The wireless network adapter fails to search out wireless signals from SMCWEB-N2.**
	When SMCWEB-N2 that is in the Client mode or in the Reaper mode but disconnected to the uplink AP does not support wireless client access and can be connected to through an Ethernet cable only. If the problem persists, causes may be that SMCWEB-N2 is far distant from the terminal device or obstacles placed between them block wireless signals. You can position SMCWEB-N2 in a closer distance from the terminal device, reduce obstacles between them, or add a wireless repeater. In addition, place microwave ovens, Bluetooth devices, and wireless phones that interrupt WLAN signals far away from WLAN devices.
2	**The wireless network adapter fails to connect to SMCWEB-N2.**
	Some early-version wireless network adapters may not support WPA2 authentication. You can set the authentication and encryption to WPA-AES, WPA-TKIP, or WEP.
3	**SMCWEB-N2 in the Repeater or Client mode fails to connect to the uplink AP, for example, the domestic gateway, to access the Internet, or it frequently gets disconnected from the Internet.**
	Check that SMCWEB-N2 is in the wireless signal coverage of its uplink device. Click **Site Survey** in the **Wireless Client Function** page and check whether SMCWEB-N2 can search out strong wireless signals from the uplink AP
4	**Wired connection to SMCWEB-N2 is abnormal**
	Check status of the Ethernet indicator on the SMCWEB-N2. If the Ethernet indicator turns off, check whether the Ethernet cable is connected properly. If the problem persists, replace the Ethernet cable.
5	**You cannot access the Internet.**
	Check whether the network adapter connected to the SMCWEB-N2 can automatically obtain an IP address. If it fails, enable DHCP for the domestic gateway or manually set the IP address of the network adaptor and DNS.
6	**You fails to configure SMCWEB-N2 using the Web page.**
	Check whether the IP address of the network adapter and that of SMCWEB-N2 are in the same network segment. Manually set the IP address of your network adapter in the network segment of 192.168.2.2/253 according to procedures described in Chapter 5 “Configuring Your Computer and Wireless Connection”. Choose **Network Settings** > **LAN Interface Settings** and set the IP address of SMCWEB-N2 in the same network address as that of the domestic network gateway.

7	**WPS connection fails.**
	Ensure that one and the only WPS device connected to SMCWEB-N2 starts the WPS session within 2 minutes. Note the WPS difference between SMCWEB-N2 serving as the uplink AP and that as the downlink client device in the Repeater mode (see section 9.5.2 “WPS Setup”). Refer to Table 4.1 for description on WPS indicator status.

NOTE: 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 or more of the following measures:

—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:(1)This device may not canse harmful interference, and (2)this device must accept any interference received,including interference that may cause undesired operation.

This equipment complies with FCC'S and IC'S RF radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must be installed and operated to provide a separation at distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter. Installers must ensure that 20cm separation distance will be maintained between the device (excluding its handset) and users.

SMC Networks

Headquarters

No. 1, Creation Rd. III
Hsinchu Science Park
Taiwan 30077
Tel: +886 3 5770270
Fax: +886 3 5780764

English: Technical Support information available at www.smc.com

English: (for Asia-Pacific): Technical Support information at www.smc-asia.com

English: (for Middle East): Technical Support information at muneer@smc-asia.com

Deutsch: Technischer Support und weitere Information unter www.smc.com

Español: En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

Français: Informations Support Technique sur www.smc.com

Português: Informações sobre Suporte Técnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgängligt på www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym sa dostepne na www.smc.com

Čeština: Technicka podpora je dostupna na www.smc.com

Magyar: Műszaki tamogat informacio elerhető -on www.smc.com

简体中文：技术支持讯息可通过www.smc-prc.com查询

繁體中文：產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smcnetworks.co.kr 을 참고하시기 바랍니다

INTERNET
E-mail address: www.smc.com→ Support→ By email
Driver updates: www smc com→ Support→ Downloads

SMCWEB-N2