SMC®
Networks

USER GUIDE

BARRICADE™ N
300Mbps 4-Port Wireless Broadband Router

SMCWBR14-N5

Wireless Broadband Router User Guide

SMC®
Networks

No. 1, Creation Road III,
Hsinchu Science Park,
30077, Taiwan, R.O.C.
TEL: +886 3 5638888
Fax: +886 3 6686111

E012013-AP-R06

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

SMC Networks, Inc.

No. 1 Creation Road III,
Hsinchu Science Park,
30077, Taiwan, R.O.C.

Trademarks:

SMC is a registered trademark; and Barricade, EZ Switch, TigerStack, TigerSwitch, and TigerAccess are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

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

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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 cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

Taiwan NCC

根據國家通信傳播委員會低功率電波輻射性電機管理辦法規定：

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電台與不受被干擾保障條件下於室內使用。

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。

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)

Country	Restriction	Reason/Remark
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: Do not use the product outdoors in France.

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:

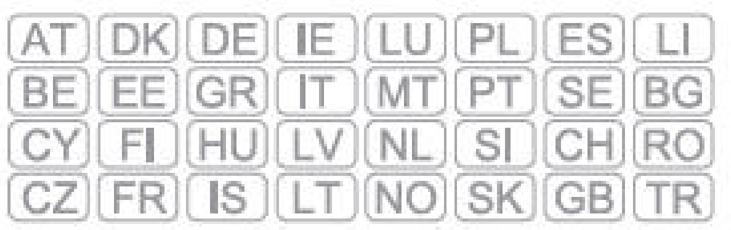
- EN 60950-1:2006 + A11: 2009
  Safety of Information Technology Equipment.
- EN 300 328 V1.7.1: 2006-10
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.
- EN 301 489-17 V1.8.1/ 2008-04
  EN 301 489-17 V2.1.1/ 2009-05
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 55022: 2006 + A1: 2007
  Limits and methods of measurement of radio disturbance characteristics of information technology equipment.
- EN 55024: 1998 + A1: 2001 + A2: 2003
  Information technology equipment immunity characteristics limits and methods of measurement.
- EN 62311: 2008
  Assessment 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 alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
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 Romană	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.

BSMI Notice

在進行安裝及設定之前，建議您先閱讀以下注意事項：

1. 確認寬頻的線路是否正常：請先確認當 ADSL 或 Cable 或是對外的線路，直接結到您的電腦時，是否能正常的連接到網際網路。

2. 移除撥號軟體：若您已經安裝 ISP 所提供的 ADSL 撥接（號）軟體，請先將其移除后再開始進行連線設定。

3. 系統需求：本產品只需要使用網頁瀏覽器（Browser）來進行設定安裝，不需要額外安裝任何程式，在開始設定之前，建議您使用 Internet Explorer 6.0 或更新的版本來進行安裝設定。

4. 設定時無需連上網際網路（Internet），只需要透過區域連線（LAN）即可進行設定。※ 僅需從電腦端拉一條網路線連接至 SMCWBR14-N5 的 LAN 埠，WAN 埠則先不要連上 ISP 線路。此動作作用是用來確認您可以正常連到此設備。

5. SMCWBR14-N5 只需要設定一次，其餘要透過 SMCWBR14-N5 的電腦或者設備只需要做相關的 TCP/IP 設定即可。

About This Guide

Purpose This guide details the hardware features of the wireless router, including its physical and performance-related characteristics, and how to install the device and use its configuration software.

Audience This guide is for PC users with a working knowledge of computers. You should be familiar with Windows operating system concepts.

Conventions The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications The following publication gives basic information on how to install and use the wireless router.

Quick Installation Guide

Also, as part of the wireless router's software, there is online help that describes all configuration related features.

Revision History This section summarizes the changes in each revision of this guide.

December 2012 Revision

This is the sixth revision of this guide. It includes the following change:

- Added Daylight Saving to Time Settings.

October 2012 Revision

This is the fifth revision of this guide. It includes the following change:

- Add BSMI Notice to the Compliances section.

September 2012 Revision

This is the fourth revision of this guide. It includes the following change:

- Updated the Compliances section.

November 2011 Revision

This is the third revision of this guide. It includes the following change:

- Updated the Compliances section.

September 2011 Revision

This is the second revision of this guide. It includes the following change:

- Updated the Compliances section.

July 2011 Revision

This is the first revision of this guide.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

OVERVIEW OF THE ROUTER

The Barricade™ SMCWBR14-N5 300Mbps 4-Port Wireless Broadband Router delivers exceptional range and speed, which can fully meet the needs of Small Office/Home Office (SOHO) networks and users demanding higher network performance. The router integrates a 4-port switch, firewall, NAT router, and wireless access point (AP).

INCREDIBLE SPEED

The SMCWBR14-N5 provides up to 300 Mbps wireless connections with other 802.11n wireless clients, and the speed makes the routers ideal for handling multiple data streams at the same time, which ensures your network remains stable and smooth. The routers are compatible with all IEEE 802.11g and IEEE 802.11b products.

MULTIPLE SECURITY PROTECTIONS

With multiple protection measures, including SSID broadcast control, 64/128/152-bit WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced firewall protection, the routers provide complete data privacy.

FLEXIBLE ACCESS CONTROL

The routers provide flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

SIMPLE INSTALLATION

Since the routers are compatible with all major operating systems, it is easy to manage. A Quick Setup Wizard is supported and detailed step-by-step instructions are provided in this User Guide. Before installing the router, read through this guide to understand all the router’s features.

MAIN FEATURES

- IEEE 802.11n wireless technology provides a wireless data rate of up to 300 Mbps.
- One 10/100 Mbps Auto-Negotiation RJ-45 WAN port, four 10/100 Mbps Auto-Negotiation RJ-45 LAN ports, supporting Auto MDI/MDIX.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting dynamic IP/static IP/PPPoE Internet access.
- Supports Virtual Server, Forwarding, and DMZ host.
- Supports UPnP, DDNS, Static Routing.
- Provides automatic and scheduled connection to the Internet.
- Connects to the Internet on demand, and disconnects from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address assignment.
- Supports Stateful Packet Inspection.
- Supports VPN Passthrough.
- Supports Parental Control and Access Control.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

KEY HARDWARE FEATURES

The following table describes the main hardware features of the Router.

Table 1: Key Hardware Features

Feature	Description
WAN Port	One 100BASE-TX RJ-45 port for connecting to the Internet.
LAN Port	Four 100BASE-TX RJ-45 ports for local network connections.
WPS Button	For WPS security and resetting the unit.
LEDs	Provides LED indicators for Power, WAN port, LAN port, and WLAN status.

PACKAGE CONTENTS

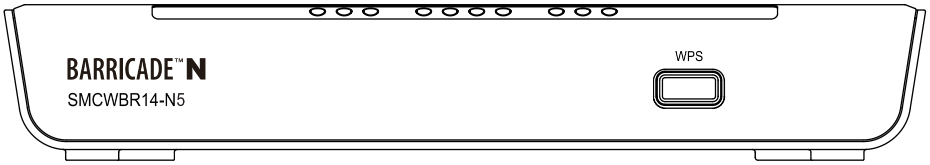
The following items should be found in your package:

- SMCWBR14-N5 300Mbps 4-Port Wireless Broadband Router,
- AC Power Adapter
- Quick Installation Guide
- Resource CD, including:
  - This Guide
  - Other Helpful Information

NOTE: Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

FRONT PANEL

Figure 1: Front Panel



LED INDICATORS

The Router includes eight status LED indicators, as described in the following table.

Table 2: LED Behavior

LED	Status	Description
Power	On	The unit is receiving power and is operating normally.
	Off	There is no power currently being supplied to the unit.
System	On	The Router is initializing or may have a system error.
	Blinking	The Router is working properly.
	Off	The Router has a system error.
WLAN	On/Blinking	The Wireless function is enabled.
	Off	The Wireless function is disabled.

Table 2: LED Behavior (Continued)

LED	Status	Description
WAN LAN (1-4)	On	There is a device linked to the corresponding port, but there is no activity.
	Blinking	There is an active device linked to the corresponding port.
	Off	There is no device linked to the corresponding port.
WPS	On	A wireless device has been successfully added to the network by WPS. The LED will remain on for about 5 minutes.
	Slow Blinking	A wireless device is connecting to the network by WPS. This process lasts for about 2 minutes.
	Off	WPS is not in progress.

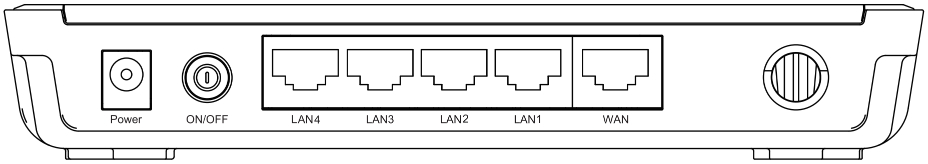
WPS Button

Push this button to start WPS authentication of a wireless device. Push and hold down this button for more than 5 seconds to reset the unit.

NOTE: After a device is successfully added to the network by WPS, the WPS LED will remain on for about 5 minutes and then turn off. When press and hold the WPS Button for more than 5 seconds, you will reset the router.

Rear Panel

Figure 2: Rear Panel



The following items are located on the rear panel (from left to right).

Wireless Antennas

Receives and transmits wireless data.

Power

The Power socket is where you connect the power adapter. Use the power adapter provided with the Router.

ETHERNET WAN PORT

This WAN port is where you connect the DSL/cable Modem.

ETHERNET LAN PORTS

LAN1,2,3,4: These ports (1, 2, 3, 4) connect the Router to local PCs.

2 Connecting the Router

System Requirements

You must meet the following minimum requirements:

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ-45 connector.
- PCs with working Ethernet adapters and Ethernet cables with RJ-45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari.

Installation Environment Requirements

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct exposure to any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating Temperature: 0 °C ~ 40 °C (32 °F ~ 104 °F)
- Operating Humidity: 10% ~ 90% RH, Non-condensing

Connecting the Router

Before installing the Router, make sure your PC is successfullyconnected to the Internet through the broadband service. If there are any problems, first contact your ISP. After that, install the Router according to the following steps.

Connecting the Router in Router Mode

1. Power off your PC, Cable/DSL Modem, and the Router.

2. Locate an optimum location for the Router. The best place is usually at the center of your network. The place must meet the Installation Environment Requirements.

3. Adjust the direction of the antennas. Normally, upright is the best direction.

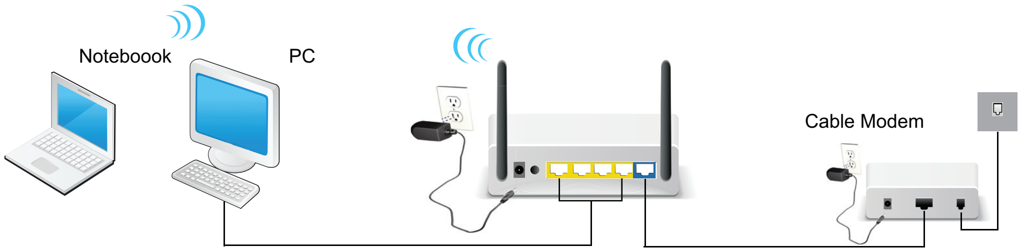
4. Connect PCs and any switch in your LAN to the LAN Ports on the Router, as shown in Figure 3.

5. Connect the DSL/Cable Modem to the WAN port on the Router, as shown in Figure 3.

6. Connect the AC power adapter to the power socket on the Router, and the other end into an electrical outlet. The Router will start to work automatically.

7. Power on your PC and Cable/DSL Modem.

Figure 3: Harewall Installation



3 QUICK INSTALLATION GUIDE

This chapter shows you how to quickly configure the basic functions of your Router using the Quick Setup Wizard.

TCP/IP CONFIGURATION

The default IP address of the Router is 192.168.2.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, all the default values are used for descriptions.

Connect local PCs to the LAN ports of the Router. And then you can configure the IP address for your PC in the following two ways.

CONFIGURE THE IP ADDRESS MANUALLY

1. Set up the TCP/IP Protocol for your PC. If you need instructions on how to do this, refer to Appendix A: "Configuring the PC" on page 117.

2. Configure the network parameters. The IP address is 192.168.2.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.2.1 (the Router's default IP address).

OBTAIN AN IP ADDRESS AUTOMATICALLY

1. Set the TCP/IP Protocol to "Obtain an IP address automatically" mode on your PC. If you need instructions as to how to do this, refer to Appendix A: "Configuring the PC" on page 117.

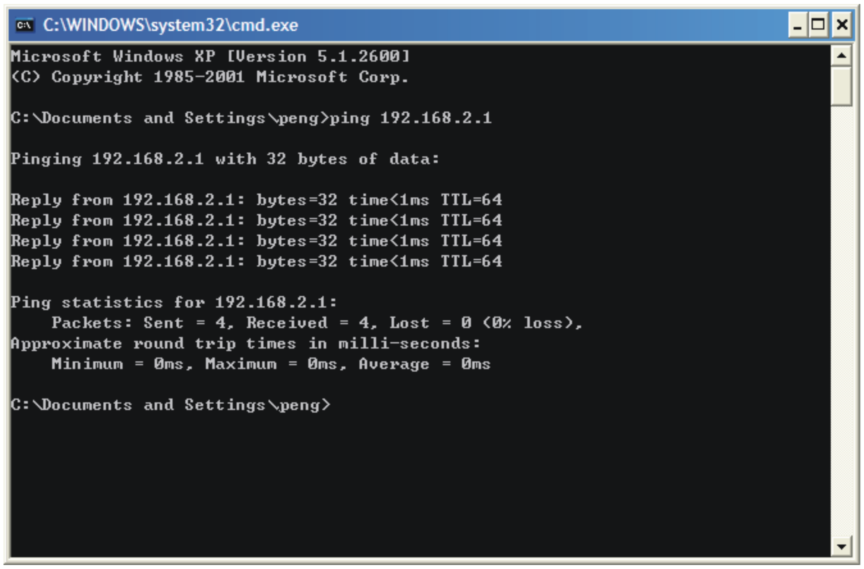
2. Then the built-in DHCP server will assign IP address for the PC.

Now you can run the Ping command at the command prompt to verify the network connection between your PC and the Router. The following example is for Windows 2000.

Open a command prompt and type "ping 192.168.2.1", and then press Enter.

If the result displayed is similar to the Figure 4 on page 32, it means a connection between your PC and the Router has been established.

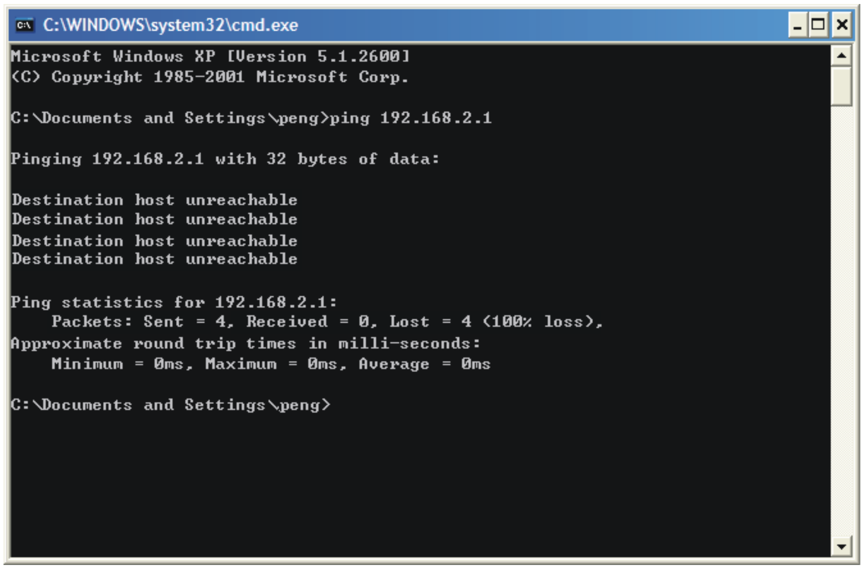
Figure 4: Success Result of a Ping Command



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\peng>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\peng>
```

If the result displayed is similar to Figure 5, it means the connection between your PC and the Router has failed.

Figure 5: Failure of a Ping Command



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\peng>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Destination host unreachable
Destination host unreachable
Destination host unreachable
Destination host unreachable

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\peng>
```

Follow these steps to check the connection:

1. Is the connection between your PC and the Router correct?

   The LAN port LED on the Router and the LED on your PC's adapter should be on.

2. Is the TCP/IP configuration for your PC correct?

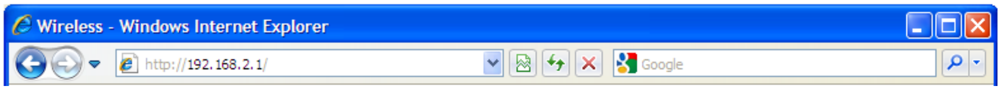
If the Router's IP address is 192.168.2.1, your PC's IP address must be within the range of 192.168.2.2 ~ 192.168.2.254.

QUICK INSTALLATION GUIDE

Using the Web-based utility, it is easy to configure and manage the Router. The Web-based utility can be used on any Windows, Macintosh, or UNIX system with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.2.1 in the address field of the browser.

Figure 6: Log in to the Router

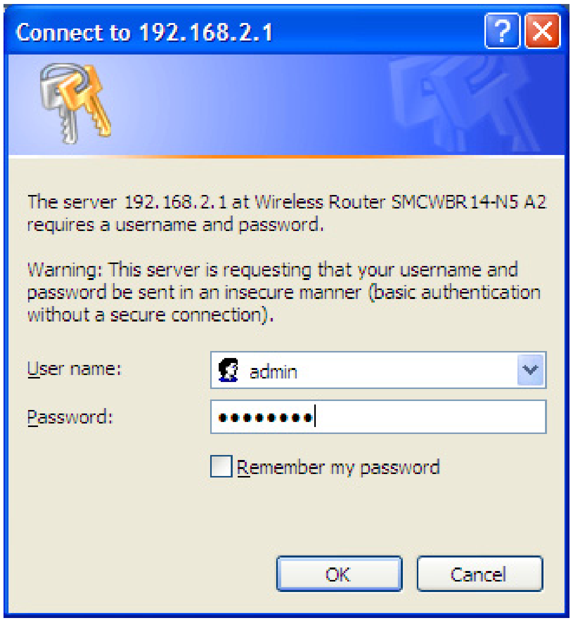


Wireless - Windows Internet Explorer

http://192.168.2.1/

After a moment, a login window appears similar to Figure 7. Enter "admin" for the User Name and "smcadmin" for the Password, both in lower case letters. Then click the OK button or press the Enter key.

Figure 7: Windows Login



Connect to 192.168.2.1

The server 192.168.2.1 at Wireless Router SMCWBR14-N5 A2 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

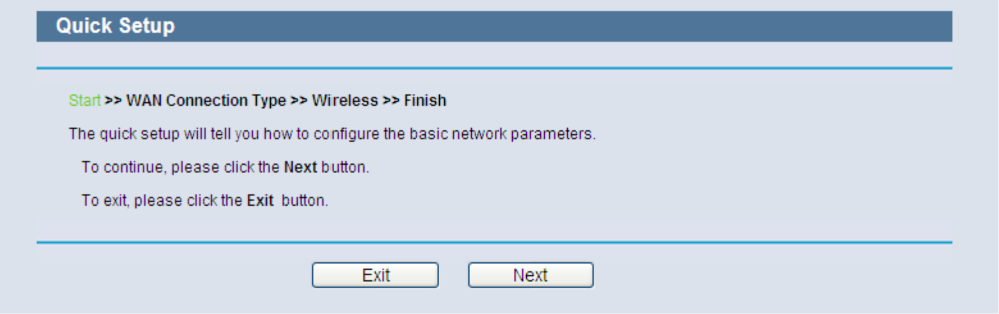
Password: ••••••••

□ Remember my password

NOTE: If the above screen does not display, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, and in the screen that displays, cancel the "Using Proxy" checkbox, and click OK.

2. After successfully logging in, click "Quick Setup" to quickly configure your Router.

Figure 8: Quick Setup



Quick Setup

Start >> WAN Connection Type >> Wireless >> Finish

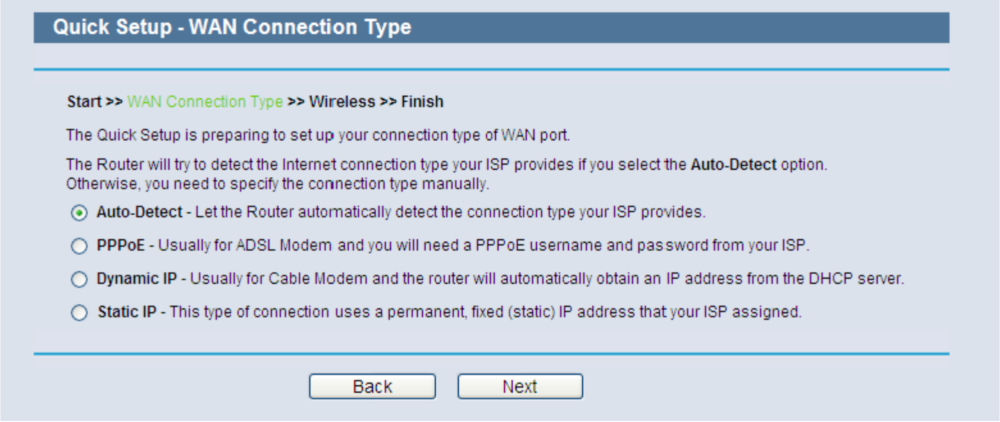
The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

3. Click Next. The WAN Connection Type page will appear, as shown in Figure 9.

Figure 9: Choose the WAN Connection Type



Quick Setup - WAN Connection Type

Start >> WAN Connection Type >> Wireless >> Finish

The Quick Setup is preparing to set up your connection type of WAN port.

The Router will try to detect the Internet connection type your ISP provides if you select the **Auto-Detect** option. Otherwise, you need to specify the connection type manually.

● **Auto-Detect** - Let the Router automatically detect the connection type your ISP provides.

○ **PPPoE** - Usually for ADSL Modem and you will need a PPPoE username and password from your ISP.

○ **Dynamic IP** - Usually for Cable Modem and the router will automatically obtain an IP address from the DHCP server.

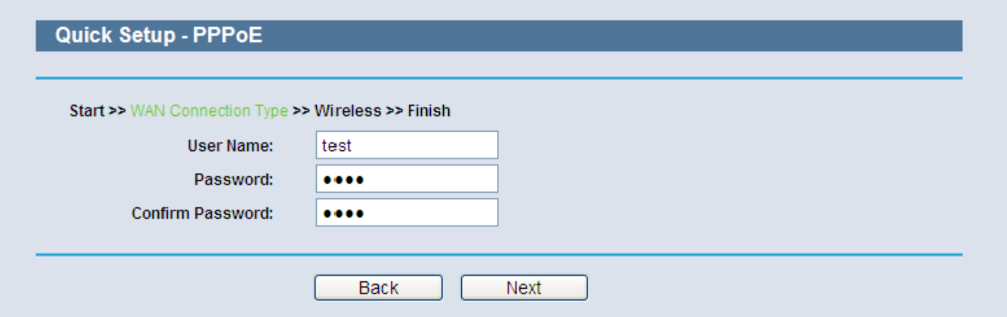
○ **Static IP** - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.

The Router provides an auto-detect function and supports three popular ways (PPPoE, Dynamic IP, and Static IP) to connect to the Internet. It is recommended that you make use of the auto-detect function. If you are sure of what kind of connection type your ISP provides, you can select the type and click Next to go on configuring.

4. If you select auto-detect, the Router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the Router.

   a. If the connection type detected is PPPoE, the screen shown in Figure 10 will display.

Figure 10: Quick Setup – PPPoE



Quick Setup - PPPoE

Start >> WAN Connection Type >> Wireless >> Finish

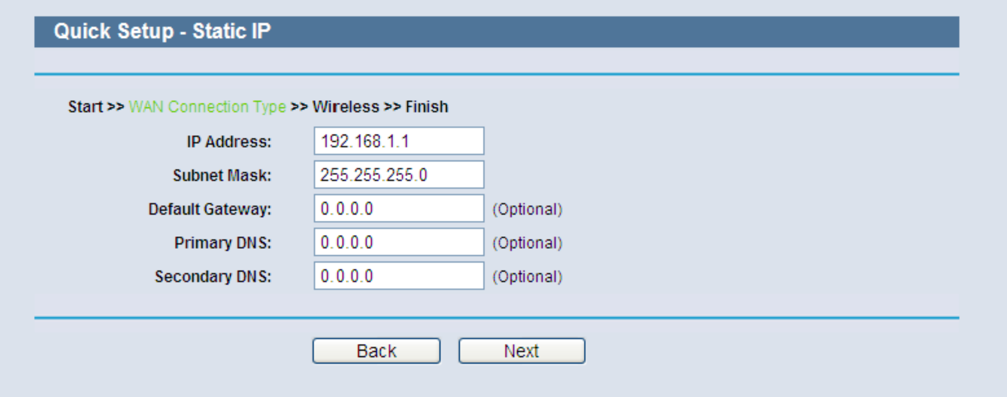
User Name:	test
Password:	••••
Confirm Password:	••••

- **User Name and Password** — Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, contact your ISP.

b. If the connection type detected is Dynamic IP, the screen shown in Figure 12 will display. You can then continue with the wireless configuration.

c. If the connection type detected is Static IP, the screen shown in Figure 11 will display.

Figure 11: Quick Setup - Static IP



Quick Setup - Static IP

Start >> WAN Connection Type >> Wireless >> Finish

IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Default Gateway:	0.0.0.0	(Optional)
Primary DNS:	0.0.0.0	(Optional)
Secondary DNS:	0.0.0.0	(Optional)

- **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.

- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.

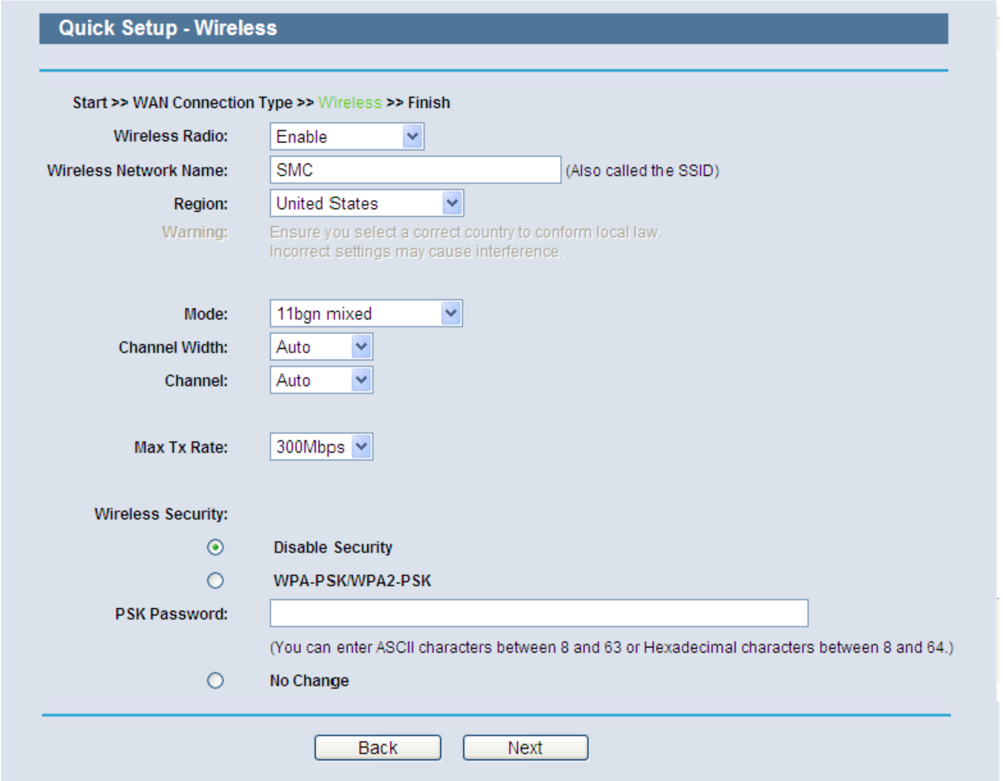
- **Default Gateway** - Enter the gateway IP address into the box, if required.

- **Primary DNS** - Enter the DNS Server IP address into the box, if required.

- **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

5. Click Next to continue. The Wireless settings page will appear, as shown in Figure 12.

Figure 12: Quick Setup – Wireless



Quick Setup - Wireless

Start >> WAN Connection Type >> Wireless >> Finish

Wireless Radio: Enable

Wireless Network Name: SMC (Also called the SSID)

Region: United States

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed

Channel Width: Auto

Channel: Auto

Max Tx Rate: 300Mbps

Wireless Security:

● Disable Security

○ WPA-PSK/WPA2-PSK

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

○ No Change

- **Wireless Radio** - Enable or disable the wireless radio choosing from the pull-down list.

- **Wireless Network Name** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to “SMC”. This value is case-sensitive. For example, “TEST” is NOT the same as “test”.

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, contact your local government agency for assistance.

- **Mode** - This field determines the wireless mode in which the Router works.

- **Channel Width** - Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.
- **Channel** - This field determines which operating frequency will be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Max Tx Rate** - You can limit the maximum transmission rate of the Router through this field.
- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA-PSK/WPA2-PSK** - Select WPA based on pre-shared passphrase.
  - PSK Password - You can enter ASCII or Hexadecimal characters.

    For **ASCII**, the key can be made up of any numbers 0 to 9 and any letters A to Z, the length should be between 8 and 63 characters.

    For **Hexadecimal**, the key can be made up of any numbers 0 to 9 and letters A to F, the length should be between 8 and 64 characters.

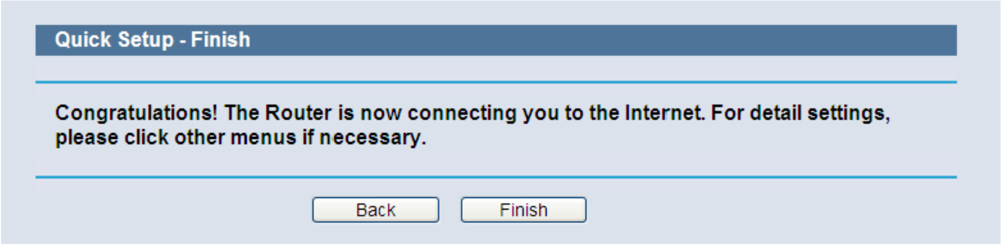
    Please also note the key is case sensitive, this means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings.
- **No Change** - If you chose this option, wireless security configuration will not change.

These settings are only for basic wireless parameters. For advanced settings, please refer to “Wireless” on page 60.

6. Click the Next button. You will then see the Finish page.

   If you don’t make any changes on the **Wireless** page, you will see the **Finish** page, as shown in Figure 13. Click the **Finish** button to finish the **Quick Setup**.

Figure 13: Quick Setup – Finish



Quick Setup - Finish

Congratulations! The Router is now connecting you to the Internet. For detail settings, please click other menus if necessary.

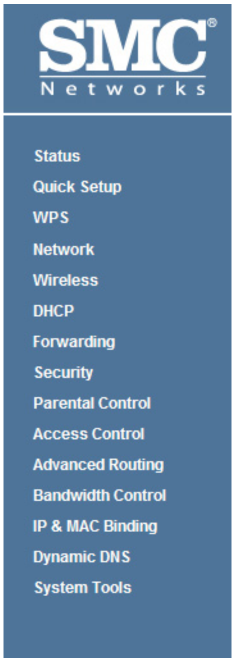
4 Configuring the Router

This chapter shows each Web page's key functions and the configuration method.

Login

After successful login, you see the main menu on the left of the Web page. On the right, there are the corresponding explanations and instructions.

Figure 14: The Main Menu

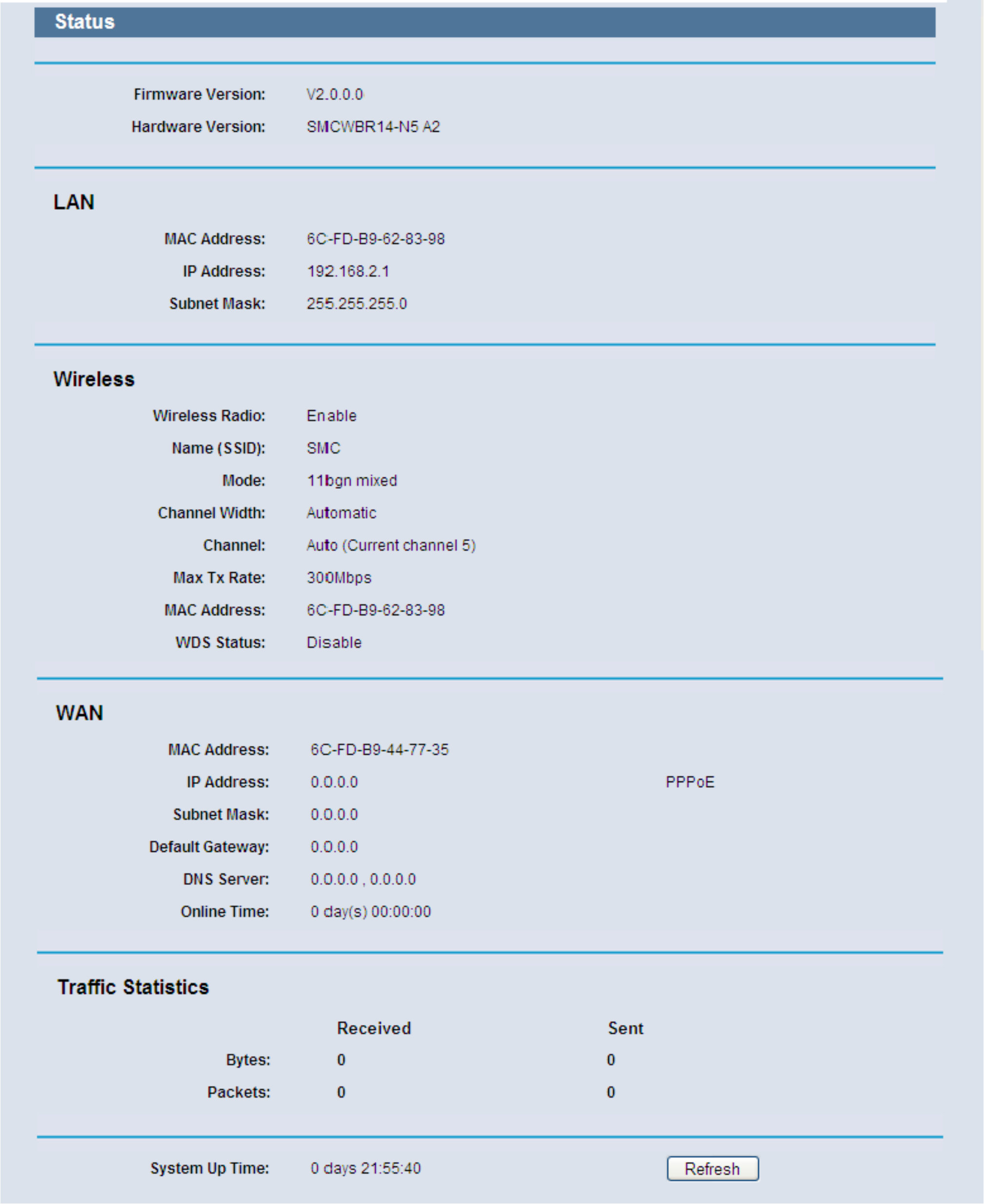


The detailed explanations for each Web page’s key functions are listed below.

STATUS

The Status page provides the current status information about the Router. All information is read-only.

Figure 15: Status



Status

Firmware Version: V2.0.0.0

Hardware Version: SMCWBR14-N5 A2

LAN

MAC Address: 6C-FD-B9-62-83-98

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enable

Name (SSID): SMC

Mode: 11bgn mixed

Channel Width: Automatic

Channel: Auto (Current channel 5)

Max Tx Rate: 300Mbps

MAC Address: 6C-FD-B9-62-83-98

WDS Status: Disable

WAN

MAC Address: 6C-FD-B9-44-77-35

IP Address: 0.0.0.0 PPPoE

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0 , 0.0.0.0

Online Time: 0 day(s) 00:00:00

Traffic Statistics

	Received	Sent
Bytes:	0	0
Packets:	0	0

System Up Time: 0 days 21:55:40

QUICK SETUP

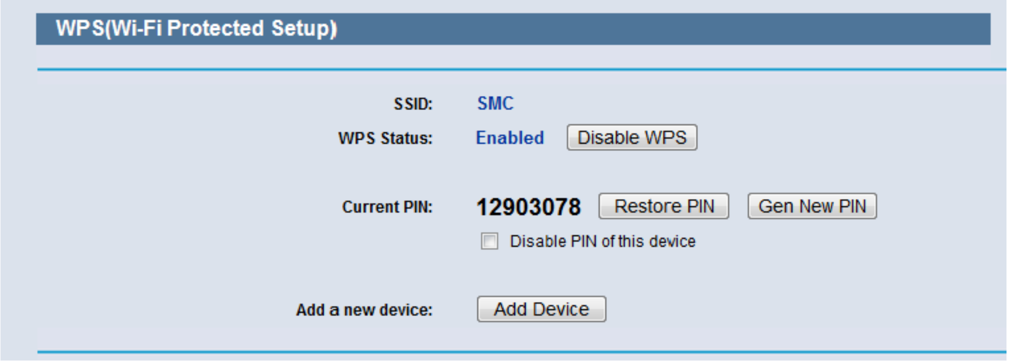
Refer to "Quick Installation Guide" on page 31.

WPS

This section shows how to quickly add a new wireless device to an existing network using **WPS** (Wi-Fi Protected Setup).

1. Select **WPS** from the menu. You will see the next screen, as shown in Figure 16.

Figure 16: WPS (Wi-Fi Protected Setup)



WPS(Wi-Fi Protected Setup)

SSID: SMC

WPS Status: Enabled

Current PIN: 12903078

□ Disable PIN of this device

Add a new device:

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of the Router's PIN is displayed here. The default PIN of the Router can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the Router to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- **Add device** - You can add a new device to the existing network manually by clicking this button.

TO ADD A NEW DEVICE:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method.

NOTE: To make a successful connection using WPS, you should also perform the corresponding WPS configuration on the new device.

For the configuration of a new device, this example uses an SMC Wireless Adapter.

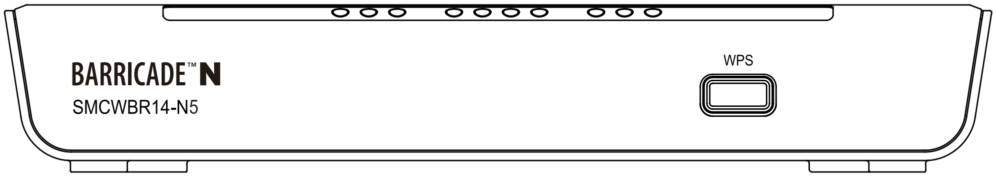
BY PBC

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

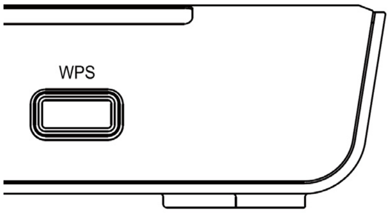
1. Enable the WPS function from Web management page.
2. Press the WPS button on the front panel of the Router.

Figure 17: Front Panel



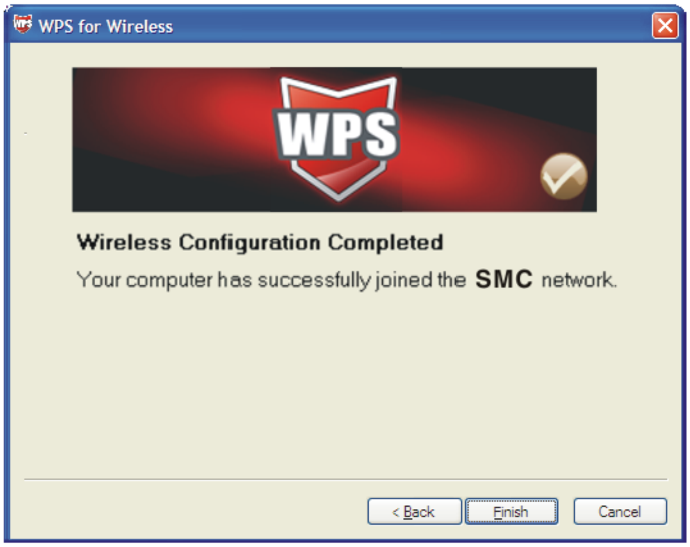
3. Press and hold the WPS button of the wireless client for 2 or 3 seconds.

Figure 18: WPS Button



4. Wait until the next screen appears. Click Finish to complete the WPS configuration.

Figure 19: WPS-Wireless Configuration Completed



Wireless Configuration Completed

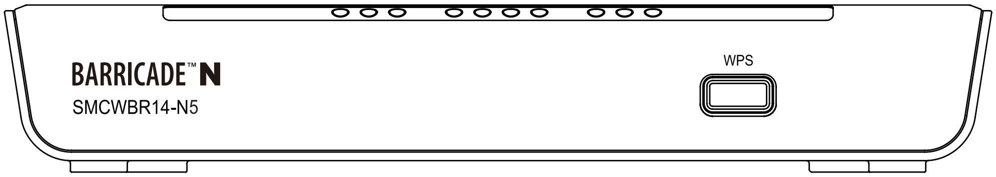
Your computer has successfully joined the SMC network.

Method Two:

1. Enable the WPS function from Web management page.

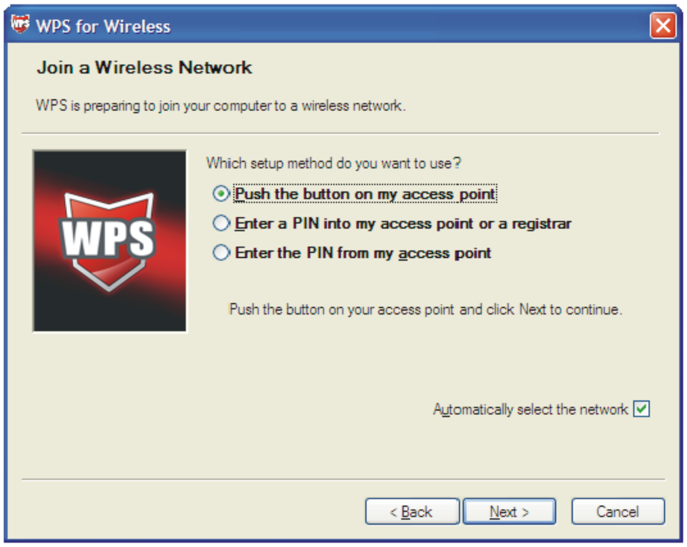
2. Press the WPS button on the front panel of the Router.

Figure 20: Front Panel



3. For the configuration of the wireless adapter, select “**Push the button on my access point**” in the WPS configuration, as below, and click Next.

Figure 21: WPS-Push the button on my access point



WPS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

● Push the button on my access point

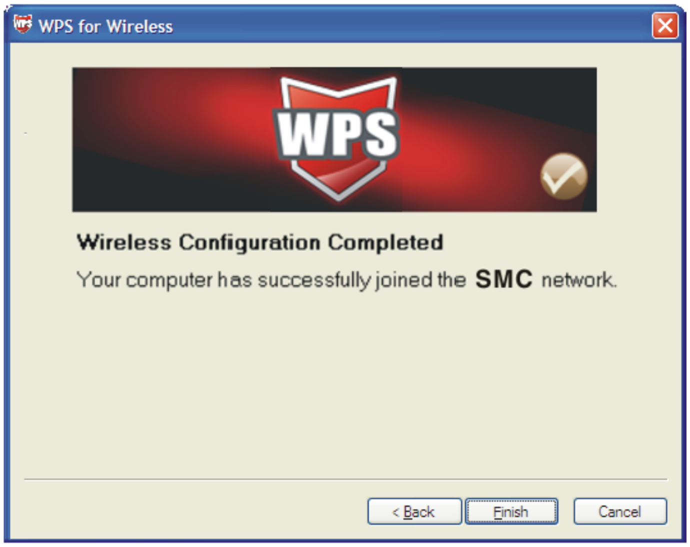
○ Enter a PIN into my access point or a registrar

○ Enter the PIN from my access point

Push the button on your access point and click Next to continue.

4. Wait until the next screen appears. Click Finish to complete the WPS configuration.

Figure 22: WPS-Wireless Configuration Completed



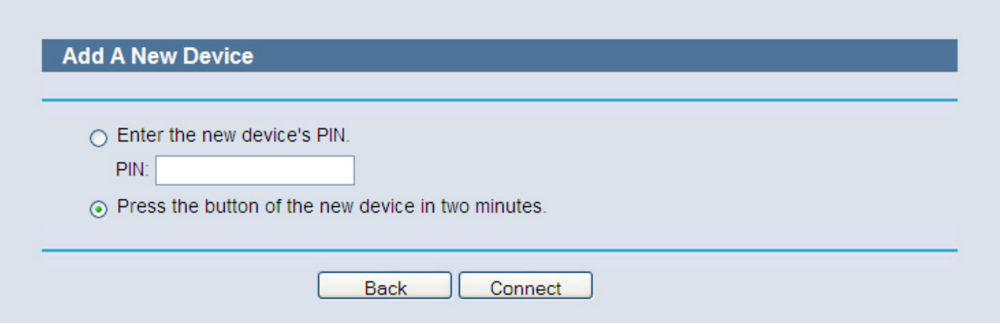
Wireless Configuration Completed

Your computer has successfully joined the **SMC** network.

Method Three:

1. Keep the default WPS Status as Enabled and click the "Add device" button in Figure 23, then the following screen will appear.

Figure 23: Add A New Device



Add A New Device

○ Enter the new device's PIN.

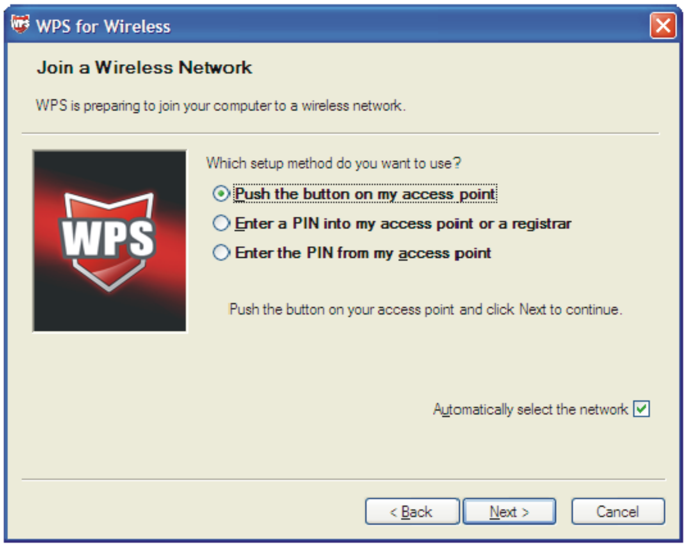
PIN:

● Press the button of the new device in two minutes.

2. Select "Press the button of the new device in two minutes" and click **Connect.**

3. For the configuration of the wireless adapter, select "Push the button on my access point" in the WPS configuration utility, as below, and click Next.

Figure 24: WPS-Push the button on my access point



WPS for Wireless

Join a Wireless Network

WPS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

● Push the button on my access point

○ Enter a PIN into my access point or a registrar

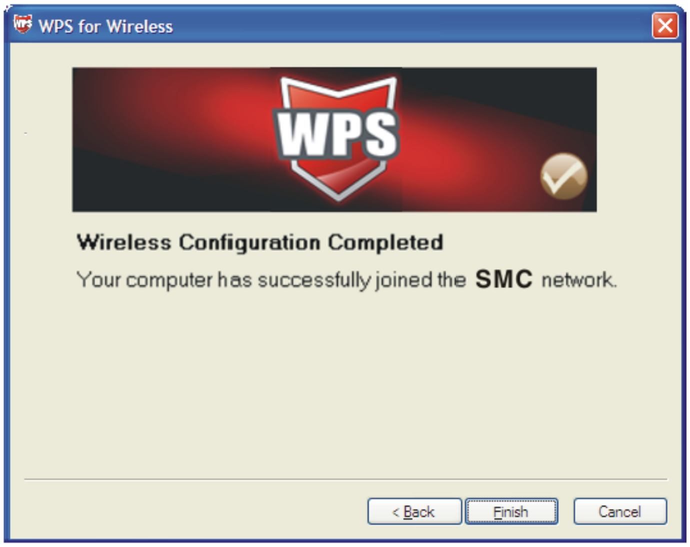
○ Enter the PIN from my access point

Push the button on your access point and click Next to continue.

Automatically select the network ☑

4. Wait until the next screen appears. Click Finish to complete the WPS configuration.

Figure 25: WPS-Wireless Configuration Completed



Wireless Configuration Completed

Your computer has successfully joined the **SMC** network.

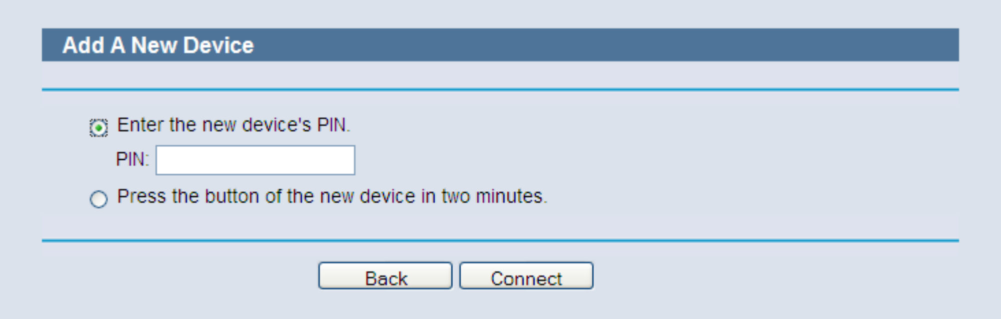
BY PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my Router.

1. Keep the default WPS Status as Enabled and click the "Add device" button in Figure 26, then the following screen will appear.

Figure 26: Add Device



Add A New Device

● Enter the new device's PIN.

PIN:

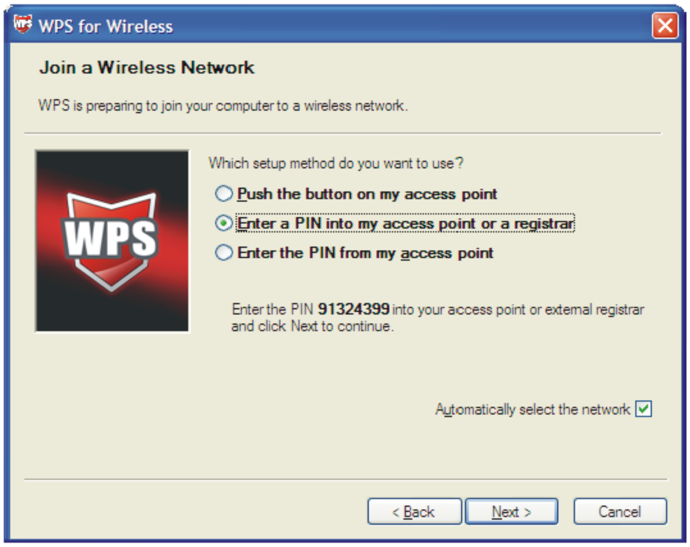
○ Press the button of the new device in two minutes.

2. Select "Enter the new device's PIN" and enter the PIN code of the wireless adapter in the field after **PIN**, as shown in the figure above. Then click **Connect**.

NOTE: The PIN code of the adapter is always displayed on the WPS configuration screen.

3. For the configuration of the wireless adapter, selected “Enter a PIN into my access point or a registrar” in the WPS configuration, as below, and click Next.

Figure 27: WPS-Enter a PIN into my access point



WPS for Wireless

Join a Wireless Network

WPS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

○ Push the button on my access point

● Enter a PIN into my access point or a registrar

○ Enter the PIN from my access point

Enter the PIN **91324399** into your access point or external registrar and click Next to continue.

Automatically select the network ☑

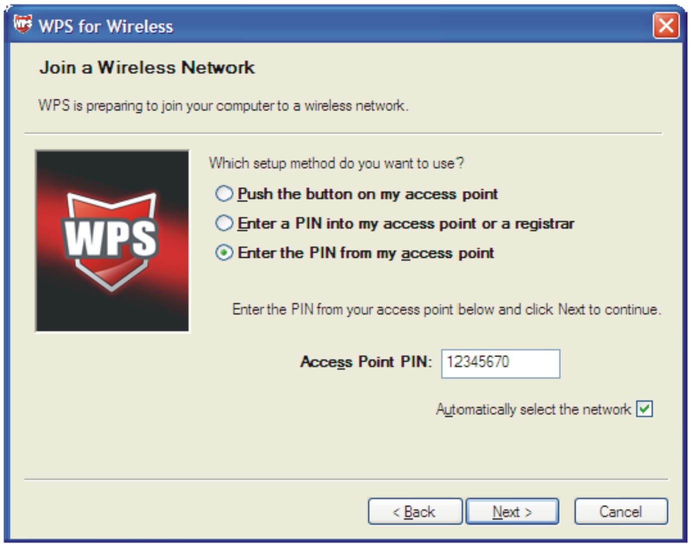
NOTE: In this example, the default PIN code of the adapter is 16952898, as shown in the above figure.

Method Two: Enter the PIN from my Router.

1. Read the Current PIN code of the Router in Figure 23 (each Router has its unique PIN code. This example has the Router PIN code 12345670).

2. For the configuration of the wireless adapter, select “Enter a PIN from my access point” in the WPS configuration utility, as below, and enter the PIN code of the Router into the field after “Access Point PIN”. Then click Next.

Figure 28: WPS-Enter a PIN from my access point



WPS for Wireless

Join a Wireless Network

WPS is preparing to join your computer to a wireless network.

Which setup method do you want to use?

○ Push the button on my access point

○ Enter a PIN into my access point or a registrar

● Enter the PIN from my access point

Enter the PIN from your access point below and click Next to continue.

Access Point PIN: 12345670

Automatically select the network ☑

NOTE: The default PIN code of the Router can be found on its label, or in the WPS configuration screen, as shown in Figure 23.

Then the new device successfully connected to the network.

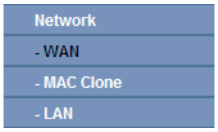
NOTE: The WPS LED on the Router will turn on green for five minutes when a device has been successfully added to the network.

NOTE: The WPS function cannot be configured if the wireless function of the Router is disabled. Make sure the wireless function is enabled before configuring WPS.

NETWORK

There are three submenus under the Network menu (shown in Figure 29): **WAN**, **MAC Clone** and **LAN**. Click any of them to configure the corresponding function.

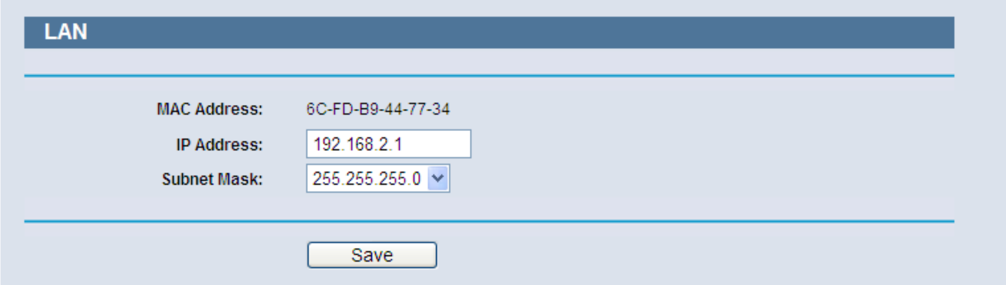
Figure 29: The Network Menu



LAN

Choose menu "**Network-> LAN**", you can configure the IP parameters of the LAN on the screen as below.

Figure 30: LAN



MAC Address: 6C-FD-B9-44-77-34

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

- **MAC Address** - The physical address of the Router, as seen from the LAN. The value cannot be changed.
- **IP Address** - Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.2.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

NOTE: If you change the IP Address of LAN, you must use the new IP Address to login the Router.

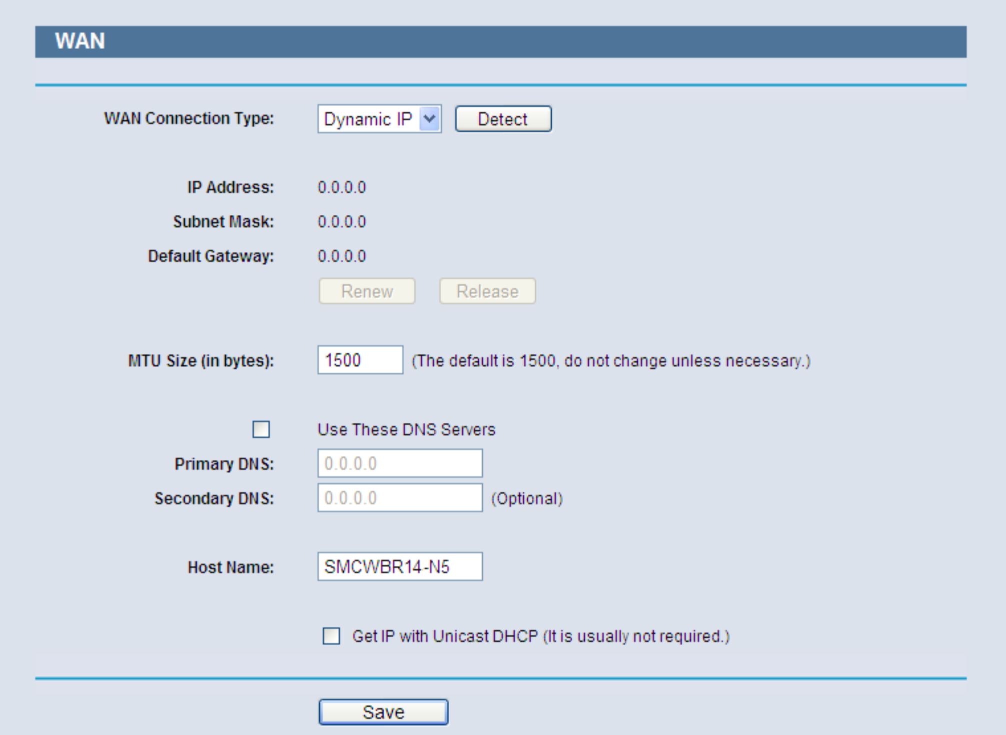
NOTE: If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

WAN

Select "**Network>WAN**", you can configure the IP parameters of the WAN on the screen below.

1. If your ISP provides the DHCP service, choose **Dynamic IP**, and the Router will automatically receive IP parameters from your ISP. You can see the page as follows (Figure 31).

Figure 31: WAN-Dynamic IP



WAN

WAN Connection Type:	Dynamic IP
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
□	Use These DNS Servers
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0 (Optional)
Host Name:	SMCWBR14-N5
	□ Get IP with Unicast DHCP (It is usually not required.)

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the Release button to release the IP parameters.

- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.

- **Use These DNS Servers** - If your ISP gives you one or two DNS addresses, select Use These DNS Servers and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

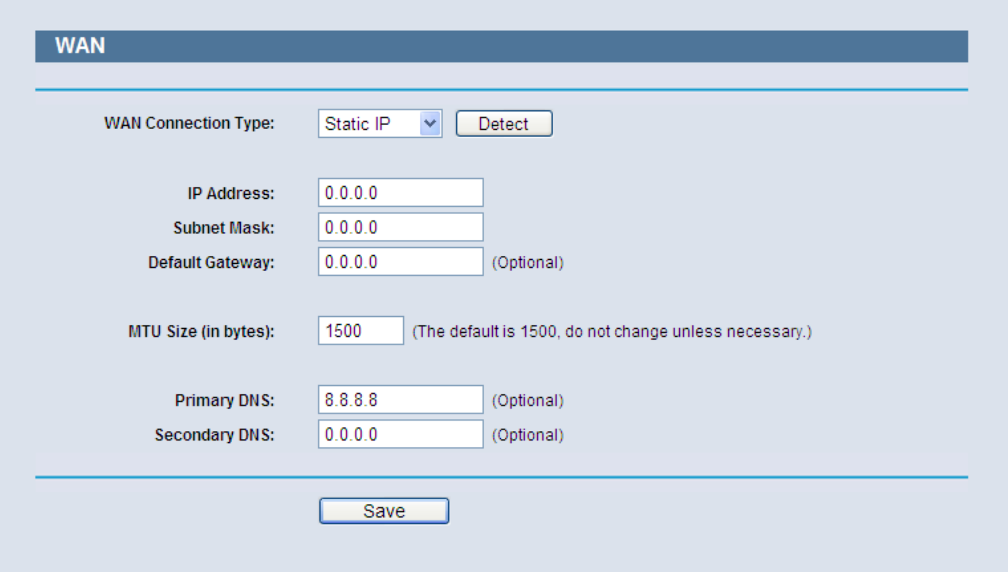
NOTE: If you find an error when you go to a Web site after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to check the DNS server addresses.

- **Get IP with Unicast DHCP** - Some ISP DHCP servers do not support broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)

Click the Save button to save your settings.

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select Static IP. The Static IP settings page will appear, shown in Figure 32.

Figure 32: WAN-Static IP



WAN

WAN Connection Type: Static IP

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 (Optional)

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS: 8.8.8.8 (Optional)
Secondary DNS: 0.0.0.0 (Optional)

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.

- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.

- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.

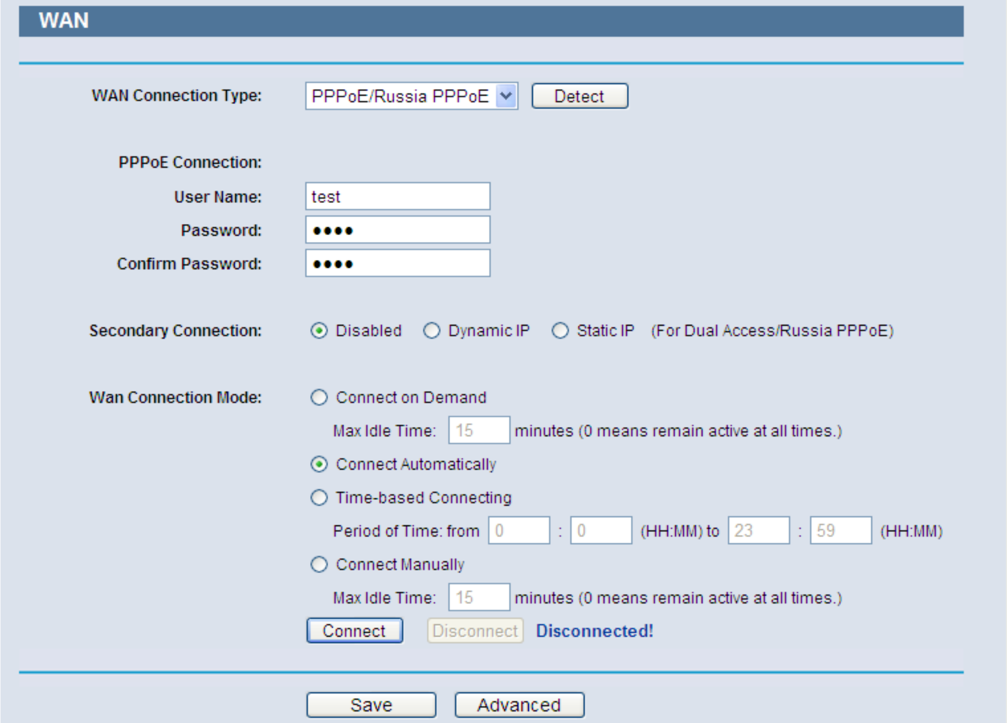
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.

- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

Click the Save button to save your settings.

3. If your ISP provides a PPPoE connection, select PPPoE option. And you should enter the following parameters (Figure 33):

Figure 33: WAN-PPPoE



WAN

WAN Connection Type: PPPoE/Russia PPPoE

PPPoE Connection:

User Name: test

Password: ●●●●

Confirm Password: ●●●●

Secondary Connection: ● Disabled ○ Dynamic IP ○ Static IP (For Dual Access/Russia PPPoE)

Wan Connection Mode:

○ Connect on Demand

Max Idle Time: 15 minutes (0 means remain active at all times.)

● Connect Automatically

○ Time-based Connecting

Period of Time: from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

○ Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

Disconnected!

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Secondary Connection** - It is available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.

  - **Disabled** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.

  - **Dynamic IP** - You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.

  - **Static IP** - You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.

- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

- **Connect Automatically** - The connection can be re-established automatically when it was down.

- **Time-based Connecting** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

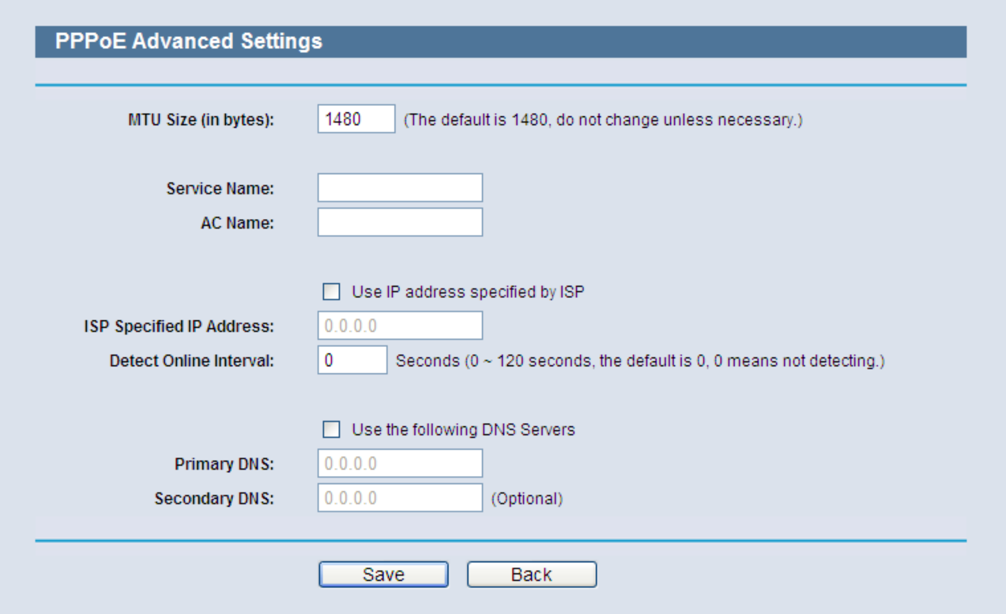
NOTE: Only when you have configured the system time on System Tools -> Time page, will the Time-based Connecting function can take effect.

- **Connect Manually** - You can click the Connect/ Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

CAUTION: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

4. If you want to do some advanced configurations, please click the Advanced button, and the page shown in Figure 34 will then appear:

Figure 34: WAN-PPPoE Advanced Settings



PPPoE Advanced Settings

MTU Size (in bytes): 1480 (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

□ Use IP address specified by ISP

ISP Specified IP Address: 0.0.0.0

Detect Online Interval: 0 Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)

□ Use the following DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

- **MTU Size** - The default MTU size is “1480” bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.

- **Service Name/AC Name** - The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the Router during login, please click “Use IP address specified by ISP” check box and enter the IP address provided by your ISP in dotted-decimal notation.

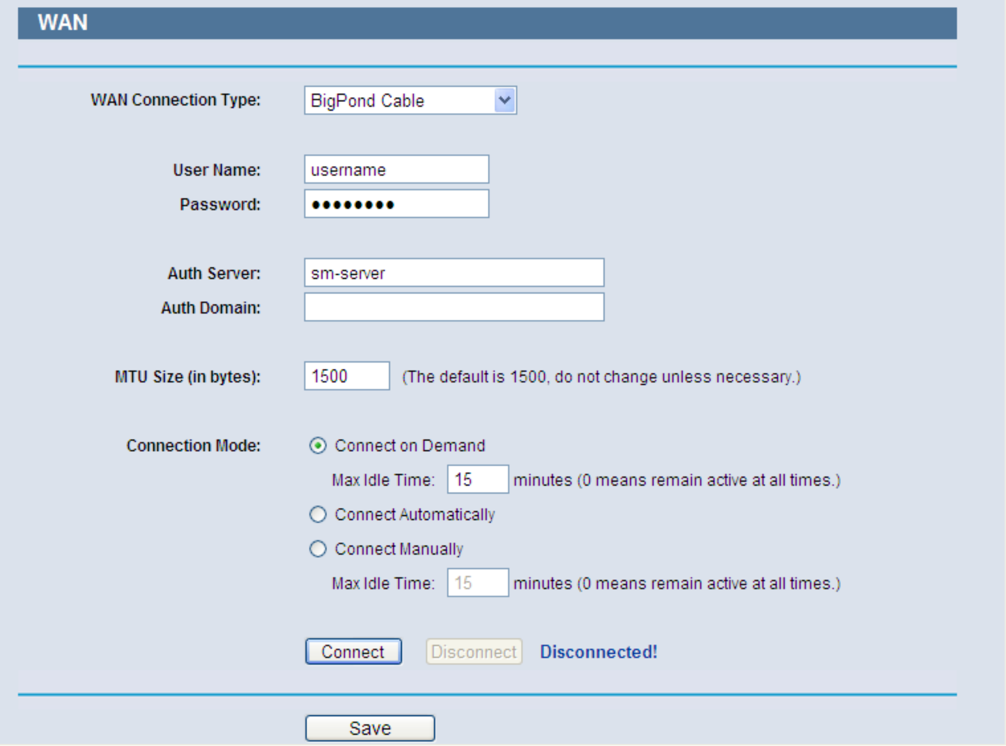
- **Detect Online Interval** - The Router will detect Access Concentrator online at every interval. The default value is “0”. You can input the value between “0”and “120”. The value “0” means no detect.

- **DNS IP address** - If your ISP does not automatically assign DNS addresses to the Router during login, please click “Use the following DNS servers” check box and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the Save button to save your settings.

5. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select BigPond Cable. And you should enter the following parameters (Figure 33):

Figure 35: WAN-BigPond Cable



WAN

WAN Connection Type:	BigPond Cable
User Name:	username
Password:	••••••••
Auth Server:	sm-server
Auth Domain:	
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
Connection Mode:	● Connect on Demand Max Idle Time: 15 minutes (0 means remain active at all times.) ○ Connect Automatically ○ Connect Manually Max Idle Time: 15 minutes (0 means remain active at all times.)

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Auth Server** - Enter the authenticating server IP address or host name.

- **Auth Domain** - Type in the domain suffix server name based on your location.

  For example:

  NSW / ACT - nsw.bigpond.net.au
  VIC / TAS / WA / SA / NT - vic.bigpond.net.au
  QLD - qld.bigpond.net.au

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.

- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

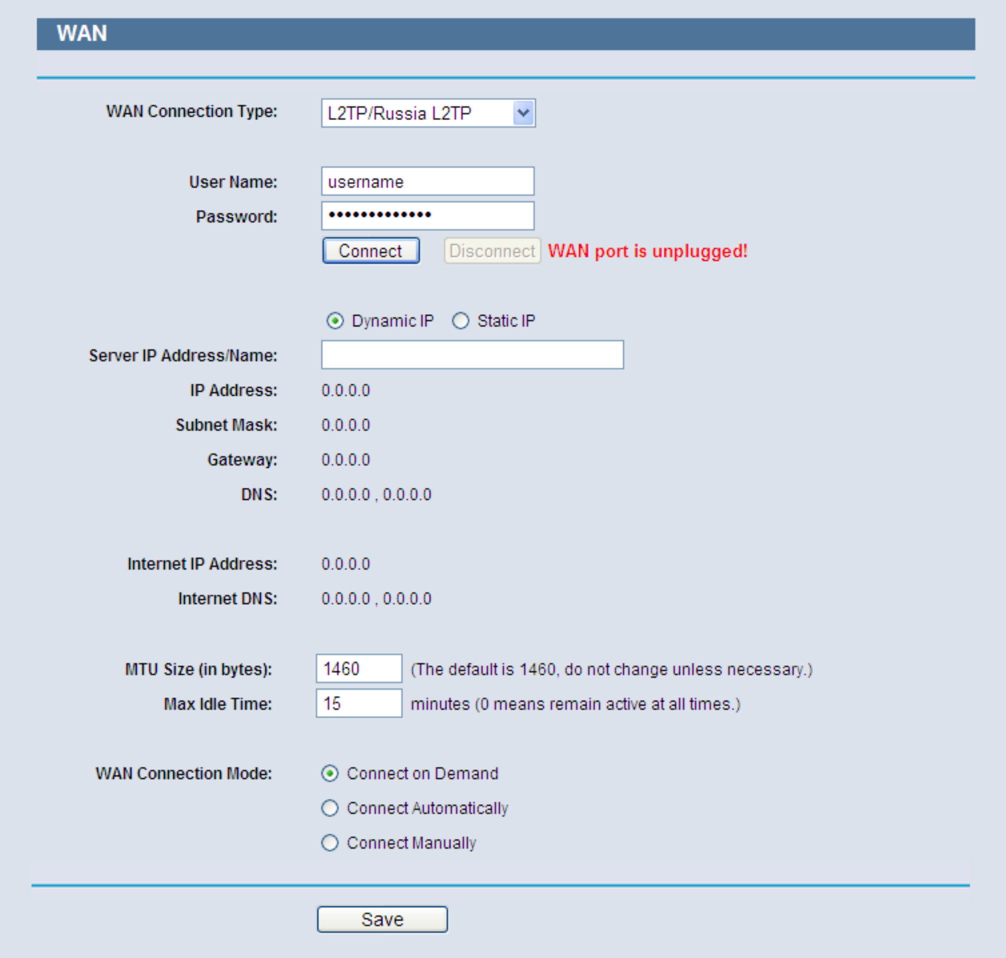
- **Connect Automatically** - The connection can be re-established automatically when it was down.

- **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.

CAUTION: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

6. If your ISP provides L2TP connection, please select L2TP option. And you should enter the following parameters (Figure 36):

Figure 36: WAN-L2TP



WAN

WAN Connection Type:	L2TP/Russia L2TP
User Name:	username
Password:	•••••••••••••
	Connect Disconnect WAN port is unplugged!
	● Dynamic IP ○ Static IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0.0 , 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0 , 0.0.0.0
MTU Size (in bytes):	1460 (The default is 1460, do not change unless necessary.)
Max Idle Time:	15 minutes (0 means remain active at all times.)
WAN Connection Mode:	● Connect on Demand ○ Connect Automatically ○ Connect Manually

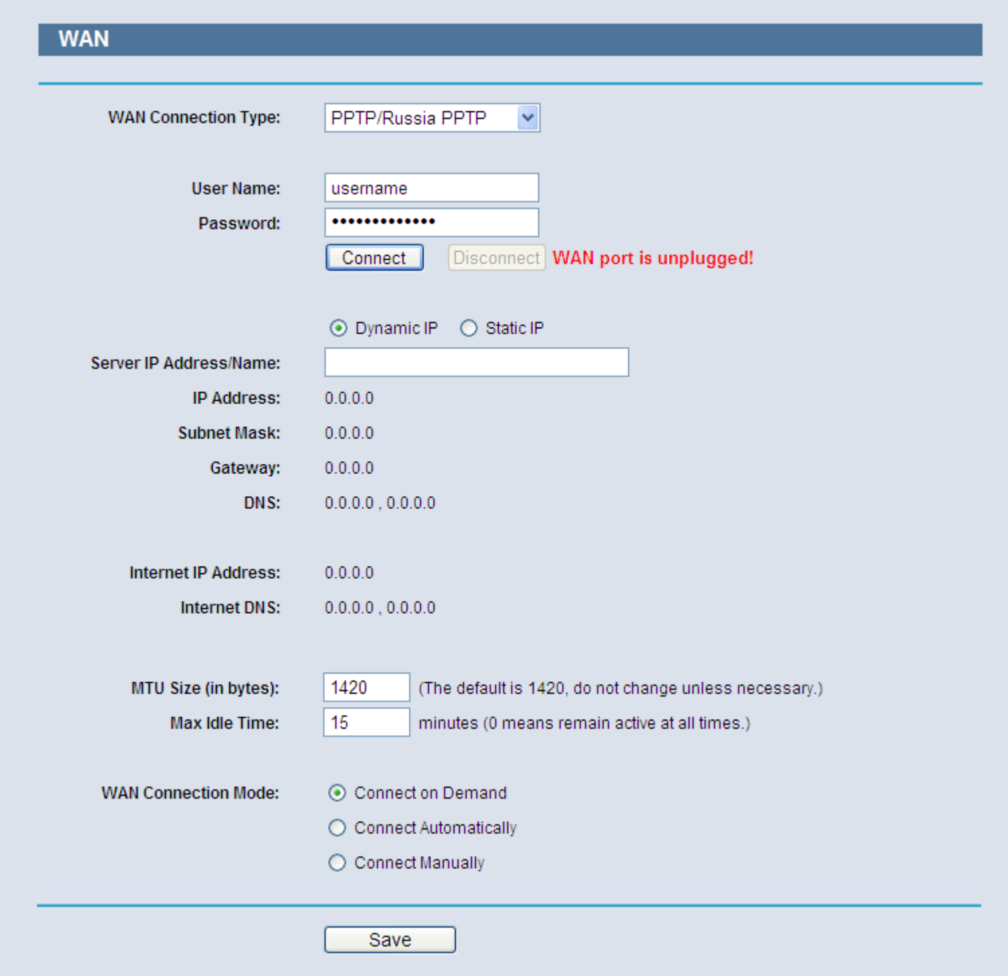
Save

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

CAUTION: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

7. If your ISP provides PPTP connection, please select PPTP option. And you should enter the following parameters (Figure 37):

Figure 37: WAN-PPTP



WAN

WAN Connection Type: PPTP/Russia PPTP

User Name: username
Password: ••••••••••••••
Connect Disconnect WAN port is unplugged!

● Dynamic IP ○ Static IP
Server IP Address/Name:
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
DNS: 0.0.0.0 , 0.0.0.0

Internet IP Address: 0.0.0.0
Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): 1420 (The default is 1420, do not change unless necessary.)
Max Idle Time: 15 minutes (0 means remain active at all times.)

WAN Connection Mode:
● Connect on Demand
○ Connect Automatically
○ Connect Manually

Save

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP and enter the ISP's IP address or the domain name. If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the Save button. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.

- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this option, click the radio button.

- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

CAUTION: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

NOTE: If you do not know how to choose the appropriate connection type, click the Detect button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

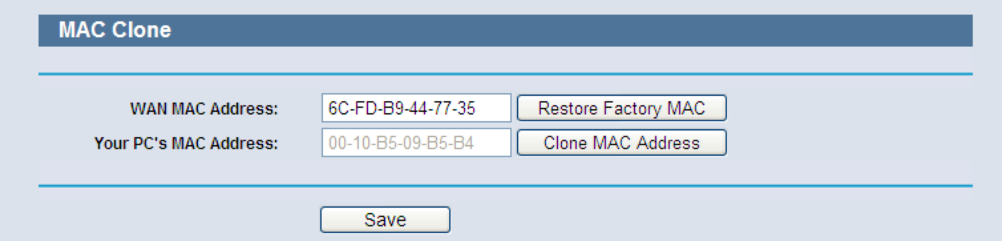
- PPPoE - Connections which use PPPoE that requires a user name and password.
- Dynamic IP - Connections which use dynamic IP address assignment.
- Static IP - Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

MAC CLONE

Choose menu “**Network->MAC Clone**”, you can configure the MAC address of the WAN on the screen below, Figure 38:

Figure 38: MAC Address Clone



MAC Clone

WAN MAC Address: 6C-FD-B9-44-77-35

Your PC's MAC Address: 00-10-B5-09-B5-B4

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the Router. If the MAC address is required, you can click the Clone MAC Address To button and this MAC address will fill in the WAN MAC Address field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

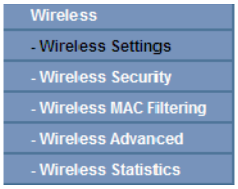
Click the **Save** button to save your settings.

NOTE: Only the PC on your LAN can use the MAC Address Clone function.

WIRELESS

There are five submenus under the Wireless menu (shown in Figure 39): **Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced,** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

Figure 39: Wireless Menu

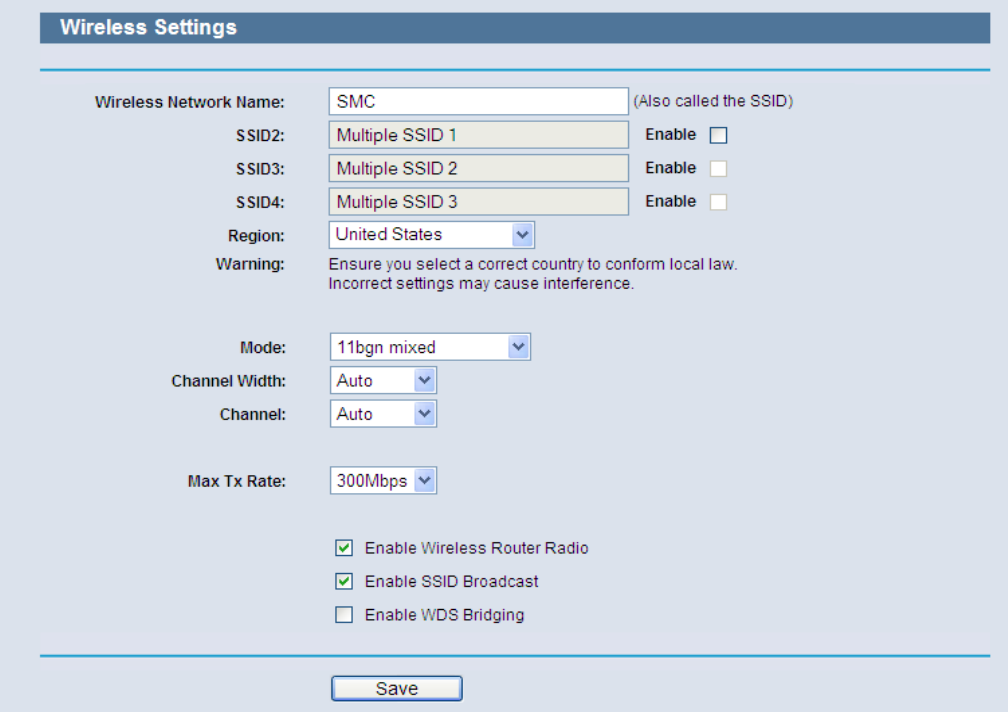


WIRELESS SETTINGS (ROUTER MODE)

Choose menu **Wireless -> Wireless Setting**; you can configure the basic settings for the wireless network on this page.

The wireless settings section displays configuration settings for the access point functionality of the Wireless AP/router. It includes the following sections:

Figure 40: Wireless Settings



Wireless Settings

Wireless Network Name: SMC (Also called the SSID)

SSID2: Multiple SSID 1 Enable □

SSID3: Multiple SSID 2 Enable □

SSID4: Multiple SSID 3 Enable □

Region: United States

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed

Channel Width: Auto

Channel: Auto

Max Tx Rate: 300Mbps

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

□ Enable WDS Bridging

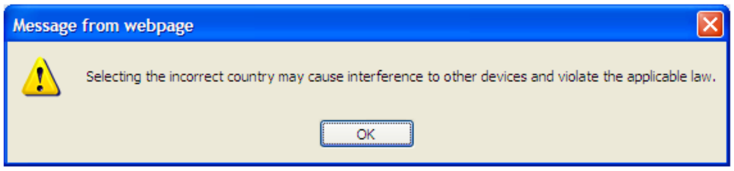
- **Wireless Network Name** - Enter a value of up to 32 characters. The same SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be "SMC". This value is case-sensitive. For example, "TEST" is NOT the same as "test".

- **SSID (2-4)** - Up to four SSIDs for each BSS can be set, the names can be up to 32 characters. The multi-SSID function is available only when Enable is checked.

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, click the Save button, then the Note Dialog appears. Click OK.

Figure 41: Note Dialog



Message from webpage

Selecting the incorrect country may cause interference to other devices and violate the applicable law.

NOTE: Limited by local law regulations, the version for North America does not have a region selection option.

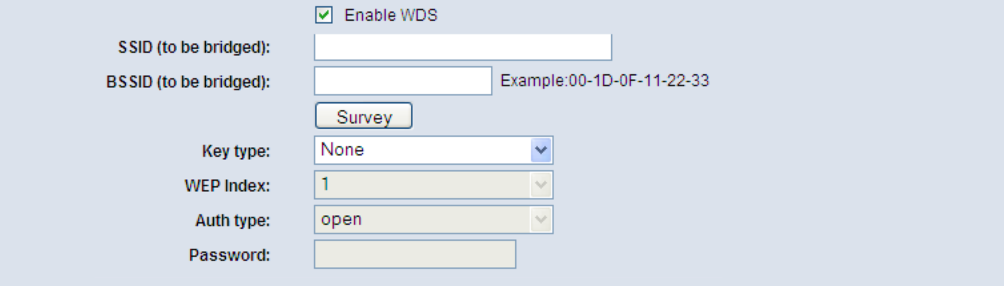
- **Mode** - Select the operating mode. The default is **11b/g/n mixed**.
  - **11b only** - Select if all of your wireless clients are 802.11b.
    11g only - Select if all of your wireless clients are 802.11g.
    11n only- Select only if all of your wireless clients are 802.11n.
    11b/g mixed - Select if you are using both 802.11b and 802.11g wireless clients.
    11b/g/n mixed - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

    When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the Router. It is strongly recommended to set the mode to 11b/g/n mixed, then all 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.
- **Channel width** - Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.
- **Channel** - This field determines which operating frequency will be used for wireless operation. The default setting is Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

NOTE: If 11b only, 11g only, or 11bg mixed is selected in the Mode field, the Channel Width selecting field will turn grey and the value will become 20M, which cannot be changed.

- **Max Tx Rate** - You can limit the maximum transmit rate of the Router through this field.
- **Enable Wireless Router Radio** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- **Enable SSID Broadcast** - When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the Enable SSID Broadcast checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- **Enable WDS** - Check this box to enable WDS. With this function, the Router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown in Figure 42. Make sure the following settings are correct.

Figure 42: Enable WDS



☑ Enable WDS

SSID (to be bridged):

BSSID (to be bridged): Example:00-1D-0F-11-22-33

Key type: None

WEP Index: 1

Auth type: open

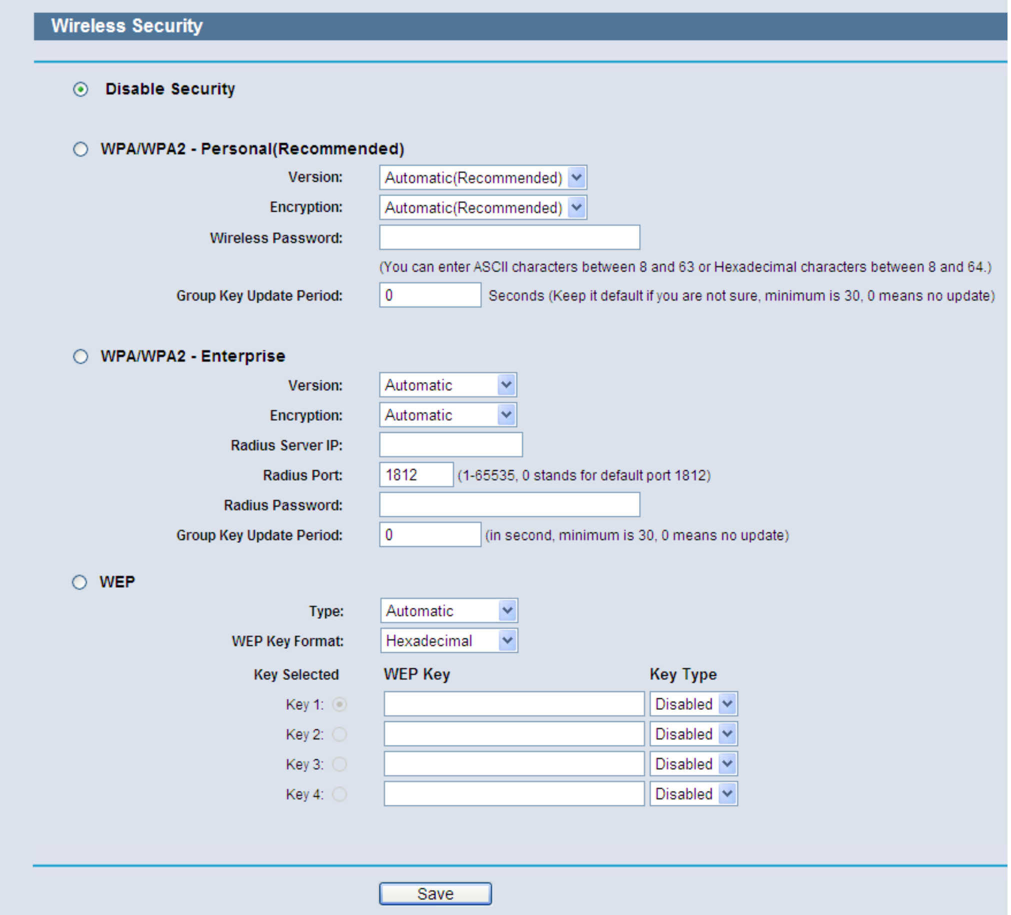
Password:

WIRELESS SECURITY

Choose menu "**Wireless->Wireless Security**"; you can then configure the security settings of your wireless network.

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key), and WPA-PSK (Pre-Shared Key).

Figure 43: Wireless Security



Wireless Security

● Disable Security

○ WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended)

Encryption: Automatic(Recommended)

Wireless Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

○ WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ WEP

Type: Automatic

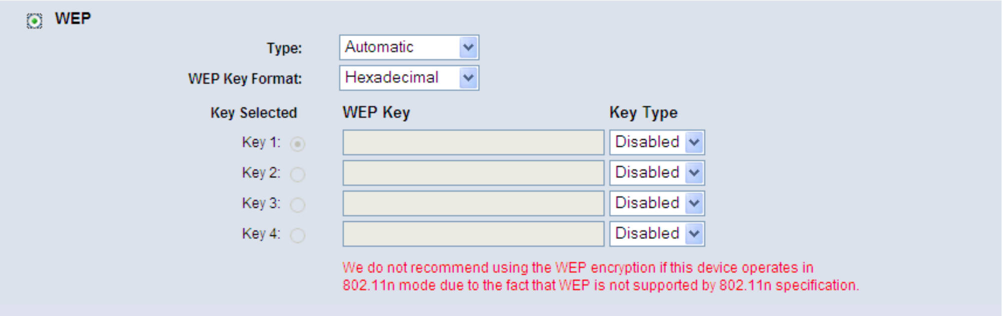
WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

- **Disable Security** - If you do not want to use wireless security, select this check box. However, it is strongly recommended to choose one of the following modes to enable security.

- **WEP** - This security is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red, as shown in Figure 44.

Figure 44: WEP



◉ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

We do not recommend using the WEP encryption if this device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.

  - **Type** - you can choose the type for the WEP security on the pull-down list. The default setting is Automatic, which can select Open System or Shared-Key authentication type automatically based on the wireless station's capability and request.

  - **WEP Key Format** - Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.

  - **WEP Key**- Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.

  - **Key Type** - You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

    - **64-bit** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.
      128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.
      152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

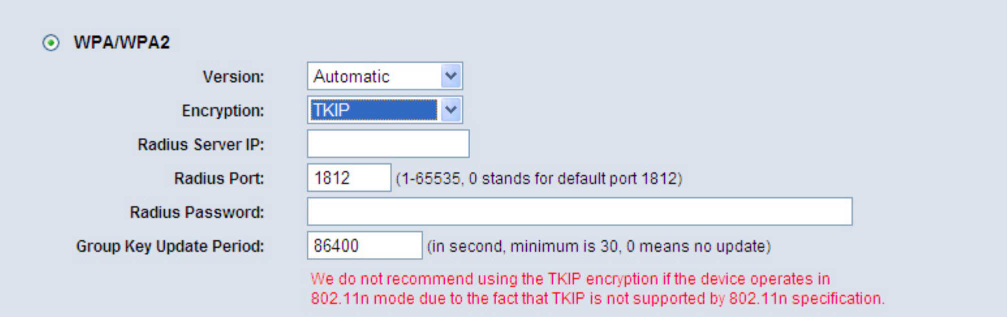
NOTE: If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as the Authentication Type.

- **WPA /WPA2 Enterprise** - Authentication that uses a RADIUS Server.

- **Version** - you can choose the version of the WPA security on the pull-down list. The default setting is Automatic, which can select WPA (Wi-Fi Protected Access) or WPA2 (WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption** - You can select either Automatic, TKIP, or AES.

NOTE: If you check the WPA/WPA2 radio button and choose TKIP encryption, you will find a notice in red, as shown in Figure 45.

Figure 45: WPA/WPA2-Enterprise



◉ WPA/WPA2

Version: Automatic

Encryption: TKIP

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 86400 (in second, minimum is 30, 0 means no update)

We do not recommend using the TKIP encryption if the device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

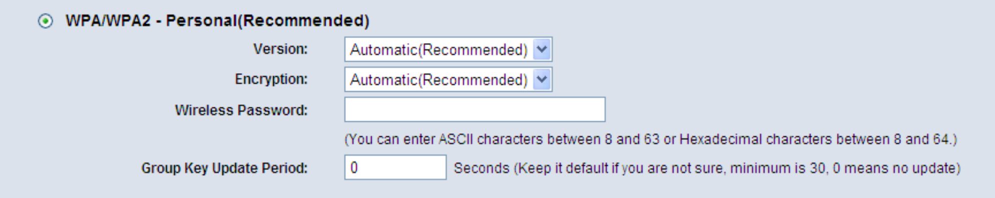
- **Radius Server IP** - Enter the IP address of the RADIUS Server.
- **Radius Port** - Enter the port that the RADIUS service uses.
- **Radius Password** - Enter the password for the RADIUS server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

◆ **WPA/WPA2 Personal** - The WPA/WPA2 authentication type based on a pre-shared passphrase.

- **Version** - You can choose the version of the WPA-PSK security from the drop-down list. The default setting is Automatic, which can select WPA-PSK (Pre-shared key of WPA) or WPA2-PSK (Pre-shared key of WPA2) automatically based on the wireless station's capability and request.
- **Encryption** - When WPA-PSK or WPA is set as the Authentication Type, you can select either Automatic, TKIP, or AES as the encryption type.

NOTE: If you check the WPA-PSK/WPA2-PSK radio button and choose TKIP encryption, you will find a notice in red, as shown in Figure 46.

Figure 46: WPA/WPA2 - Personal(Recommended)



● WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended)

Encryption: Automatic(Recommended)

Wireless Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

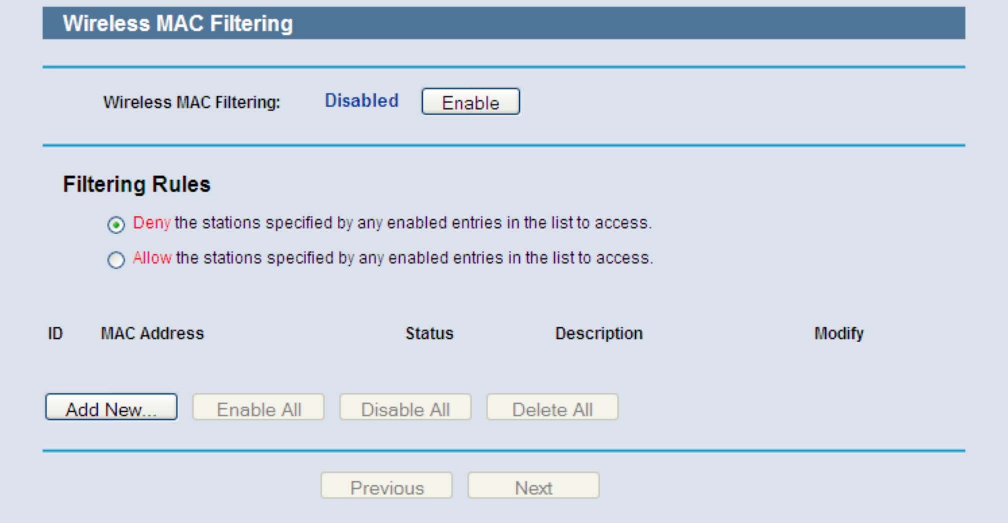
- **PSK Passphrase** - You can enter between 8 and 63 ASCII characters, or 8 to 64 Hexadecimal characters.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Be sure to click the Save button to save your settings on this page.

WIRELESS MAC FILTERING

Choose **Wireless -> MAC Filtering** from the menu; you can then control wireless access by configuring the Wireless MAC Address Filtering function, as shown in Figure 47.

Figure 47: Wireless MAC Address Filtering



Wireless MAC Filtering

Wireless MAC Filtering: Disabled

Filtering Rules

● Deny the stations specified by any enabled entries in the list to access.

○ Allow the stations specified by any enabled entries in the list to access.

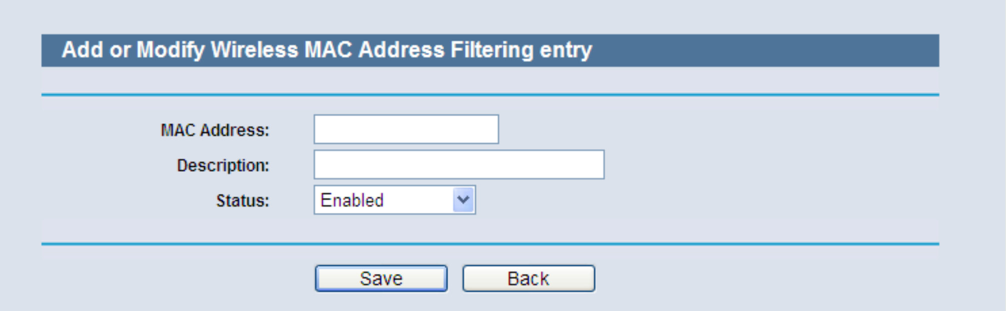
ID	MAC Address	Status	Description	Modify

To filter wireless users by MAC Address, click Enable. The default setting is Disable.

- **MAC Address** - The wireless station's MAC address that you want to filter.
- **Status** - The status of this entry, either Enabled or Disabled.
- **Description** - A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the "Add New" button. The "Add or Modify Wireless MAC Address Filtering entry" page will appear, as shown in Figure 48:

Figure 48: Add or Modify Wireless MAC Address Filtering Entry



Add or Modify Wireless MAC Address Filtering entry

MAC Address:

Description:

Status: Enabled

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the MAC Address field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-00-07-8A.
2. Provide a simple description of the wireless station in the Description field. For example: Wireless station A.
3. Select Enabled or Disabled for this entry on the Status pull-down list.
4. Click the Save button to save this entry.

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete button.
2. Modify the information.
3. Click the Save button.

   Click the Enable All button to make all entries enabled.

   Click the Disabled All button to make all entries disabled.

   Click the Delete All button to delete all entries.

   Click the Next button to go to the next page.

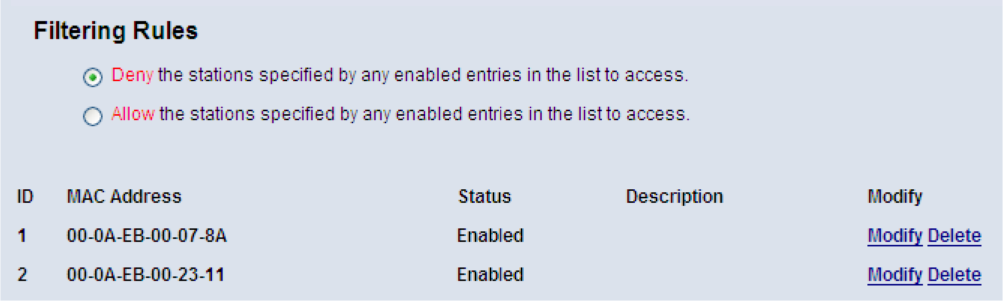
   Click the Previous button to return to the previous page.

For example: If you want wireless station A (MAC address 00-0A-EB-00-07-8A) and wireless station B (MAC address 00-0A-EB-00-23-11) to be able to access the Router, but not all the other wireless stations, you can configure the Wireless MAC Address Filtering list as follows:

1. Click the Enable button to enable this function.
2. Select the radio button: Deny the stations not specified by any enabled entries in the list to access for Filtering Rules.
3. Delete all or disable all entries if there are any entries already.
4. Click the Add New button.
   1. Enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the MAC Address field.
   2. Enter wireless station A/B in the Description field.
   3. Select Enabled in the Status pull-down list.
   4. Click the Save Button.
   5. Click the Back button.

The filtering rules that are configured should look similar to the following list:

Figure 49: Filtering Rules



Filtering Rules

● Deny the stations specified by any enabled entries in the list to access.

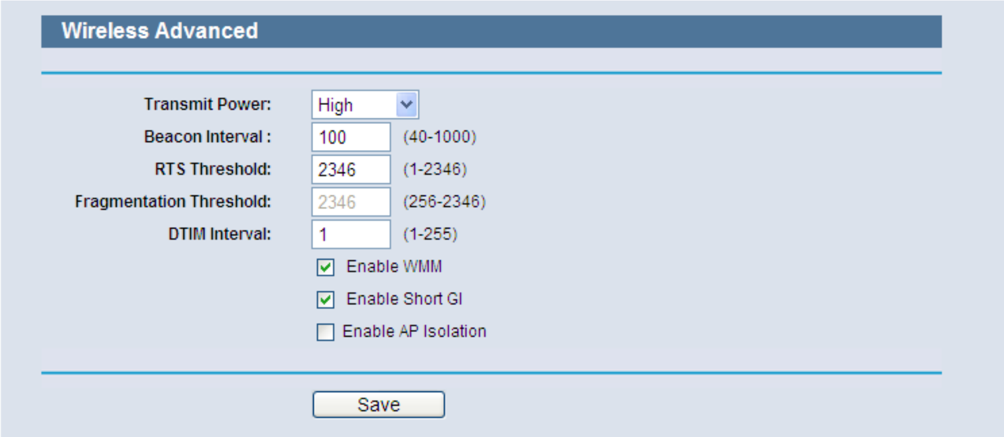
○ Allow the stations specified by any enabled entries in the list to access.

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-8A	Enabled		Modify Delete
2	00-0A-EB-00-23-11	Enabled		Modify Delete

WIRELESS ADVANCED

Choose **Wireless -> Wireless Advanced** from the menu; you can then configure the advanced settings of your wireless network.

Figure 50: Wireless Advanced



Transmit Power: High
Beacon Interval : 100 (40-1000)
RTS Threshold: 2346 (1-2346)
Fragmentation Threshold: 2346 (256-2346)
DTIM Interval: 1 (1-255)
☑ Enable WMM
☑ Enable Short GI
□ Enable AP Isolation

- **Transmit Power** - Here you can specify the transmit power of the Router. You can select High, Middle, or Low. High is the default setting and is recommended.

- **Beacon Interval** - Enter a value between 20-1000 milliseconds for the Beacon Interval. The beacons are packets sent by the router to synchronize a wireless network. The Beacon Interval value determines the time interval of beacons. The default value is 100.

- **RTS Threshold** - Specifies the RTS (Request to Send) Threshold. If a packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold** - This value determines the maximum size before packets are fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets may be sent. The default setting is 2346 and is recommended.

- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

- **Enable WMM** - The WMM function guarantees that packets with high-priority messages are transmitted before other packets. It is strongly recommended to enable this feature.

- **Enable Short GI** - This function is recommended, since it increases the data capacity by reducing the guard interval time.

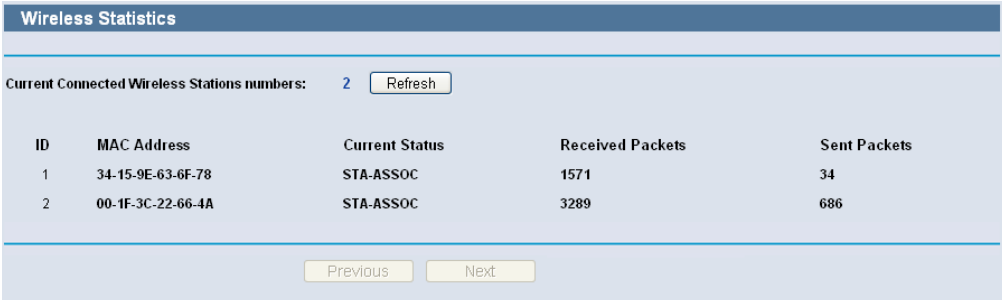
- **Enabled AP Isolation** - This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router, but not with each other. To use this function, check this box. AP Isolation is disabled by default.

NOTE: If you are not familiar with the settings on this page, it is strongly recommended to keep the default values; otherwise it may result in lower wireless network performance.

WIRELESS STATISTICS

Select **Wireless -> Wireless Statistics** from the menu; you can see the MAC Address, Current Status, Received Packets, and Sent Packets for each connected wireless station.

Figure 51: Wireless Statistics



Wireless Statistics

Current Connected Wireless Stations numbers: 2

ID	MAC Address	Current Status	Received Packets	Sent Packets
1	34-15-9E-63-6F-78	STA-ASSOC	1571	34
2	00-1F-3C-22-66-4A	STA-ASSOC	3289	686

- **MAC Address** - The connected wireless station's MAC address.

- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.

- **Received Packets** - Packets received by the station.

- **Sent Packets** - Packets sent by the station.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the Refresh button.

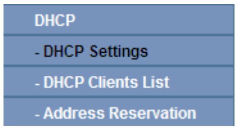
If the numbers of connected wireless stations go beyond one page, click the Next button to go to the next page, and click the Previous button to return the previous page.

NOTE: This page will be refreshed automatically every 5 seconds.

DHCP

There are three submenus under the DHCP menu (shown in Figure 52): **DHCP Settings**, **DHCP Clients List**, and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

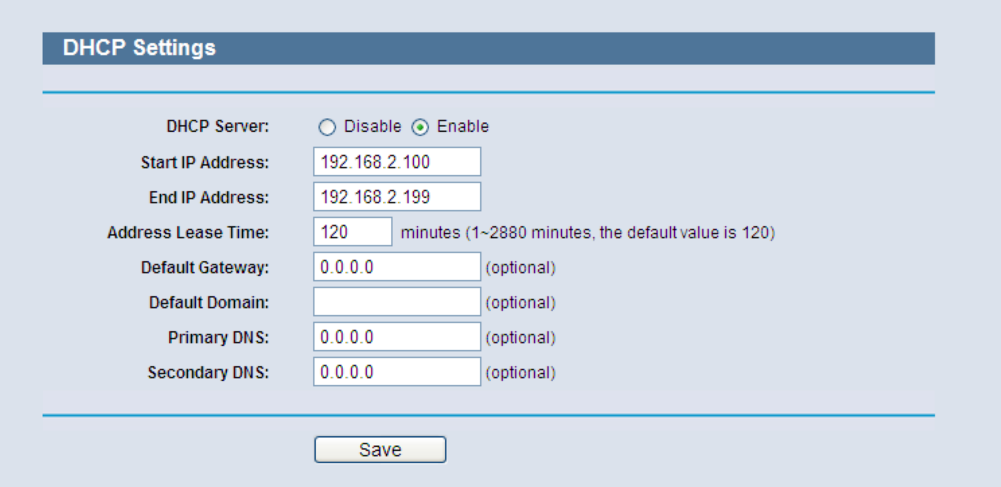
Figure 52: The DHCP Menu



DHCP SETTINGS

Select **DHCP -> DHCP Settings** from the menu. You can configure the DHCP Server on the page, as shown in Figure 53. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the Router on the LAN.

Figure 53: DHCP Settings



DHCP Settings

DHCP Server:	○ Disable ● Enable
Start IP Address:	192.168.2.100
End IP Address:	192.168.2.199
Address Lease Time:	120 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	0.0.0.0 (optional)
Default Domain:	(optional)
Primary DNS:	0.0.0.0 (optional)
Secondary DNS:	0.0.0.0 (optional)

- **DHCP Server** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server in your network or you must configure computers manually.

- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.2.100 is the default start address.

- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.2.199 is the default end address.

- **Address Lease Time** - The amount of time a network user will be allowed connection to the Router with their current dynamic IP Address.

Enter the amount of time in minutes and the user will be “leased” this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

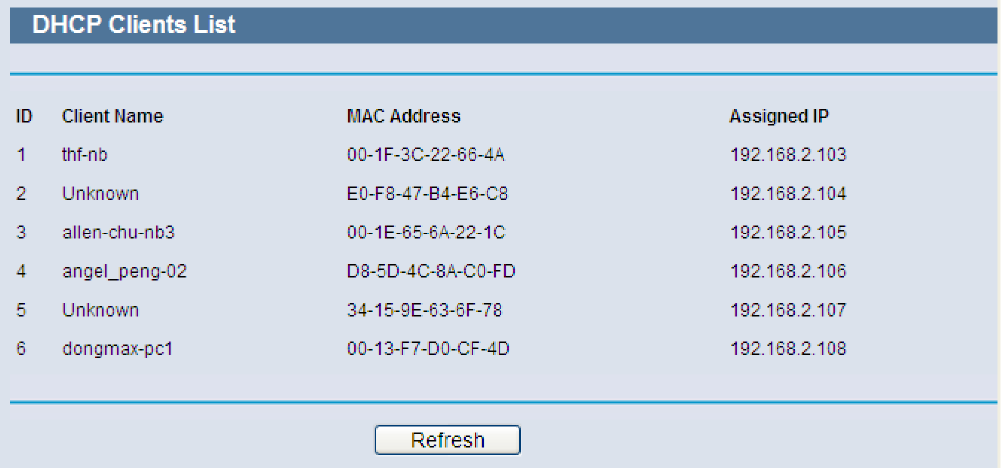
- **Default Gateway** - (Optional.) Suggest to input the IP address of the LAN port of the Router, default value is 192.168.2.1
- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

NOTE: To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode.

DHCP CLIENTS LIST

Select **DHCP -> DHCP Clients List** from the menu; you can view the information about the clients attached to the Router in the next screen (shown in Figure 54).

Figure 54: DHCP Clients List



DHCP Clients List

ID	Client Name	MAC Address	Assigned IP
1	thf-nb	00-1F-3C-22-66-4A	192.168.2.103
2	Unknown	E0-F8-47-B4-E6-C8	192.168.2.104
3	allen-chu-nb3	00-1E-65-6A-22-1C	192.168.2.105
4	angel_peng-02	D8-5D-4C-8A-C0-FD	192.168.2.106
5	Unknown	34-15-9E-63-6F-78	192.168.2.107
6	dongmax-pc1	00-13-F7-D0-CF-4D	192.168.2.108

- **ID** - The index of the DHCP Client.
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the Router has allocated to the DHCP client.

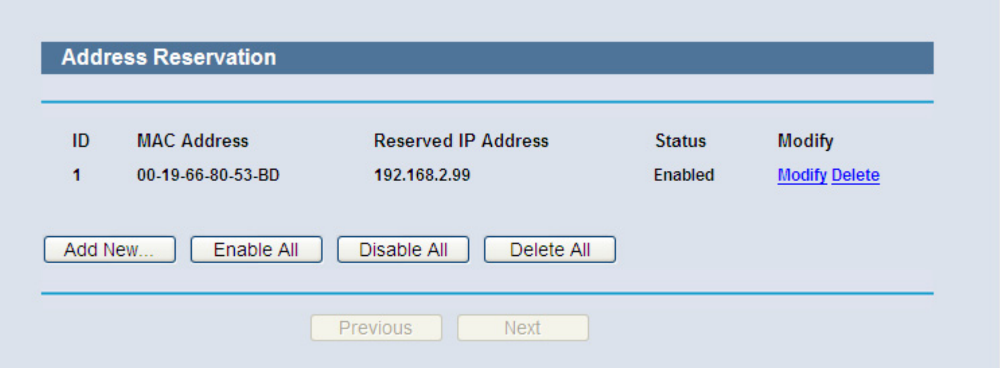
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the Refresh button.

ADDRESS RESERVATION

Select **DHCP -> Address Reservation** from the menu; you can view and add reserved addresses for clients from the next screen (shown in Figure 55). When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

Figure 55: Address Reservation



Address Reservation

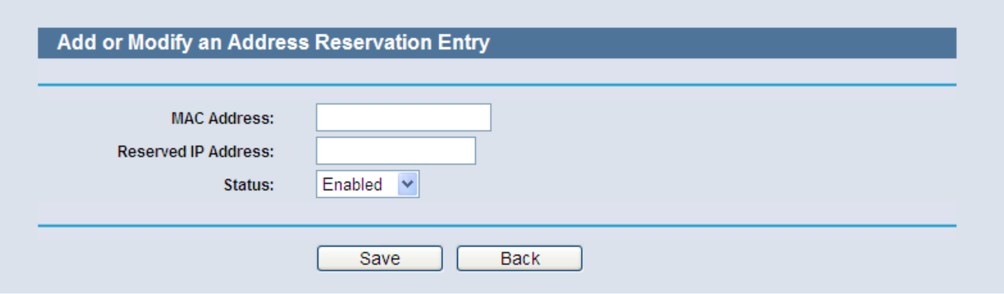
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-19-66-80-53-BD	192.168.2.99	Enabled	Modify Delete

- **MAC Address** - The MAC address of the PC for which you want to reserve an IP address.
- **Assigned IP Address** - The reserved IP address for the PC.
- **Status** - The status of this entry either Enabled or Disabled.

To Reserve IP addresses:

1. Click the “Add New” button (as shown in Figure 56).
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the Save button when finished.

Figure 56: Add or Modify an Address Reservation Entry



Add or Modify an Address Reservation Entry

MAC Address:
Reserved IP Address:
Status: Enabled

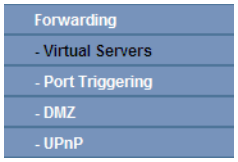
To modify or delete an existing entry:

1. Click **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.
4. Click the **Enable/Disable All** button to enable/disable all entries.
5. Click the **Delete All** button to delete all entries.
6. Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

FORWARDING

There are four submenus under the Forwarding Application menu (shown in Figure 57): **Virtual Servers**, **Port Triggering**, **DMZ**, and **UPnP**. Click any of them and you will be able to configure the corresponding function.

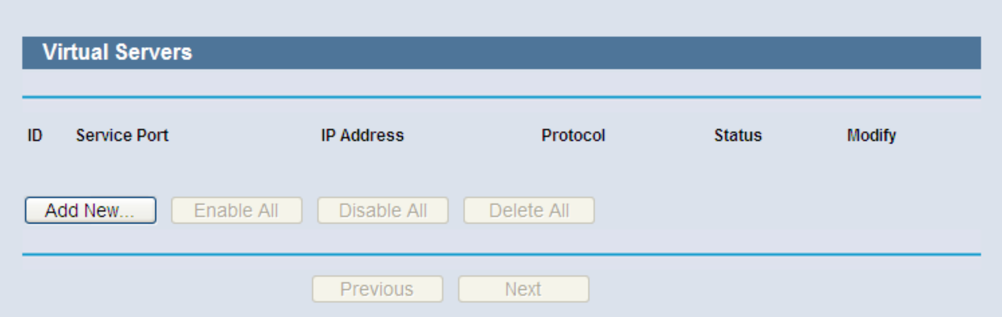
Figure 57: The Forwarding Menu



VIRTUAL SERVERS

Select **Forwarding->Virtual Servers** from the menu; you can view and add virtual servers in the next screen (as shown in Figure 58). Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

Figure 58: Virtual Servers

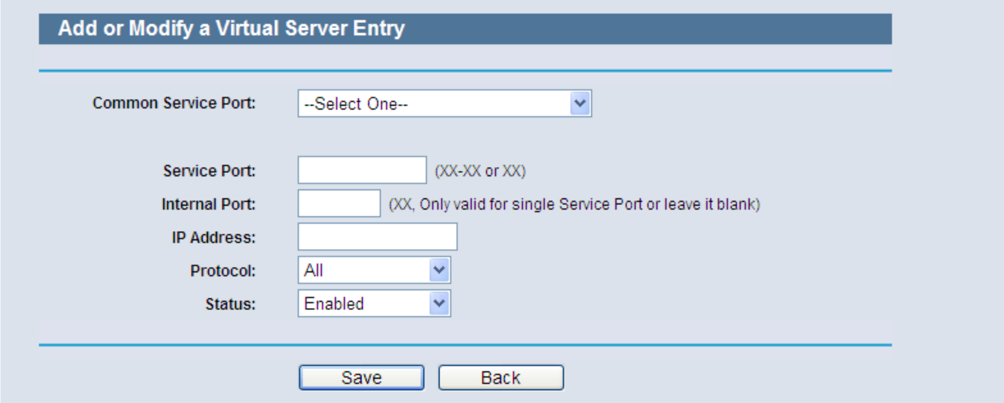


- **Service Port** - The number of an external port. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the Router).
- **Status** - The status of this entry either Enabled or Disabled.

To setup a virtual server entry:

1. Click the **Add New**... button. (Figure 59)
2. Select the service you want to use from the **Common Service Port** list. If the Common **Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **IP Address** box.
4. Select the protocol used for this application, either **TCP, UDP**, or **All**.
5. Select the **Enable** check box to enable the virtual server.
6. Click the **Save** button.

Figure 59: Add or Modify a Virtual Server Entry



Add or Modify a Virtual Server Entry

Common Service Port:	--Select One--
Service Port:	(XX-XX or XX)
Internal Port:	(XX, Only valid for single Service Port or leave it blank)
IP Address:	
Protocol:	All
Status:	Enabled

NOTE: If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

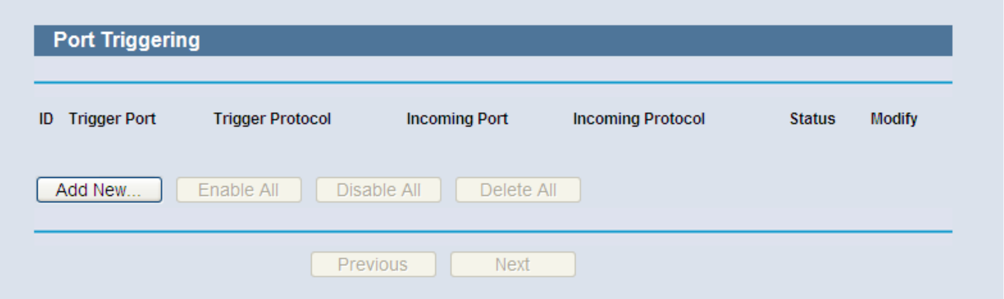
1. Click **Modify** for the entry you want to modify. If you want to delete the entry, click **Delete**.
2. Modify the information.
3. Click the Save button.
4. Click the **Enable/Disable All** button to enable/disable all entries.
5. Click the **Delete All** button to delete all entries.
6. Click the Next button to go to the next page and click the Previous button to return the previous page.

NOTE: If you set the service port of the virtual server as 80, you must set the Web management port on "**Security –> Remote Management**" page to be any other value except 80, such as 8080. Otherwise there will be a conflict, which will disable the virtual server.

PORT TRIGGERING

Select **Forwarding -> Port Triggering** from the menu; you can view and add port triggering in the next screen (shown in Figure 60). Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with a NAT Router.

Figure 60: Port Triggering



Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.

2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.

- **Trigger Protocol** - The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the Router).

- **Incoming Ports Range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

- **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the Router).

- **Status** - The status of this entry either Enabled or Disabled.

To add a new rule, follow the steps below.

1. Click the “Add New” button, the next screen will pop-up as shown in Figure 61.

2. Select a common application from the Common Applications drop-down list, then the Trigger Port field and the Incoming Ports field will be automatically filled. If the Common Applications do not have the application you need, enter the Trigger Port and the Incoming Ports manually.

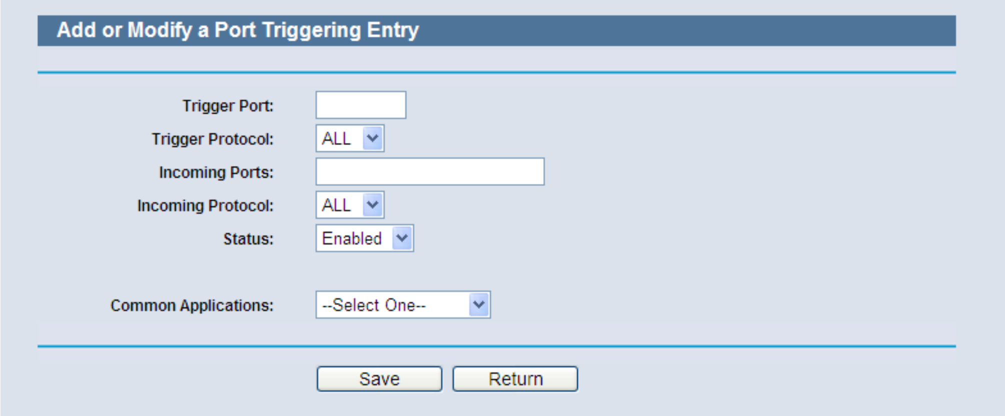
3. Select the protocol used for Trigger Port from the Trigger Protocol drop-down list, either TCP, UDP, or All.

4. Select the protocol used for Incoming Ports from the Incoming Protocol drop-down list, either TCP or UDP, or All.

5. Select Enable in Status field.

6. Click the Save button to save the new rule.

Figure 61: Add or Modify a Triggering Entry



Add or Modify a Port Triggering Entry

Trigger Port:
Trigger Protocol: ALL
Incoming Ports:
Incoming Protocol: ALL
Status: Enabled

Common Applications: --Select One--

To modify or delete an existing entry:

1. Click **Modify** in the entry you want to modify. If you want to delete the entry, click **Delete**.

2. Modify the information.

3. Click the Save button.

4. Click the **Enable All** button to make all entries enabled

5. Click the **Disabled All** button to make all entries disabled.

6. Click the **Delete All** button to delete all entries

NOTE: When the trigger connection is released, the according opening ports will be closed.

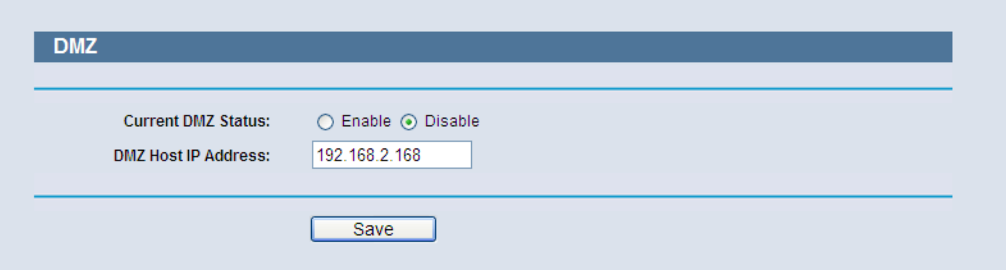
NOTE: Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

NOTE: Incoming Port Ranges cannot overlap each other.

DMZ

Select **Forwarding -> DMZ** from the menu; you can view and configure the DMZ host in the screen (shown in Figure 62).The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

Figure 62: DMZ



DMZ

Current DMZ Status: ○ Enable ● Disable

DMZ Host IP Address: 192.168.2.168

To assign a computer or server to be a DMZ server:

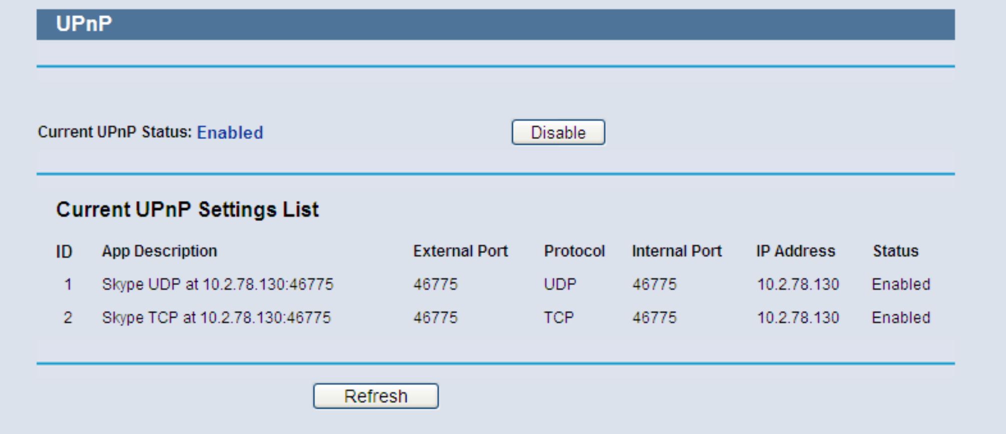
1. Click the Enable radio button
2. Enter the local host IP Address in the DMZ Host IP Address field
3. Click the Save button.

NOTE: After you set the DMZ host, the firewall related to the host will not work.

UPNP

Select **Forwarding -> UPnP** from the menu; you can view the information about UPnP (Universal Plug and Play) in the screen (shown in Figure 63). The UPnP feature allows devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Figure 63: UPnP



UPnP

Current UPnP Status: Enabled

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	Skype UDP at 10.2.78.130:46775	46775	UDP	46775	10.2.78.130	Enabled
2	Skype TCP at 10.2.78.130:46775	46775	TCP	46775	10.2.78.130	Enabled

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the Enable or Disable button. As allowing this may present a risk to security, this feature is enabled by default.

- **Current UPnP Settings List** - This table displays the current UPnP information.

  - **App Description** - The description provided by the application in the UPnP request

  - **External Port** - External port, which the router opened for the application.

  - **Protocol** - Shows which type of protocol is opened.

  - **Internal Port** - Internal port, which the router opened for local host.

  - **IP Address** - The UPnP device that is currently accessing the router.

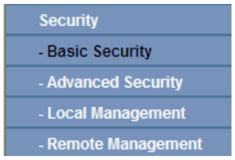
  - **Status** - The port's status displayed here. "Enabled" means that port is still active. Otherwise, the port is inactive.

Click Refresh to update the Current UPnP Settings List.

SECURITY

There are four submenus under the Security menu as shown in Figure 88: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

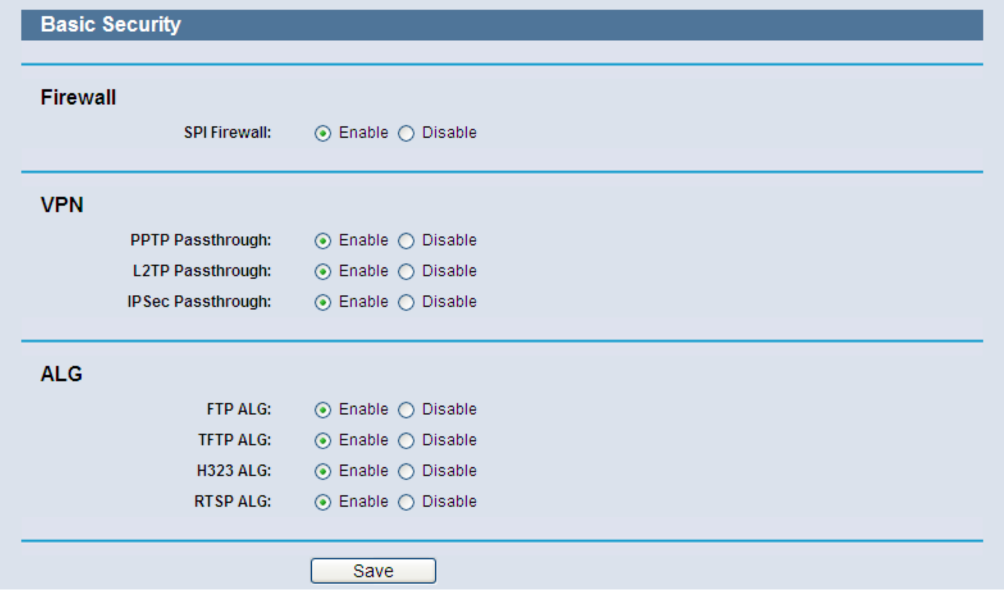
Figure 64: The Security Menu



BASIC SECURITY

Select **Security -> Basic Security** from the menu; you can configure the basic security in the screen as shown in Figure 65.

Figure 65: Basic Security



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

H323 ALG: ● Enable ○ Disable

RTSP ALG: ● Enable ○ Disable

- **Firewall** - A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.

  - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking states per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.

  - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enabled.

  - **L2TP Passthrough** - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled.

  - **IPSec Passthrough** - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, keep the default, Enabled.

- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

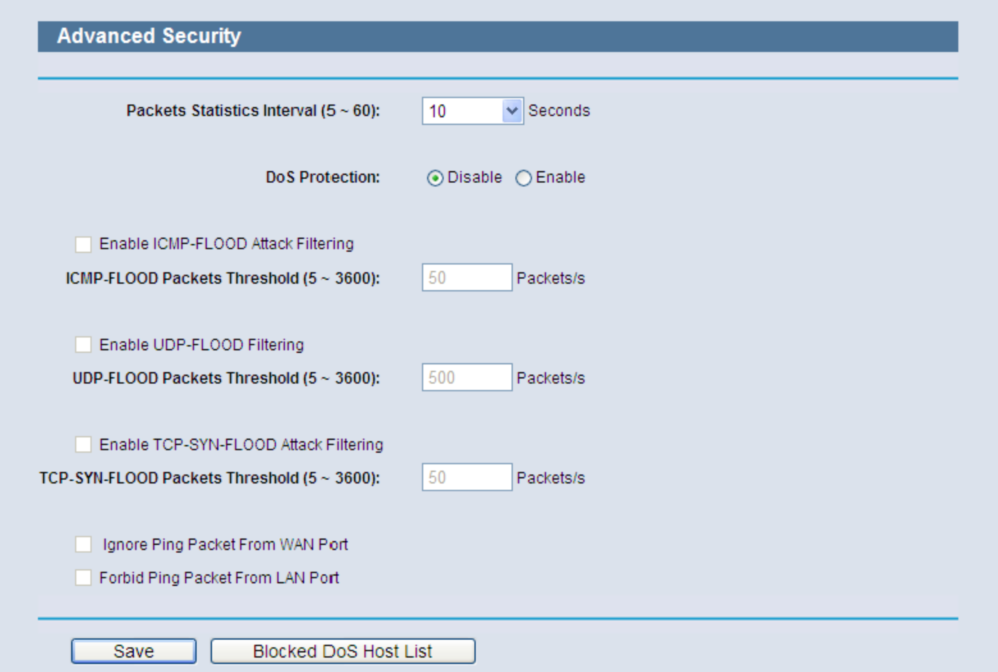
- **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, keep the default Enable.
- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep the default Enable.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click Enable. "

Click the Save button to save your settings.

ADVANCED SECURITY

Select **Security -> Advanced Security** from the menu; you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen, as shown in Figure 66.

Figure 66: Advanced Security



Advanced Security

Packets Statistics Interval (5 ~ 60): 10 Seconds

DoS Protection: ● Disable ○ Enable

□ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): 500 Packets/s

□ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Ignore Ping Packet From WAN Port

□ Forbid Ping Packet From LAN Port

- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.

- **DoS Protection** - Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

NOTE: Dos Protection will take effect only when the Traffic Statistics in "**System Tool > Traffic Statistics**" is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.

- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.

- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.

- **Ignore Ping Packet From WAN Port** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the Router.

- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. This function can be used to defend against some viruses.

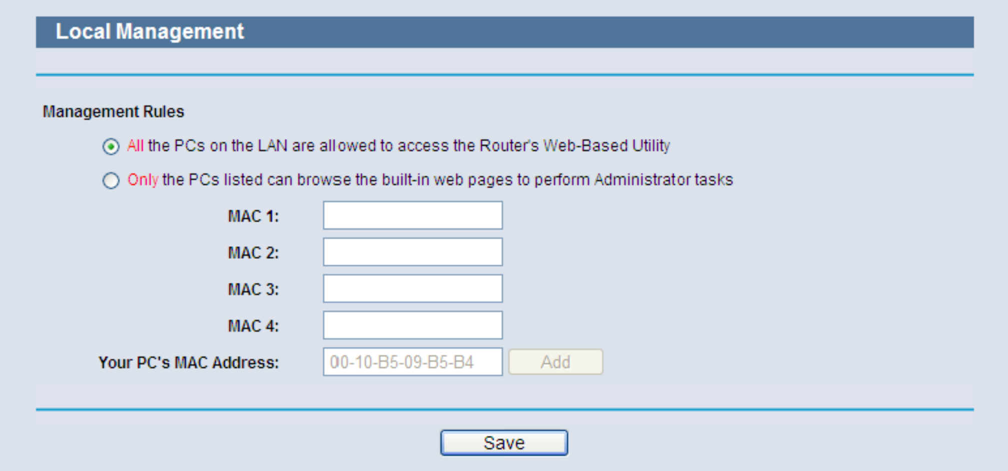
Click the **Save** button to save the settings.

- Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

LOCAL MANAGEMENT

Select **Security->Local Management** from the menu; you can configure the management rules in the screen, as shown in Figure 67. The management feature allows you to deny computers in the LAN from accessing the Router.

Figure 67: Local Management



Local Management

Management Rules

● All the PCs on the LAN are allowed to access the Router's Web-Based Utility

○ Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address: 00-10-B5-09-B5-B4

By default, the radio button "All the PCs on the LAN are allowed to access the Router's Web-Based Utility" is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check the radio button "Only the PCs listed can browse the built-in web pages to perform Administrator tasks", and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

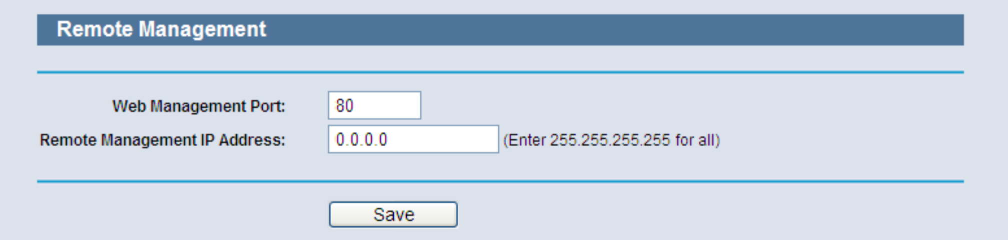
After click the Add button, your PC's MAC Address will be placed in the list above.

Click the Save button to save your settings.

REMOTE MANAGEMENT

Select **Security->Remote Management** from the menu; you can configure the Remote Management function in the screen, as shown in Figure 68. This feature allows you to manage your Router from a remote location via the Internet.

Figure 68: Remote Management



Remote Management

Web Management Port: 80

Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534, but do not use the number of any common service port.

- **Remote Management IP Address** - This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

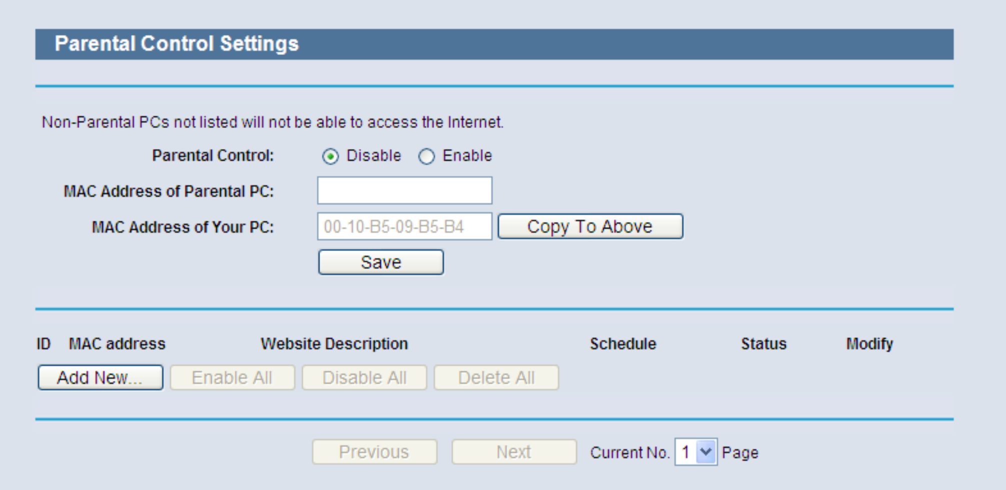
NOTE: To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.

NOTE: Be sure to change the Router's default password to a very secure password.

PARENTAL CONTROL

Select **Parental Control** from the menu; you can then configure the parental control in the displayed page, as shown in Figure 69. The Parental Control function can be used to limit children’s access to certain websites and restrict the time of surfing.

Figure 69: Parental Control Settings



Parental Control Settings

Non-Parental PCs not listed will not be able to access the Internet.

Parental Control: ● Disable ○ Enable

MAC Address of Parental PC:

MAC Address of Your PC: 00-10-B5-09-B5-B4

ID	MAC address	Website Description	Schedule	Status	Modify

Current No. 1 Page

- **Parental Control** - Check Enable if you want this function to take effect, otherwise check Disable.

- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the “Copy To Above” button below.

- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the “Copy To Above” button to fill this address to the MAC Address of Parental PC field above.

- **Website Description** - Description of the allowed website for the child PC.

- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to “**Access Control -> Schedule**”.

- **Modify** - Here you can edit or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the “Add New” button and the next screen will pop-up, as shown in Figure 70.

2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you want to control in the “MAC Address of Child PC” field. Or you can choose the MAC address from the “All Address in Current LAN” drop-down list.

3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.

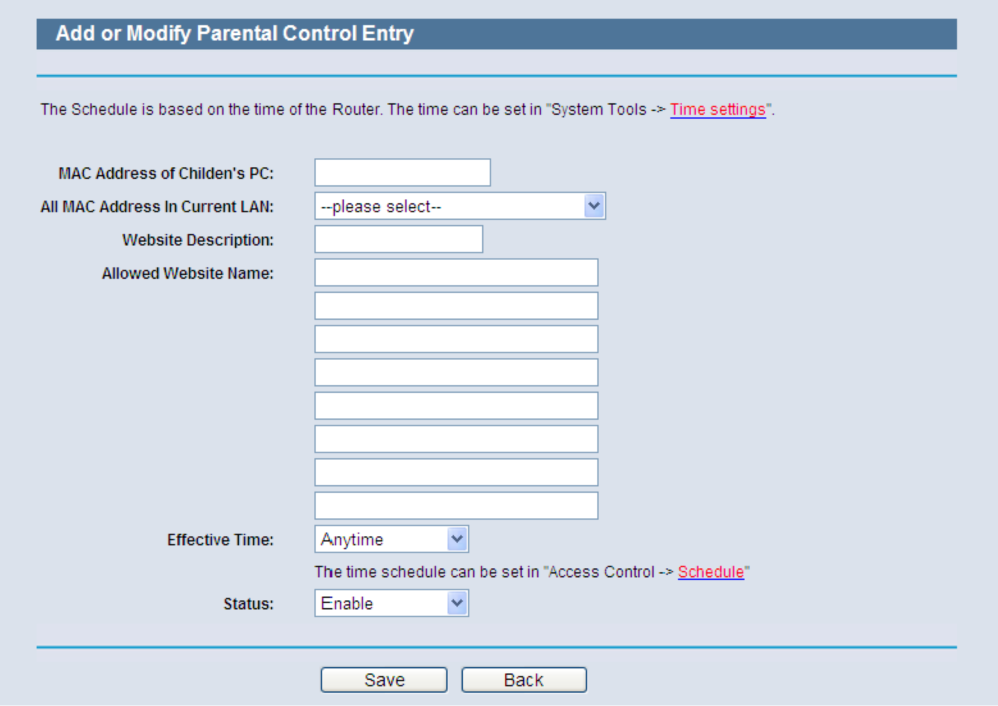
4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the Allowed Domain Name field. Any domain name with keywords in it (www.google.com.cn) will be allowed.

5. Select from the “Effective Time” drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the Schedule in red below to go to the Advance Schedule Settings page and create the schedule you need.

6. In the Status field, you can select Enabled or Disabled to enable or disable your entry.

7. Click the Save button.
   Click the Enable All button to enable all the rules in the list.
   Click the Disable All button to disable all the rules in the list.
   Click the Delete All button to delete all the entries in the table.
   Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 70: Add or Modify Parental Control Entry



Add or Modify Parental Control Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time settings".

MAC Address of Childen's PC:

All MAC Address In Current LAN: --please select--

Website Description:

Allowed Website Name:

Effective Time: Anytime

The time schedule can be set in "Access Control -> Schedule"

Status: Enable

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

1. Click **Parental Control** on the menu to enter the Parental Control Settings page. Check Enable and enter the MAC address 00-11-22-33-44-BB in the “MAC Address of Parental PC” field.

2. Click **Access Control -> Schedule** on the left to enter the Schedule Settings page. Click the “Add New” button to create a new schedule with Schedule Description “Schedule_1,” Day is “Sat” and Time is all day-24 hours.

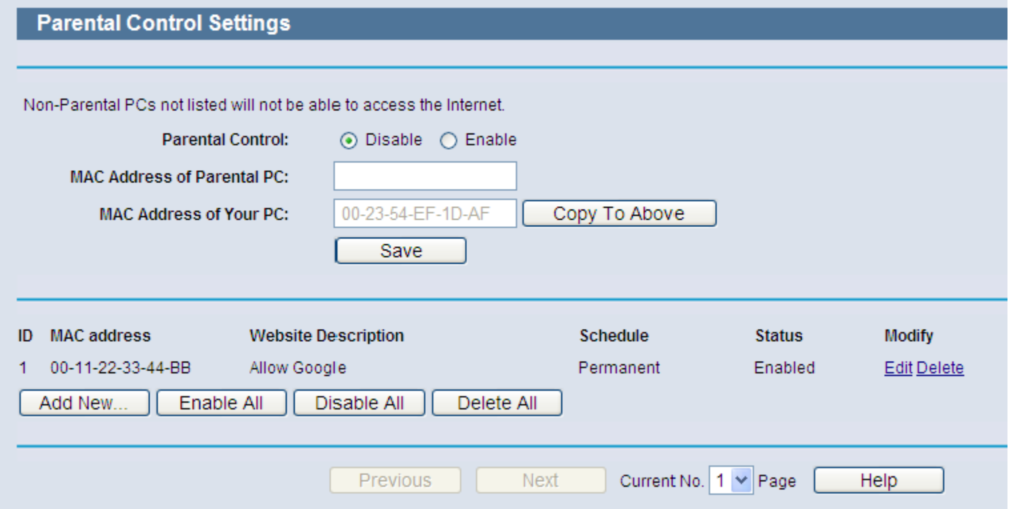
3. Click “Parental Control” menu on the left to go back to the Add or Modify Parental Control Entry page:

   - Click the “Add New” button.
   - Enter 00-11-22-33-44-AA in the MAC Address of Child PC field.
   - Enter “Allow Google” in the Website Description field.
   - Enter “www.google.com” in the Allowed Domain Name field.
   - Select “Schedule_1” you create just now from the Effective Time drop-down list.
   - In Status field, select Enable.

4. Click Save to complete the settings.

Then you will go back to the Parental Control Settings page and see the following list, as shown in Figure 71.

Figure 71: Parental Control Settings



Non-Parental PCs not listed will not be able to access the Internet.

Parental Control: ● Disable ○ Enable

MAC Address of Parental PC:

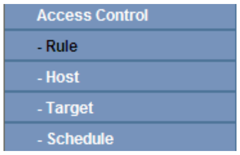
MAC Address of Your PC: 00-23-54-EF-1D-AF

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-BB	Allow Google	Permanent	Enabled	Edit Delete

ACCESS CONTROL

There are four submenus under the Access Control menu as shown in Figure 72: **Rule**, **Host**, **Target**, and **Schedule.** Click any of them, and you will be able to configure the corresponding function.

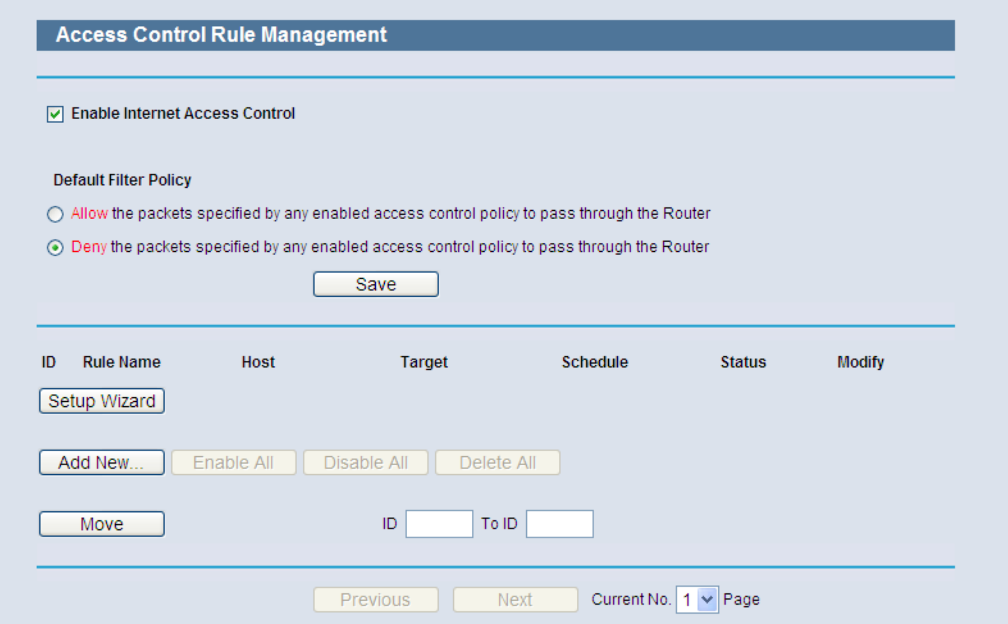
Figure 72: Access Control



RULE

Select **Access Control->Rule** from the menu; you can view and set access control rules in the screen, as shown in Figure 73.

Figure 73: Access Control Rule Management



Access Control Rule Management

☑ Enable Internet Access Control

Default Filter Policy

○ Allow the packets specified by any enabled access control policy to pass through the Router

● Deny the packets specified by any enabled access control policy to pass through the Router

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Rule Name** - Here displays the name of the rule and this name is unique.
- **Host** - Here displays the host selected in the corresponding rule.
- **Target** - Here displays the target selected in the corresponding rule.
- **Schedule** - Here displays the schedule selected in the corresponding rule.
- **Status** - This field displays the status of the rule. Enabled means the rule will take effect, Disabled means the rule will not take effect.
- **Modify** - Here you can edit or delete an existing rule.

To add a new rule, please follow the steps below.

1. Click the "Add New" button and the next screen will pop-up, as shown in Figure 74.
2. Give a name (e.g. Rule_1) for the rule in the Rule Name field.
3. Select a host from the Host drop-down list or choose "Click Here To Add New Host List".
4. Select a target from the Target drop-sown list or choose "Click Here To Add New Target List".

5. Select a schedule from the Schedule drop-down list or choose "Click Here To Add New Schedule".

6. In the Action field, select Deny or Allow.

7. In the Status field, select Enabled or Disabled to enable or disable your entry.

Click the Save button.

Click the Enable All button to enable all the rules in the list.

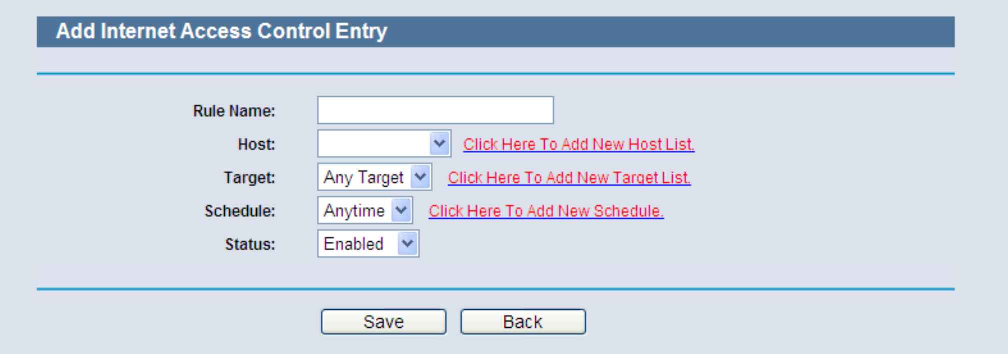
Click the Disable All button to disable all the rules in the list.

Click the Delete All button to delete all the entries in the table.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the Move button to change the entry's order.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 74: Add or Modity Internet Access Control Entry



Add Internet Access Control Entry

Rule Name:
Host:
Target: Any Target
Schedule: Anytime
Status: Enabled

Click Here To Add New Host List.
Click Here To Add New Target List.
Click Here To Add New Schedule.
Save
Back

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click "Access Control->Host" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.

2. Click "Access Control->Target" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.

3. Click "Access Control->Schedule" in the left to enter the Schedule Settings page. Add a new entry with the Schedule Description is

Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.

4. Click “Access Control->Rule” in the left to return to the Access Control Rule Management page. Select “Enable Internet Access Control” and choose "Deny the packets not specified by any access control policy to pass through the Router".

5. Click the “Add New” button to add a new rule as follows:

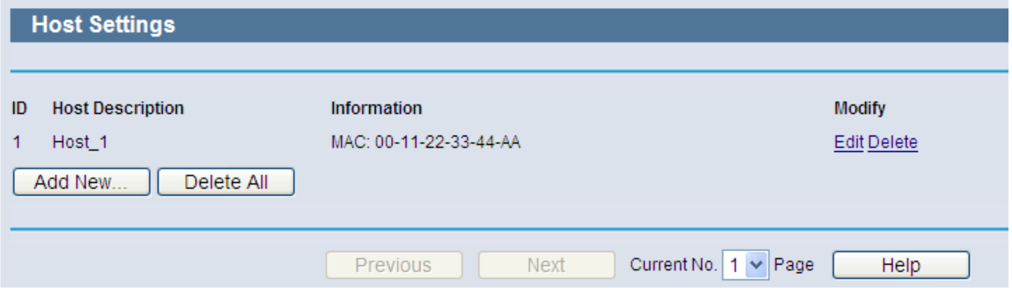
   - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In Host field, select Host_1.
   - In Target field, select Target_1.
   - In Schedule field, select Schedule_1.
   - In Action field, select Allow.
   - In Status field, select Enable.
   - Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

Host

Select **Access Control->Host** from the menu; you can view and set a Host list in the screen, as shown in Figure 75. The host list is necessary for the Access Control Rule.

Figure 75: Host Settings



Host Settings

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

- **Host Description** - Displays the description of the host and this description is unique.
- **Information** - Displays the information about the host. It can be IP or MAC.
- **Modify** - To modify or delete an existing entry.

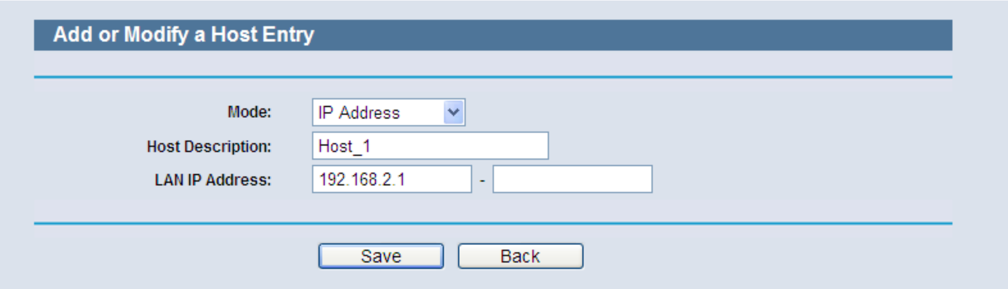
To add a new entry, please follow the steps below.

1. Click the "Add New" button.
2. In the Mode field, select IP Address or MAC Address.
   - If you select IP Address, the screen in Figure 76 is displayed.
     - In the Host Description field, create a unique description for the host (e.g. Host_1).
     - In LAN IP Address field, enter the IP address.
   - If you select MAC Address, the screen in Figure 77 is displayed.
     - In Host Description field, create a unique description for the host (e.g. Host_1).
     - In MAC Address field, enter the MAC address.
3. Click the Save button to complete the settings.

Click the **Delete All** button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 76: Add or Modify an IP Host Entry



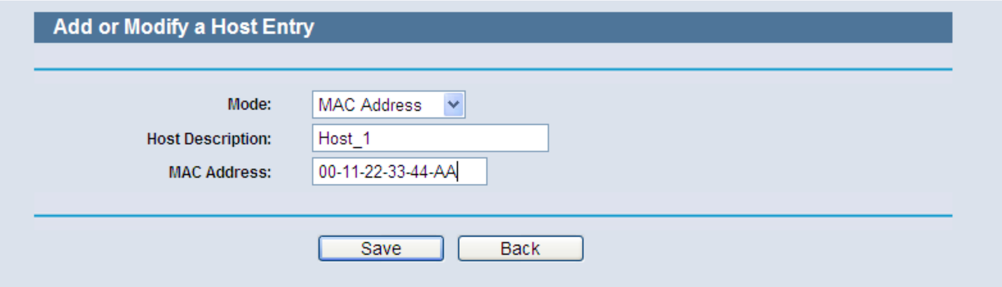
Add or Modify a Host Entry

Mode: IP Address

Host Description: Host_1

LAN IP Address: 192.168.2.1 -

Figure 77: Add or Modify a MAC Host Entry



Add or Modify a Host Entry

Mode: MAC Address

Host Description: Host_1

MAC Address: 00-11-22-33-44-AA

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click “Add New” button in Figure 75 to enter the “Add or Modify a Host Entry” page.

2. In Mode field, select MAC Address from the drop-down list.

3. In Host Description field, create a unique description for the host (e.g. Host_1).

4. In MAC Address field, enter 00-11-22-33-44-AA.

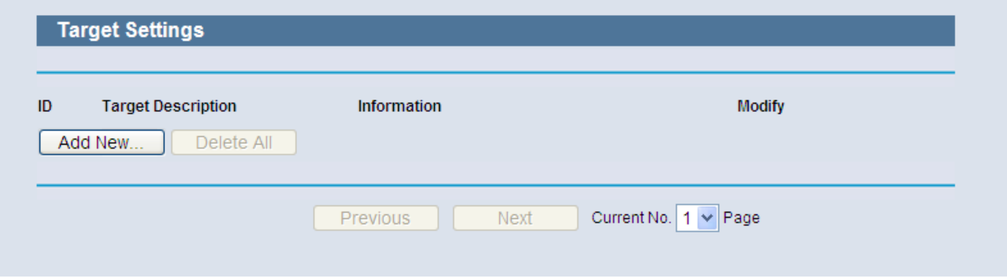
5. Click Save to complete the settings.

Then you will go back to the Host Settings page and see the following list.

TARGET

Select **Access Control -> Target** from the menu; you can view and set a Target list in the screen, as shown in Figure 78. The target list is necessary for Access Control Rules.

Figure 78: Target Settings



- **Target Description** - Here displays the description about the target and this description is unique.

- **Information** - The target can be IP address, port, or domain name.

- **Modify** - To modify or delete an existing entry.

To add a new entry, follow the steps below.

1. Click the “Add New” button.

2. In Mode field, select IP Address or Domain Name.

   a. If you select IP Address, the screen in Figure 79 is shown.

      - In Target Description field, create a unique description for the target (e.g. Target_1).

      - In IP Address field, enter the IP address of the target.

      - Select a common service from Common Service Port drop-down list, so that the Target Port will be automatically filled. If the

Common Service Port drop-down list doesn't have the service you want, specify the Target Port manually.

- In Protocol field, select TCP, UDP, ICMP or ALL.

b. If you select Domain Name, the screen in Figure 80 is shown.

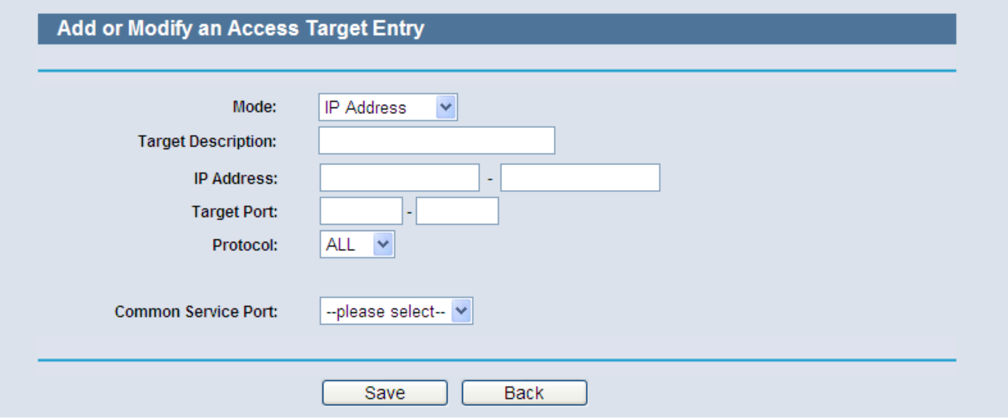
- In Target Description field, create a unique description for the target (e.g. Target_1).
- In Domain Name field, enter the domain name, either the full name or the keywords (for example google) in the blank. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter 4 domain names.

3. Click the Save button.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 79: Add or Modify an IP Access Target Entry

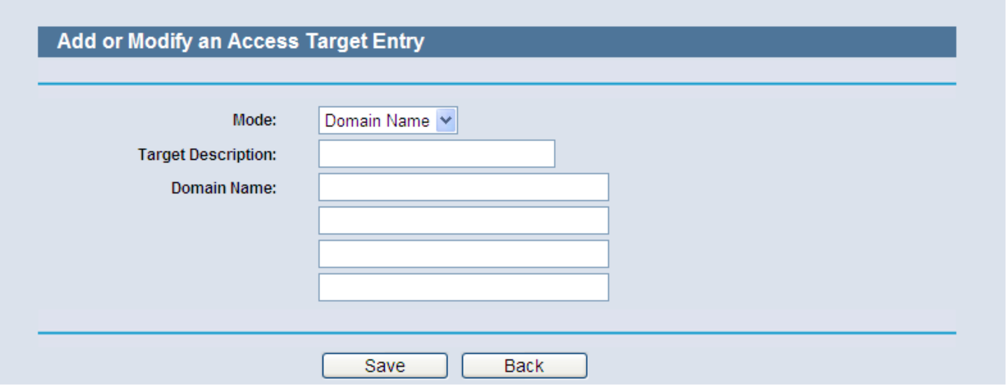


Add or Modify an Access Target Entry

Mode: IP Address
Target Description:
IP Address: -
Target Port: -
Protocol: ALL

Common Service Port: --please select--

Figure 80: Add or Modify a Domain Name Access Target Entry



Add or Modify an Access Target Entry

Mode: Domain Name
Target Description:
Domain Name:

For example: If you desire to restrict the internet activities of a host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:

1. Click the “Add New” button in Figure 78 to enter the Add or Modify an Access Target Entry page.

2. In Mode field, select Domain Name from the drop-down list.

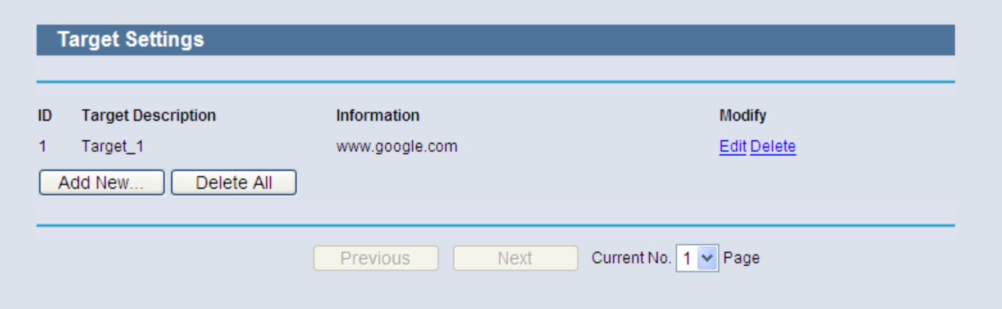
3. In Target Description field, create a unique description for the target (e.g. Target_1).

4. In Domain Name field, enter www.google.com.

5. Click Save to complete the settings.

Then you will go back to the Target Settings page and see the following list.

Figure 81: Target Setting

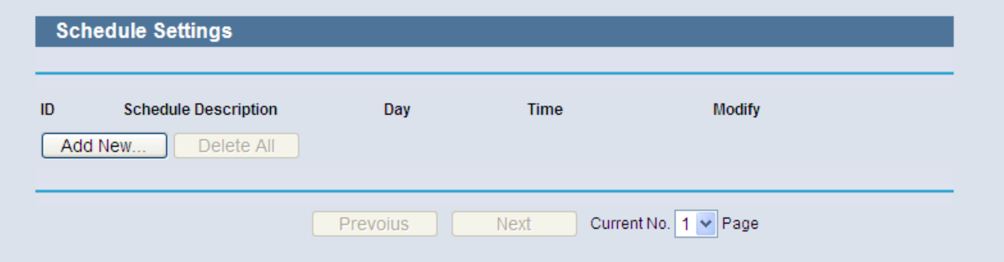


ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

SCHEDULE

Select **Access Control -> Schedule** from the menu; you can view and set a schedule list in the next screen, as shown in Figure 82. The schedule list is necessary for Access Control Rules.

Figure 82: Schedule Settings



ID	Schedule Description	Day	Time	Modify

- **Schedule Description** - Here displays the description of the schedule and this description is unique.

- **Day** - Here displays the day(s) in a week.

- **Time** - Here displays the time period in a day.

- **Modify** - Here you can edit or delete an existing schedule.

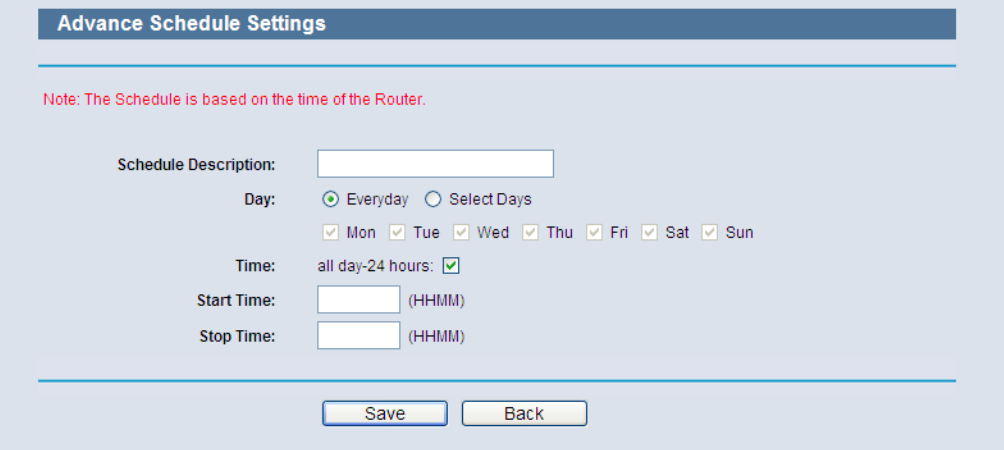
To add a new schedule, follow the steps below.

1. Click the "Add New" button shown in Figure 82 and the next screen will pop-up as shown in Figure 83.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, select the day or days you need.
4. In Time field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click Save to complete the settings.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 83: Advanced Schedule Settings



Advance Schedule Settings

Note: The Schedule is based on the time of the Router.

Schedule Description:

Day: ● Everyday ○ Select Days

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time: all day-24 hours: ☑

Start Time: (HHMM)

Stop Time: (HHMM)

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:

1. Click the "Add New" button shown in Figure 83 to enter the Advanced Schedule Settings page.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, check the Select Days radio button and then select Sat and Sun.

4. In Time field, enter 1800 in Start Time field and 2000 in Stop Time field.

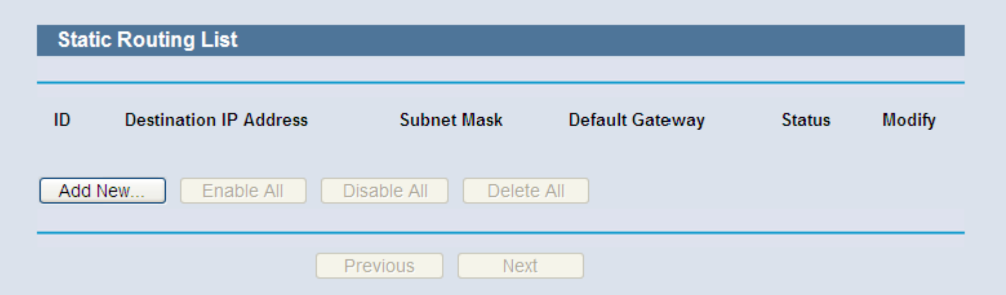
5. Click Save to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

ADVANCED ROUTING

Select **static routing list** from the menu; you can configure the static route in the next screen (Figure 84). A static route is a pre-determined path that network information must travel to reach a specific host or network.

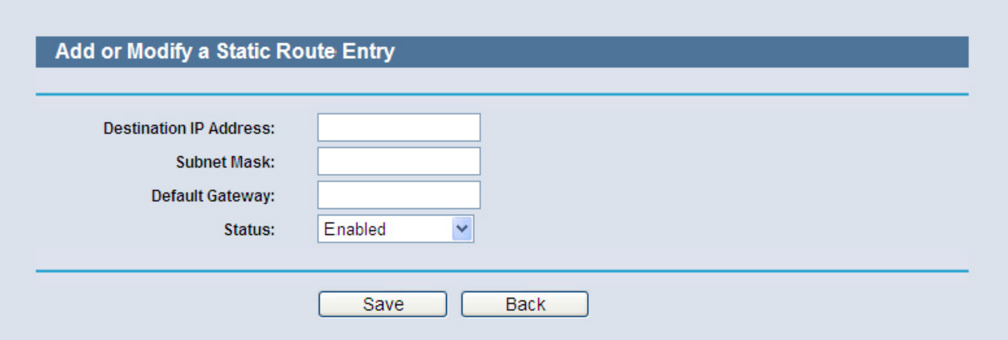
Figure 84: Static Routing



To add static routing entries:

1. Click Add New.

Figure 85: Add or Modify a Static Route Entry



Status: Enabled

2. Enter the following data:

- **Destination IP Address** - The Destination IP Address is the address of the network or host that you want to assign to a static route.

- **Subnet Mask** - The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.

- **Gateway** - This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

3. Select Enabled or Disabled for this entry on the Status pull-down list.

4. Click the Save button to make the entry take effect.

Other configurations for the entries:

Click the Delete button to delete the entry.

Click the Enable All button to enable all the entries.

Click the Disable All button to disable all the entries.

Click the Delete All button to delete all the entries.

Click the Previous button to view the information in the previous screen.

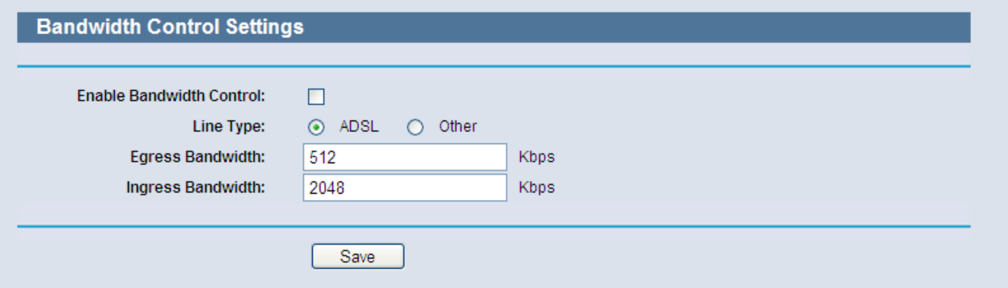
Click the Next button to view the information in the next screen.

BANDWIDTH CONTROL

CONTROL SETTINGS

Select **Bandwidth Control->Control Settings** from the menu; you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. The values you configure should be less than 100000 Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Figure 86: Bandwidth Control



Bandwidth Control Settings

Enable Bandwidth Control: □

Line Type: ● ADSL ○ Other

Egress Bandwidth: 512 Kbps

Ingress Bandwidth: 2048 Kbps

- **Enable Bandwidth Control** - Check this box so that the bandwidth control settings can take effect.

- **Line Typ**e - Select the right type for you network connection. If you do not know which type to choose, ask your ISP for the information.

- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

RULES LIST

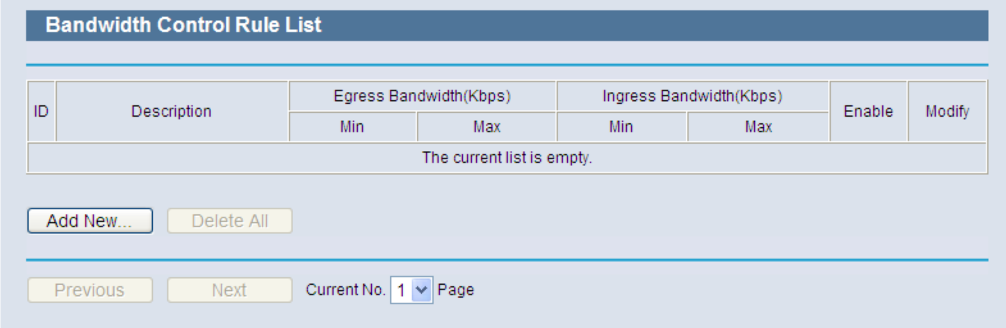
Select **Bandwidth Control->Rules List** from the menu; you can view and configure the bandwidth control rules in the screen below.

- **Description** - This is the information about the rules such as address range.
- **Egress bandwidth** - This field displays the maximum and minimum upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth** - This field displays the maximum and minimum download bandwidth through the WAN port, the default is 0.
- **Enable** - This displays the status of the rule.
- **Modify** - Click Modify to edit the rule. Click Delete to delete the rule.

To add/modify a QoS rule, follow the steps below.

1. Click "Add New," as shown in Figure 87, you will see a new screen shown in Figure 88.
2. Enter the information like the screen shown below.
3. Click the Save button.

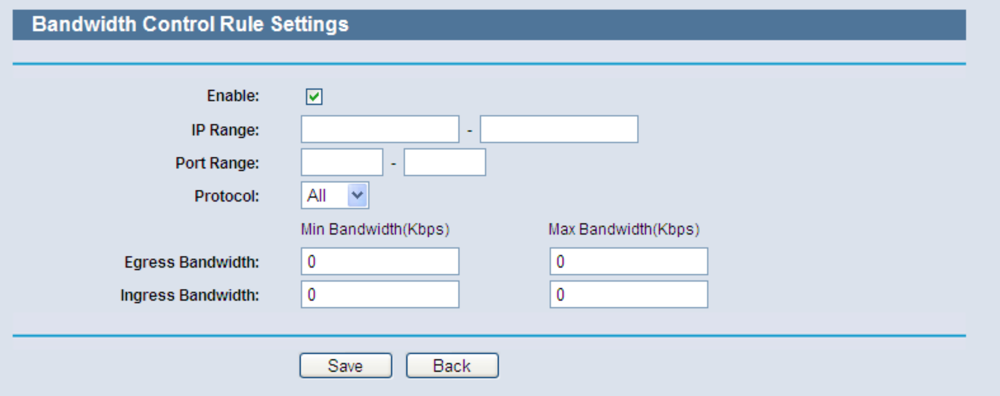
Figure 87: Rule List



Bandwidth Control Rule List

ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							

Figure 88: Rule Settings



Bandwidth Control Rule Settings

Enable: ☑

IP Range: [ ] - [ ]

Port Range: [ ] - [ ]

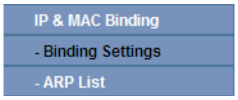
Protocol: All

	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:	0	0
Ingress Bandwidth:	0	0

IP & MAC BINDING

There are two submenus under the IP &MAC Binding menu (shown in Figure 90): **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

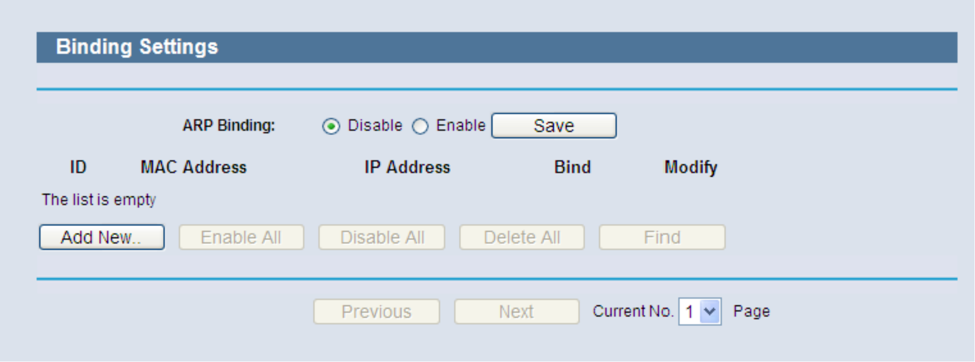
Figure 89: The IP & MAC Binding Menu



BINDING SETTING

This page displays the **IP & MAC Binding Setting table**; you can configure it as needed (as shown in Figure 90).

Figure 90: Binding Setting



Binding Settings

ARP Binding: ● Disable ○ Enable

ID	MAC Address	IP Address	Bind	Modify

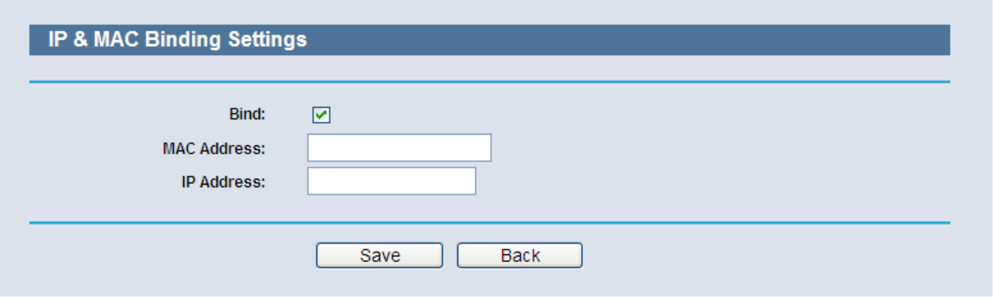
The list is empty

Current No. 1 Page

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** - To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the "Add New" button or "Modify" button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (as shown in Figure 91).

Figure 91: IP & MAC Binding Setting (Add & Modify)



IP & MAC Binding Settings

Bind: ☑
MAC Address:
IP Address:

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New**... button as shown in Figure 90.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the Save button to save it.

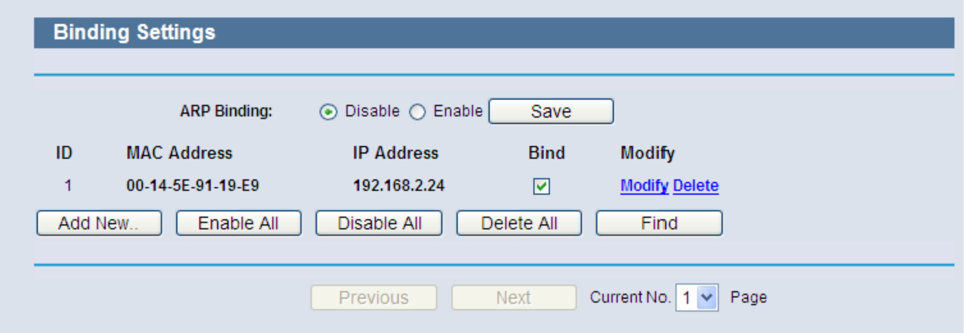
To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click Modify or Delete in the Modify column.

To find an existing entry, follow the steps below.

1. Click the Find button as shown in Figure 92.
2. Enter the MAC Address or IP Address.
3. Click the Find button in the page as shown in Figure 92.

Figure 92: Find IP & MAC Binding Entry



Binding Settings

ARP Binding: ● Disable ○ Enable

ID	MAC Address	IP Address	Bind	Modify
1	00-14-5E-91-19-E9	192.168.2.24	☑	Modify Delete

Current No. 1 Page

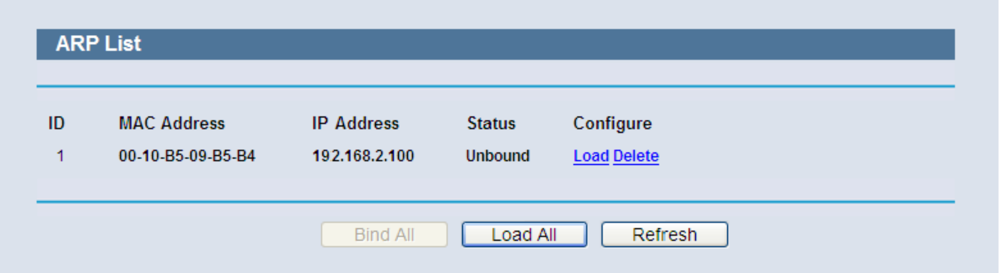
Click the “Enable All” button to make all entries enabled.

Click the “Delete All” button to delete all entries.

ARP LIST

Select **IP & MAC Binding->ARP List** from the menu; you can view and set ARP List in the screen, as shown in Figure 93. To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries as shown below.

Figure 93: ARP List



ARP List

ID	MAC Address	IP Address	Status	Configure
1	00-10-B5-09-B5-B4	192.168.2.100	Unbound	Load Delete

- **MAC Address** - The MAC address of the controlled computer in the LAN.

- **IP Address** - The assigned IP address of the controlled computer in the LAN.

- **Status** - Indicates whether or not the MAC and IP addresses are bound.

- **Configure** - Load or delete an item.

  - l Load - Load the item to the IP & MAC Binding list.

  - l Delete - Delete the item.

Click the Bind All button to bind all the current items, available after enable.

Click the Load All button to load all items to the IP & MAC Binding list.

Click the Refresh button to refresh all items.

NOTE: An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

DDNS

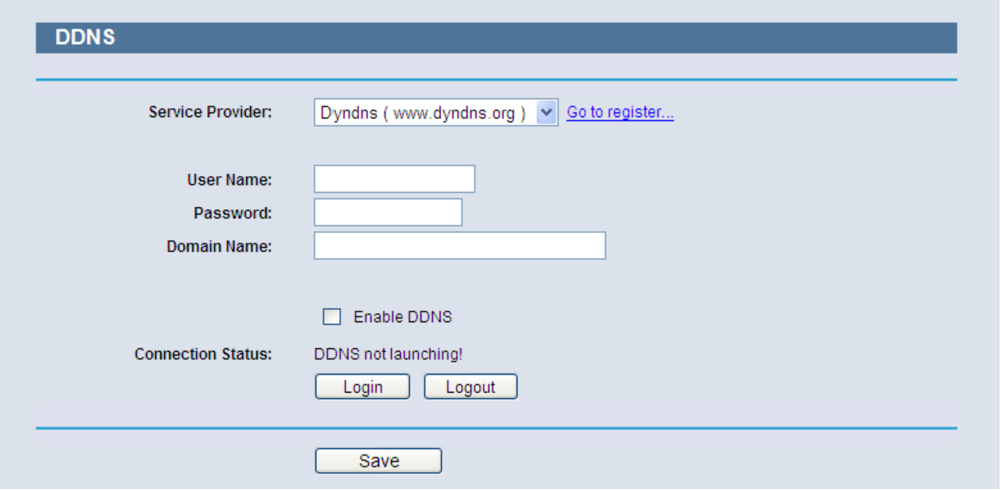
Choose menu “DDNS”, and you can configure the DDNS function.

The Router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The DDNS client service provider will give you a password or key.

DYNDNS.ORG DDNS

If the DDNS Service Provider you select is www.dyndns.org, the page will appear as shown in Figure 94.

Figure 94: Dyndns.org DDNS Settings



DDNS

Service Provider: Dyndns (www.dyndns.org)

User Name:

Password:

Domain Name:

□ Enable DDNS

Connection Status: DDNS not launching!

To set up for DDNS, follow these instructions:

1. Type the Domain Name received from your DDNS service provider.

2. Type the User Name for your DDNS account.

3. Type the Password for your DDNS account.

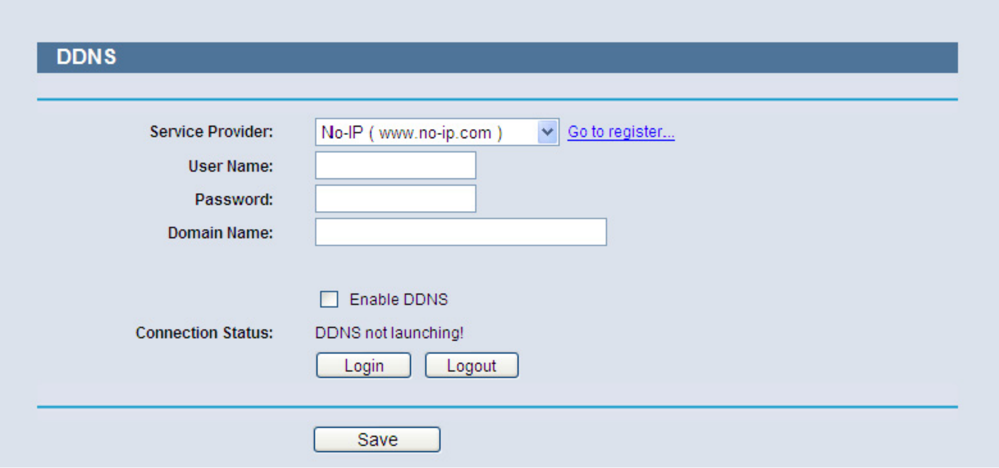
4. Click the Login button to log in to the DDNS service.

- **Connection Status** -The status of the DDNS service connection is displayed here.

NO-IP.COM DDNS

If the DDNS Service Provider you select is www.no-ip.com, the page will appear as shown in Figure 95.

Figure 95: No-ip.com DDNS Settings



DDNS

Service Provider: No-IP (www.no-ip.com)

User Name:

Password:

Domain Name:

□ Enable DDNS

Connection Status: DDNS not launching!

- **Connection Status** - The status of the DDNS service connection is displayed here.

- Click **Logout** to log out the DDNS service.

To set up for DDNS, follow these instructions:

1. Type the User Name for your DDNS account.

2. Type the Password for your DDNS account.

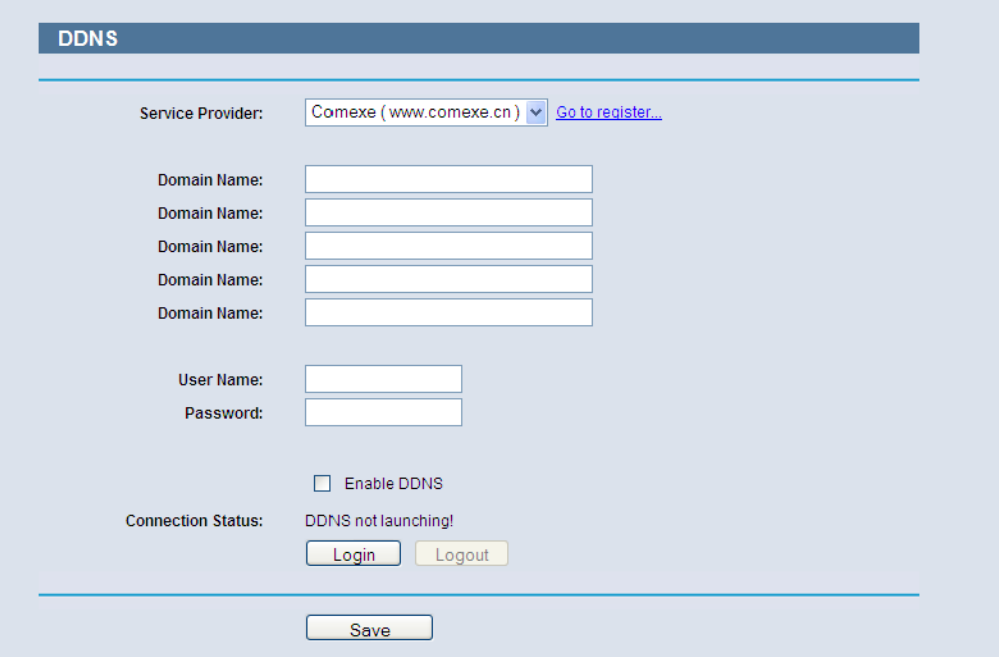
3. Type the Domain Name you received from DDNS service provider.

Click the Login button to log in the DDNS service.

COMEXE.CN DDNS

If the DDNS Service Provider you select is www.comexe.cn, the page will appear as shown in Figure 95.

Figure 96: Comexe.cn DDNS Settings



DDNS

Service Provider: Comexe (www.comexe.cn)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

□ Enable DDNS

Connection Status: DDNS not launching!

- **Connection Status** - The status of the DDNS service connection is displayed here.
- Click **Logout** to log out the DDNS service.

To set up for DDNS, follow these instructions:

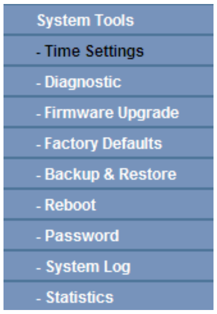
1. Type the User Name for your DDNS account.
2. Type the Password for your DDNS account.
3. Type the Domain Name you received from DDNS service provider.

Click the Login button to log in the DDNS service.

SYSTEM TOOLS

Select **System Tools**, and you can see the submenus under the main menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

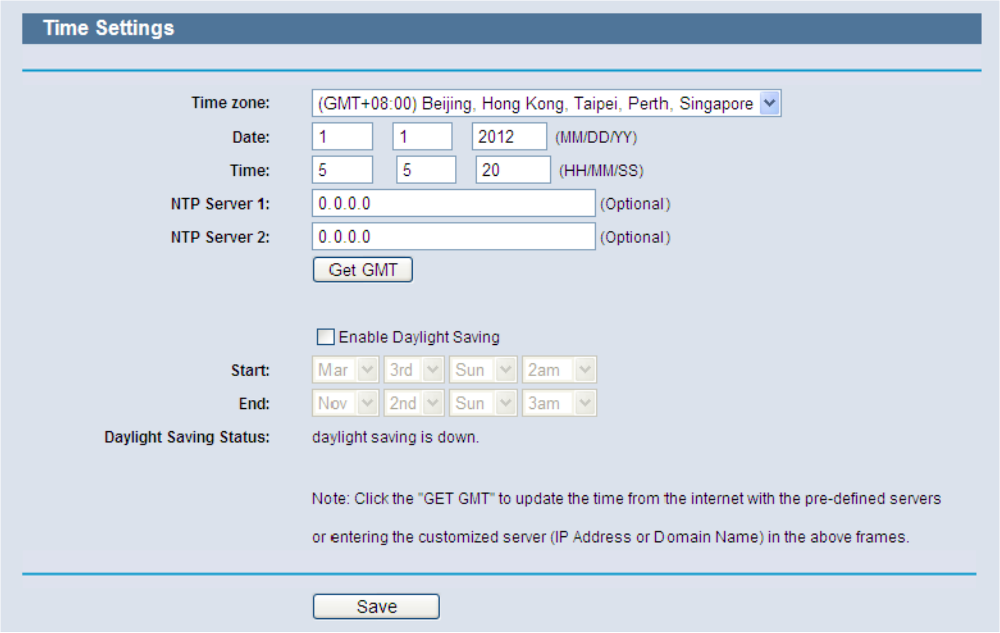
Figure 97: The System Tools Menu



TIME SETTINGS

Select **System Tools->Time Setting** from the menu; you can configure the time on the following screen.

Figure 98: Time Settings



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Taipei, Perth, Singapore

Date: 1 1 2012 (MM/DD/YY)

Time: 5 5 20 (HH/MM/SS)

NTP Server 1: 0.0.0.0 (Optional)

NTP Server 2: 0.0.0.0 (Optional)

Get GMT

□ Enable Daylight Saving

Start: Mar 3rd Sun 2am

End: Nov 2nd Sun 3am

Daylight Saving Status: daylight saving is down.

Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.

Save

- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior** - Enter the address for the NTP Server, then the Router will get the time from the NTP Server preferentially. In addition, the Router includes some common NTP Servers, so it can get the time automatically once it connects the Internet.
- **Enable Daylight Saving -** Check the box to enable the Daylight Saving function.

- **Start -**The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **End -**The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Daylight Saving Status -**Displays the status whether the Daylight Saving is in use."

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.
3. Click Save to save the configuration.

To configure the system automatically:

1. Select your local time zone.
2. Enter the IP address for NTP Server Prior.
3. Click the Get GMT button to get system time from Internet if you have connected to the Internet.

NOTE: This setting will be used for some time-based functions such as the firewall. You must specify your time zone once you login to the router successfully, otherwise these functions will not take effect.

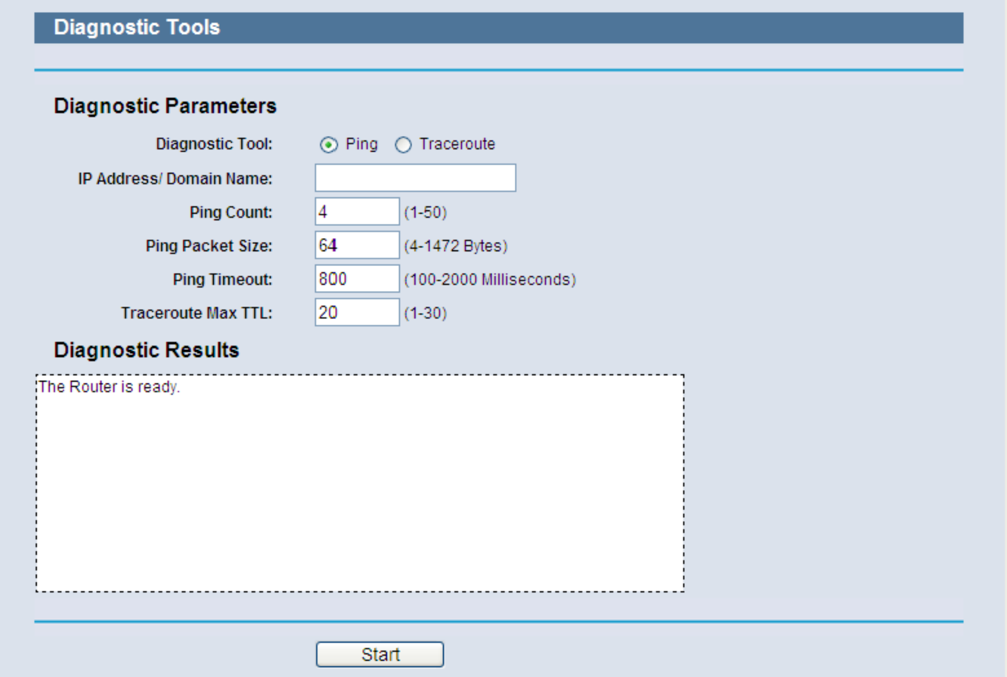
NOTE: The time will be lost if the router is turned off.

NOTE: The router will obtain GMT automatically from Internet if it has been already connected to the Internet.

DIAGNOSTIC

Select **System Tools->Diagnostic** from the menu; you can use Ping or Traceroute functions to check connectivity of your network in the following screen.

Figure 99: Diagnostic Tools



Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	● Ping ○ Traceroute	
IP Address/ Domain Name:		
Ping Count:	4	(1-50)
Ping Packet Size:	64	(4-1472 Bytes)
Ping Timeout:	800	(100-2000 Milliseconds)
Traceroute Max TTL:	20	(1-30)

Diagnostic Results

```
The Router is ready.
```

- **Diagnostic Tool** - Check the radio button to select one diagnostic too.
  - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - **Traceroute** - This diagnostic tool tests the performance of a connection.

NOTE: You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Type the destination IP address (such as 202.108.22.5) or Domain name (such as http://www.smc.com)
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.

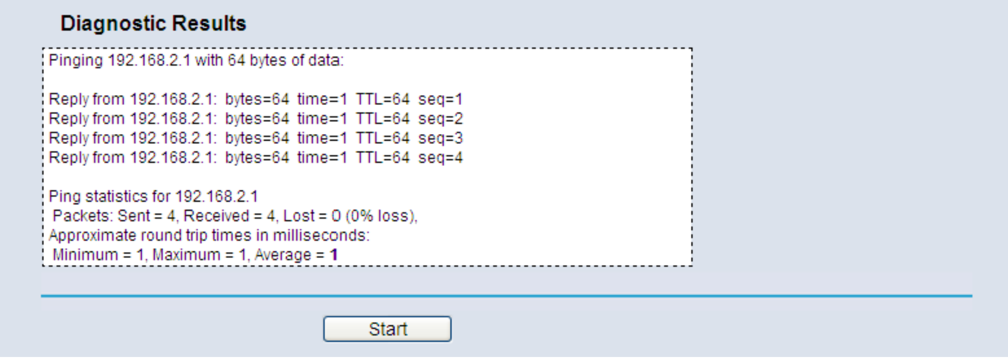
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

Click **Start** to check the connectivity of the Internet.

The Diagnostic Results page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

Figure 100: Diagnostic Results



Diagnostic Results

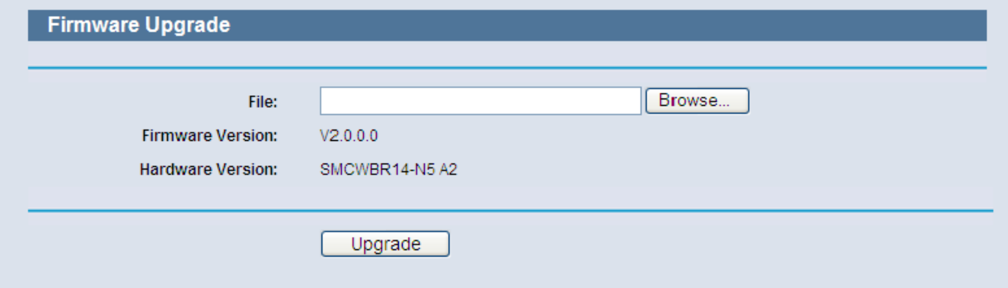
```
Pinging 192.168.2.1 with 64 bytes of data:

Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=1
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=2
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=3
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=4

Ping statistics for 192.168.2.1
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
 Minimum = 1, Maximum = 1, Average = 1
```

NOTE: Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

FIRMWARE UPGRADE

Select **System Tools->Firmware Upgrade** from the menu; you can update the latest version of firmware for the Router on the following screen.

Figure 101: Firmware Upgrade



Firmware Upgrade

File:

Firmware Version: V2.0.0.0

Hardware Version: SMCWBR14-N5 A2

- **Firmware Version** - This displays the current firmware version.
- **Hardware Version** - This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

To upgrade the Router's firmware, follow the instructions below:

1. Download a more recent firmware upgrade file from the SMC website (http://www.smc.com).

2. Type the path and file name of the update file into the File field. Or click the Browse button to locate the update file.

3. Click the Upgrade button.

NOTE: New firmware versions are posted at http://www.smc.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.

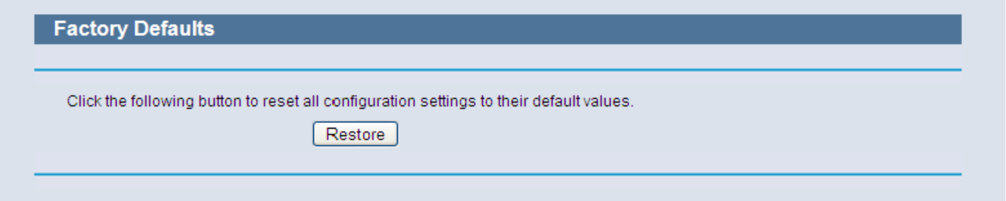
NOTE: When you upgrade the Router's firmware, you may lose its current configuration, so before upgrading the firmware write down some of your customized settings to avoid losing them.

NOTE: Do not turn off the Router or press the WPS button while the firmware is being upgraded, otherwise, the Router may be damaged. When press and hold the WPS Button for more than 5 seconds, you will reset the Router.

FACTORY DEFAULTS

Select **System Tools-> Factory Defaults** from the menu; you can restore the configuration of the Router to factory defaults on the following screen.

Figure 102: Restore Factory Default



Factory Defaults

Click the following button to reset all configuration settings to their default values.

Click the Restore button to reset all configuration settings to their default values.

- The default User Name: admin
- The default Password: smcadmin
- The default IP Address: 192.168.2.1
- The default Subnet Mask: 255.255.255.0

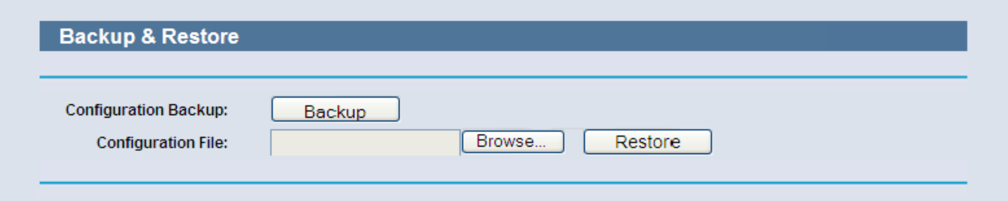
NOTE: Any settings you have saved will be lost when the default settings are restored.

NOTE: When press and hold the WPS Button for more than 5 seconds, you will reset the router.

BACKUP & RESTORE

Select **System Tools-> Backup & Restore** from the menu; you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 103.

Figure 103: Backup & Restore Configuration



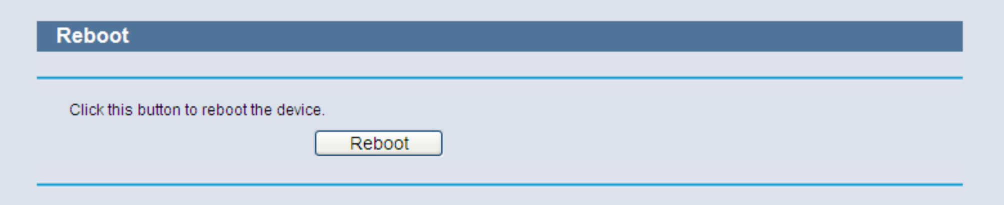
- Click the Backup button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the Browse… button to locate the update file for the Router, or enter the exact path to the Setting file in the text box.
  - Click the Restore button.

NOTE: The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

REBOOT

Select **System Tools->Reboot** from the menu; you can click the Reboot button to reboot the Router via the next screen.

Figure 104: Reboot



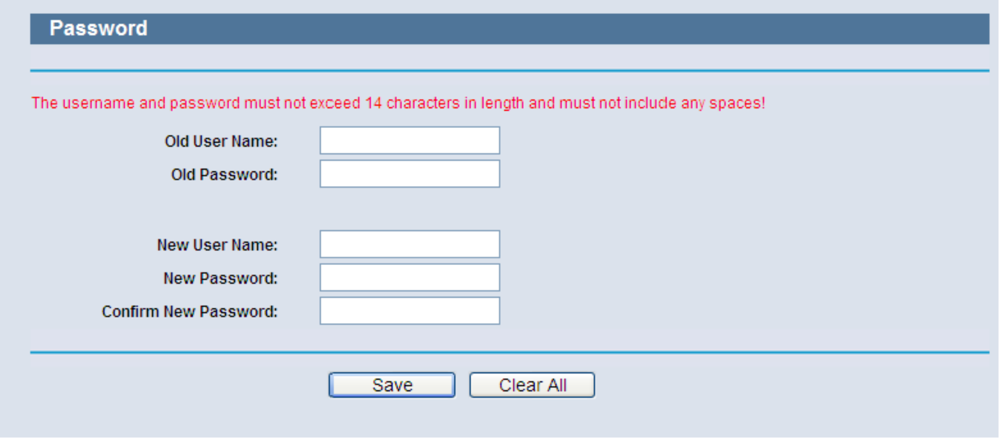
Some settings of the Router will take effect only after rebooting, which include

- Change of the LAN IP Address (system will reboot automatically).
- Change of DHCP Settings.
- Change of Wireless configurations.
- Change of the Web Management Port.
- Upgrade of the Router firmware (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration from a file (system will reboot automatically).

PASSWORD

Select **System Tools->Password** from the menu; you can change the factory default user name and password of the Router in the next screen as shown in Figure 105.

Figure 105: Password



Password

The username and password must not exceed 14 characters in length and must not include any spaces!

Old User Name:	
Old Password:	
New User Name:	
New Password:	
Confirm New Password:	

It is strongly recommended that you should change the factory default user name and password of the Router, because all users who try to access the Router's Web-based utility or Quick Setup will be prompted for the Router's default user name and password.

NOTE: The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

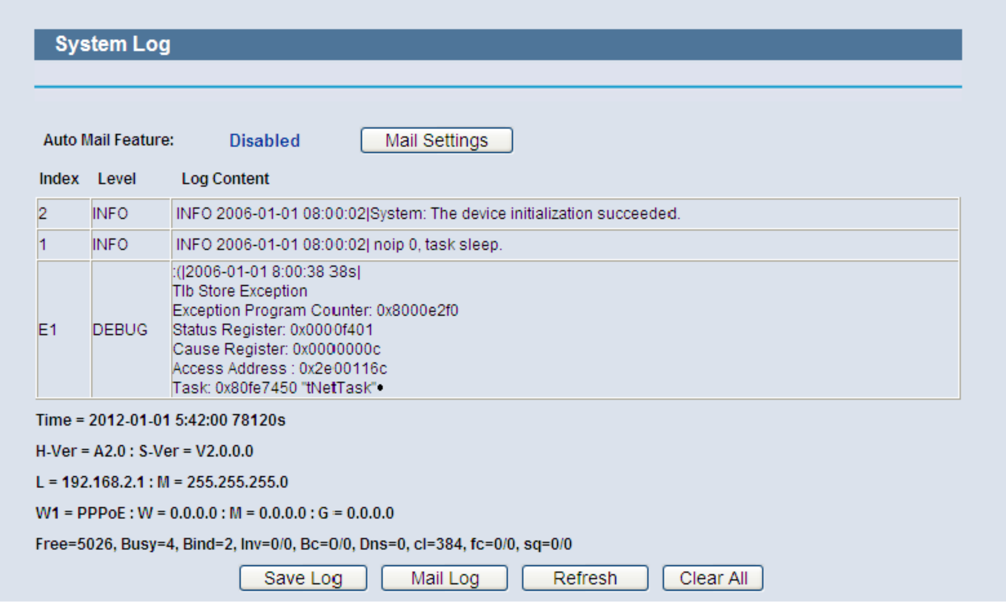
Click the Save button when finished.

Click the Clear All button to clear all.

SYSTEM LOG

Selct **System Tools->System Log** from the menu; you can view the logs of the Router.

Figure 106: System Log



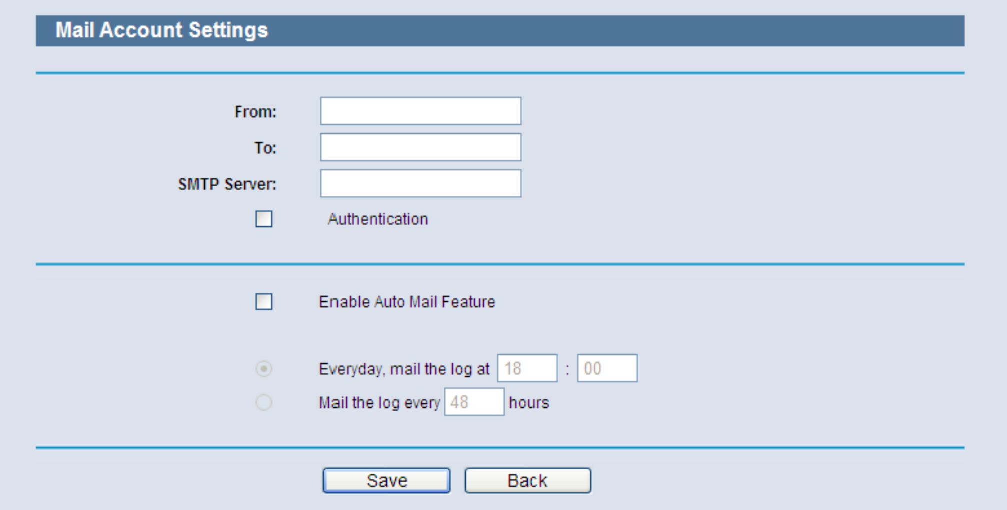
Auto Mail Feature: Disabled

Index	Level	Log Content
2	INFO	INFO 2006-01-01 08:00:02|System: The device initialization succeeded.
1	INFO	INFO 2006-01-01 08:00:02| noip 0, task sleep.
E1	DEBUG	:(|2006-01-01 8:00:38 38s| Tlb Store Exception Exception Program Counter: 0x8000e2f0 Status Register: 0x0000f401 Cause Register: 0x0000000c Access Address : 0x2e00116c Task: 0x80fe7450 "tNetTask"•

```
Time = 2012-01-01 5:42:00 78120s

H-Ver = A2.0 : S-Ver = V2.0.0.0

L = 192.168.2.1 : M = 255.255.255.0

W1 = PPPoE : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Free=5026, Busy=4, Bind=2, Inv=0/0, Bc=0/0, Dns=0, cl=384, fc=0/0, sq=0/0
```

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 107.
- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

Figure 107: Mail Account Settings



Mail Account Settings

From:

To:

SMTP Server:

□ Authentication

□ Enable Auto Mail Feature

● Everyday, mail the log at 18 : 00

○ Mail the log every 48 hours

- **From** - Your mail box address. The Router would connect it to send logs.

- **To** - Recipient’s address. The destination mailbox where the logs would be received.

- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the From field. You can log on the relevant website for Help if you are not clear with the address.

- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

NOTE: Only when you select Authentication, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part after @ is excluded.

- **Password** - Your mail account password.

- **Confirm The Password** - Enter the password again to confirm.

- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 107.

Click Save to keep your settings.

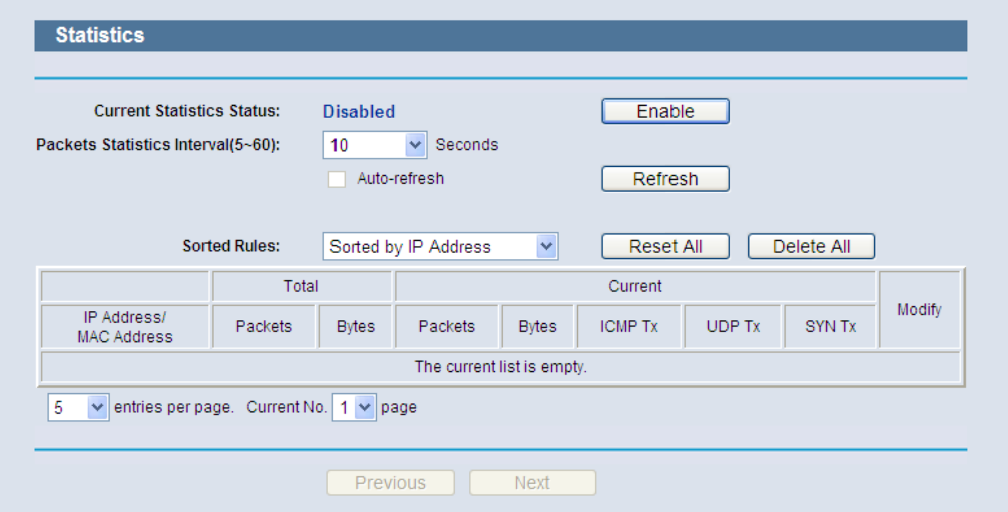
Click Back to return to the previous page.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

STATISTICS

Select **System Tools->Statistics** from the menu; you can view the statistics of the Router, including total traffic and current traffic of the last Packets Statistic Interval.

Figure 108: Statistics



Statistics

Current Statistics Status: Disabled

Packets Statistics Interval(5~60): 10 Seconds

□ Auto-refresh

Sorted Rules: Sorted by IP Address

	Total		Current					Modify
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
The current list is empty.								

5 entries per page. Current No. 1 page

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the Enable button.
- **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.

  Select the Auto-refresh checkbox to refresh automatically.

  Click the Refresh button to refresh immediately.
- **Sorted Rules** - Select a rule from the pull-down list to display the corresponding statistics..

Click Reset All to reset the values of all the entries to zero.

Click Delete All to delete all entries in the table.

Statistics Table:

IP/MAC Address - The IP/MAC Address displayed with statistics

Total Packets - The total amount of packets received and transmitted by the Router.

Total Bytes - The total amount of bytes received and transmitted by the Router.

Current Packets - The total amount of packets received and transmitted in the last Packets Statistic interval seconds.

Current Bytes - The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.

Current ICMP Tx - The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.

Current UDP Tx - The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.

Current TCP SYN Tx - The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

There are 5 entries on each page. Click Previous to return to the previous page and Next to the next page.

A

CONFIGURING THE PC

The section shows how to install and configure TCP/IP settings correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

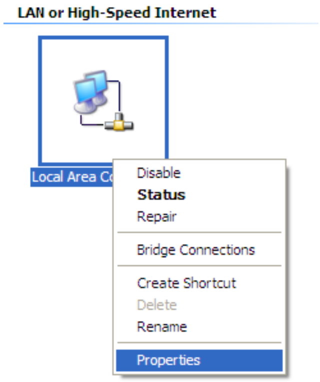
INSTALL TCP/IP COMPONENTS

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Click the Network and Internet Connections icon, and then click on the Network Connections tab in the following window.

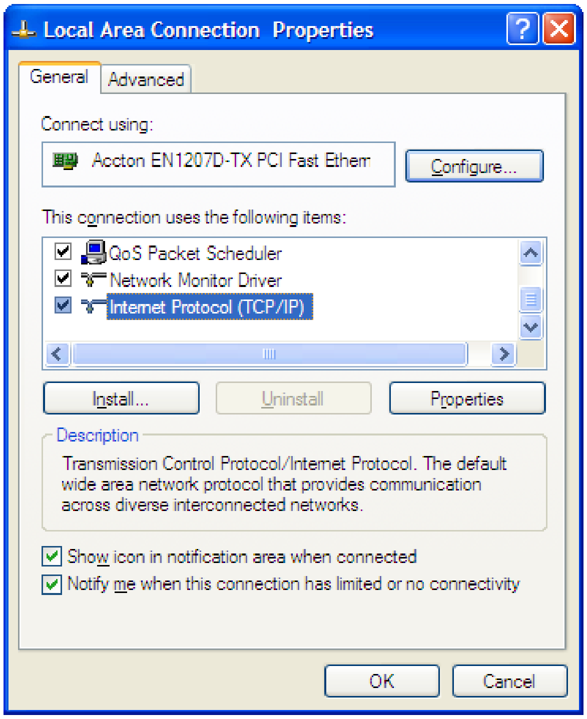
3. Right click the icon that is shown below, then select Properties from the menu.

Figure 109: TCP/IP



4. In the window that is shown below, double click on "Internet Protocol (TCP/IP)."

Figure 110: Internet Protocol



Connect using:
Accton EN1207D-TX PCI Fast Ethern

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Network Monitor Driver
- ☑ Internet Protocol (TCP/IP)

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

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

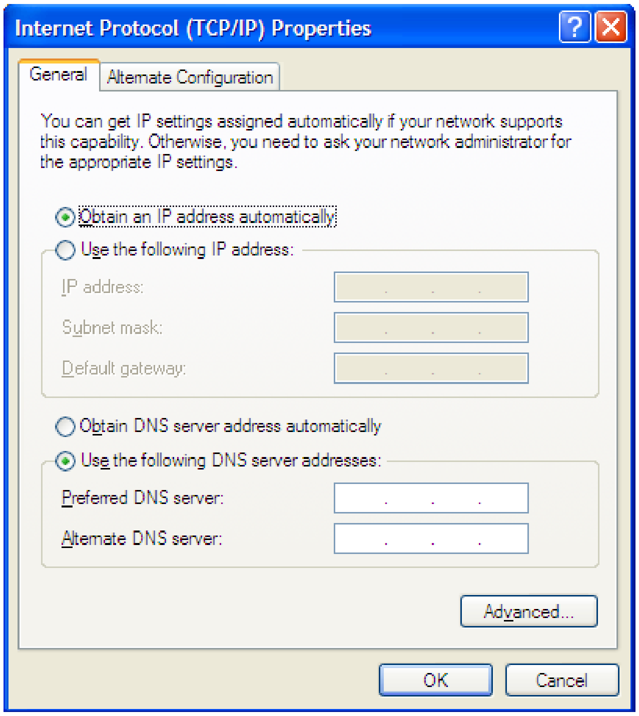
5. The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

   Now you have two ways to configure the TCP/IP protocol below:

   a. Set the IP address automatically.

      Select "Obtain an IP address automatically," and "Obtain DNS server automatically," as shown in the Figure below:

Figure 111: Internet Protocol Properties



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

b. Set the IP address manually.

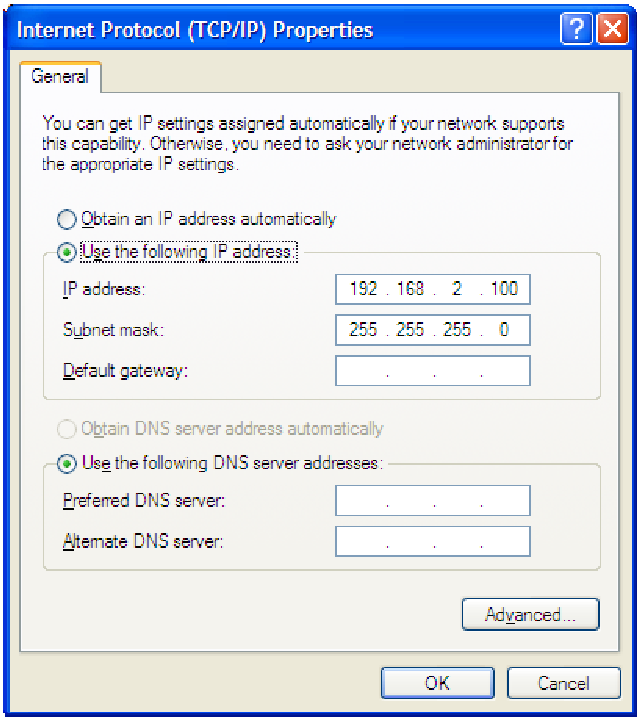
Select “Use the following IP address” radio button and enter the following items:

— If the Router's LAN IP address is 192.168.2.1, type an IP address such as 192.168.2.x (where x is from 2 to 254), and Subnet mask as 255.255.255.0.

— Type the Router’s LAN IP address (the default IP is 192.168.2.1) into the Default gateway field.

— Select “Use the following DNS server addresses” radio button. In the “Preferred DNS Server” field, type the DNS server IP address that has been provided by your ISP.

Figure 112: Setting the IP Address Manually



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

6. Click OK to keep your settings.

B FAQ

How do I configure the Router for Internet access by ADSL users?

1. Configure the ADSL Modem in RFC1483 bridge mode.

2. Connect Ethernet cable from the ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

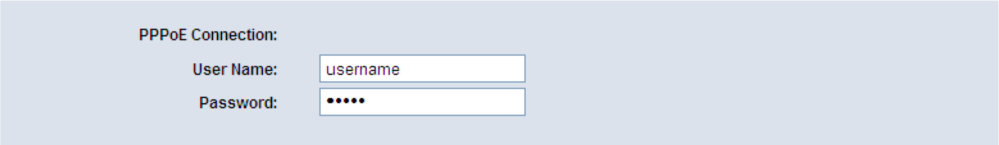
3. Log in to the Router, click "Network" on the web page menu and then click "WAN" on the submenu.

   a. On the WAN page, select "PPPoE" for the WAN connection type.

   b. Type the user name in the "User Name" field and the password in the "Password" field.

   c. Finish by clicking "Connect".

Figure 113: PPPoE Connection Type



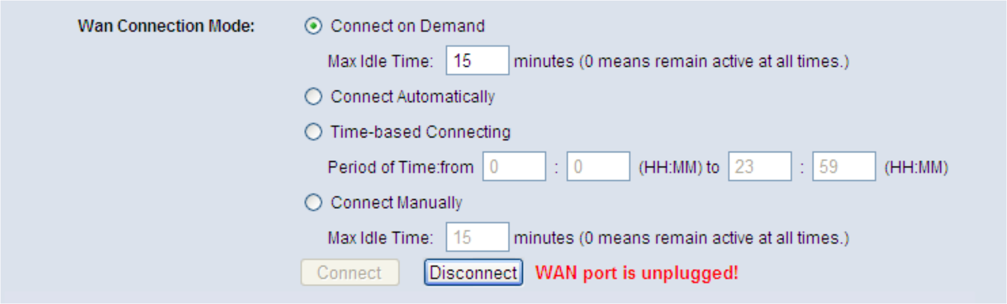
PPPoE Connection:

User Name: username

Password: •••••

4. If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand," or "Connect Manually" for Internet connection mode. Type an appropriate value for the "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.

Figure 114: PPPoE Connection Mode



Wan Connection Mode: ● Connect on Demand

Max Idle Time: 15 minutes (0 means remain active at all times.)

○ Connect Automatically

○ Time-based Connecting

Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

○ Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

WAN port is unplugged!

NOTE: Sometimes the connection cannot be disconnected although you have specified a Max Idle Time, since some applications may be visiting the Internet continually in the background.

NOTE: If you are a Cable user, configure the Router following the above steps.

HOW DO I CONFIGURE THE ROUTER FOR INTERNET ACCESS BY ETHERNET USERS?

1. Log in to the Router, click “Network” on the web page menu, and then click "WAN" on the submenu.

   a. On the WAN page, select “Dynamic IP” for the WAN connection type.

   b. Finish by clicking **Save**.

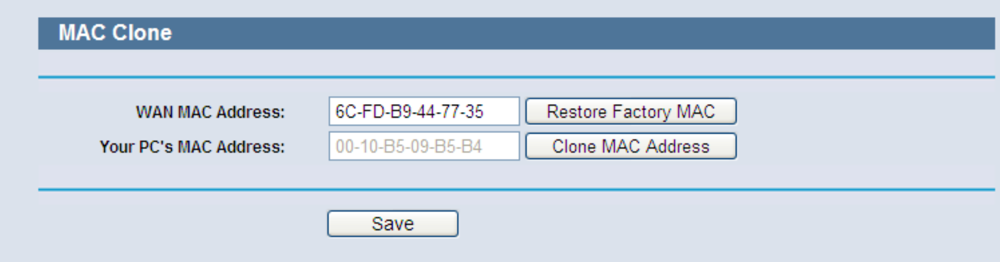
2. Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires this, log in to the Router and click the "Network" menu link, and then click the "MAC Clone" submenu link.

   a. On the “MAC Clone” page, click the "Clone MAC Address" button if your PC’s MAC address is a proper MAC address. Your PC’s MAC address will fill in the “WAN MAC Address” field.

      Otherwise, type the MAC Address into the “WAN MAC Address” field. The format for the MAC Address is XX-XX-XX-XX-XX-XX.

   b. Click the **Save** button. Settings take effect after rebooting.

Figure 115: MAC Clone



MAC Clone

WAN MAC Address: 6C-FD-B9-44-77-35

Your PC's MAC Address: 00-10-B5-09-B5-B4

I WANT TO USE NETMEETING, WHAT DO I NEED TO DO?

1. If you start Netmeeting as a host, you do not need to change anything on the Router.

2. If you start as a response, you need to configure a Virtual Server or DMZ Host, and make sure the H323 ALG is enabled.

3. Configure a Virtual Server:

   a. Log in to the Router, click "Forwarding" on the menu, and then click "Virtual Servers" on the submenu.

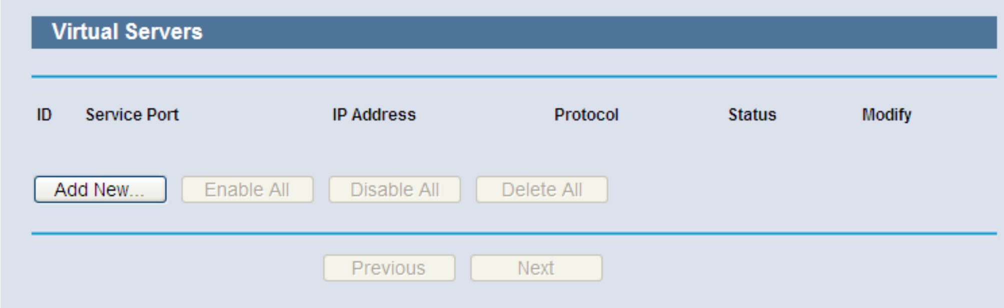
   b. On the "Virtual Servers" page, click "Add New".

   c. On the "Add or Modify a Virtual Server Entry" page, enter "1720" for the "Service Port".

   d. Enter your IP address in the "IP Address" field (for example, 192.168.2.169).

   e. Set to Enable and then Save.

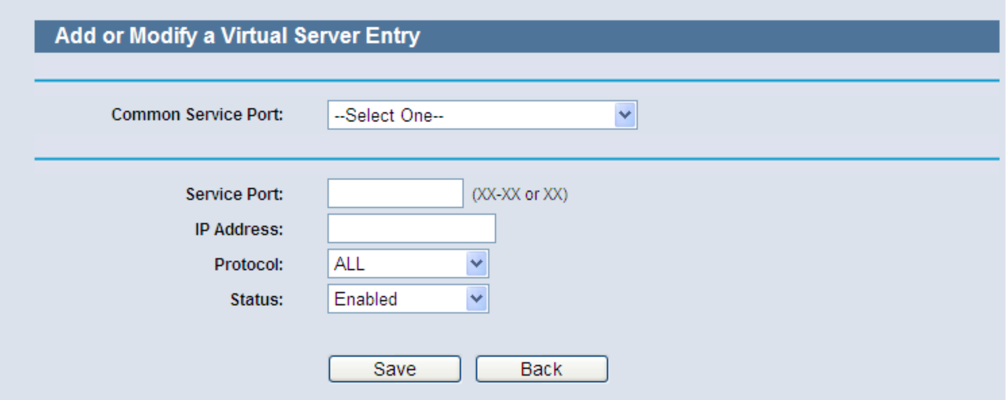
Figure 116: Virtual Servers



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure 117: Add or Modify a Virtual Server Entry



Add or Modify a Virtual Server Entry

Common Service Port: --Select One--

Service Port: (XX-XX or XX)
IP Address:
Protocol: ALL
Status: Enabled

NOTE: The other party should call your WAN IP, which is displayed on the "Status" page.

4. Enable a DMZ Host:

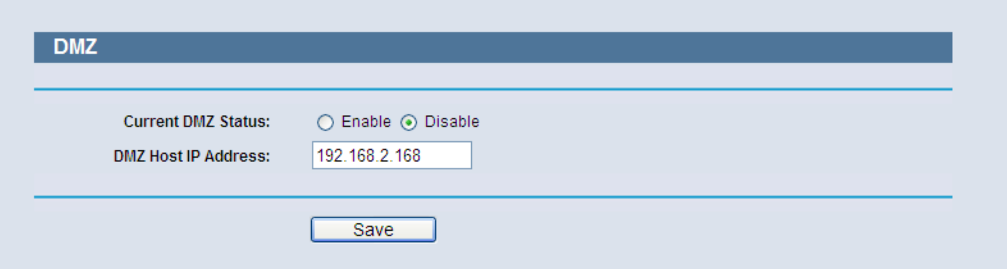
a. Log in to the Router, click "Forwarding" on the menu, and then click "DMZ" on the submenu.

b. On the "DMZ" page, click the Enable radio button.

c. Type your IP address into the "DMZ Host IP Address" field (for example, 192.168.2.169).

d. Click the Save button.

Figure 118: DMZ



DMZ

Current DMZ Status: ○ Enable ● Disable

DMZ Host IP Address: 192.168.2.168

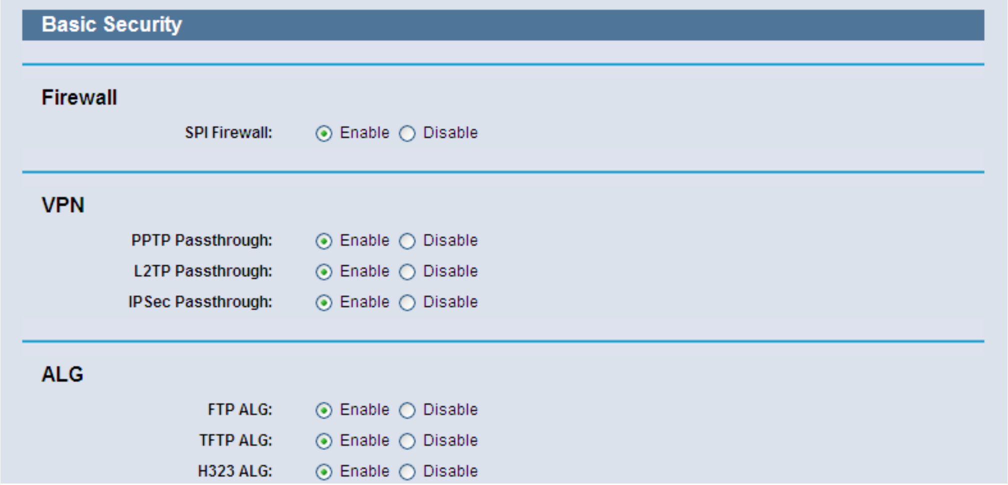
5. Enable the H323 ALG:

a. Log in to the Router, click "Security" on the menu, and then click "Basic Security" on the submenu.

b. On the "Basic Security" page, check the Enable radio button next to H323 ALG.

c. Click the Save button.

Figure 119: Basic Security



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

H323 ALG: ● Enable ○ Disable

I WANT TO BUILD A WEB SERVER ON THE LAN, WHAT SHOULD I DO?

1. Change the Web management port number:

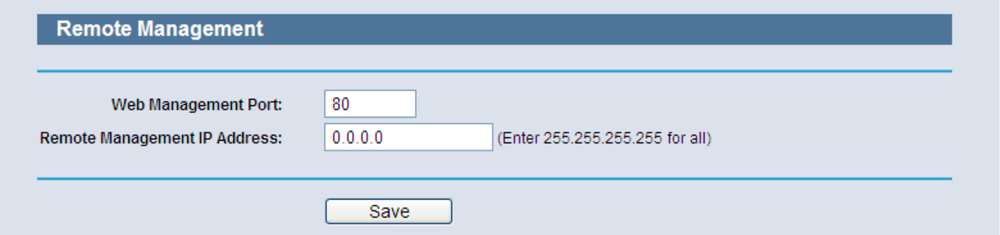
   Because the Web Server port 80 will interfere with the Web management port 80 on the Router, you must change the Web management port number to avoid interference.

   a. Log in to the Router, click “Security” on the menu, and then click "Remote Management" on the submenu.

   b. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field.

   c. Click Save and reboot the Router.

Figure 120: Remote Management



Remote Management

Web Management Port: 80

Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

NOTE: When the above configuration takes effect, you can configure the Router by typing “http://192.168.2.1:88” (the Router’s LAN IP address: Web Management Port) in the address field of the Web browser.

2. Configure a Virtual Server:

a. Log in to the Router, click “Forwarding” on the menu, and then click "Virtual Servers" on the submenu.

b. On the "Virtual Servers" page, click “Add New”.

c. On the “Add or Modify a Virtual Server” page, enter “80” into the field for the “Service Port”.

d. Enter your IP address in the “IP Address” field (for example, 192.168.2.188).

e. Set to Enable and then Save.

Figure 121: Virtual Servers

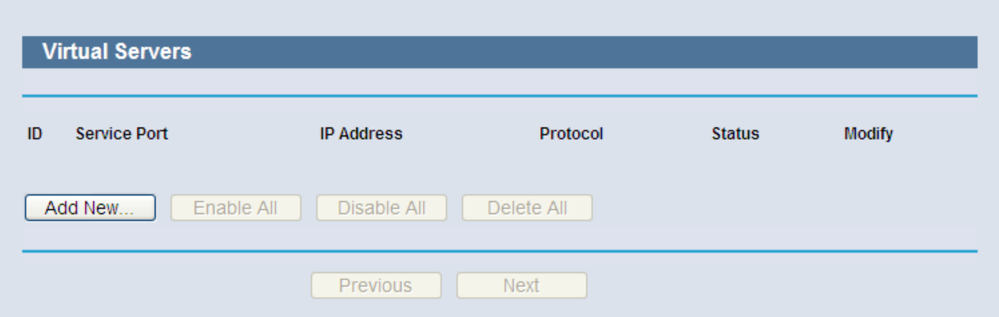
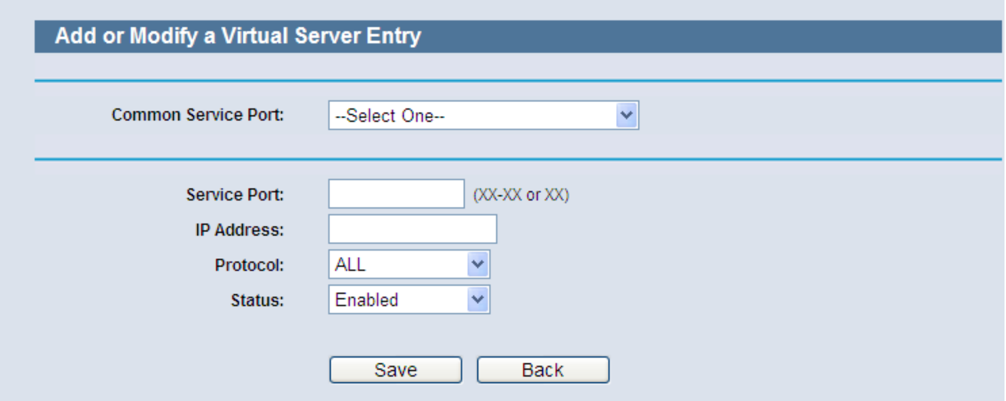


Figure 122: Add or Modify a Virtual Server Entry



Common Service Port: --Select One--

Service Port: (XX-XX or XX)

Protocol: ALL

Status: Enabled

WIRELESS STATIONS CANNOT CONNECT TO THE ROUTER

1. Make sure the "Wireless Router Radio" is enabled.

2. Make sure that the SSID of wireless stations is the same as the Router's SSID.

3. Make sure wireless stations have the right encryption key for the Router security.

4. If the wireless connection is ready, but you cannot access the Router, check the IP Address of your wireless station.

C

Specifications

Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX 802.11b 802.11g 802.11n
Protocol	TCP/IP, PPPoE, DHCP, IGMP, NAT, SNTP
Ports	One 10/100 Mbps Auto-Negotiation RJ-45 WAN port Four 10/100 Mbps Auto-Negotiation RJ-45 LAN ports All ports support Auto MDI/MDIX
Cabling Type	10BASE-T: UTP Category 3, 4, 5 cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m) 100BASE-TX: UTP Category 5, 5e cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m)
LED Indicators	Power, System, WLAN, WAN, LAN (1-4), WPS
Frequency Band	2.4~2.4835 GHz
Radio Data Rate	11b: 11/5.5/2/1 Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6 Mbps (Automatic) 11n: up to 300 Mbps (Automatic, SMCWBR14-N5)
Channels	1~13
Frequency Expansion	DSSS (Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	270 Mbps: -68dBm@10% PER 130 Mbps: -68dBm@10% PER 108 Mbps: -68dBm@10% PER 54 Mbps: -68dBm@10% PER 11 Mbps: -85dBm@8% PER 6 Mbps: -88dBm@10% PER 1 Mbps: -90dBm@8% PER
Antenna Gain	5dBi
Temperature	Operating: 0 °C to 40 °C (32 to 104 °F) Storage: -40 °C to 70 °C (-40 to 158 °F)
Humidity	Operating: 10% to 90% (non-condensing) Storge: 5%-90% (non-condensing)

Glossary

IEEE 802.11b A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.11n A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 27, 54, 81, 108, 162, 216, 243, 270, 300 Mbps. IEEE 802.11n is also backward compatible with IEEE 802.11b/g.

DDNS (Dynamic Domain Name System) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DMZ (Demilitarized Zone) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

DNS (Domain Name System) An Internet Service that translates the names of websites into IP addresses.

Domain Name A descriptive name for an address or group of addresses on the Internet.

DSL (Digital Subscriber Line) A technology that allows data to be sent or received over existing traditional phone lines.

ISP (Internet Service Provider) A company that provides access to the Internet.

MTU (Maximum Transmission Unit) The size in bytes of the largest packet that can be transmitted.

NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

PPPoE (Point to Point Protocol over Ethernet) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit, 128-bit, or 152-bit shared-key algorithm, as described in the IEEE 802.11 standard.

Wi-Fi A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

INDEX

SMC®
Networks

Headquarters

No. 1, Creation Rd. III
Hsinchu Science Park
Taiwan 30077
Tel: +886 3 5638888
Fax: +886 3 6686111

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

English: (for Asia-Pacific): Technical Support information at www.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: สามารถหาข้อม้ลทางด้านเทคนิคได้ที่ 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

SMCWBR14-N5