Edge-corE NETWORKS

SMC Networks

USER GUIDE

ADSL2 BARRICADE™ N
4-Port ADSL/ADSL2+ Wireless Router

SMC7904WBRAS-N2 v2

4-Port ADSL/ADSL2+ Wireless Router User Guide

SMC® Networks

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

March 2012
Pub. # 149xxxxxxxxx
SMC-UG-0312-01

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.

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. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

FCC - Part 68

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: 1KRDL09BSMC7800A. If requested, this number must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have those entire devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact please contact our company at the numbers shown on back of this manual for information on obtaining service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

REN (Ringer Equivalent Numbers) Statement

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Attachment Limitations Statement

Notice: This equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment with the Industry Canada certification number. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

CE MARK DECLARATION OF CONFORMANCE FOR EMI AND SAFETY (EEC)

SMC contact for these products in Europe is:

SMC Networks Europe,
C/Fructuós Gelabert 6-8, 2º, 2ª,
Edificio Conata II,
08970 - Sant Joan Despí, Barcelona, Spain.

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

NATIONAL RESTRICTIONS

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

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

NOTE: 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 + A1: 2010 + A12: 2011
  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).

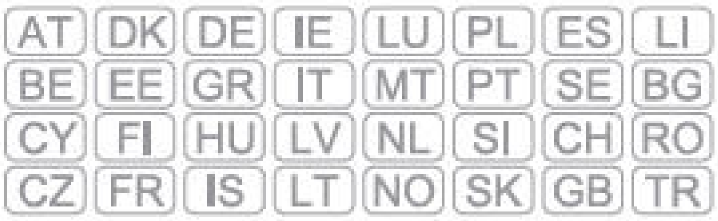
This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

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.

CE (!)

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	Manufacturer tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish Dansk	Undertegnede Manufacturer 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 Manufacturer 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 Manufacturer dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, Manufacturer, 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 Manufacturer seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish Suomi	Valmistaja Manufacturer 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 Manufacturer 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 Manufacturer, 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 Manufacturer 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 Manufacturer δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ.
Hungarian Magyar	Alulírott, Manufacturer nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Italian Italiano	Con la presente Manufacturer 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 Manufacturer deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo Manufacturer deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Maltese Malti	Hawnhekk, Manufacturer, 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 Manufacturer oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	Manufacturer 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	Manufacturer týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	Manufacturer 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 Manufacturer 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 Manufacturer 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.

ENVIRONMENTAL STATEMENT

The manufacturer of this product endeavours to sustain an environmentally-friendly policy throughout the entire production process. This is achieved though the following means:

- Adherence to national legislation and regulations on environmental production standards.
- Conservation of operational resources.
- Waste reduction and safe disposal of all harmful un-recyclable by-products.
- Recycling of all reusable waste content.
- Design of products to maximize recyclables at the end of the product's life span.
- Continual monitoring of safety standards.

END OF PRODUCT LIFE SPAN

This product is manufactured in such a way as to allow for the recovery and disposal of all included electrical components once the product has reached the end of its life.

MANUFACTURING MATERIALS

There are no hazardous nor ozone-depleting materials in this product.

DOCUMENTATION

All printed documentation for this product uses biodegradable paper that originates from sustained and managed forests. The inks used in the printing process are non-toxic.

About This Guide

Purpose This guide gives specific information on how to install the ADSL Gateway Router and its physical and performance related characteristics. It also gives information on how to operate and use the management functions of the ADSL Gateway Router.

Audience This guide is for users with a basic 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.

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

March 2012 Revision
This is the first revision of this guide.

Contents

FIGURES

TABLES

SECTION I

GETTING STARTED

This section provides an overview of the ADSL Gateway Router, and describes how to install and mount the unit.

This section includes these chapters:

1 INTRODUCTION

The Barricade ADSL Gateway Router (SMC7904WBRAS-N2 v2) is an ADSL2/2+ modem contained in a compact unit. The router enables multiple wired and wireless users to securely access the Internet through a single-user account with the ADSL service provider. The router provides four 10/100 Mbps Ethernet ports for connection to end users, an IEEE 802.11b/g/n wireless interface, and one ADSL line for connection to the Internet service provider.

FEATURES AND BENEFITS

The features of the ADSL Gateway Router include:

- Full-rate ADSL router, support for Router and Bridge modes
- ITU G.992.3(ADSL2) and ITU G.992.5(ADSL2+)
- ITU G.992.1 (G.dmt) Annex A and ITU G.992.2 (G.lite)
- ANSI T1.413 Issue 2
- Provides 24 Mbps downstream and 1 Mbps upstream
- Maximum transmission range: 5.4 Kilometers
- Four Ethernet ports, 10/100 Mbps Auto-MDI/MDIX
- 802.11n 2.4 GHz radio supporting four SSID interfaces
- Friendly web-based user interface for configuration
- Configurable as a DHCP server on your network
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of your configuration, and links to the configuration pages.
- Downloadable flash software upgrades
- Support of up to 8 Permanent Virtual Circuits (PVC)
- Support of up to 8 PPPoE sessions

DESCRIPTION OF HARDWARE

This ADSL Gateway Router is a high bit-rate Digital Subscriber Line (DSL) modem that can connect to an ADSL Internet service provider.

This unit provides the following ports on the rear panel:

- One RJ-11 port for connection to your ADSL service provider's incoming line.
- Four RJ-45 ports for connection to PCs, or to a 10/100BASE-TX Ethernet Local Area Network switch. The ports operate at 10/100 Mbps, half/full duplex. It supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections. (See "10/100BASE-TX Pin Assignments" on page 148.)

The following two figures show the components of the Gateway:

Figure 1: Top Panel

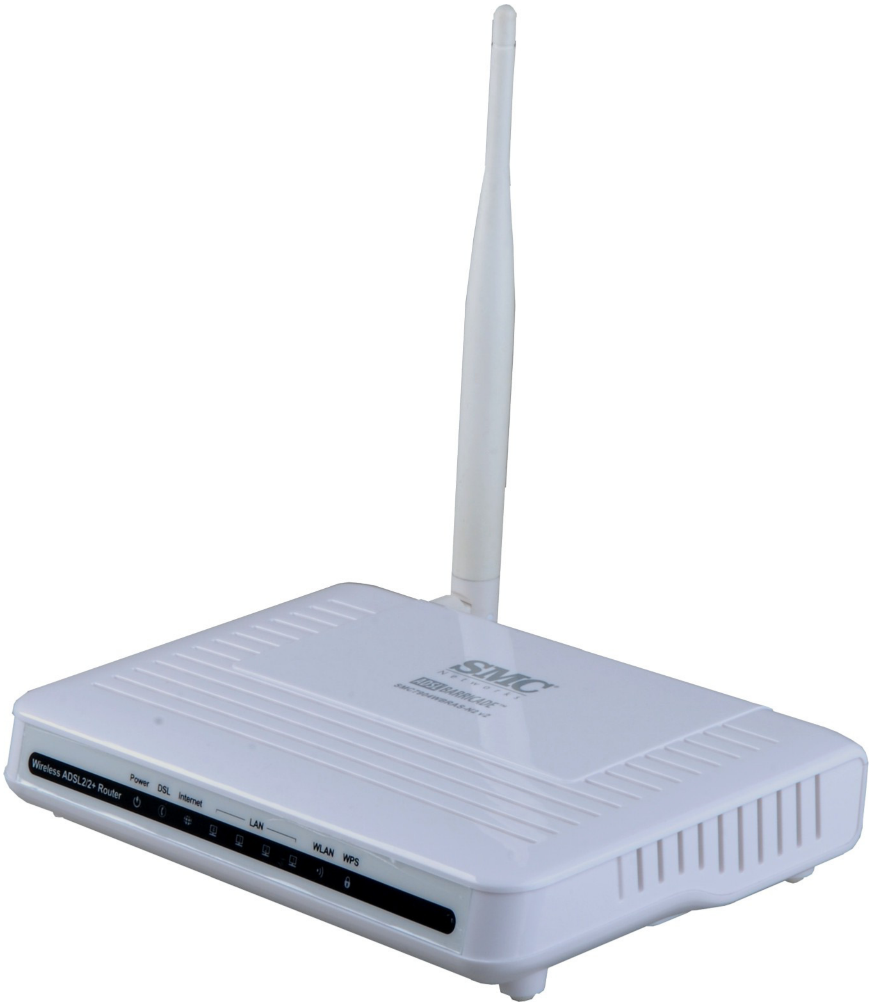


Figure 2: Rear Panel

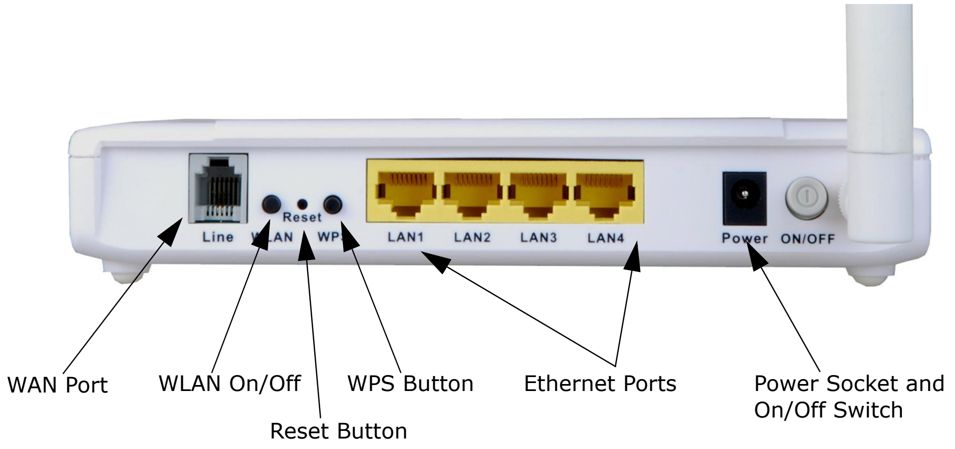
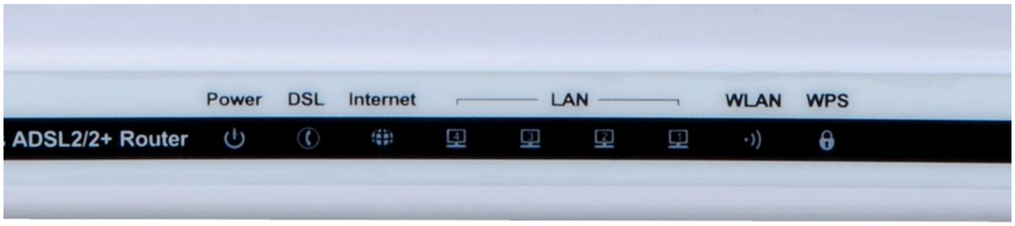


Figure 3: Front Panel LEDs



The ADSL Gateway Router includes key system and port indicators that simplify installation and network troubleshooting. The LEDs, which are located on the top of the unit for easy viewing, are described in the following table.

Table 1: LED Display Indicators

LED	Status	Description
Power	On Green	The router is being supplied with power.
	On Red	The router is running its self-test or the self-test has failed.
	Off	The router is not receiving power.
DSL	On Green	The DSL Line port has a link with the service provider.
	Fast Blinking Green	A DSL link is being established with the service provider.
	Slow Blinking Green	No DSL signal detected.
Internet	On Green	The Internet connection is in its normal routing mode (for example, PPP dial-up is successful), but no data is being transmitted.
	Blinking Green	Internet data is being transmitted in routing mode.
	On Red	The Internet connection has failed after successful synchronization in routing mode (for example, PPP dial-up has failed).
	Off	The device is in bridge mode.

Table 1: LED Display Indicators (Continued)

LED	Status	Description
LAN (1-4)	On Green	Ethernet port has a valid link with attached device.
	Blinking Green	Data is being transmitted or received on the port.
	Off	Ethernet port has no link with an attached device.
WLAN	On Green	The Wi-Fi radio is enabled.
	Blinking Green	Data is being transmitted through the WLAN interface.
	Off	The Wi-Fi radio is disabled.
WPS	On Green	WPS is activated and the router is waiting for negotiation with wireless clients.
	Off	WPS is not activated.

POWER CONNECTOR

The ADSL Gateway Router must be powered with its supplied power adapter. Failure to do so results in voiding of any warrantly supplied with the product. The power adapter automatically adjusts to any voltage between 100~240 volts at 50 or 60 Hz, and supplies 12 volts DC power to the unit. No voltage range settings are required.

POWER BUTTON

The ADSL Gateway Router has a power button. When the AC power adapter is attached and connected to a power source, the power button must be depressed to power on the unit.

WLAN BUTTON

Turns the ADSL Gateway Router’s Wi-Fi radio on or off. The WLAN LED on the front panel indicates when the Wi-Fi radio is enabled.

WPS BUTTON

Push this button to start WPS authentication of a wireless device. 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.

RESET BUTTON

This button is used to restore the factory default configuration. If you press and hold down the button for 8 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the unit.

2 Installing the Router

Before installing the ADSL Gateway Router, verify that you have all the items listed in “Package Contents.” If any items are missing or damaged, contact your local distributor. Also, be sure you have all the necessary tools and cabling before installing the router.

Package Contents

After unpacking the ADSL Gateway Router, check the contents of the box to be sure that you have received the following components:

- Barricade ADSL Gateway Router, SMC7904WBRAS-N2 v2
- RJ-45 Category 5 network cable
- RJ-11 telephone cable
- ADSL splitter
- AC power adapter
- Quick Installation Guide
- Documentation CD
- SMC warranty information card

Please inform your dealer if there are any incorrect, missing, or damaged parts. If possible, retain the carton, including the original packing materials in case there is a need to return the unit for repair.

System Requirements

Before you start installing the router, make sure you can provide the right operating environment. See the following installation requirements:

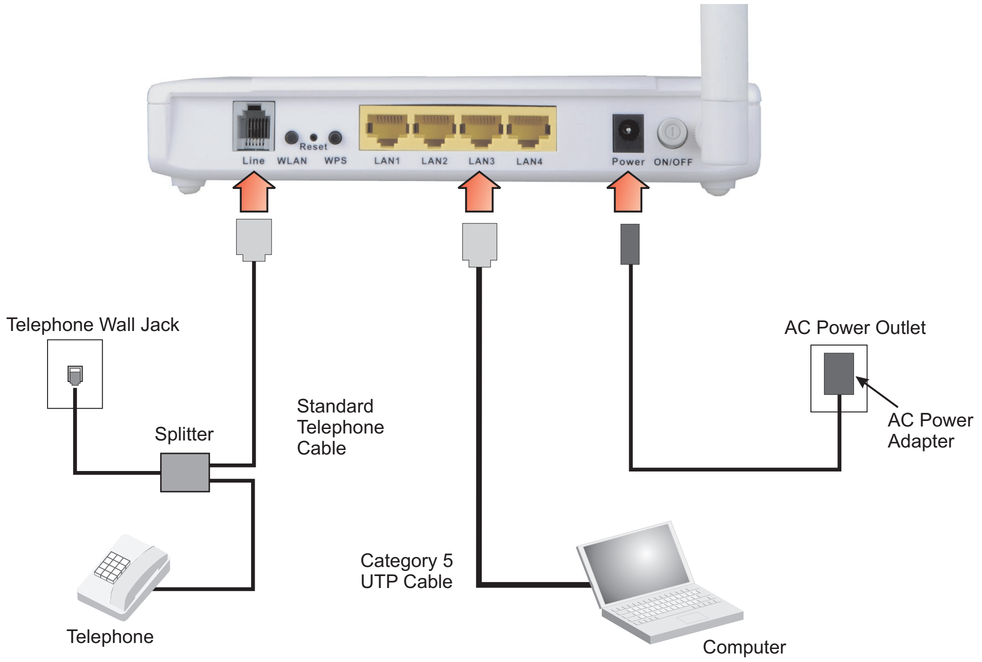
- A PC or Macintosh with a 10/100 Mbps Ethernet adapter card installed. Or, a Windows PC with an available USB port.
- For Internet access, the computer must be configured for TCP/IP.

- Power requirements: 12 VDC using the included AC power adapter. Make sure that a properly grounded power outlet is within 1.8 m (6 ft) of the router.
- The router should be located in a cool dry place, with at least 5 cm (2 in.) of space on all sides for ventilation.
- Place the router out of direct sunlight, and away from heat sources or areas with a high amount of electromagnetic interference. The temperature and humidity should be within the ranges listed in the specifications.

CABLE CONNECTIONS

The ADSL Gateway Router needs to be connected to the DSL telephone line from the service provider, and to a computer or LAN switch.

Figure 4: Connecting the Router



To install the router, follow these steps:

1. Using standard telephone cable, connect the Line port on the included ADSL splitter to the RJ-11 telephone wall jack providing the ADSL service.
2. Using standard telephone cable, connect the Modem port on the included ADSL splitter to the RJ-11 Line port on the ADSL Gateway Router.

3. The Phone port on the ADSL splitter can be connected to a standard telephone set using telephone cable.

4. Connect one end of the included Ethernet cable to an Ethernet port on the ADSL Gateway Router, and the other end to a PC’s RJ-45 network port. Alternatively, you can connect an Ethernet port to a LAN switch.

CAUTION: Do not plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

NOTE: When connecting to any network device (such as a PC, hub or switch), you can use either straight-through or crossover cabling. (Refer to “Cables and Pinouts” on page 147 for a description of cable types.)

NOTE: Make sure the twisted-pair Ethernet cable connected to the router’s Ethernet port does not exceed 100 meters (328 feet).

POWERING ON

Plug the power adapter cord into the DC 12V power socket on the router, and then plug the power adapter directly into a power outlet. Check the LED marked “Power” on the top of the unit to be sure it is on. If the Power indicator does not light up, refer to “Troubleshooting” on page 141.

If the router is properly configured, it will take about 30 seconds to establish a connection with the ADSL service provider after powering up. During this time the Link indicator will blink during synchronization. After the ADSL connection has been established, the Link indicator will stay on.

CONFIGURING THE TCP/IP PROTOCOLS

To connect the router to a computer through its Ethernet port, the computer must have an Ethernet network adapter card installed, and be configured for the TCP/IP protocol. Your service provider will configure TCP/IP for client computers automatically using a networking technology known as Dynamic Host Configuration Protocol (DHCP).

Carry out the following steps to check that the computer’s Ethernet port is correctly configured for DHCP.

WINDOWS 95/98/NT

1. Click “Start/Settings/Control Panel.”

2. Click the “Network” icon.

3. For Windows NT, click the “Protocols” tab.

4. Select "TCP/IP" from the list of network protocols; this may include details of adapters installed in your computer.

5. Click "Properties."

6. Check the option "Obtain an IP Address."

WINDOWS 2000

1. Click "Start/Settings/Network/Dial-up Connections."

2. Click "Local Area Connections."

3. Select "TCP/IP" from the list of network protocols.

4. Click on "Properties."

5. Select the option "Obtain an IP Address."

WINDOWS XP

1. Click "Start/Control Panel/Network Connections."

2. Right-click the "Local Area Connection" icon for the adapter you want to configure.

3. Highlight "Internet Protocol (TCP/IP)."

4. Click on "Properties."

5. Select the option "Obtain an IP address automatically" and "Obtain DNS server address automatically."

WINDOWS VISTA

1. Click Start/Control Panel.

2. Double-click "Network and Sharing Center."

3. Click "View status."

4. Click "Properties." If the "User Account Control" window appears, click "Continue."

5. Highlight "Internet Protocol Version 6 (TCP/IPv6)" or "Internet Protocol Version 4 (TCP/IPv4)," and click "Properties."

6. Select the option "Obtain an IP address automatically" and "Obtain DNS server address automatically."

MAC OS

1. Pull down the Apple Menu. Click "Control Panels" and select "TCP/IP."

2. In the TCP/IP dialog box, verify that "Ethernet" is selected in the "Connect Via:" field.

3. If "Using DHCP Server" is already selected in the "Configure" field, your computer is already configured for DHCP. Otherwise, select "Using DHCP Server" in the "Configure" field and close the window.

4. Another box will appear asking whether you want to save your TCP/IP settings. Click "Save."

5. Your service provider will now be able to automatically assign an IP address to your computer.

SECTION II

WEB CONFIGURATION

This section describes the basic settings required to access the web management interface and provides details on configuring the Gateway.

This section includes these chapters:

3 SYSTEM CONFIGURATION

USING THE WEB INTERFACE

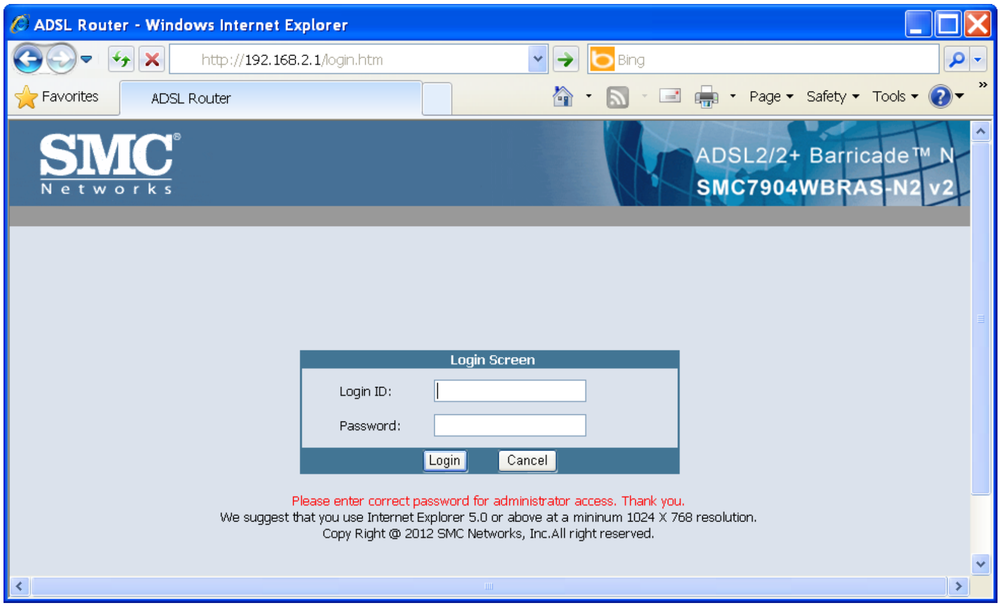
The router provides a web-based management interface for configuring device features and viewing statistics to monitor network activity. This interface can be accessed by any computer on the network using a standard web browser (such as Internet Explorer 5.0, Netscape 6.2, Mozilla Firefox 2.0, or above).

To make an initial connection to the management interface, connect a PC to one of the router’s LAN ports. Set your PC with a static address within the same subnet as that used by the router (that is, 192.168.2.x with the subnet mask 255.255.255.0).

To access the configuration menu, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.

Figure 5: Web Login



Please enter correct password for administrator access. Thank you.
We suggest that you use Internet Explorer 5.0 or above at a mininum 1024 X 768 resolution.
Copy Right @ 2012 SMC Networks, Inc.All right reserved.

2. Log in to the router’s management interface using this account:

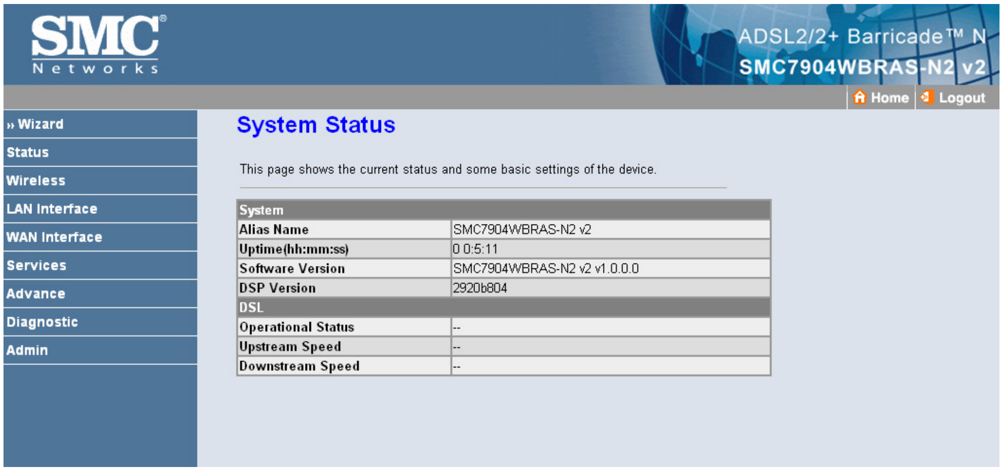
   Login ID: admin
   Password: smcadmin

NOTE: It is strongly recommended to change the default password the first time you access the web interface. For information on changing the password, see "Password Setup" on page 135.

HOME PAGE

When your web browser connects with the router's web agent, the home page is displayed as shown below. Basic information can be viewed using the Status menu. To carry out detailed configuration tasks, use the other menu items.

Figure 6: Home Page



System Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	SMC7904WBRAS-N2 v2
Uptime(hh:mm:ss)	0 0:5:11
Software Version	SMC7904WBRAS-N2 v2 v1.0.0.0
DSP Version	2920b804
DSL	
Operational Status	--
Upstream Speed	--
Downstream Speed	--

The main menu is displayed on the left side of the screen. Click on any of these items to open the sub-menu list. The information in this chapter is organized to reflect the structure of the web management screens for easy reference. The configuration pages include the options listed in the table below. For details on configuring each feature, refer to the corresponding page number.

Table 2: Configuration Menu

Menu	Description	Page
Wizard	Starts the setup wizard	40
Status		
System	Shows hardware/software version numbers, DSL connection status, and Internet connection settings	45
LAN	Shows the LAN IP and DHCP server settings	46
WLAN	Shows wireless interface settings	47
WAN	Shows WAN interface functional status (including connection mode – single or multiple service, IGMP), and connection status	48
Port Mapping	Shows the port mapping settings	49
Statistics		

Table 2: Configuration Menu (Continued)

Menu	Description	Page
Statistics	Shows the network traffic statistics	50
DSL Statistics	Shows the ADSL line statistics	51
ARP	Shows entries in the ARP table	52
Wireless		
Basic Settings	Configures basic wireless settings	55
Advanced Settings	Configures advanced wireless settings	57
Security	Configures wireless security settings	59
Access Control	Configures wireless access control settings	64
WPS	Configures WPS security	65
MBSSID	Enables multiple SSID interfaces	66
WDS	Configures Wireless Distribution System settings	68
LAN Interface		
LAN Interface	Configures the LAN management interface, including IP address, and IGMP snooping on LAN side	73
IPv6 LAN Config	Configures IPv6 LAN settings	74
DHCP Config		
DHCP Mode	Sets DHCP server and DHCP relay settings	76
Static IP	Configures static DHCP assignments	80
WAN Interface		
Channel Config	Configures the DSL channel settings	82
ATM Settings	Configures DSL ATM settings	84
ADSL Settings	Configures ADSL settings	86
Services		
DNS		
DNS Server	Configures DNS server settings	89
IPv6 DNS	Configures IPv6 DNS server settings	89
Dynamic DNS	Configures DDNS settings	90
Access Control List		
ACL Config	Configures ACLs for LAN or WAN interfaces	92
IP/Port Filtering	Configures IP filtering settings	95
NAT/NAPT		
Virtual Server	Configures the virtual server forwarding table	97
NAT Exclude IP	Configures excluded IPs on the WAN interface	99
NAT Forwarding	Configures forwarding for access to local servers	99
NAT ALG and Pass-Through	Configures NAT passthrough for specific application protocols	100
NAT Port Trigger	Restricts Internet access for specific ports	101

Table 2: Configuration Menu (Continued)

Menu	Description	Page
FTP ALG Configuration	Configures FTP server and client ports	102
NAT IP Mapping	Configures IP address mapping for NAT	102
IP QoS	Configures IP-based QoS settings	103
MAC Filtering	Configures MAC address filtering	105
DMZ	Configures DMZ settings	106
URL Block	Sets URL key words to block	107
Software Forbidden	Blocks Internet access for specific software	108
DoS Setting	Configures denial-of-service settings	109
IGMP Proxy	Configures IGMP Proxy settings for multicast traffic	111
RIP	Configures Routing Information Protocol settings	113
ARP Binding	Configures Address Resolution Protocol binding	114
Advance		
Bridge Setting	Configures aging time and Spanning Tree settings	116
Log Setting	Configures system log settings	117
Routing	Configures static routing	118
UPnP	Enables UPnP for the WAN interface	120
SNMP	Configures SNMP settings	121
System Time	Configures NTP time server settings	122
Others	Configures Half Bridge settings	123
Port Mapping	Maps LAN ports to WAN interfaces	124
Diagnostic		
Diag-Test	Runs diagnostic tests for the ADSL link	126
Ping	Sends Ping echo requests to other devices	127
Ping6	Sends IPv6 Ping echo requests to other devices	127
Traceroute	Checks routes to other devices	128
ADSL	Runs ADSL diagnostic tone tests	130
Admin		
Commit/Reboot	Reboots the unit and/or restores factory defaults	133
Backup/Restore	Backs up or restores configuration settings	134
Password Setup	Changes the web access passwords	135
Upgrade Firmware	Upgrades the unit’s software version	136
Configure TR-069	Configures parameters for establishing a connection between the router and an auto-configuration server	137

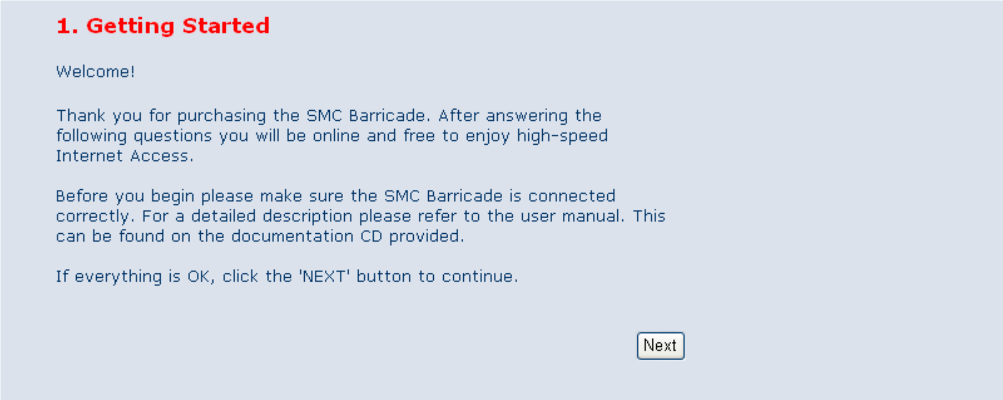
SETUP WIZARD

The Wizard is designed to help you configure the basic settings required to get the ADSL Gateway Router up and running. Click "Wizard" in the main menu to get started.

STEP 1 - GETTING STARTED

After reading the wizard welcome message, click Next to continue.

Figure 7: Wizard Step 1 - Getting Started



1. Getting Started

Welcome!

Thank you for purchasing the SMC Barricade. After answering the following questions you will be online and free to enjoy high-speed Internet Access.

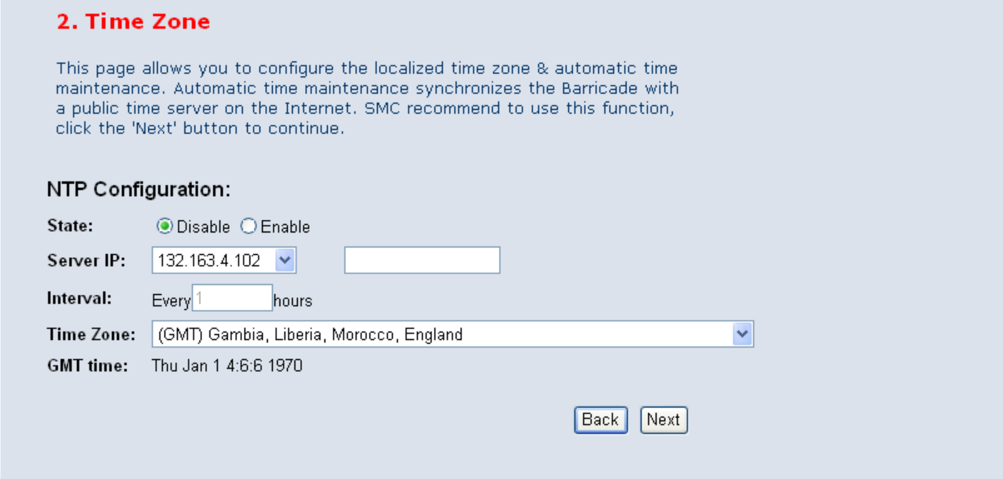
Before you begin please make sure the SMC Barricade is connected correctly. For a detailed description please refer to the user manual. This can be found on the documentation CD provided.

If everything is OK, click the 'NEXT' button to continue.

STEP 2 - TIME ZONE

Configure a Network Time Protocol (NTP) server to poll for time updates. To synchronize the router with an NTP server, specify the IP address of a public time server, select your local time zone, and click Next.

Figure 8: Wizard Step 2 - Time Zone Configuration



2. Time Zone

This page allows you to configure the localized time zone & automatic time maintenance. Automatic time maintenance synchronizes the Barricade with a public time server on the Internet. SMC recommend to use this function, click the 'Next' button to continue.

NTP Configuration:

State: ● Disable ○ Enable

Server IP: 132.163.4.102

Interval: Every 1 hours

Time Zone: (GMT) Gambia, Liberia, Morocco, England

GMT time: Thu Jan 1 4:6:6 1970

The following items are displayed on this page:

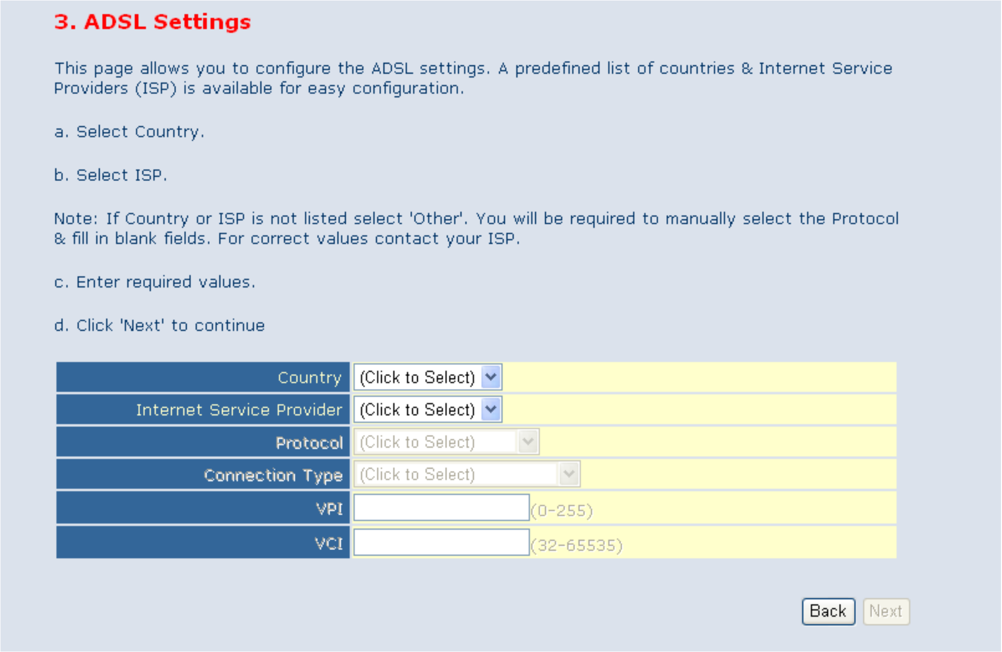
- **Status** – Enables or disables time synchronization with external servers.

- **Server IP** – Specifies the IP address of a public NTP time server on the Internet.
- **Interval** – Specifies the time interval for polling the NTP server.
- **Time Zone** – A drop-down box provides access to predefined time zones. Each choice indicates it’s offset from GMT and lists at least one major city or commonly known zone name covered by the time zone.

STEP 3 - ADSL SETTINGS

The third page of the wizard configures the ADSL country settings, Internet service provider, protocol, connection type and username and password.

Figure 9: Wizard Step 3 - ADSL Settings



3. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	(Click to Select)
Internet Service Provider	(Click to Select)
Protocol	(Click to Select)
Connection Type	(Click to Select)
VPI	(0-255)
VCI	(32-65535)

The following items are displayed on the first page of the Wizard:

- **Country** — Choose your country of operation from the drop down menu. If your country is not listed, contact your service provider for detailed settings.
- **Internet Service Provider** — The chosen country will determine the list of available Internet Service Providers. Choose the service provider with which you have a contract.
- **Protocol** — The protocol used will be specified by your service provider. Choose from the following options:
  - **PPPoE** — Point-to-Point Protocol over Ethernet (PPPoE).
  - **PPPoA** — Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA).

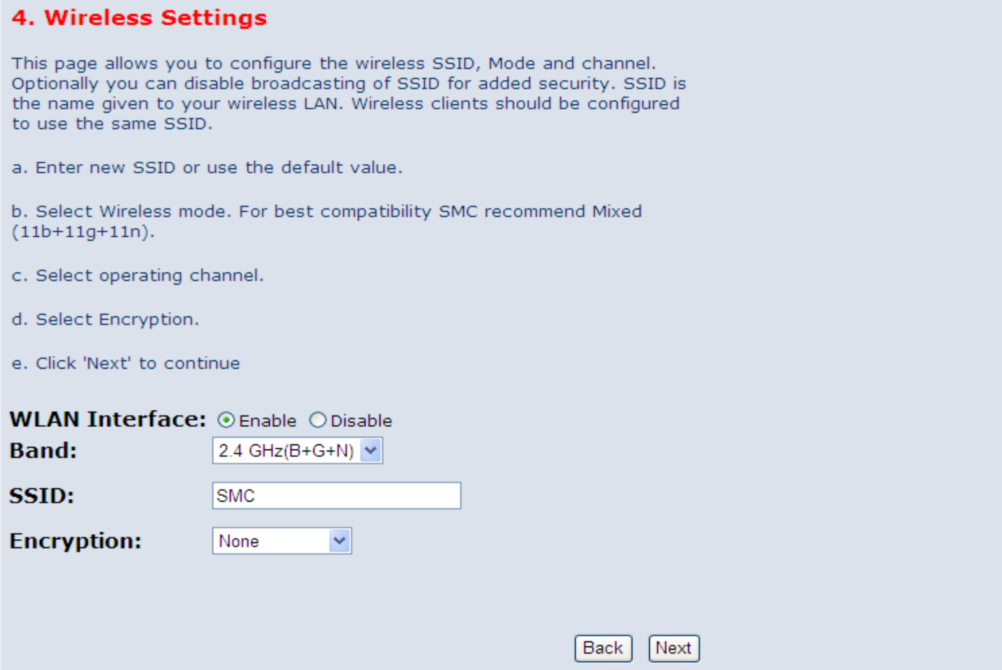
  - **1483 MER : DHCP** — 1483 MER is an RFC standard MAC Encapsulated Routing protocol.
  - **1483 MER : Static IP** — 1483 MER is an RFC standard MAC Encapsulated Routing protocol.
  - **1483 Bridged** — The Bridged RFC 1483 Encapsulated Traffic over ATM feature allows you to send bridged RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs).
  - **1483 Routed** — Allows you to send routed RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs).
  - **IPoA** — Dynamic IP over ATM (IPoA).

- **Connection Type** — Your connection type will also be specified by your service provider. Choose from the following options:
  - **VC-Mux** — Virtual circuit multiplexing (VC-Mux).
  - **LLC** — Logical Link Control (LLC).
- **VPI** — The ATM Virtual Path Identifier. (Range: 0-255)
- **VCI** — The ATM Virtual Channel Identifier. (Range: 32-65535)
- **Username** — Enter the username provided by your service provider.
- **Password** — Enter the password provided by your service provider.
- **Confirm Password** — Re-enter your password.

STEP 4 - WIRELESS SETTINGS

The fourth page of the wizard configures wireless settings for the ADSL router.

Figure 10: Wizard Step 4 - Wireless Settings



4. Wireless Settings

This page allows you to configure the wireless SSID, Mode and channel. Optionally you can disable broadcasting of SSID for added security. SSID is the name given to your wireless LAN. Wireless clients should be configured to use the same SSID.

a. Enter new SSID or use the default value.

b. Select Wireless mode. For best compatibility SMC recommend Mixed (11b+11g+11n).

c. Select operating channel.

d. Select Encryption.

e. Click 'Next' to continue

WLAN Interface: ● Enable ○ Disable

Band: 2.4 GHz(B+G+N)

SSID: SMC

Encryption: None

The following items are displayed on the first page of the Wizard:

- **WLAN Interface** — Enables/disables the wireless 802.11b/g/n interface.
- **Band** — Selects the operating band and mode. The router supports the 2.4 GHz band and can operate in any combination of 802.11b, g, or n modes.
- **SSID** — Specifies an SSID (service set identifier) which must be the same as that on all wireless clients that wish to associate with the unit.
- **Encryption** — Specifies the security used to protect your wireless network. (Default: None)
  - **None:** Allows any wireless client within range to associate with the ADSL/Router.
  - **WEP:** Provides a basic level of security using static shared keys that are distributed to all clients. Be sure to configure at least one static key. Alternatively, enable 802.1X authentication to dynamically create and distribute keys from a RADIUS server.
  - **WPA(TKIP/AES):** Wi-Fi Protected Access (WPA) using either a static pre-shared key, or 802.1X authentication through a RADIUS server. The encryption used is either TKIP or AES.

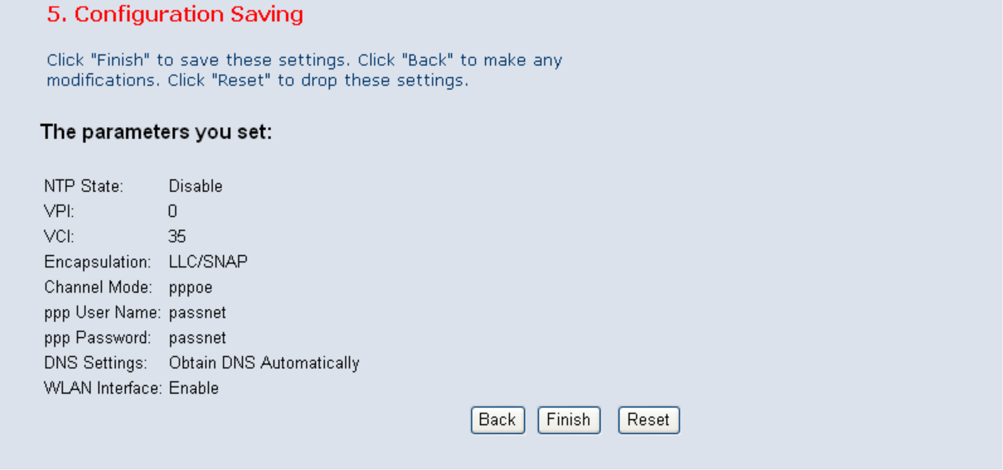
- **WPA2(TKIP/AES):** WPA2 using either a static pre-shared key, or 802.1X authentication through a RADIUS server. The encryption used is either TKIP or AES.

- **WPA2 Mixed:** WPA and WPA2 using either a static pre-shared key, or 802.1X authentication through a RADIUS server. Either TKIP or AES encryption is used depending on the client.

STEP 4 - CONFIGURATION SAVING

The final step in the setup wizard saves the configuration changes. Click Finish to complete the wizard, then click Save.

Figure 11: Wizard Step 3 - Configuration Saving



5. Configuration Saving

Click "Finish" to save these settings. Click "Back" to make any modifications. Click "Reset" to drop these settings.

The parameters you set:

NTP State:	Disable
VPI:	0
VCI:	35
Encapsulation:	LLC/SNAP
Channel Mode:	pppoe
ppp User Name:	passnet
ppp Password:	passnet
DNS Settings:	Obtain DNS Automatically
WLAN Interface:	Enable

4 Device Information

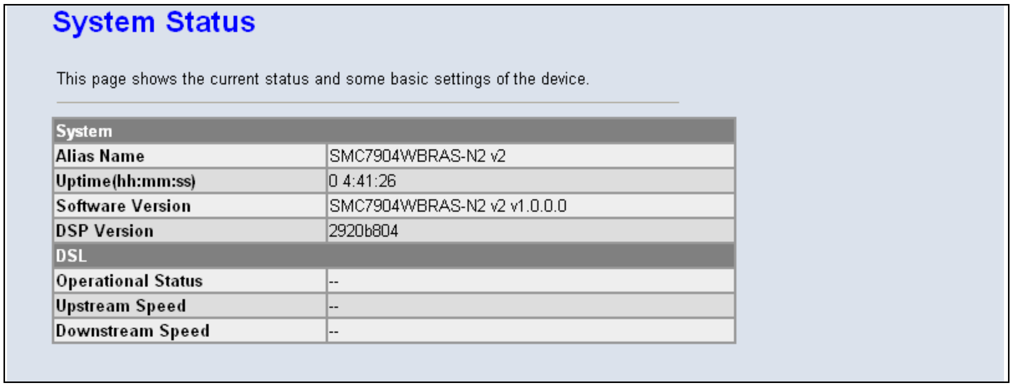
The Status pages display information on hardware/software versions, LAN and WAN connection status, statistics, and the ARP table.

System Status

The System Status page displays the hardware and software versions, and the WAN connection status and speed.

Click Status, System.

Figure 12: System Status



System Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	SMC7904WBRAS-N2 v2
Uptime(hh:mm:ss)	0 4:41:26
Software Version	SMC7904WBRAS-N2 v2 v1.0.0.0
DSP Version	2920b804
DSL	
Operational Status	--
Upstream Speed	--
Downstream Speed	--

The following items are displayed on this page:

System:

- **Alias Name** – An alias for the ADSL Router, enabling the device to be uniquely identified on the network.

- **Uptime** – The length of time in minutes that the unit has been powered on.

- **Software Version** – The current version of firmware running on the unit.

- **DSP Version** – The current hardware version of the digital signal processor (DSP).

DSL:

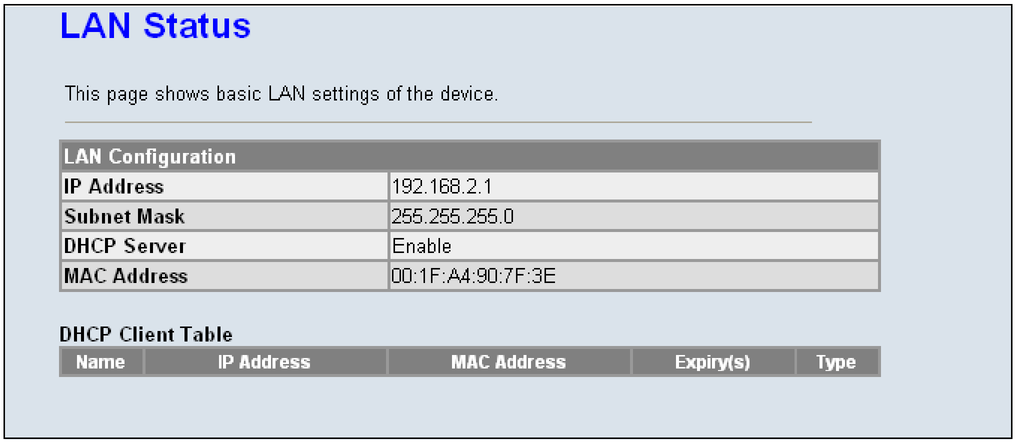
- **Operational Status** – Displays the status of the DSL connection.

- **Upstream Speed** – The current upload speed of the DSL connection.
- **Downstream Speed** – The current download speed of the DSL connection.

LAN STATUS

The ADSL Router LAN window displays basic LAN port settings including DHCP information.

Figure 13: Status - LAN



LAN Status

This page shows basic LAN settings of the device.

LAN Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:1F:A4:90:7F:3E

DHCP Client Table

Name	IP Address	MAC Address	Expiry(s)	Type

The following items are displayed on this page:

LAN STATUS

Displays the basic information of the LAN port.

- **IP Address** — Displays an IP address for local area connection to the ADSL Router.
- **Subnet Mask** — Displays the local subnet mask.
- **DHCP Server** — Displays whether the DHCP server has been enabled or not.
- **MAC Address** — Displays the physical layer address of the LAN port.

DHCP CLIENT TABLE

Displays information on the DHCP configuration and lease time.

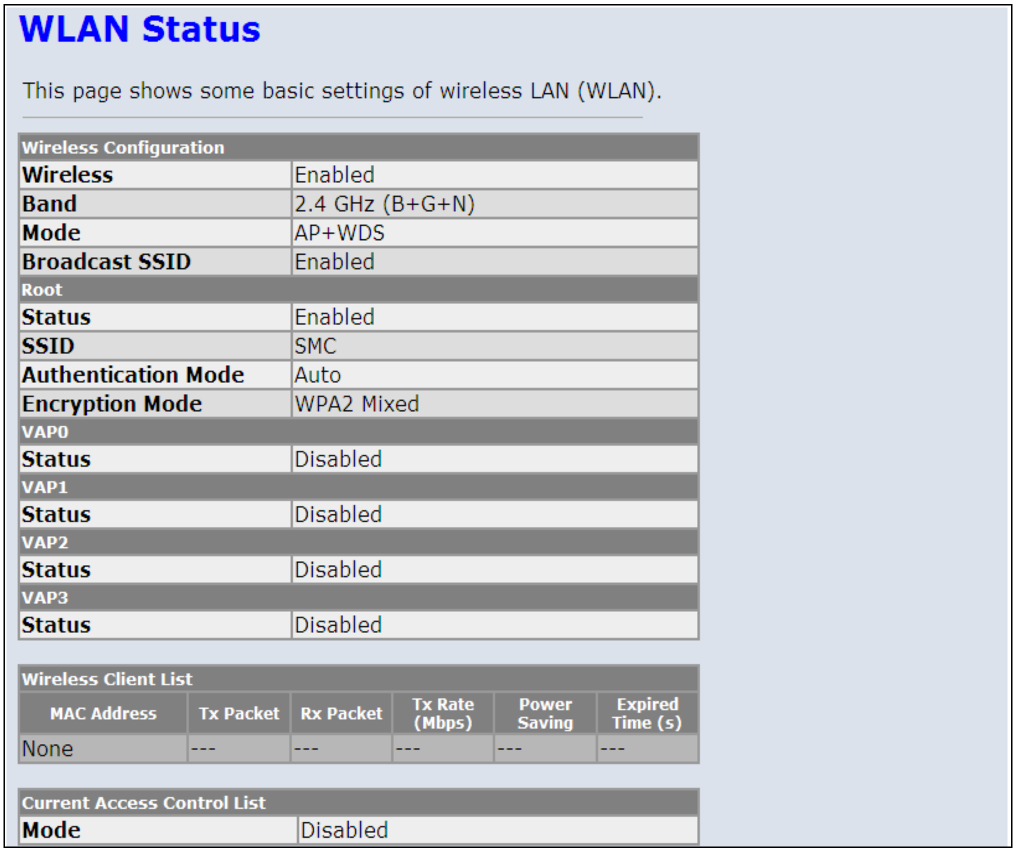
- **Name** — Displays the name of the client device.
- **IP Address** — Displays the DHCP Client IP address.
- **MAC Address** — Displays the physical layer address of the DHCP Client.

- **Expiry(s)** — Displays the duration of the lease time.
- **Type** — Indicates if the entry is dynamic or static.

WLAN STATUS

The WLAN Status window displays basic wireless interface settings.

Figure 14: Status - WLAN



WLAN Status

This page shows some basic settings of wireless LAN (WLAN).

Wireless Configuration	
Wireless	Enabled
Band	2.4 GHz (B+G+N)
Mode	AP+WDS
Broadcast SSID	Enabled
Root	
Status	Enabled
SSID	SMC
Authentication Mode	Auto
Encryption Mode	WPA2 Mixed
VAP0	
Status	Disabled
VAP1	
Status	Disabled
VAP2	
Status	Disabled
VAP3	
Status	Disabled

Wireless Client List

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Current Access Control List	
Mode	Disabled

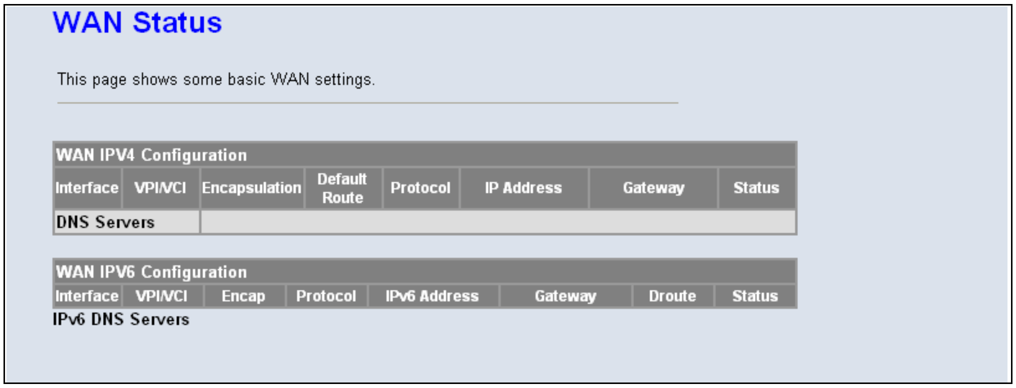
The following items are displayed on this page:

- **Wireless Configuration** — Indicates wireless interfaces that are enabled. The router supports four multiple SSID interfaces: Root, and VAP0-VAP3.
- **Wireless Client List** — Lists all wireless clients associated to the router.
- **Wireless Access Control List** — Displays current wireless access control list settings.

WAN STATUS

The ADSL Router WAN window displays basic IPv4 and IPv6 WAN port settings.

Figure 15: Status - WAN



WAN Status

This page shows some basic WAN settings.

WAN IPV4 Configuration							
Interface	VPI/VCI	Encapsulation	Default Route	Protocol	IP Address	Gateway	Status
DNS Servers							

WAN IPV6 Configuration							
Interface	VPI/VCI	Encap	Protocol	IPv6 Address	Gateway	Droute	Status

IPv6 DNS Servers

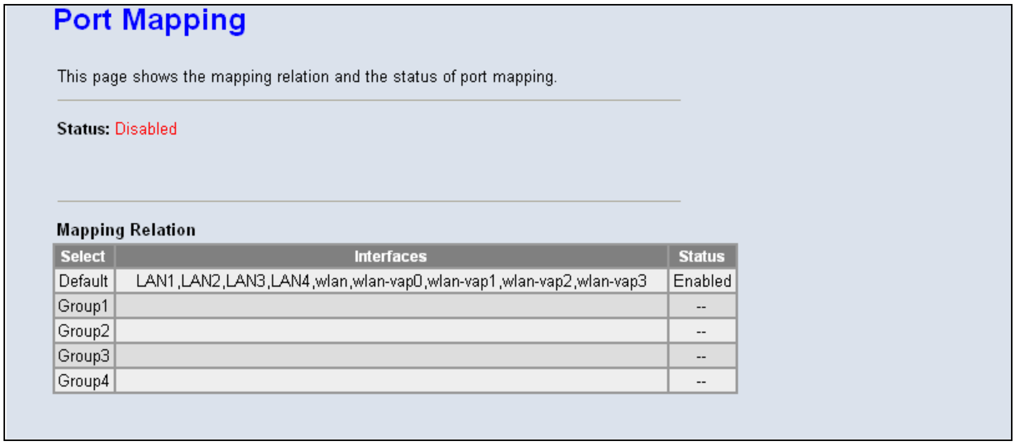
The following items are displayed on this page:

- **Interface** — Displays the interface identifier.
- **VPI/VCI** — Displays the ATM channel identifiers.
- **Encapsulation** — Displays the encapsulation type chosen, either LLC to VX-Mux.
- **Default Route** — Dipslays if a default route has been enabled.
- **Protocol** — Displays the protocol used for transmission of data packets
- **IP Address** — Displays the local IP address of the WAN port.
- **Default Gateway** — Displays the network route, or gateway used by the unit when no other known route exists for a given IP packet's destination address.
- **Status** — Specifies the status of the interface.
- **DNS Servers** — Specifies the IP addresses of DNS servers.

PORT MAPPING

The Port Mapping status shows the mapping of WAN and LAN interfaces to specific groups.

Figure 16: Status - Port Mapping



Port Mapping

This page shows the mapping relation and the status of port mapping.

Status: Disabled

Mapping Relation

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3	Enabled
Group1		--
Group2		--
Group3		--
Group4		--

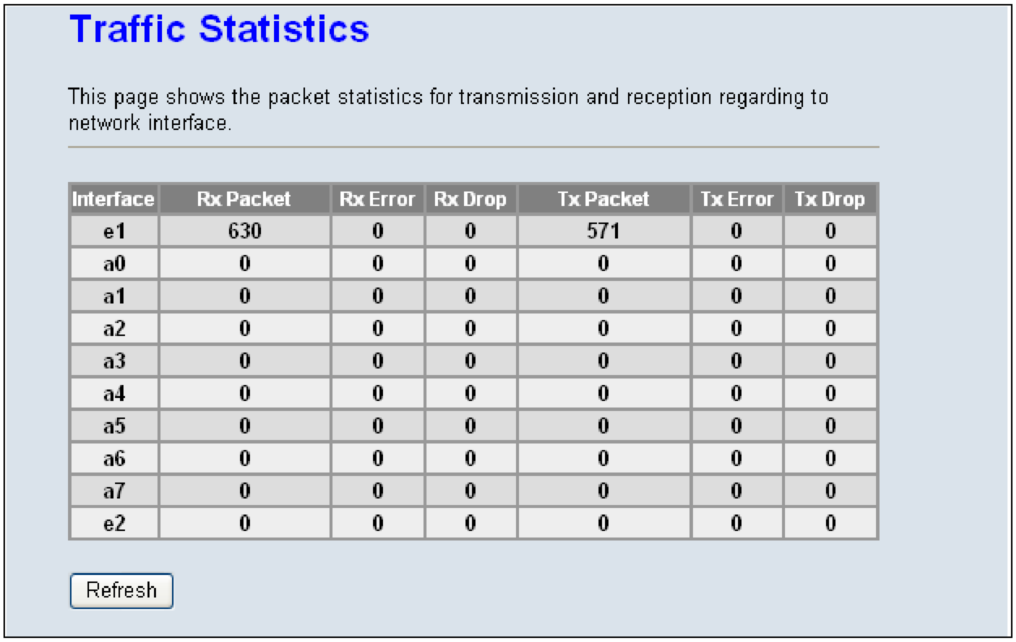
The following items are displayed on this page:

- **Status** — Indicates if port mapping is enabled or disabled.
- **Select** — Indicates the group identification.
- **Interfaces** — Specifies the WAN and LAN interfaces in the group.
- **Status** — Indicates if the group mapping is enabled.

TRAFFIC STATISTICS

The ADSL Router Traffic Statistics - Interfaces window displays received and transmitted packet statistics for all interfaces on the ADSL Router.

Figure 17: Status - Traffic Statistics



Traffic Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx Packet	Rx Error	Rx Drop	Tx Packet	Tx Error	Tx Drop
e1	630	0	0	571	0	0
a0	0	0	0	0	0	0
a1	0	0	0	0	0	0
a2	0	0	0	0	0	0
a3	0	0	0	0	0	0
a4	0	0	0	0	0	0
a5	0	0	0	0	0	0
a6	0	0	0	0	0	0
a7	0	0	0	0	0	0
e2	0	0	0	0	0	0

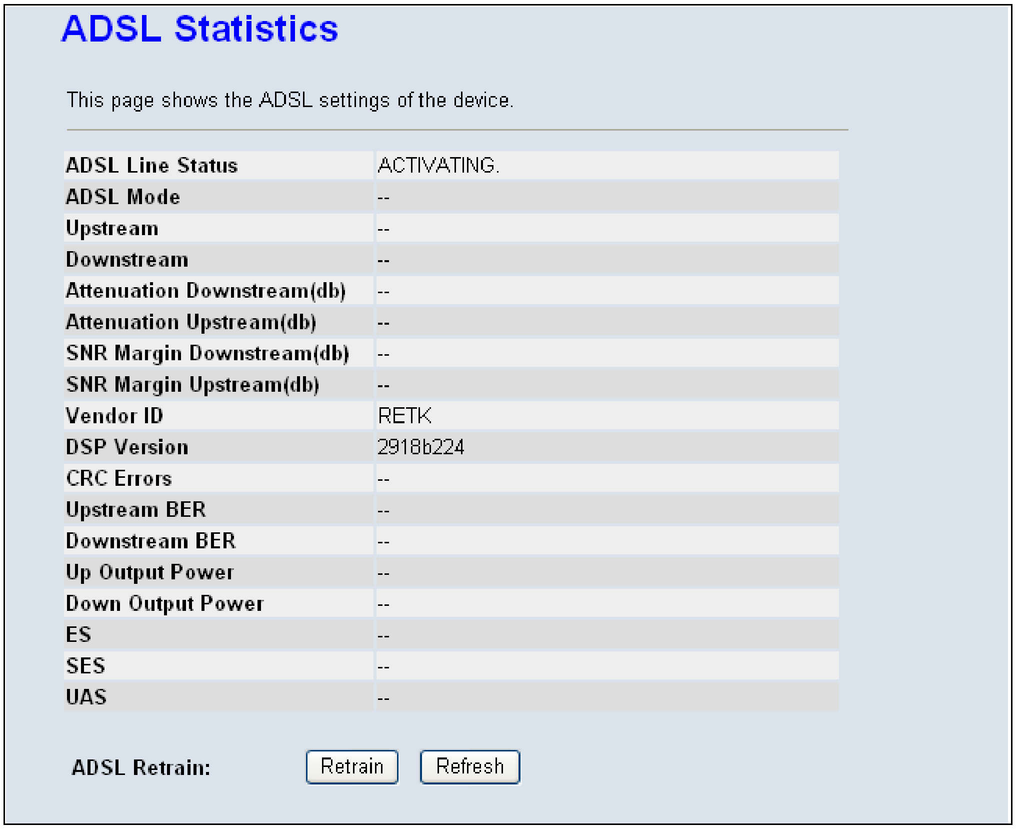
The following items are displayed on this page:

- **Interface** — Displays the interface on which traffic is being monitored.
- **Rx Packet** — Displays the total number of packets received by the specified interface.
- **Rx Error** — Displays the total number of packet errors received by the specified interface, if any.
- **Rx Drop** — Displays the total number of received packets dropped by the specified interface.
- **Tx Packet** — Displays the total number of packets transmitted by the specifed interface.
- **Tx Error** — Displays the total number of packet errors occured during transmission by the specified interface.
- **Tx Drop** — Displays the total number of packets transmitted but dropped by the specified interface.
- **Refresh** — Updates the statistical table for all interfaces.

DSL STATISTICS

The ADSL Router DSL Statistics window displays received and transmitted packet statistics for all interfaces on the ADSL Router.

Figure 18: Status - DSL Statistics



ADSL Statistics

This page shows the ADSL settings of the device.

ADSL Line Status	ACTIVATING.
ADSL Mode	--
Upstream	--
Downstream	--
Attenuation Downstream(db)	--
Attenuation Upstream(db)	--
SNR Margin Downstream(db)	--
SNR Margin Upstream(db)	--
Vendor ID	RETK
DSP Version	2918b224
CRC Errors	--
Upstream BER	--
Downstream BER	--
Up Output Power	--
Down Output Power	--
ES	--
SES	--
UAS	--

The following items are displayed on this page:

- **ADSL Status** — Displays the ADSL connection status (“activating”, “up” or null).
- **ADSL Mode** — Displays the connection mode for the ADSL Router, which is fixed at ADSL2+.
- **Upstream** — Displays the actual payload carried on the upstream channels.
- **Downstream** — Displays the actual payload carried on the downstream channels.
- **Attentuation Downstream/Upstream (db)** — Displays the amount of attenuation in signal strength due to conductive losses in transmission medium. Attenuation affects the propagation of waves and signals in electrical circuits, expressed in decibels (dB).

- **SNR Margin Downstream/Upstream (db)** — Displays the current signal-to-noise margin expressed in decibels (dB). SNR is the ratio of signal power to the noise power corrupting the signal.

- **Vendor ID** – The vendor name of the digital signal processor (DSP).

- **DSP Version** – The current hardware version of the digital signal processor (DSP).

- **CRC Errors** — Displays the CRC (cyclic redunancy check) - a type of function that takes as input a data stream of any length, and produces as output a value of a certain space, commonly a 32-bit integer.

- **Upstream/Downstream BER** – The the rate at which bits in the data stream that have been altered by noise.

- **Up/Down Output Power** — Displays the upstream/downstream power level employed for ADSL port filtering.

- **ES** — Displays the total error seconds, the number of second intervals during which there was one or more CRC anomalies, or one or more Loss of Signal (LOS) or Loss of Framing (LOF) defects.

- **SES** — Displays the total severly errored seconds. The number of second intervals containing 18 or more CRC-8 anomalies, one or more Loss of Signal (LOS) defects, one or more Severely Errored Frame (SEF) defects, or one or more Loss of Power (LPR) defects.

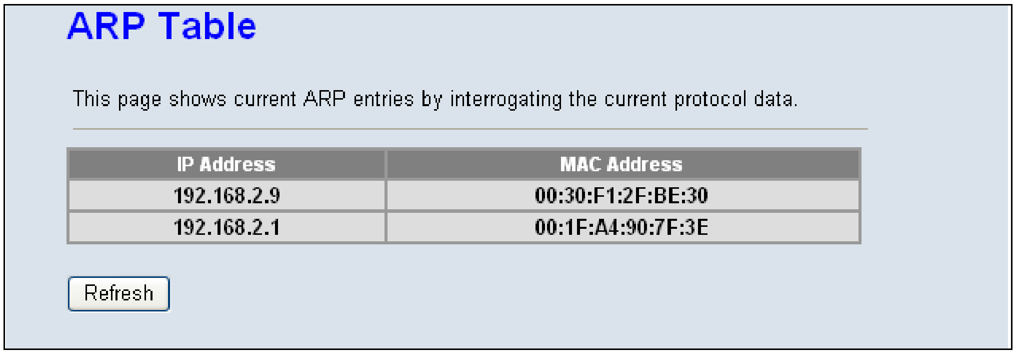
- **UAS** — Displays the total unavailable errored seconds, the number of seconds during which the ADSL transceiver is powered up but not available.

- **ADSL Retrain** — Retrains the DSL line.

ARP TABLE

The ARP page displays IP address to MAC address mapping entries determined by the Address Resolution Protocol.

Figure 19: Status - ARP Table



ARP Table

This page shows current ARP entries by interrogating the current protocol data.

IP Address	MAC Address
192.168.2.9	00:30:F1:2F:BE:30
192.168.2.1	00:1F:A4:90:7F:3E

The following items are displayed on this page:

- **IP Address** — IP address of a local entry in the cache.
- **MAC Address** — MAC address mapped to the corresponding IP address.
- **Refresh** — Sends a request to update the current parameters.

5 WLAN Configuration

This chapter describes wireless configuration on the ADSL Router. The unit contains an onboard IEEE 802.11b/g/n access point (AP), which provides wireless data communications between the router and wireless devices.

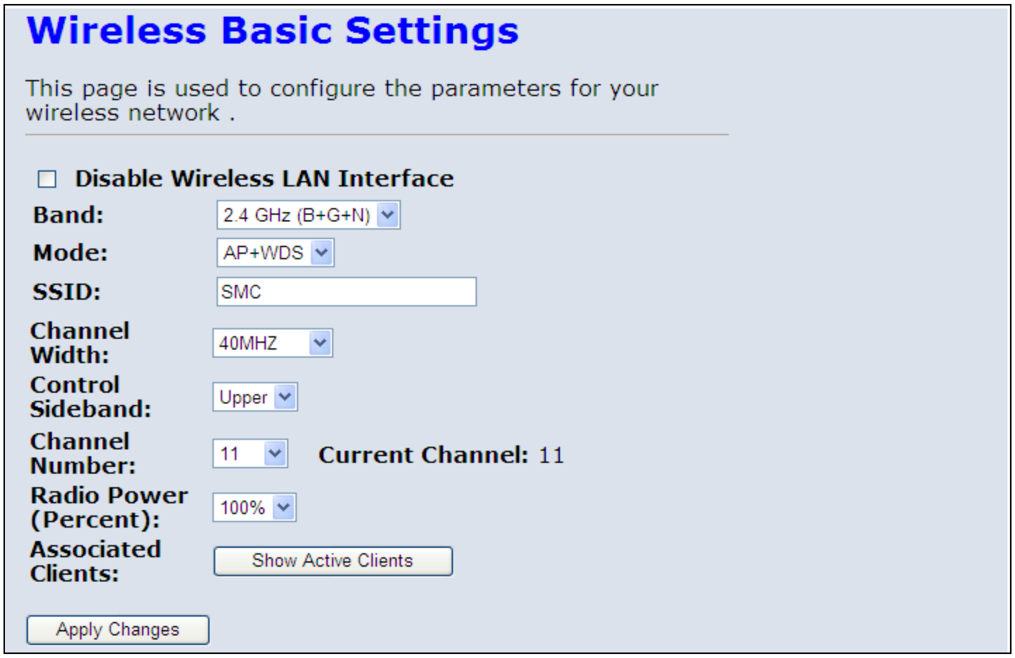
WLAN Configuration contains the following sections:

WLAN BASIC SETTINGS

The unit's access point can function in one of three modes, mixed 802.11b/g, 802.11b only, or 802.11g only. Also note that 802.11g is backward compatible with 802.11b at slower data rates.

Note that the unit supports two virtual access point (VAP) interfaces.

Figure 20: WLAN Basic Settings



Wireless Basic Settings

This page is used to configure the parameters for your wireless network .

☐ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G+N)

Mode: AP+WDS

SSID: SMC

Channel Width: 40MHZ

Control Sideband: Upper

Channel Number: 11 **Current Channel:** 11

Radio Power (Percent): 100%

Associated Clients:

The following items are displayed on this page:

- **Disable Wireless LAN Interface** — Disables the Wireless LAN interface. (Default: Enabled)
- **Band** — Defines the radio mode. (Default: 2.4Ghz (B+G))
- **Mode** — The unit can function as an access point alone, allowing connection to wireless clients, or both access point and WDS (wireless distribution system), allowing WDS transparent bridging between APs. (Default: AP+WDS)
- **SSID** — The service set identifyer for the access point. (Default: SMC)
- **Channel Width** — The router provides a channel bandwidth of 40 MHz by default giving an 802.11g connection speed of 108 Mbps (sometimes referred to as Turbo Mode) and a 802.11n connection speed of up to 150 Mbps. Setting the HT Channel Bandwidth to 20 MHz slows connection speed for 802.11g and 802.11n to 54 Mbps and 74

Mbps respectively and ensures backward compliance for slower 802.11b devices. (Default: 40MHz)

- **Control Sideband** — Specifies if the extension channel should be in the Upper or Lower sideband. When a 40MHz channel bandwidth has been set, the extension channel option will be enabled in the upper or lower sideband. The extension channel allows you to get extra bandwidth.

- **Channel Number** — The radio channel that the ADSL Router uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the ADSL Router to which it is linked. (Default: Auto; Range: 1~11)

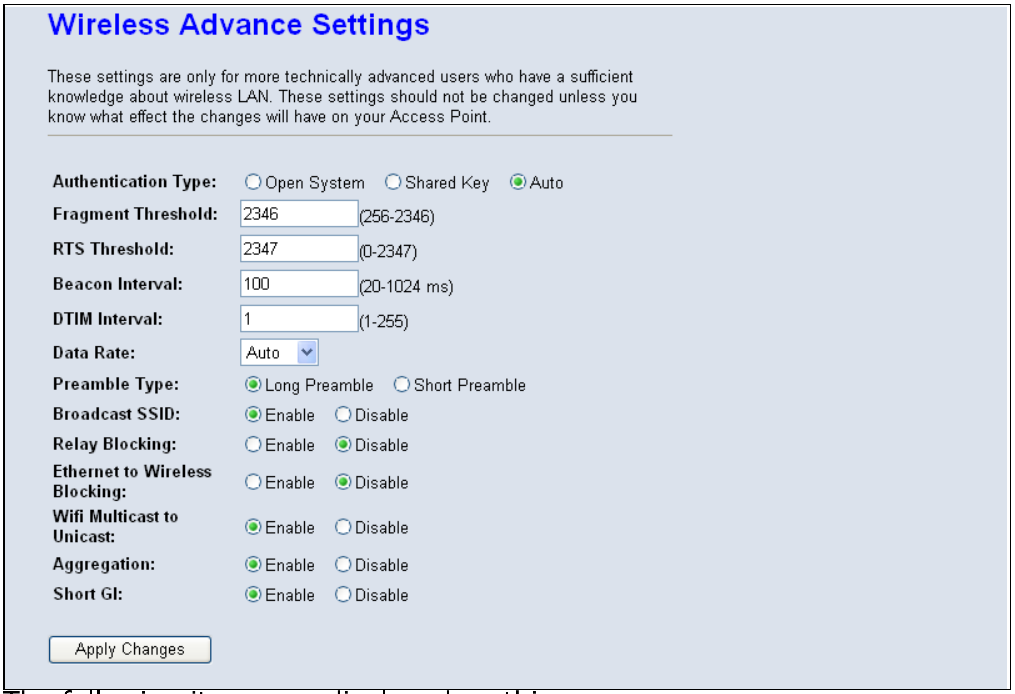
- **Radio Power (percent)** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Default: 100%; Range: 100%, 80%, 50%, 25%, 10%)

- **Associated Clients** — Opens a window that displays information on current connected wireless clients.

ADVANCED SETTINGS

The advanced radio configuration settings are described in the page that follows.

Figure 21: Wireless Security Setup - Advanced Settings



Wireless Advance Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Ethernet to Wireless Blocking:	○ Enable ● Disable
Wifi Multicast to Unicast:	● Enable ○ Disable
Aggregation:	● Enable ○ Disable
Short GI:	● Enable ○ Disable

The following items are displayed on this page:

- **Authentication Type** — Sets the basic authentication method.

- **Fragment Threshold** — Configures the minimum packet size that can be fragmented when passing through the wireless interface. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)

- **RTS Threshold** — Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The wireless interface sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the wireless interface. The beacon signals allow wireless clients to maintain contact with the ADSL Router. They may also carry power-management information. (Range: 20-1000 TUs; Default: 100 TUs)

- **DTIM Interval** — The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

  Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of one beacon indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 1 beacon)

- **Data Rate** — The maximum data rate at which the wireless interface transmits multicast and broadcast packets. (Options: Auto, 1, 2, 5.5, 11, 6, 9, 18, 24, 36, 48, 54 Mbps; Default: Auto)

- **Preamble Type** — Sets the length of the signal preamble that is used at the start of a data transmission. (Default: Long)

  - **Long Preamble:** Sets the preamble to long (192 microseconds). Using a long preamble ensures the wireless interface can support all 802.11b and 802.11g clients.

  - **Short Preamble:** Sets the preamble according to the capability of clients that are currently asscociated. Uses a short preamble (96 microseconds) if all associated clients can support it, otherwise a long preamble is used. The wireless interface can increase data throughput when using a short preamble, but will only use a short preamble if it determines that all associated clients support it.

- **Broadcast SSID** — Enables/disables the wireless interface to broadcast an SSID (service set identifier) to uniquely identify it on the network.

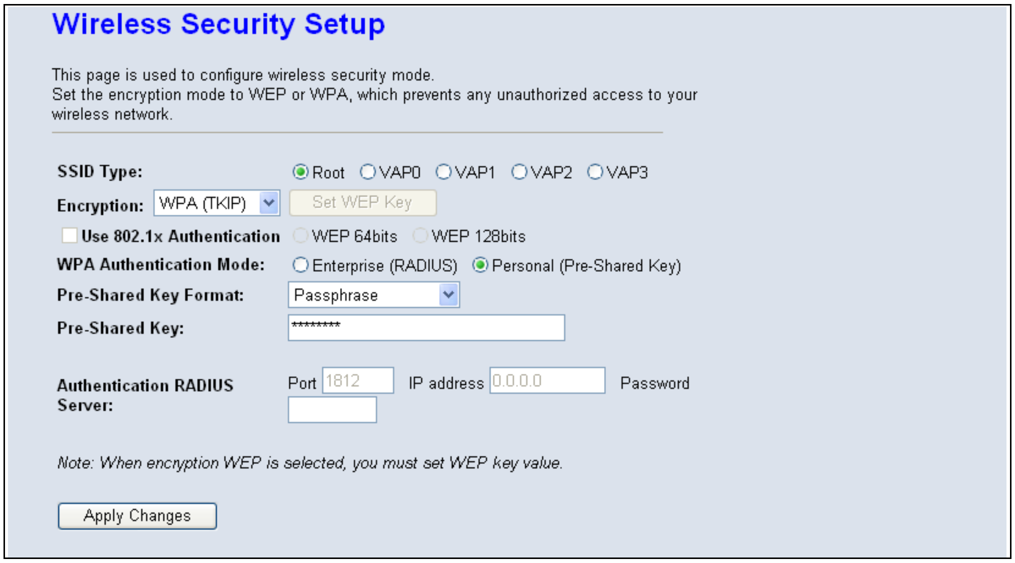
- **Aggregation** — This option enables Mac Service Data Unit (MSDU) aggregation. (Default: Enabled)

- **Short GI** — The guard interval between symbols helps receivers overcome the effects of multipath delays. You can enable a short interval to increase throughput. (Default: Enabled)

WIRELESS SECURITY SETUP

Describes the wireless security settings for each VAP, including association mode, encryption, and authentication.

Figure 22: Wireless Security Setup - None



Wireless Security Setup

This page is used to configure wireless security mode.
Set the encryption mode to WEP or WPA, which prevents any unauthorized access to your wireless network.

SSID Type: ● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3

Encryption: WPA (TKIP) [Set WEP Key]

□ **Use 802.1x Authentication** ○ WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

[Apply Changes]

COMMON WIRELESS PARAMETERS

The following items are displayed all pages of the Wireless Security Setup:

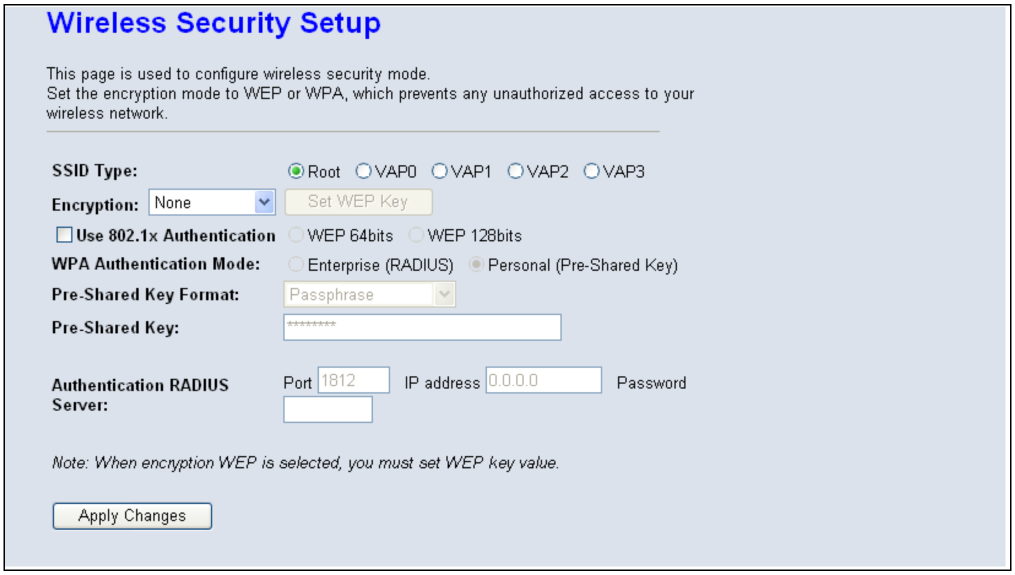
- **SSID TYPE** — Selects the VAP to apply security settings to. (Options: Root, VAP0-VAP3)
- **Encryption** — Selects the encryption type to deploy on the specified VAP. The options are:
  - **None:** No security.
  - **WEP:** WEP is used as the multicast encryption cipher. You should select WEP only when both WPA and WEP clients are supported.
  - **WPA(TKIP/AES):** WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. TKIP or AES is used as the multicast encryption cipher.
  - **WPA2(TKIP/AES):** WPA2 – WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X

and PSK modes of operation. TKIP or AES is used as the multicast encryption cipher.

- **WPA2(Mixed):** Clients using WPA or WPA2 are accepted for authentication. TKIP or AES is used as the multicast encryption cipher.

The following figures illustrate the various options available with each security setting:

Figure 23: Wireless Security Setup - None



Wireless Security Setup

This page is used to configure wireless security mode.
Set the encryption mode to WEP or WPA, which prevents any unauthorized access to your wireless network.

SSID Type: ● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3

Encryption: None | Set WEP Key

□ Use 802.1x Authentication ○ WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********

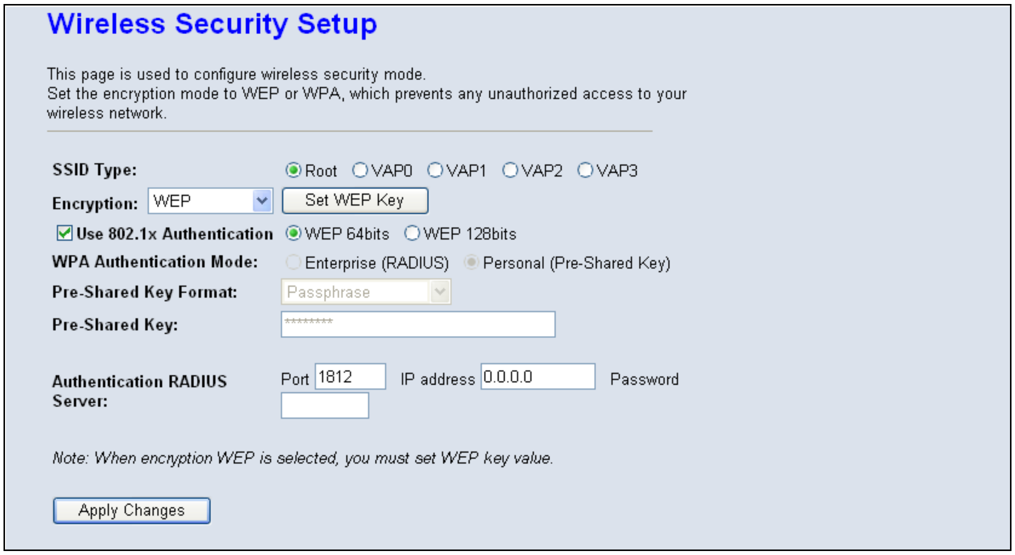
Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

WEP SECURITY

The following page describes the WEP security setup on the ADSL Router.

Figure 24: Wireless Security Setup - WEP



Wireless Security Setup

This page is used to configure wireless security mode.
Set the encryption mode to WEP or WPA, which prevents any unauthorized access to your wireless network.

SSID Type: ● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3

Encryption: WEP | Set WEP Key

☑ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

The following items are displayed on this page:

- **Set WEP Key** — Configures the WEP key setup. This is displayed in the screen below.
- **Use 802.1x Authentication** — Enables/disables 802.1x authentication. When enabled the above screen displays.
- **WEP 64bits/128bits** — Selects between 64 bit and 128 bit keys.

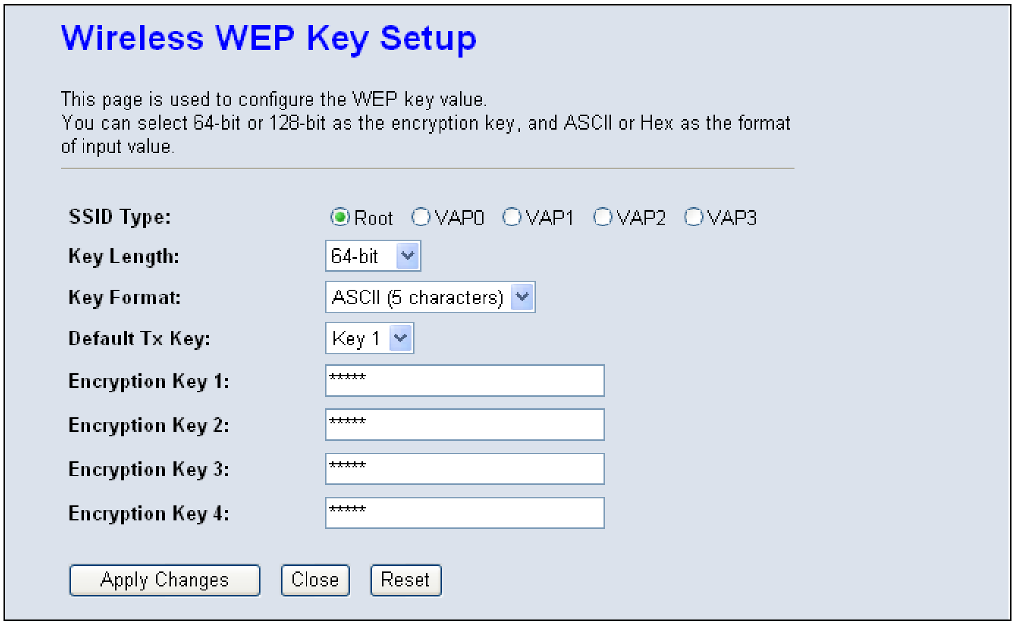
RADIUS SERVER

- **Port** — Specifies the port number used to communicate with the RADIUS server.
- **IP Address** — Specifies the IP address used to communicate with the RADIUS server.
- **Password** — Specifies the key necessary for RADIUS server authentication.

WEP KEY SETUP

The following page describes the WEP key setup.

Figure 25: Wireless Security Setup - WEP Key Setup



Wireless WEP Key Setup

This page is used to configure the WEP key value.
You can select 64-bit or 128-bit as the encryption key, and ASCII or Hex as the format of input value.

SSID Type:	● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3
Key Length:	64-bit
Key Format:	ASCII (5 characters)
Default Tx Key:	Key 1
Encryption Key 1:	*****
Encryption Key 2:	*****
Encryption Key 3:	*****
Encryption Key 4:	*****

The following items are displayed on this page:

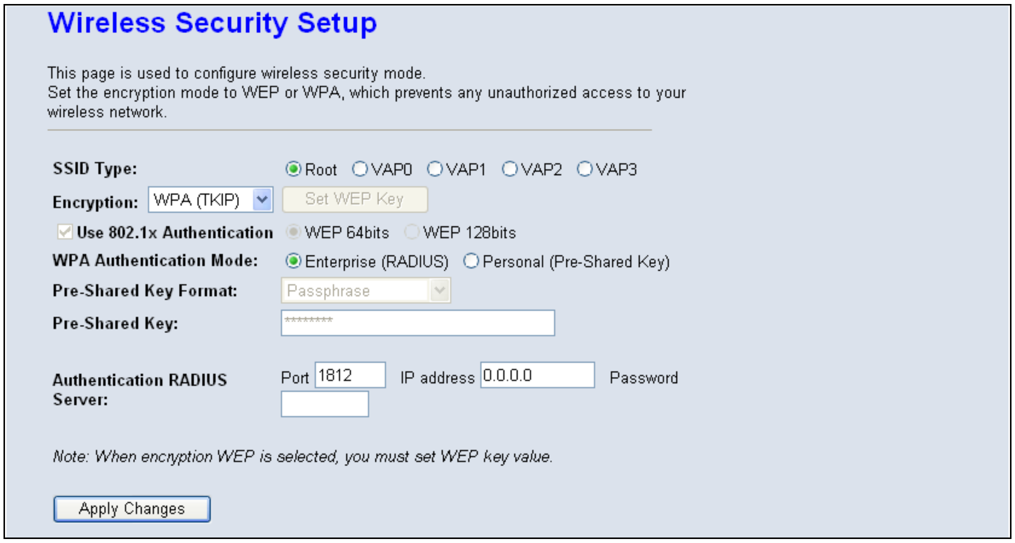
- **SSID Type** — Selects the VAP to configure the WEP security settings to.

- **Authentication Type** — Selects the authentication type to use. Options are:
  - **Open System:** If you don’t set up any other security mechanism on the access point, the network has no protection and is open to all users. This is the default setting.
  - **Shared Key:** Sets the access point to use WEP shared keys. If this option is selected, you must configure at least one key on the access point and all clients.
  - **Auto:** Automatically selects the best authentication type to use.
- **Key Length** — Selects between 64 bit and 128 bit keys.
- **Key Format** — Selects the preferred method of entering WEP encryption keys on the unit:
  - Alphanumeric: Enter keys as 5 alphanumeric characters for 64 bit keys, 13 alphanumeric characters for 128 bit keys. This is the default setting.
  - Hexadecimal: Enter keys as 10 hexadecimal digits (0-9 and A-F) for 64 bit keys, or 26 hexadecimal digits for 128 bit keys.
- **Default Tx Key** — Selects the default key used for transmission.
- **Encryption Key 1~4** — Specifies the user defined WEP keys.

WPA SECURITY

The following section describes WPA, WPA2 and WPA2-mixed settings.

Figure 26: Wireless Security Setup - WPA/WPA2 Setup



Wireless Security Setup

This page is used to configure wireless security mode.
Set the encryption mode to WEP or WPA, which prevents any unauthorized access to your wireless network.

SSID Type: ● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3

Encryption: WPA (TKIP) Set WEP Key

☑ Use 802.1x Authentication ● WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

The following items are displayed on this page:

- **WPA Authentication Mode** — Selects between modes of WPA authentication. Options are:
  - **Enterprise:** Uses a RADIUS server for authentication. This applies to enterprise deployment.
  - **Personal:** Uses a pre-shared key for authentication.

ENTERPRISE (RADIUS)

- **Port** — Specifies the port number used to communicate with the RADIUS server.
- **IP Address** — Specifies the IP address used to communicate with the RADIUS server.
- **Password** — Specifies the password necessary for access to RADIUS server authentication.

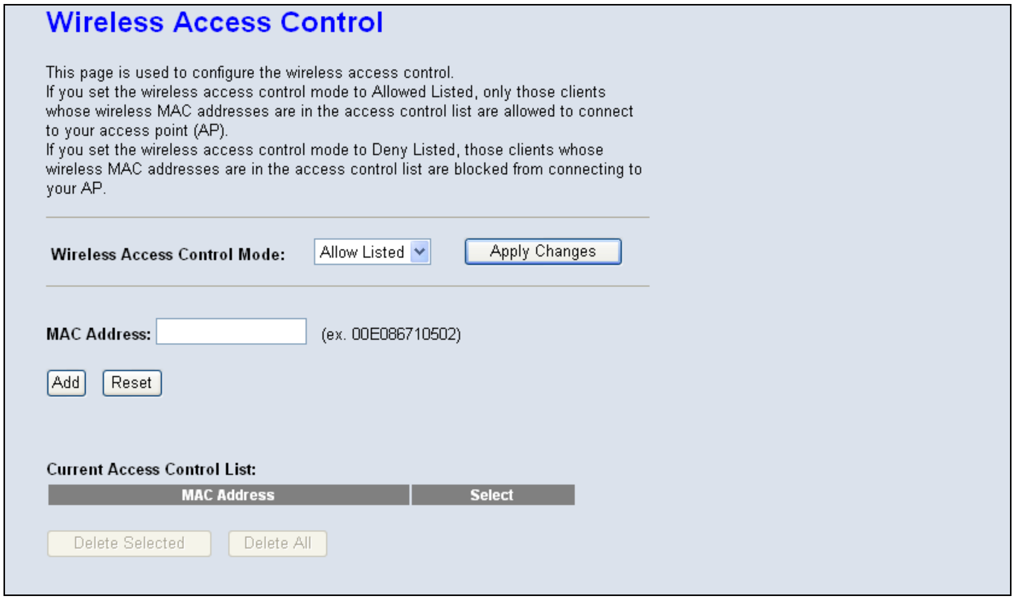
PERSONAL (PRE-SHARED KEY)

- **Pre-Shared Key Format** — Selects the format of the pre-shared key from the following options:
  - **Passphrase:** Enter a key as an easy-to-remember form of letters and numbers. The string must be from 8 to 63 characters, which can include spaces.
  - **Hexadecimal:** Enter a key as a string of 64 hexadecimal numbers.
- **Pre-Shared Key** — Enter the pre-shared key noting the type chosen.

ACCESS CONTROL

Access control configures ACLs (access control lists) which allow or deny wireless traffic based on the sender's MAC address.

Figure 27: Wireless Security Setup - Wireless Access Control



Wireless Access Control

This page is used to configure the wireless access control.
If you set the wireless access control mode to Allowed Listed, only those clients whose wireless MAC addresses are in the access control list are allowed to connect to your access point (AP).
If you set the wireless access control mode to Deny Listed, those clients whose wireless MAC addresses are in the access control list are blocked from connecting to your AP.

Wireless Access Control Mode: Allow Listed

MAC Address: (ex. 00E086710502)

Current Access Control List:

MAC Address	Select

The following items are displayed on this page:

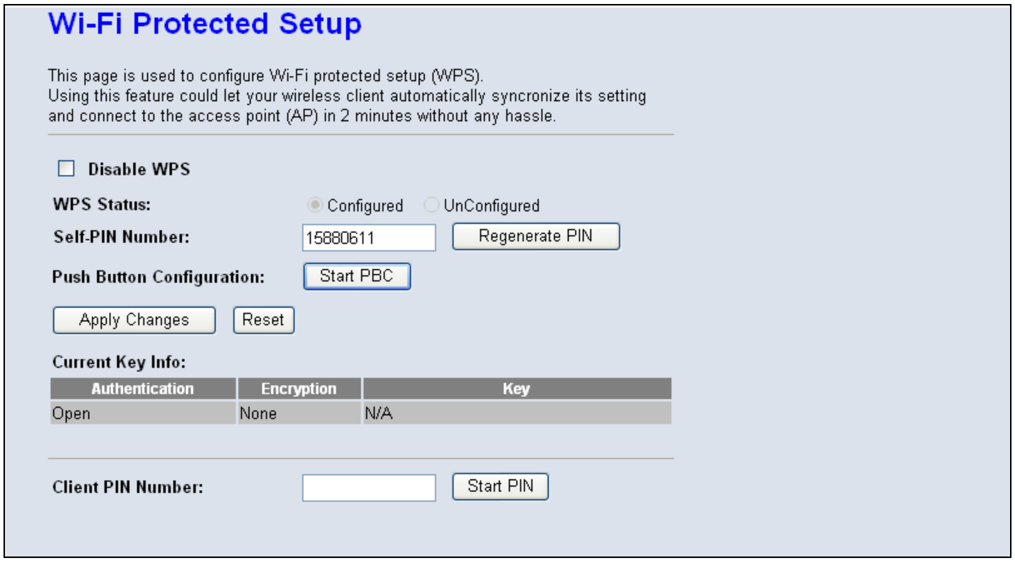
- **Wireless Access Control Mode** — Enables/disables ACLs on the ADSL Router. Options are:
  - **Disable:** Disables all ACLs.
  - **Allow Listed:** Configures an allowed list of MAC addresses. Those MAC addresses not in the allowed list will not be allowed to connect to the wireless interface.
  - **Deny Listed:** Configures a denied list of MAC addresses. The MAC addresses specified will not be allowed to connect to the wireless interface.
- **MAC Address** — The specified MAC address in the ACL Allowed or Denied list.
- **Select** — Selects a MAC address from the list.
- **Delete Selected** — Deletes a selected MAC address.
- **Delete All** — Deletes all entries from the ACL table.

WI-FI PROTECTED SETUP (WPS)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the router can be pressed at any time to allow a single device to easily join the network.

The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button.

Figure 28: WPS Configuration



Wi-Fi Protected Setup

This page is used to configure Wi-Fi protected setup (WPS).
Using this feature could let your wireless client automatically syncronize its setting and connect to the access point (AP) in 2 minutes without any hassle.

□ Disable WPS

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 15880611

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

The following items are displayed on this page:

- **Disable WPS** — Disables WPS configuration. (Default: Disabled)
- **WPS Status** — Displays if there is currently any WPS traffic connecting to the router.
- **Self PIN Number** — Displays the PIN Code for the router. The default is exclusive for each unit.
- **Regenerate PIN** — Click the button to generate a new PIN number that is used by the router.
- **Push Button Configuration** — The "Start PBC" button has the same effect as pressing the physical WPS button that is located on the rear of the router. After clicking on the button you have up to two minutes to activate WPS on a device that needs to join the network.
- **Apply Changes** — Applies the current WPS settings.

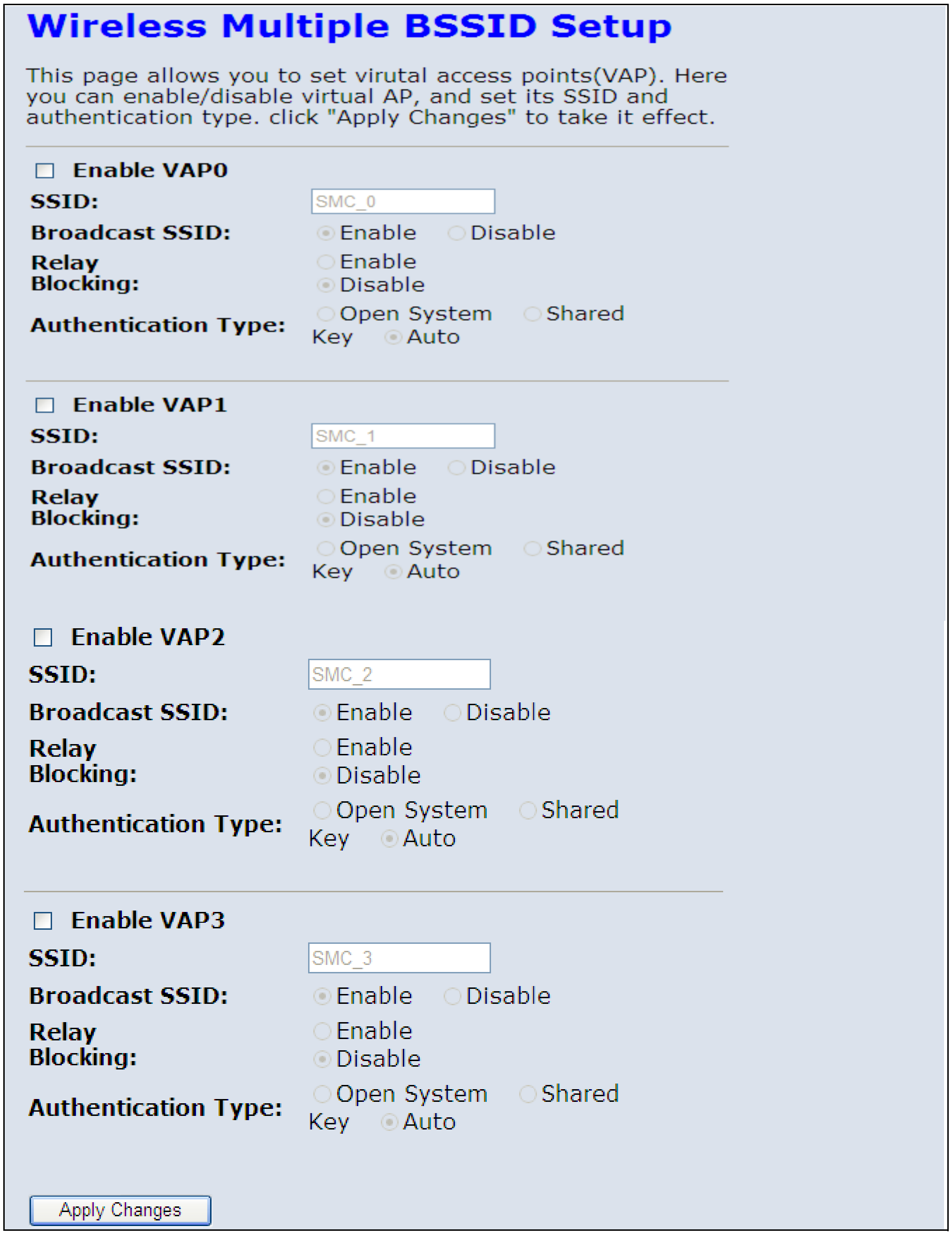
- **Reset** — Resets the WPS settings to factory default values.
- **Client PIN Number** — Enters a PIN number of a wireless client device that needs to join the network. Click “Start PIN” to activate the WPS process.

MBSSID

This page configures up to four VAPs (virtual access points) on the ADSL Router. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to both VAP interfaces.

The VAPs function similar to a VLAN, with each VAP mapped to its own VLAN ID. Traffic to specific VAPs can be segregated based on user groups or application traffic. Each VAP can have its own wireless clients, whereby the clients associate with these VAPs the same as they would with a physical access point.

Figure 29: Second BSSID



Wireless Multiple BSSID Setup

This page allows you to set viritual access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

□ **Enable VAP0**

SSID:	SMC_0
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ **Enable VAP1**

SSID:	SMC_1
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ **Enable VAP2**

SSID:	SMC_2
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ **Enable VAP3**

SSID:	SMC_3
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

The following items are displayed on this page:

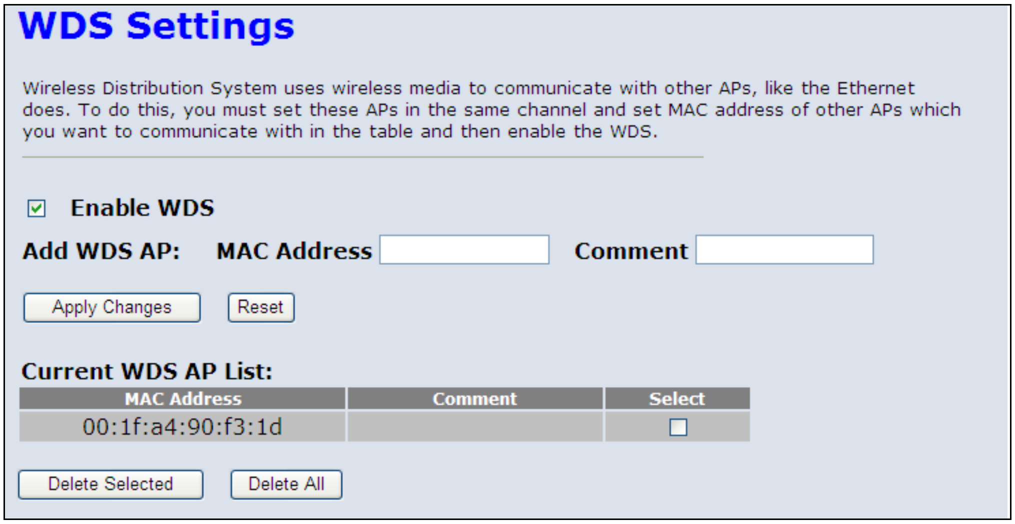
- **Enable (VAP0-VAP3)** — Enables up to four VAP interfaces on the router. (Default: Disabled)
- **SSID** — Configures the service set identifier of a VAP on the wireless interface.

- **Broadcast SSID** — Enables/disables the wireless interface to broadcast an SSID (service set identifier) to uniquely identify it on the network.
- **Relay Blocking** — Blocks traffic between SSID interfaces.
- **Authentication Type** — Sets the basic authentication method for the VAP interface.

WDS

Each access point radio interface can be configured to operate as a bridge, which allows it to forward traffic directly to other access point units. To set up bridge links between access point units, you must configure the wireless Distribution System (WDS) forwarding table by specifying the wireless MAC address of all units to which you want to forward traffic. Up to six WDS bridge links can be specified for each unit in the wireless bridge network.

Figure 30: WDS Configuration



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☑ Enable WDS

Add WDS AP: MAC Address ____ Comment ____

Current WDS AP List:

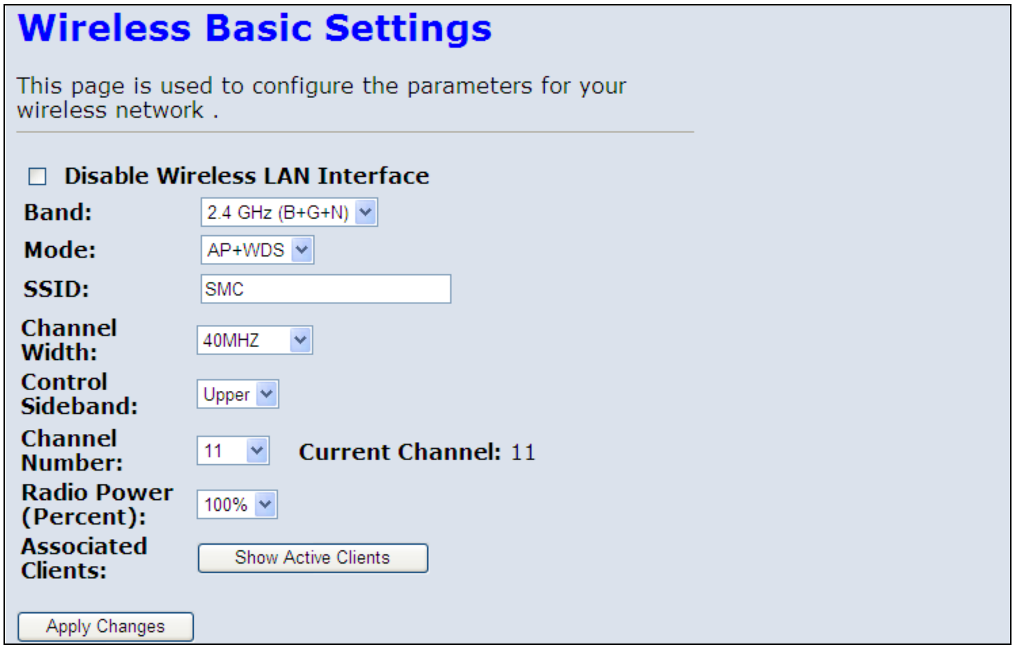
MAC Address	Comment	Select
00:1f:a4:90:f3:1d		□

To set up WDS all connected routers should be in the same subnet, with DHCP disabled on all routers not connected to the WAN and the MAC address of each router set first.

Follow the steps detailed below:

1. The wireless setup must be the same on all connected routers.

Figure 31: WDS Wireless Setup



Wireless Basic Settings

This page is used to configure the parameters for your wireless network .

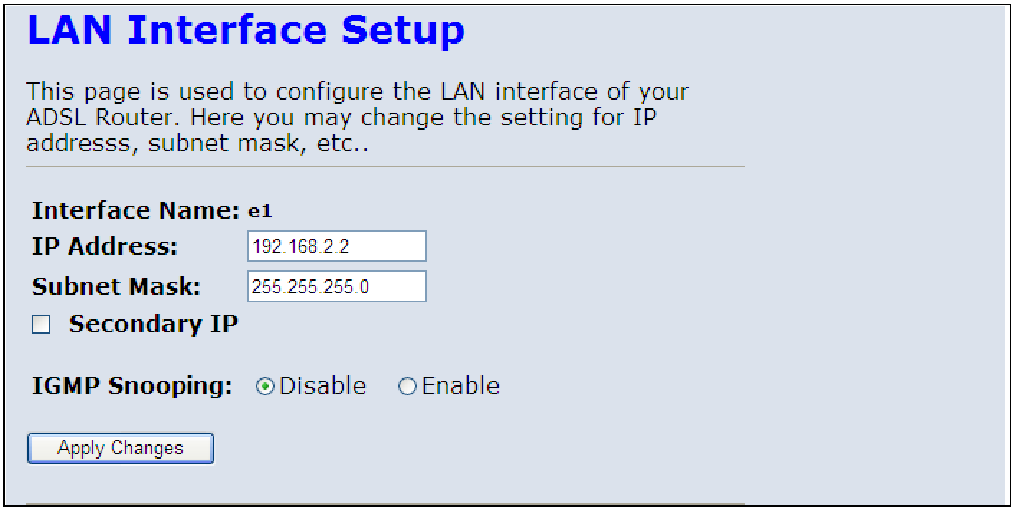
☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP+WDS
SSID:	SMC
Channel Width:	40MHZ
Control Sideband:	Upper
Channel Number:	11 Current Channel: 11
Radio Power (Percent):	100%
Associated Clients:	Show Active Clients

2. The MAC addresses on all connected routers must be set.

3. Change the LAN address on routers so as to avoid an IP conflict.

Figure 32: LAN Basic Setup



LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresss, subnet mask, etc..

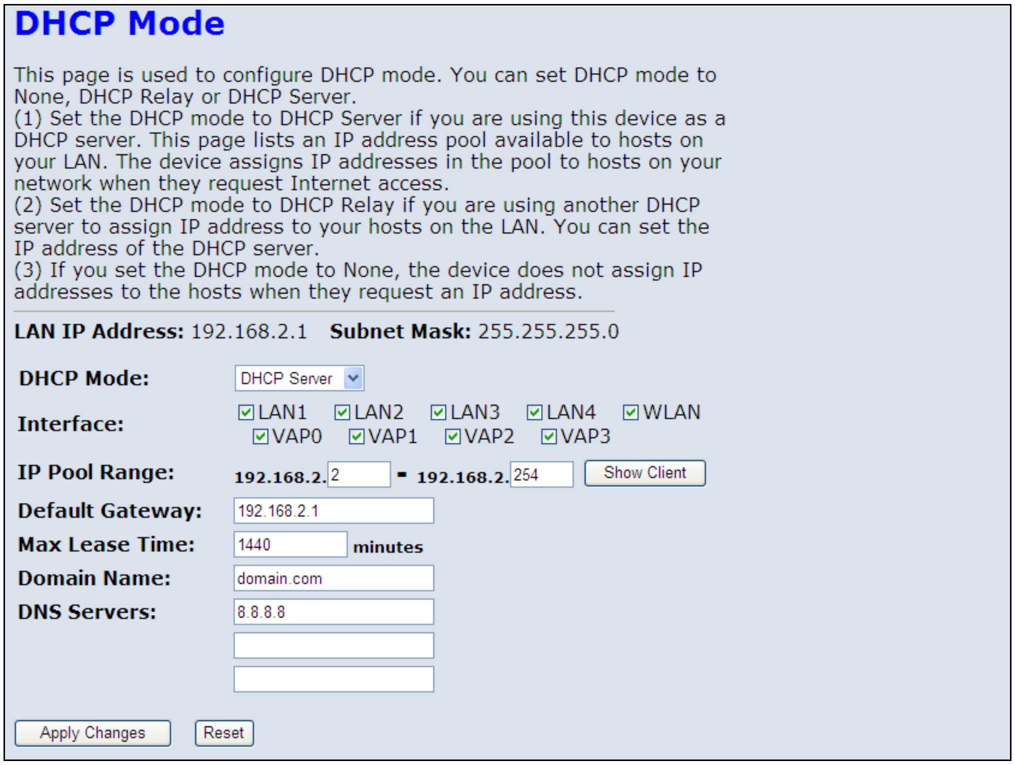
Interface Name:	e1
IP Address:	192.168.2.2
Subnet Mask:	255.255.255.0

☐ Secondary IP

IGMP Snooping: ● Disable ○ Enable

4. DIsable the DHCP server.

Figure 33: Disabling DHCP



DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.
(1) Set the DHCP mode to DHCP Server if you are using this device as a DHCP server. This page lists an IP address pool available to hosts on your LAN. The device assigns IP addresses in the pool to hosts on your network when they request Internet access.
(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.
(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.2.1 **Subnet Mask:** 255.255.255.0

DHCP Mode:	DHCP Server
Interface:	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2 ☑ VAP3
IP Pool Range:	192.168.2. 2 - 192.168.2. 254
Default Gateway:	192.168.2.1
Max Lease Time:	1440 minutes
Domain Name:	domain.com
DNS Servers:	8.8.8.8

6 LAN SETTINGS

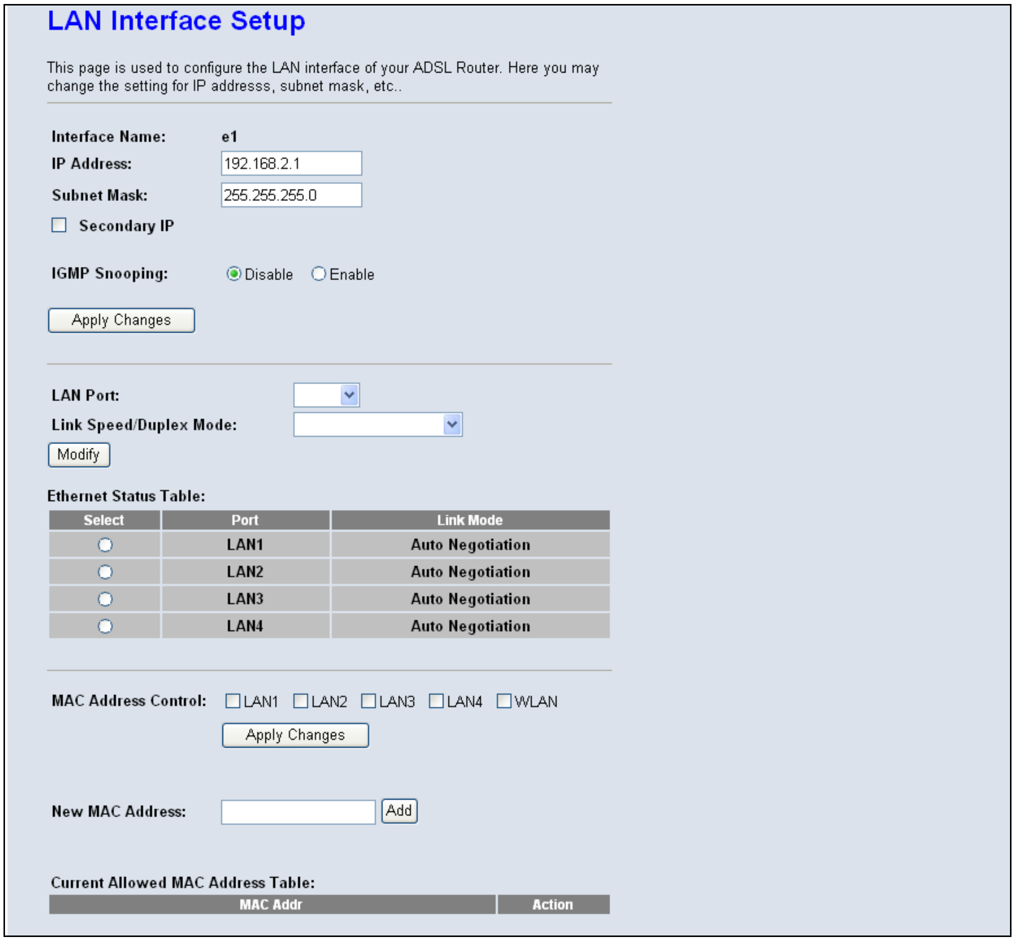
This chapter describes LAN configuration on the ADSL Router.

You can use the web browser interface to access IP addressing only if the ADSL Router already has an IP address that is reachable through your network.

LAN INTERFACE

By default, the ADSL Router is configured with the IP address 192.168.2.1, subnet mask 255.255.255.0 and a default gateway of 192.168.2.1.

Figure 34: LAN Configuration



LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresss, subnet mask, etc..

Interface Name:	e1
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

□ Secondary IP

IGMP Snooping: ● Disable ○ Enable

LAN Port:

Link Speed/Duplex Mode:

Ethernet Status Table:

Select	Port	Link Mode
○	LAN1	Auto Negotiation
○	LAN2	Auto Negotiation
○	LAN3	Auto Negotiation
○	LAN4	Auto Negotiation

MAC Address Control: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ WLAN

New MAC Address:

Current Allowed MAC Address Table:

MAC Addr	Action

The following items are displayed on this page:

- **Interface Name** — Displays the name assigned to the interface.
- **IP Address** — Specifies an IP address for management of the ADSL Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1.)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **Secondary IP Address** — Specifies a secondary IP address for management of the unit.
- **IGMP Snooping** — Enables Internet Group Management Protocol (IGMP) multicast filtering.

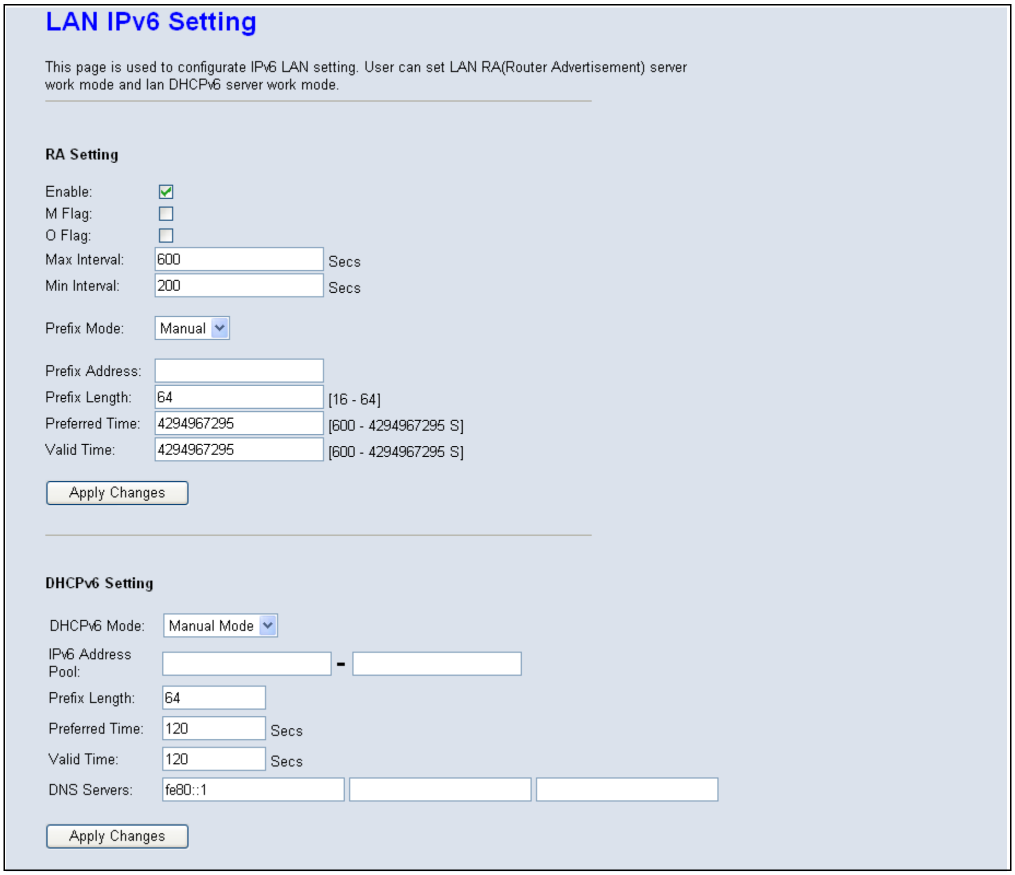
- **LAN Port** — Selects the LAN port.
- **Link Speed/Duplex Mode** — Selects the port speed and duplex mode, or sets the port for auto-negotiation.
- **MAC Address Control** — Filters out traffic with source MAC addresses not configured in the table. For devices that need Internet access through the LAN port, enter the MAC address and click Add.

IPV6 LAN CONFIGURATION

This section describes how to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets. This router supports both IPv4 and IPv6, and can be managed through either of these address types.

IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the router accessible over IPv6 for all devices attached to the same local subnet. However, to connect to a larger network with multiple segments, the router must be configured with a global unicast address.

Figure 35: IPv6 LAN Configuration



LAN IPv6 Setting

This page is used to configurate IPv6 LAN setting. User can set LAN RA(Router Advertisement) server work mode and lan DHCPv6 server work mode.

RA Setting

Enable:	☑	
M Flag:	□	
O Flag:	□	
Max Interval:	600	Secs
Min Interval:	200	Secs
Prefix Mode:	Manual	
Prefix Address:		
Prefix Length:	64	[16 - 64]
Preferred Time:	4294967295	[600 - 4294967295 S]
Valid Time:	4294967295	[600 - 4294967295 S]

DHCPv6 Setting

DHCPv6 Mode:	Manual Mode		
IPv6 Address Pool:		-	
Prefix Length:	64		
Preferred Time:	120	Secs	
Valid Time:	120	Secs	
DNS Servers:	fe80::1		

The following items are displayed on this page:

RA SETTING

- **Enable** — Enables IPv6 router advertisements on the router.
- **M Flag** — Sets the router advertisement "Managed address configuration" flag. When set, the router will use DHCPv6 to obtain stateful addresses.
- **O Flag** — Sets the router advertisement "other stateful configuration" flag. When set, the router will attempt to acquire other non-address configuration information (such as a default gateway or DNS).
- **Max Interval** — The amount of time that a remote IPv6 node is considered reachable.
- **Min Interval** — The interval between transmitting IPv6 neighbor solicitation messages.
- **Prefix Mode** — Enables manual or automatic configuration of IPv6 addresses on the router.
  - **Auto** — Enables automatic configuration of IPv6 addresses on interfaces and enables IPv6 functionality on the router. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (that is, the router's MAC address).
  - **Manual** — If auto-configuration is not selected, then an address must be manually configured using the fields described below.
- **Prefix Address** — The IPv6 address prefix sent in router advertisements.
- **Prefix Length** — The length of the IPv6 address prefix sent in router advertisements. For IPv6 unicast addresses, this is set to 64.
- **Preferred Time** — The time over which the configured address is preferred.
- **Valid Time** — The time over which the configured address is valid.

DHCPV6 SETTING

- **DHCPv6 Mode** — The DHCPv6 mode setting.
  - **None** — DHCPv6 is disabled.
  - **Manual** — If auto-configuration is not selected, then an IPv6 address pool must be manually configured.
  - **Auto** — Enables automatic assignment of IPv6 addresses on the router. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host

portion is automatically generated using the modified EUI-64 form of the client identifier (that is, the client MAC address).

- **IPv6 Address Pool** — The address range available for DHCPv6 assignment.
- **Prefix Length** — The length of the IPv6 address prefix sent in DHCPv6 assignments. For IPv6 unicast addresses, this is set to 64.
- **Preferred Time** — The time over which assigned addresses are preferred.
- **Valid Time** — The time over which the assigned addresses are valid.
- **DNS Servers** — Specifies up to three IPv6 Domain Name servers for IPv6 addresses.

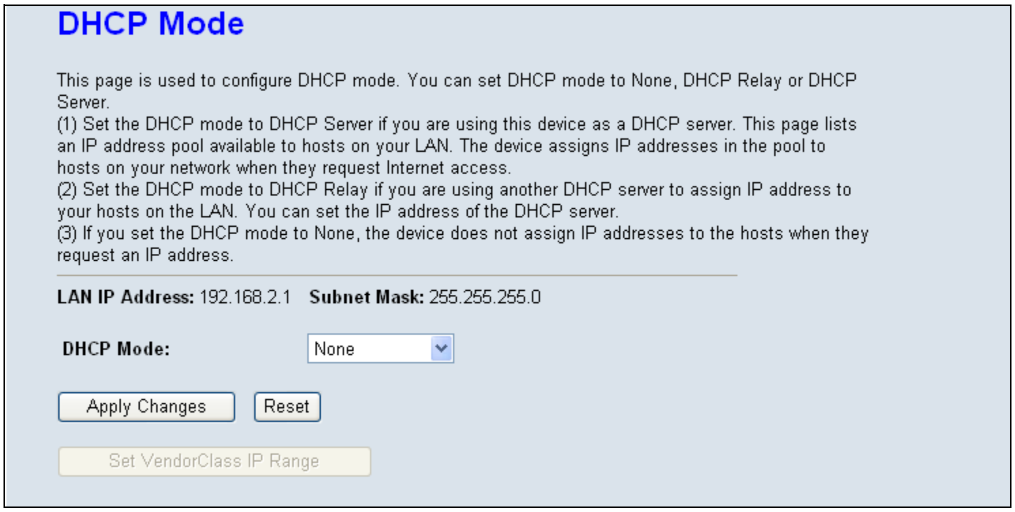
DHCP SETTINGS

The ADSL Router includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting the service, as well as a DHCP relay serivce that will route the DHCP service to other subnets than that of the unit.

DHCP DISABLED

By selecting "None," you can disable DHCP on the ADSL Router.

Figure 36: DHCP Disabled



DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.
(1) Set the DHCP mode to DHCP Server if you are using this device as a DHCP server. This page lists an IP address pool available to hosts on your LAN. The device assigns IP addresses in the pool to hosts on your network when they request Internet access.
(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.
(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.2.1 **Subnet Mask:** 255.255.255.0

DHCP Mode: None

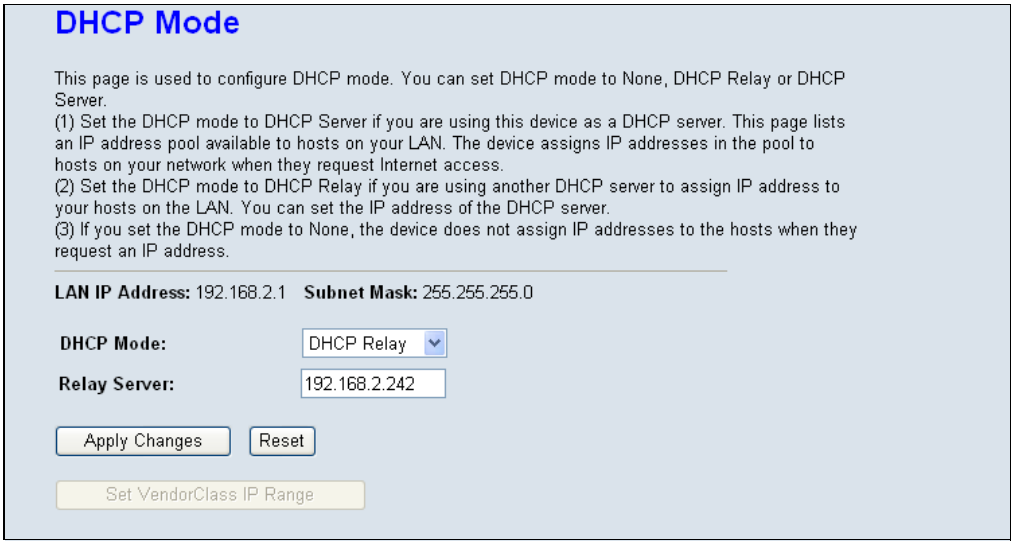
The following items are displayed on this page:

- **DHCP Mode** — When set to "None," disables DHCP on the unit.

DHCP RELAY

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients that broadcast a request. To receive the broadcast request, the DHCP server would normally have to be on the same subnet as the client. However, when the access point's DHCP relay agent is enabled, received client requests can be forwarded directly by the access point to a known DHCP server on another subnet. Responses from the DHCP server are returned to the access point, which then broadcasts them back to clients.

Figure 37: DHCP Relay



DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.
(1) Set the DHCP mode to DHCP Server if you are using this device as a DHCP server. This page lists an IP address pool available to hosts on your LAN. The device assigns IP addresses in the pool to hosts on your network when they request Internet access.
(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.
(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.2.1 **Subnet Mask:** 255.255.255.0

DHCP Mode: DHCP Relay

Relay Server: 192.168.2.242

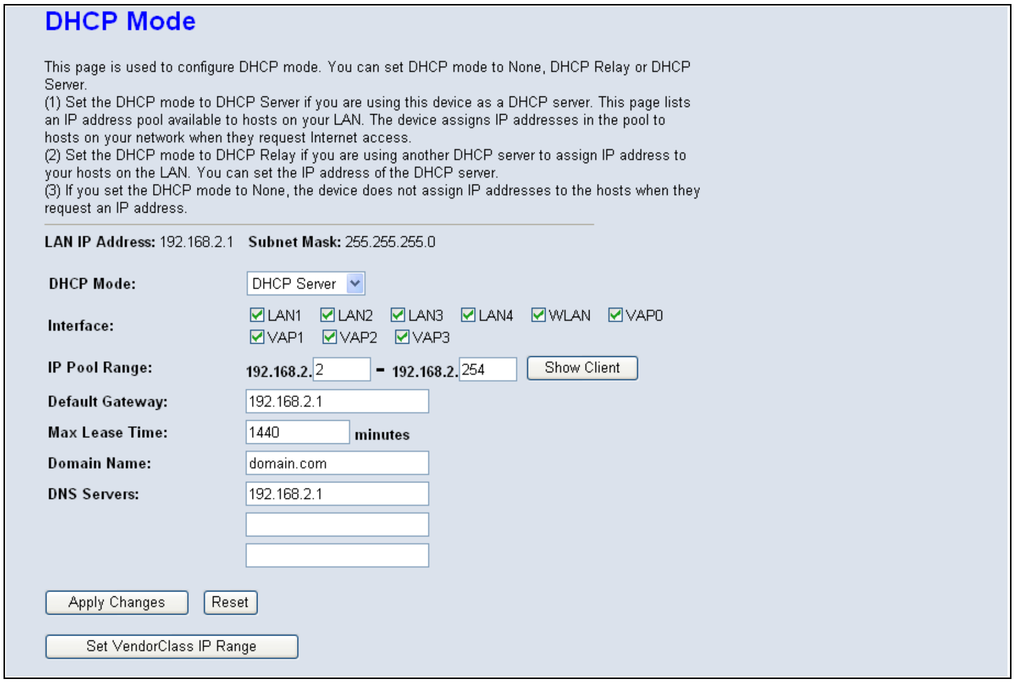
The following items are displayed on this page:

- **DHCP Mode** — When set to "DHCP Relay," enables routing of the DHCP service to units on a different subnet.
- **Relay Server** — Enter the address of the DHCP server for routing to other units.

DHCP SERVER

The unit can support up to 253 local clients. Addresses are assigned to clients from a common address pool configured on the unit. Configure an address pool by specifying start and end IP addresses. Be sure not to include the unit's IP address in the address pool range.

Figure 38: DHCP Server



DHCP Mode

This page is used to configure DHCP mode. You can set DHCP mode to None, DHCP Relay or DHCP Server.
(1) Set the DHCP mode to DHCP Server if you are using this device as a DHCP server. This page lists an IP address pool available to hosts on your LAN. The device assigns IP addresses in the pool to hosts on your network when they request Internet access.
(2) Set the DHCP mode to DHCP Relay if you are using another DHCP server to assign IP address to your hosts on the LAN. You can set the IP address of the DHCP server.
(3) If you set the DHCP mode to None, the device does not assign IP addresses to the hosts when they request an IP address.

LAN IP Address: 192.168.2.1 **Subnet Mask:** 255.255.255.0

DHCP Mode: DHCP Server

Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2 ☑ VAP3

IP Pool Range: 192.168.2.2 - 192.168.2.254 Show Client

Default Gateway: 192.168.2.1

Max Lease Time: 1440 minutes

Domain Name: domain.com

DNS Servers: 192.168.2.1

The following items are displayed on this page:

- **LAN IP Address** — Displays the LAN IP address for management of the ADSL Router. (Default: 192.168.2.1.)
- **Subnet Mask** — Displays the local subnet mask. (Default: 255.255.255.0)
- **DHCP Mode** — When set to "DHCP Server," enables the ADSL Router to act as a DHCP server.
- **Interface** — Selects either the RJ-45 LAN ports, or wireless interfaces.
- **IP Pool Range** — Configures the IP address pool for the DHCP server and determines how many IP addresses can be assigned.

NOTE: Do not enter the ADSL Router's LAN IP address as part of the IP Pool range.

- **Show Client** — Displays the current DHCP client table.
- **Default Gateway** — Specifies the gateway address through which traffic is routed from. Usually the LAN IP address of the ADSL Router

- **MAX Lease Time** — Select a time limit for the use of an IP address from the IP pool. When the time limit expires, the client has to request a new IP address. The lease time is expressed in seconds. (Default: 86400 seconds; Range: 60~86400 seconds; -1 indicates an infinite lease time)

- **Domain Name** — Specifies the unique name used to identify the ADSL Router on the network.

- **DNS Servers** — Sets up to three domain name server IP addresses.

- **Set VendorClass IP Range** — Click on this option to assign IP address ranges to specific device types.

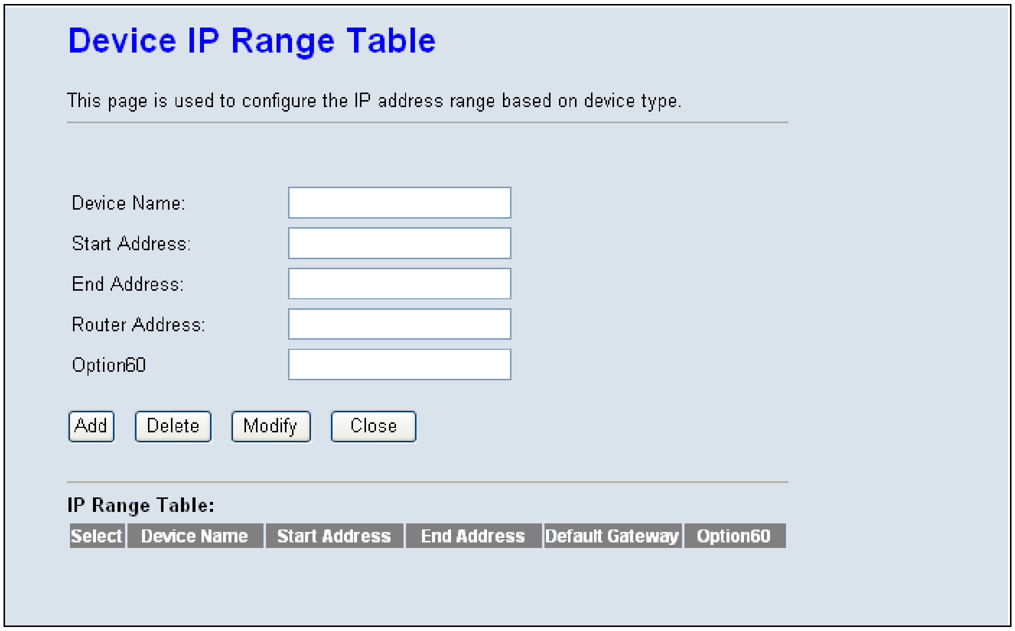
  - **Device Name** — Describes the device type.

  - **Start/End Address** — Specifies the IP addresses from the DHCP IP pool to assign to this device type.

  - **Router Address** — Specifies a default router IP address to use for traffic from this device.

  - **Option 60** — Specifies the DHCP Option 60 vendor class identifier that indicates the device type.

Figure 39: Device IP Range Table



Device IP Range Table

This page is used to configure the IP address range based on device type.

Device Name:	
Start Address:	
End Address:	
Router Address:	
Option60	

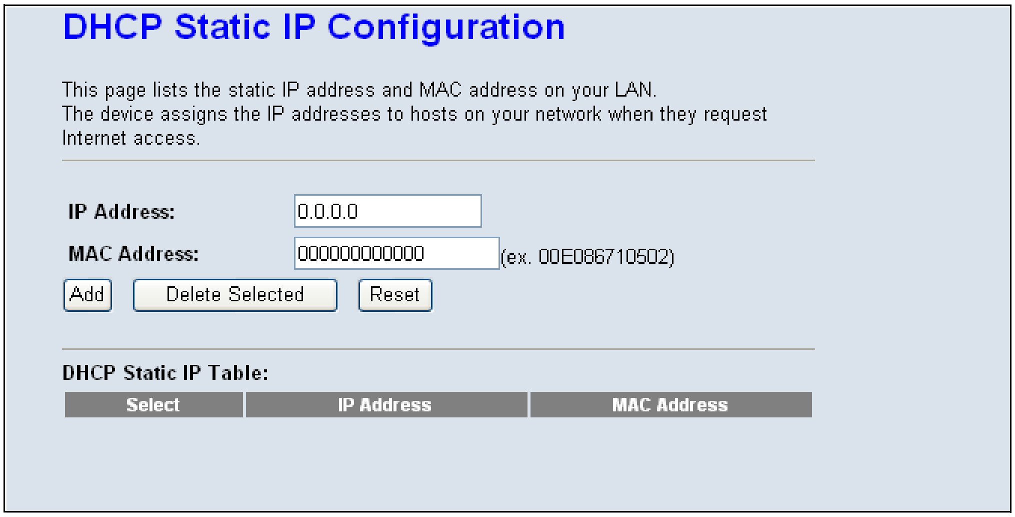
IP Range Table:

Select	Device Name	Start Address	End Address	Default Gateway	Option60

DHCP STATIC IP

Assigns a physical MAC address to the DHCP pool by mapping it to a corresponding IP address.

Figure 40: DHCP Static IP Assignment



DHCP Static IP Configuration

This page lists the static IP address and MAC address on your LAN.
The device assigns the IP addresses to hosts on your network when they request Internet access.

IP Address: 0.0.0.0

MAC Address: 000000000000 (ex. 00E086710502)

DHCP Static IP Table:

Select	IP Address	MAC Address

The following items are displayed on this page:

- **IP Address** — Enter the IP address from the DHCP address pool to assign to the specified MAC address.
- **MAC Address** — Enter the MAC address to be assigned to a static IP address from the DHCP address pool.
- **Add** — Selecting this option enters the mapped MAC address and IP address into the DHCP Static IP Table.
- **Delete Selected** — Once you select and entry in the table by clicking its corresponding radio button, this option deletes the entry.
- **Reset** — Clears the IP and MAC address fields.

7 WAN Settings

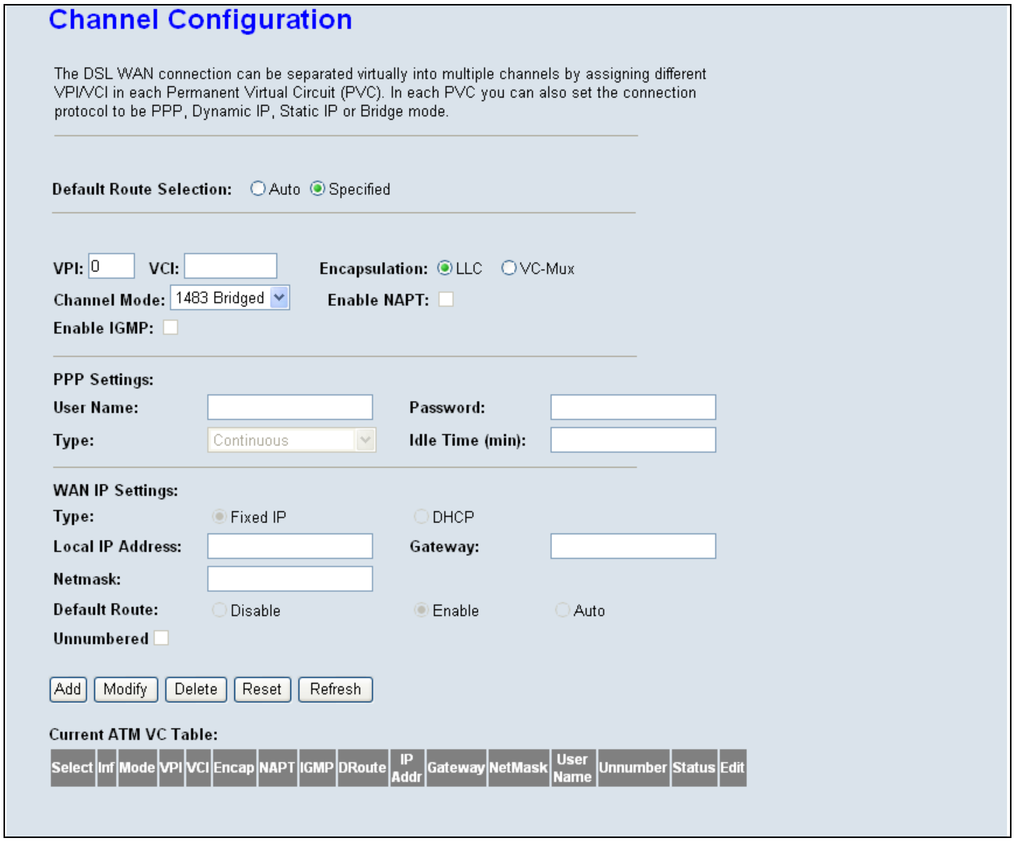
This chapter describes WAN configuration on the ADSL Router. The WAN pages are used to configure standard WAN services, including VPI, VCI, encapsulation, service type (PPPoE, IPoE, bridging), ATM settings and ADSL settings. It includes the following sections:

- "Channel Configuration" on page 82
- "ATM Settings" on page 84
- "ADSL Settings" on page 86

CHANNEL CONFIGURATION

The Channel Configuration page configures channel operation modes of the ADSL Router.

Figure 41: WAN Configuration



Channel Configuration

The DSL WAN connection can be separated virtually into multiple channels by assigning different VPI/VCI in each Permanent Virtual Circuit (PVC). In each PVC you can also set the connection protocol to be PPP, Dynamic IP, Static IP or Bridge mode.

Default Route Selection: ○ Auto ● Specified

VPI: 0 **VCI:** **Encapsulation:** ● LLC ○ VC-Mux

Channel Mode: 1483 Bridged **Enable NAPT:** □

Enable IGMP: □

PPP Settings:

User Name: **Password:**

Type: Continuous **Idle Time (min):**

WAN IP Settings:

Type: ● Fixed IP ○ DHCP

Local IP Address: **Gateway:**

Netmask:

Default Route: ○ Disable ● Enable ○ Auto

Unnumbered □

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	DRoute	IP Addr	Gateway	NetMask	User Name	Unnumber	Status	Edit

The following items are displayed on this page:

- **Default Route Selection** – Enables the default route to be specified or selected automatically.
- **VPI** (Virtual Path Identifier) – A grouping of virtual channels which connect the same end-points, and which share a traffic allocation.
- **VCI** (Virtual Channel Identifier) – A specific virtual channel connecting two end-points.
- **Encapsulation:**
  - **LLC** (Logical Link Control) – This encapsulation method allows multiplexing of multiple protocols over a single ATM virtual connection. In some cases, the LLC header is followed by a SNAP header which uniquely identifies a routed or bridged protocol. (This is the default packet encapsulation format used for carrying IP datagrams over AAL5 ATM.)

- **VC/MUX** (Virtual Circuit Multiplexing) – When using this mode, the communicating hosts agree on the high-level protocol for a given circuit, which tends to reduce fragmentation overhead. This allows a sender to pass each datagram directly to AAL5 for transfer, and requires nothing to be sent besides the datagram and the AAL5 trailer. The chief disadvantage of this scheme is that a host must create a separate virtual circuit for each high-level protocol if more than one protocol is used. Because most carriers charge for each virtual circuit, customers try to avoid using multiple circuits because it adds unnecessary cost.

- **Channel Mode** — The protocol used on the channel, as specified by the service provider. Choose from the following options:

  - **1483 Bridged** — The Bridged RFC 1483 Encapsulated Traffic over ATM feature allows you to send bridged RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs).

  - **1483 MER** — 1483 MER is an RFC standard MAC Encapsulated Routing protocol.

  - **PPPoE** — Point-to-Point Protocol over Ethernet (PPPoE).

  - **PPPoA** — Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA).

  - **1483 Routed** — Allows you to send routed RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs).

  - **IPoA** — Dynamic IP over ATM (IPoA).

- **Enabled NAPT** — Enables Network Address Port Translation for the channel.

- **Enable IGMP** — Enables IGMP for the channel.

- **PPP Settings** — Configures settings for PPPoE and PPPoA modes.

  - **User Name** — The PPP access user name provided by the ISP.

  - **Password** — The PPP access password provided by the ISP.

  - **Type** — Selects the connection type; Continuous, Connect on Demand, or Manual.

  - **Idle Time** — The number of minutes you want to have elapsed before your Internet access disconnects in Connect-on-Demand mode.

- **WAN IP Settings** — Configures settings for 1483 MER, 1483 Routed, and IPoA modes.

  - **Type** — Selects fixed IP or DHCP. When fixed IP is selected, enter the local IP address, gateway, and subnet mask. When DHCP is selected, the WAN interface IP address is assigned by the remote DHCP server.

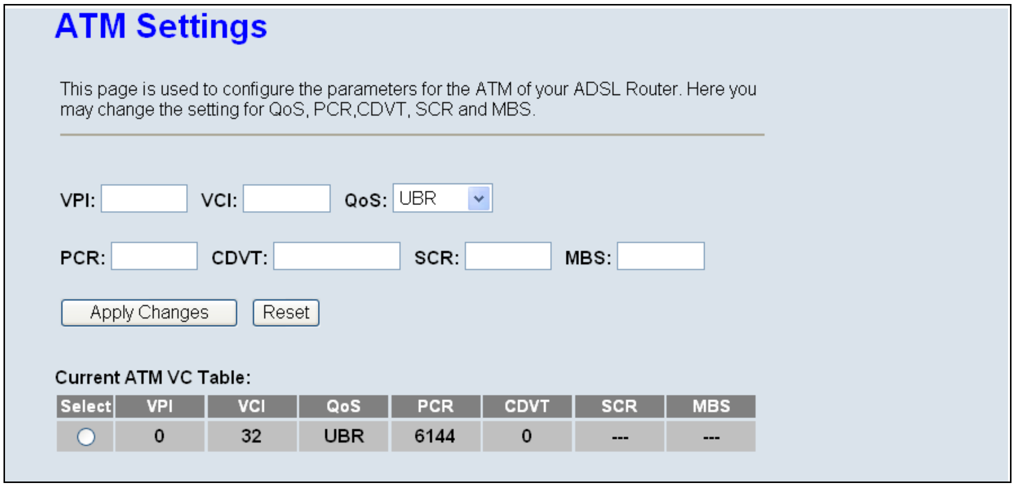
- **Local IP address** — The IP address of the WAN interface provided by the ISP.
- **Gateway** — The IP address of the remote gateway router provided by the ISP.
- **Netmask** — The subnet mask for the local IP address.
- **Default Route** — Enables or disables the default route IP address.
- **Unnmbered** — Enables the IP unnumbered feature.

ATM SETTINGS

The ATM Settings page is used to configure the settings between your ADSL Router and the remote ATM PVC switch, including connection mode (single or multiple service over one connection), and packet level QoS.

The ATM Settings parameters form a Traffic Contract that informs the network what type of traffic is to be transported and the performance requirements of the traffic.

Figure 42: ATM Settings



ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS, PCR,CDVT, SCR and MBS.

VPI: VCI: QoS: UBR

PCR: CDVT: SCR: MBS:

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	0	32	UBR	6144	0	---	---

The following items are displayed on this page:

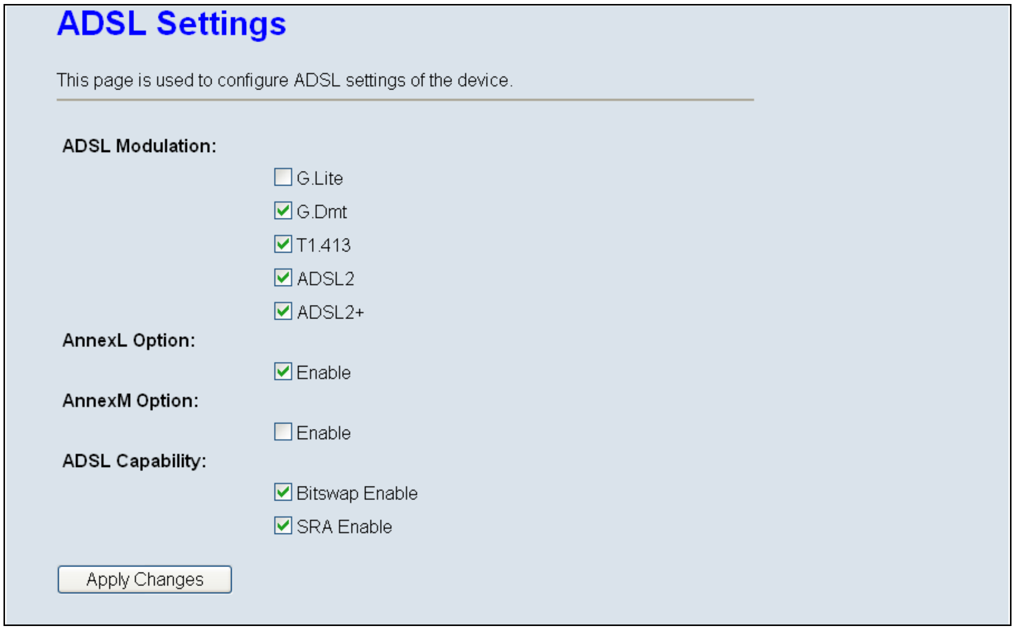
- **Select** — Clicking the radio button associated with the connection makes the parameters editable.
- **VPI** (Virtual Path Identifier) — Adds a VPI entry to the table. (Range: 0-255; Default: 0)

- **VCI** (Virtual Channel Identifier) — Adds a VCI entry to the table. (Range: 32-65535; Default: 35)
- **QoS** — Selects packet level Quality of Service (QoS) for the connection. Options are:
  - **UBR** (Unspecified Bitrate)**:** Configures a PVC with a Peak Cell Rate indicating the maximum number of ATM cells that can be sent in a burst.
  - **CBR** (Constant Bitrate)**:** Configures a PVC at a constant bit rate. This option may be required for connections that depend on precise clocking to ensure undistorted delivery.
  - **nrt-VBR** (non-realtime Variable Bitrate)**:** Configures a PVC at a non-realtime variable bit rate. This option may be used for applications not sensitive to changes in available bandwidth, such as data.
  - **rt-VBR** (realtime Variable Bitrate)**:** Configures a PVC at a real-time variable bit rate. This option may be used for applications that have a lot of variance in required bandwidth, such as voice.
- **PCR** (Peak Cell Rate) — Configures the maximum allowable rate at which cells can be transported along a connection in the ATM network. The PCR is the determining factor in how often cells are sent in relation to time in an effort to minimize jitter.
- **CDVT** (Cell Delay Variation Tolerance) — Configures the maximum amount of jitter permissable.
- **SCR** (Sustainable Cell Rate) — Configures the average allowable, long-term cell transfer rate on a specific connection.
- **MBS** (Maximum Burst Size) — Configures the maximum allowable burst size of cells that can be transmitted contiguously on a particular connection.
- **Current ATM VC Table** — The Current ATM VC Table lists the current ATM settings configured on your ADSL Router. By selecting the connection using the radio button associated with it you can edit the connection parameters.

ADSL SETTINGS

The ADSL Settings page configures the ADSL modulation type, ADSL2+ related parameters, capabilities and the ADSL tone mask.

Figure 43: ATM Settings



ADSL Settings

This page is used to configure ADSL settings of the device.

ADSL Modulation:
□ G.Lite
☑ G.Dmt
☑ T1.413
☑ ADSL2
☑ ADSL2+

AnnexL Option:
☑ Enable

AnnexM Option:
□ Enable

ADSL Capability:
☑ Bitswap Enable
☑ SRA Enable

The following items can be enabled on this page:

- **ADSL Modulation** — ADSL Modulation refers to a frequency-division multiplexing (FDM) scheme utilized as a digital multi-carrier modulation method for DSL. A large number of closely-spaced orthogonal sub-carriers are used to carry data. The data is divided into several parallel data streams or channels, one for each sub-carrier. Each sub-carrier is modulated with a conventional modulation scheme (such as G.lite, ADSL2, etc. or more commonly ADSL2+).

  - **G.lite** — A standard that defines the more economical splitterless ADSL connection that transmits data at up to 1.5 Mbps downstream and 512 Kbps upstream. This ADSL option can be installed without an on-site visit by the service provider.

  - **G.dmt** — A standard that defines full-rate ADSL, and utilizes Discrete Multi-Tone (DMT) signaling to transmit data at up to 8 Mbps downstream and 640 Kbps upstream.

  - **T1.413** — ANSI standard that defines the requirements for ADSL for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics. (The Gateway complies with Issue 2 of this standard.)

  - **ADSL2** — This standard extends the capability of basic ADSL data rates to 12 Mbit/s downstream and 3 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 Kbit/s upstream.

  - **ADSL2+** — This standard extends the capability of basic ADSL data rates to 24 Mbit/s downstream and 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's home.

- **AnnexL Option** — Annex L is an optional specification in the ITU-T ADSL2 recomendation G.992.3 titled “Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS.” It is often referred to as Reach Extended ADSL2 or READSL2. Once enabled AnnexL increases the range of DSL service, enabling the link to work at a distance of 7 kilometers, or 23,000 feet.

- **AnnexM Option** — Annex M is an optional specification in ITU-T recomendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits.

  Once enabled AnnexM increases upload speeds by the shifting the upstream/downstream frequency split from 138 kHz up to 276 kHz, allowing the maximum upstream bandwidth to be increased from 1.4 Mbit/s to 3.3 Mbit/s.

- **ADSL Capability** — ADSL Capability refers to means of manipulating the bit loading of a connection to increase quality of signal or transmission rate.

  - **Bitswap** — Enables bit swapping. Bit swapping is a way of swapping the bit-loading of a noisy tone with another tone in the symbol which is not as noisy. The bit loading from a specific tone can be increased or decreased. In addition, the TX power can be increased or decreased for a specific tone. However, there is no change in the overall payload rate after the bit swap operation.

  - **SRA** — Enables seamless rate adaptation to set the optimal transmission rate based on existing line conditions.

8 SERVICES

The Advanced Configuration settings for the ADSL Router contain advanced system management configuration settings such as DNS setup, routing configuration, bridging, SNMP and TR-069 settings.

The following sections are contained in this chapter:

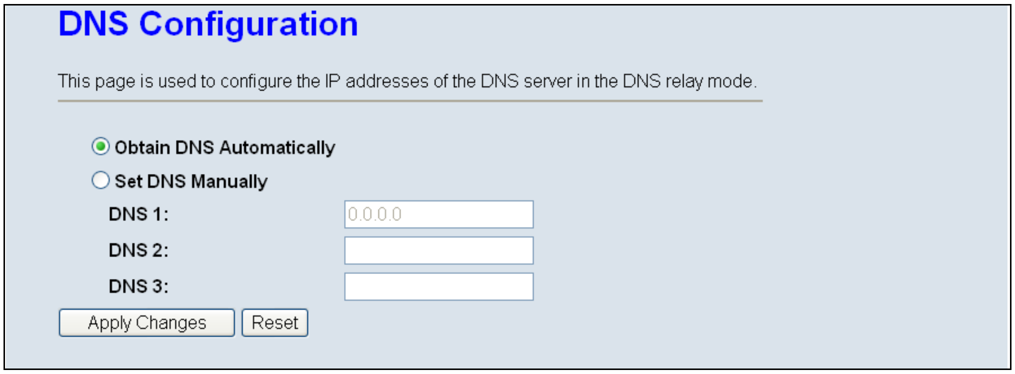
DNS SETTINGS

Sets Domain Name Server (DNS) and Dynamic DNS settings.

DNS SERVER

The Domain Name Server (DNS) implements a human recognizable web address to a numerical IP address. DNS can be set automatically or manually.

Figure 44: DNS Server Configuration



DNS Configuration

This page is used to configure the IP addresses of the DNS server in the DNS relay mode.

● Obtain DNS Automatically
○ Set DNS Manually
DNS 1: 0.0.0.0
DNS 2:
DNS 3:

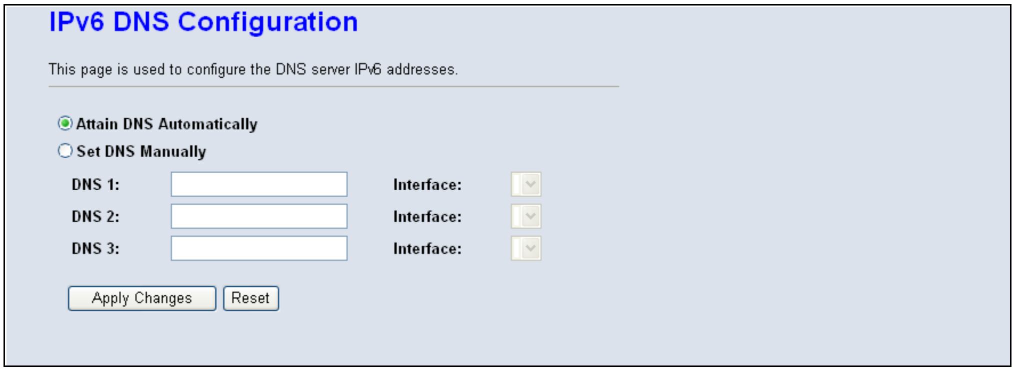
The following items are displayed on this page:

- **Obtain DNS Automatically** — The DNS server IP address is automatically configured during dynamic IP assignment.
- **Set DNS Manually** — Allows the user to set up to three DNS server IP addresses.

IPv6 DNS

The IPv6 Domain Name Server (DNS) implements a human recognizable web address to a numerical IPv6 address. DNS can be set automatically or manually.

Figure 45: IPv6 DNS Server Configuration



IPv6 DNS Configuration

This page is used to configure the DNS server IPv6 addresses.

● Attain DNS Automatically
○ Set DNS Manually
DNS 1: Interface:
DNS 2: Interface:
DNS 3: Interface:

The following items are displayed on this page:

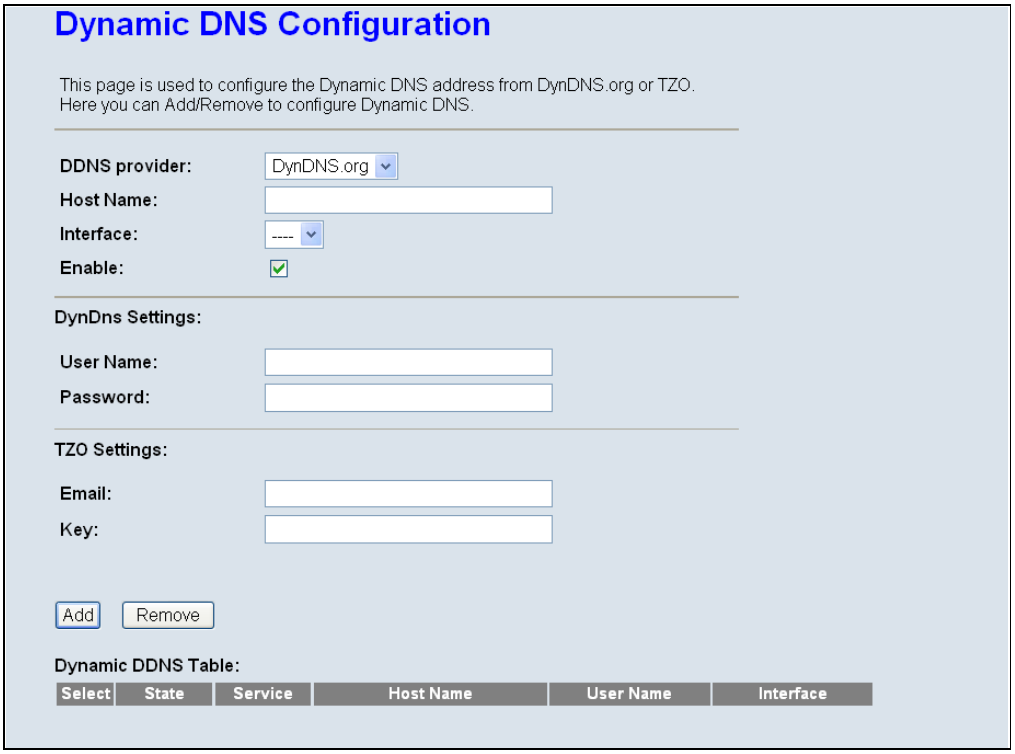
- **Obtain DNS Automatically** — The DNS server IPv6 address is automatically configured during dynamic IP assignment.
- **Set DNS Manually** — Allows the user to set up to three DNS server IPv6 addresses.

DDNS

Dynamic DNS (DDNS) provides users on the Internet with a method to tie a specific domain name to the unit's dynamically assigned IP address. DDNS allows your domain name to follow your IP address automatically by changing your DNS records when your IP address changes.

The ADSL Router provides access to two DDNS service providers, DynDns.org, and TZO. To set up an DDNS account, visit the websites of these service providers at www.dyndns.org,or www.tzo.com.

Figure 46: DDNS DynDns



Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO.
Here you can Add/Remove to configure Dynamic DNS.

DDNS provider: DynDNS.org
Host Name:
Interface: ----
Enable: ☑

DynDns Settings:

User Name:
Password:

TZO Settings:

Email:
Key:

Dynamic DDNS Table:

Select	State	Service	Host Name	User Name	Interface

The following items are displayed on these pages:

- **DDNS provider** — Specify the DDNS provider from the drop down menu. Options are: DynDns, or TZO. (Default: DynDns.org)
- **Host Name** — Specifies the prefix to identify your presence on the DDNS server, either URL or IP address.
- **Interface** — Selects the WAN interface for the DDNS service.

- **Enable** — Enables DDNS. (Default: Enabled)

DYNDNS SETTINGS

The following parameters apply to the default DynDns setting.

- **User Name** — Specifies your username for the DDNS service.
- **Password** — Specifies your password for the DDNs service.

TZO

The following parameters apply to the TZO setting.

- **Email** — Specifies your contact email address for the DDNS service.
- **Key** — Specifes an encryption key for the DDNS service.

DYNAMIC DDNS TABLE

This table displays the configured servers in the DDNS setup.

- **Select** — Highlights an entry in the Dynamic DDNS Table.
- **State** — Displays the state of the server entry, enabled or disabled.
- **Service** — Displays the type of DDNS service.
- **Host Name** — Displays the URL or IP address of the DDNS service provider.
- **User Name** — Displays the user name or contact email of the DDNS user.
- **Interface** — The WAN interface for the DDNS service.

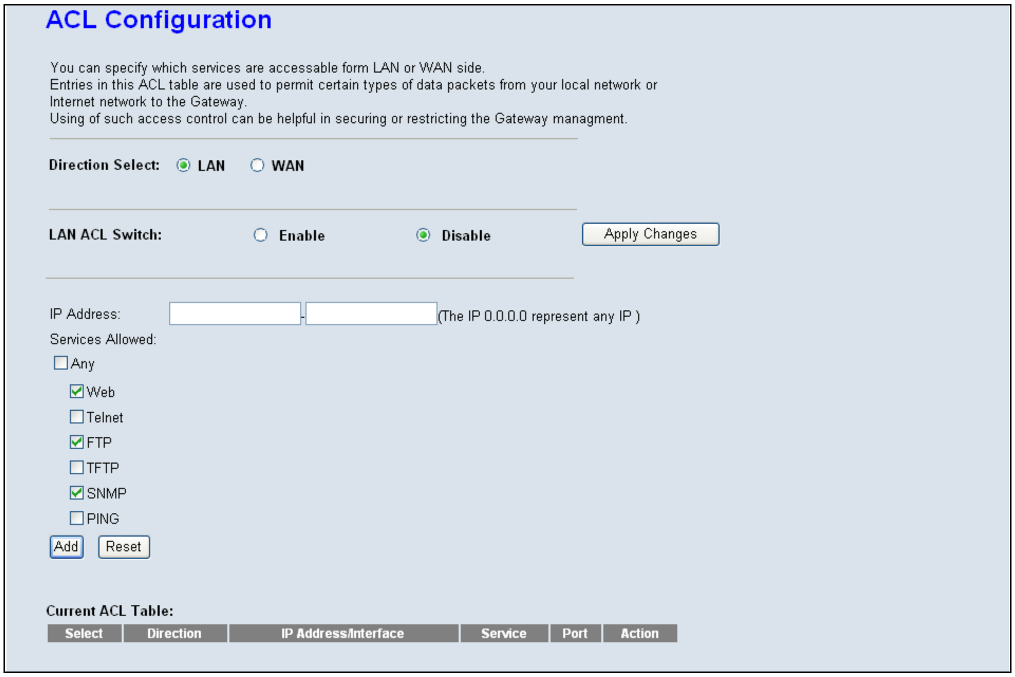
ACCESS CONTROL LISTS

The ADSL Router supports Access Control Lists that filter IP addresses allowed access on the unit's LAN and WAN interfaces. Only traffic from IP addresses in the ACL table are allow access to the ADSL Router.

LAN ACLS

When you select LAN for the ACL "direction," you can configure ACLs that apply to the LAN interfaces.

Figure 47: LAN ACL Configuration



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

IP Address: ____ - ____ (The IP 0.0.0.0 represent any IP)

Services Allowed:

□ Any
☑ Web
□ Telnet
☑ FTP
□ TFTP
☑ SNMP
□ PING

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action

The following items are displayed on this page:

- **LAN ACL Switch** — Enables LAN ACLs on the ADSL Router. (Default: Disabled)

NOTE: Do not enable ACLs without first configuring your host IP address in the ACL table, otherwise you will not be able to access the unit.

- **Apply Changes** — Implements the ACL settings on the ADSL Router.
- **IP Address** — Specify a LAN IP address or range of addresses that are allowed access to the ADSL Router.
- **Services Allowed** — Specifies services that are allowed access from LAN interfaces, or allows "any."
- **Add** — Adds the ACL to the ACL Table.

CURRENT ACL TABLE

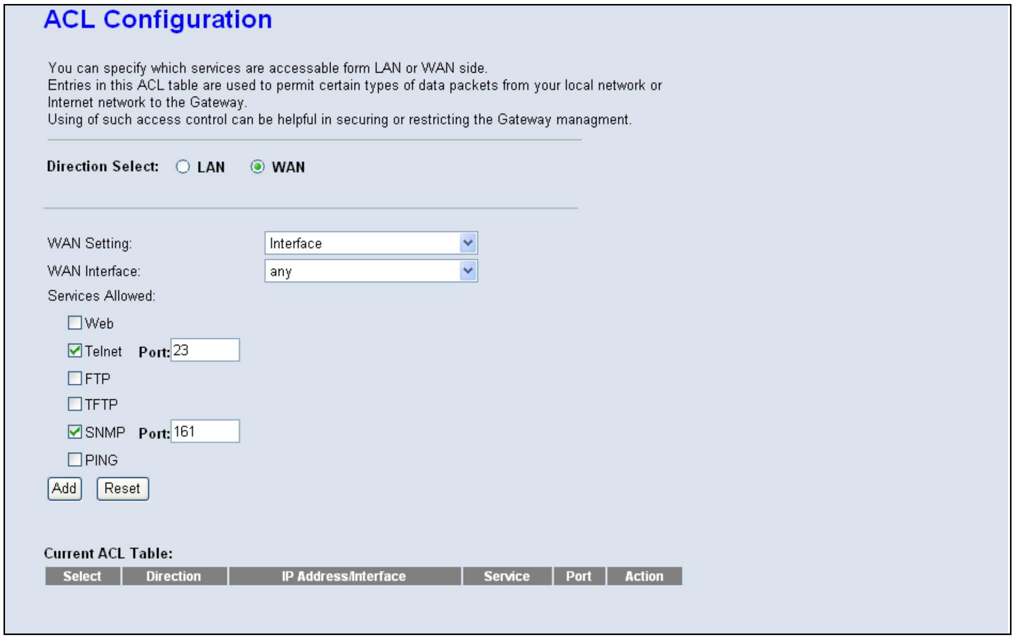
Lists the configured ACLs on the LAN ports.

- **Select** — The number of the entry in the table.
- **Direction** — Displays if the ACL is applied to a LAN or WAN interface.
- **IP Address/Interface** — Displays the allowed IP address or range.
- **Service** — Dispays the allowed service.
- **Port** — Displays the TCP/UDP port of the allowed service.
- **Action** — Click the button to remove the entry from the table.

WAN ACLS

When you select WAN for the ACL "direction," you can configure ACLs that apply to WAN interfaces.

Figure 48: WAN ACL Configuration



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ○ LAN ● WAN

WAN Setting:	Interface
WAN Interface:	any

Services Allowed:

☐ Web
☑ Telnet Port: 23
☐ FTP
☐ TFTP
☑ SNMP Port: 161
☐ PING

Add Reset

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action

The following items are displayed on this page:

- **WAN Setting** — Selects a WAN interface or IP address.
  - **WAN Interface** — Specifies a configured WAN interface for the ACL.
  - **IP Address** — Specify a LAN IP address or range of addresses that are allowed access to the ADSL Router.
- **Services Allowed** — Specifies services that are allowed access from LAN interfaces, or allows "any."

- **Add** — Adds the ACL to the ACL Table.

CURRENT ACL TABLE

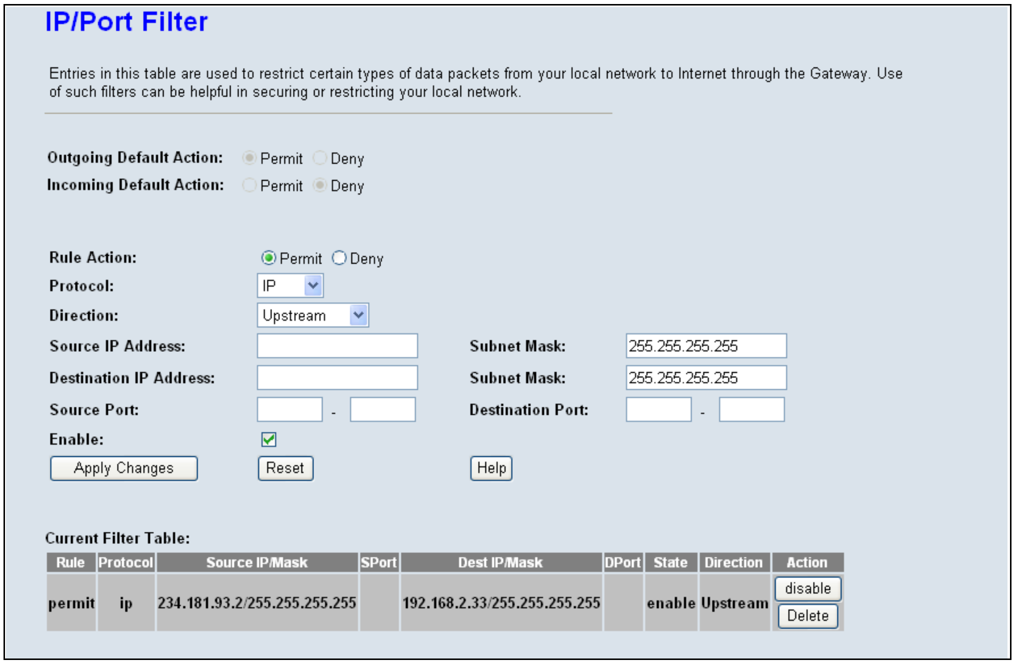
Lists the configured ACLs on the LAN ports.

- **Select** — The number of the entry in the table.
- **Direction** — Displays if the ACL is applied to a LAN or WAN interface.
- **IP Address/Interface** — Displays the allowed IP address or range.
- **Service** — Dispays the allowed service.
- **Port** — Displays the TCP/UDP port of the allowed service.
- **Action** — Click the button to remove the entry from the table.

IP/PORT FILTERING

IP/Port filtering restricts connection parameters to limit the risk of intrusion and defends against a wide array of common hacker attacks. IP/Port filtering allows the unit to permit, deny or proxy traffic through its ports and IP addresses.

Figure 49: IP/Port Filtering Settings



IP/Port Filter

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action: ● Permit ○ Deny
Incoming Default Action: ○ Permit ● Deny

Rule Action: ● Permit ○ Deny
Protocol: IP
Direction: Upstream
Source IP Address: Subnet Mask: 255.255.255.255
Destination IP Address: Subnet Mask: 255.255.255.255
Source Port: - Destination Port: -
Enable: ☑

Current Filter Table:

Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action
permit	ip	234.181.93.2/255.255.255.255		192.168.2.33/255.255.255.255		enable	Upstream	disable Delete

The following items are displayed on this page:

- **Outgoing Default Action** — Sets the default filtering action for outgoing packets that do not match a rule in the filter table. (Default: Permit, maximum 32 entries are allowed.)

- **Incoming Default Action** — Sets the default filtering action for incoming packets that do not match a rule in the filter table. (Default: Deny, maximum 32 entries are allowed.)

NOTE: The default incoming action denies all packets from the WAN port.

- **Rule Action** — Specifies if traffic should be permitted or denied. (Default: Permit)

- **Protocol** — Specifies the destination port type, TCP, UDP or ICMP. (Default: TCP).

- **Direction** — Specifies the packet destination. (Default: Outgoing)

- **Source IP Address** — Specifies the source IP address to block or allow traffic from.
- **Destination IP Address** — Specifies the destination IP address to block or allow traffic from.
- **Subnet Mask —** Specifies a subnet mask.
- **Source Port** — Specifies a range of ports to block traffic from the specified LAN IP address.
- **Destination Port** — Specifies a range of ports to block traffic from the specified LAN IP address from reaching.
- **Apply Changes** — Adds a newly configured packet filter that denies forwarding in to the local area network to the list.

CURRENT FILTER TABLE

The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from the ADSL Router.

- **Rule** — Displays if the specified traffic is allowed or denied.
- **Protocol** — Displays the destination port type.
- **Source IP/Mask** — Displays the source IP address.
- **SPort** — Displays the source port range.
- **Dest IP/Mask** — Displays the destination IP address.
- **DPort** — Displays the destination port range.
- **State** — Indicates if an entry is enabled.
- **Direction** — Displays the direction in which the rule has been applied.
- **Action** — Enables/disables or deletes the selected entry from the table.

NAT/NAPT SETTINGS

Network Address Translation (NAT) is a standard method of mapping multiple “internal” IP addresses to one “external” IP address on devices at the edge of a network. For the router, the internal (local) IP addresses are the IP addresses assigned to local PCs by the DHCP server, and the external IP address is the IP address assigned to the specified WAN interface.

The NAT function on the router enables the support of Virtual Servers, Port Triggering, and other features.

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, require multiple connections. These applications may not work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use Port Triggering to specify the additional public ports to be opened for each application. Alternatively, you can open up a client to unrestricted two-way Internet access by defining it as DMZ (demilitarized-zone) host.

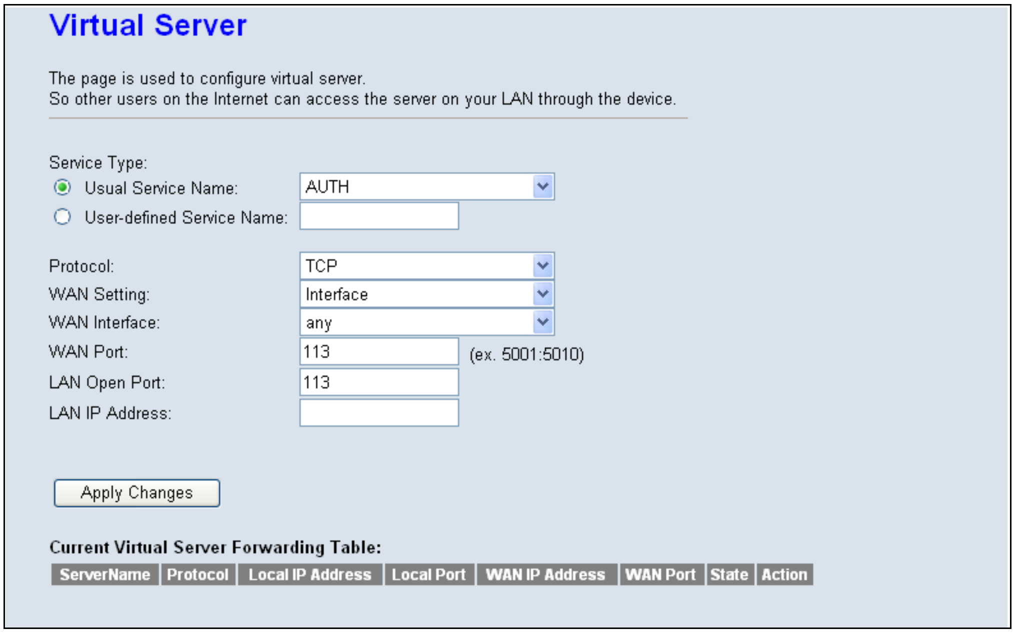
VIRTUAL SERVERS

Using the NAT Virtual Server feature, remote users can access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site thorugh your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.7.9/80, then all HTTP requests from outside users forwarded to 192.168.7.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110. Up to 32 entries can be configured in the Virtual Servers table.

Figure 50: NAT — Virtual Servers



Virtual Server

The page is used to configure virtual server.
So other users on the Internet can access the server on your LAN through the device.

Service Type:
● Usual Service Name: AUTH
○ User-defined Service Name:

Protocol: TCP
WAN Setting: Interface
WAN Interface: any
WAN Port: 113 (ex. 5001:5010)
LAN Open Port: 113
LAN IP Address:

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action

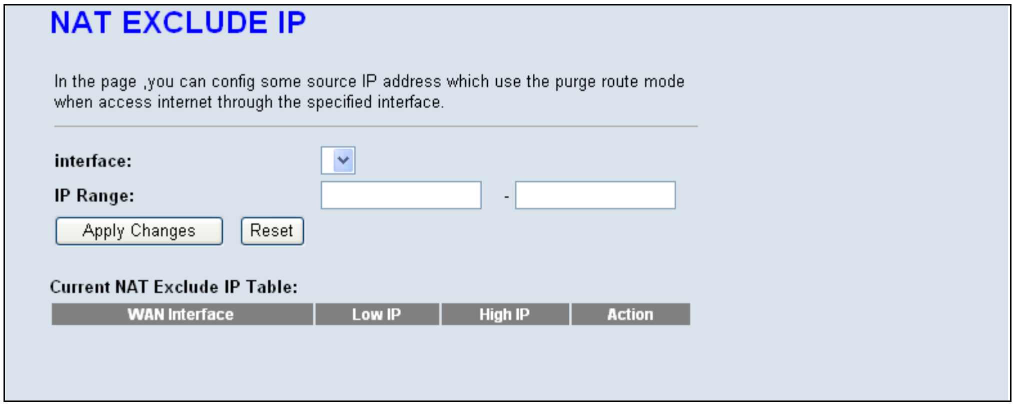
The following items are displayed on this page:

- **Service Type** – Sets a name to describe the virtual server service.
  - **Usual Service Name** – Select a name from the list of common applications.
  - **User-defined Service Name** – Set a custom name to describe the service.
- **Protocol** – Specifies the port type. (Options: TCP or UDP; Default: TCP)
- **WAN Setting** – Selects a WAN interface or IP address. Depending on the selection, either the WAN Interface or WAN IP Address setting displays.
  - **WAN Interface** – Select the WAN interface for the virtual server.
  - **WAN IP Address** – Specify the WAN IP address for the virtual server.
- **WAN Port** – Specifies the public TCP/UDP port number, or port range, used for the service on the WAN interface. (Range: 1-65535)
- **LAN Open Port** – Specifies the TCP/UDP port number, or port range, used on the local server for the service. (Range: 1-65535)
- **LAN IP Address** – The IP address of the server on the local Ethernet network. The specified address must be in the same subnet as the router and its DHCP server address pool. (Range: 192.168.2.2 to 192.168.2.254)

NAT EXCLUDE IP

You can use the Exclude IP feature to block an IP address or range of IP addresses from accessing WAN interfaces.

Figure 51: NAT — Exclude IP



NAT EXCLUDE IP

In the page ,you can config some source IP address which use the purge route mode when access internet through the specified interface.

interface:

IP Range: -

Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action

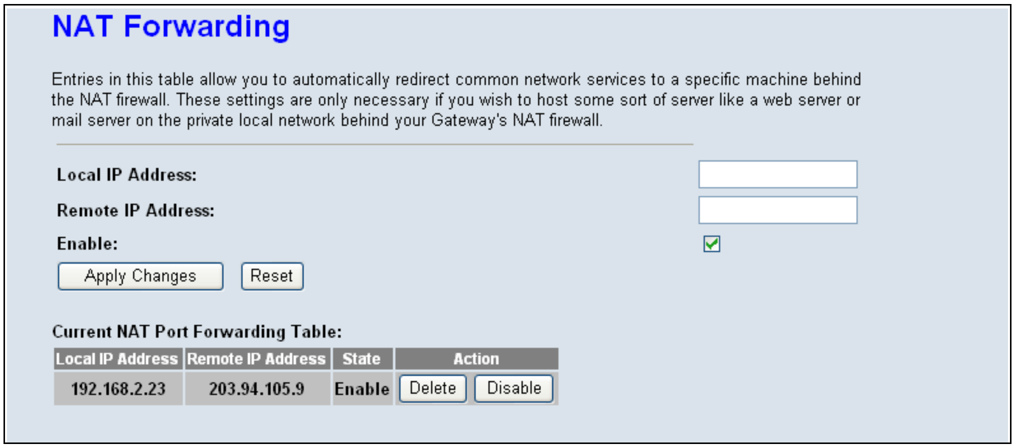
The following items are displayed on this page:

- **Interface** – Select the WAN interface for the Exclude IP service.
- **IP Range** – Specifies an IP address range to block on the WAN interface.

NAT FORWARDING

Forwarding allows an external user to reach a private IP address (inside a LAN) from the outside through a NAT-enabled router.

Figure 52: NAT Forwarding Settings



NAT Forwarding

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

Local IP Address:

Remote IP Address:

Enable: ☑

Current NAT Port Forwarding Table:

Local IP Address	Remote IP Address	State	Action
192.168.2.23	203.94.105.9	Enable	Delete Disable

The following items are displayed on this page:

- **Local IP Address** — Specifies the IP address of a computer on the local network.

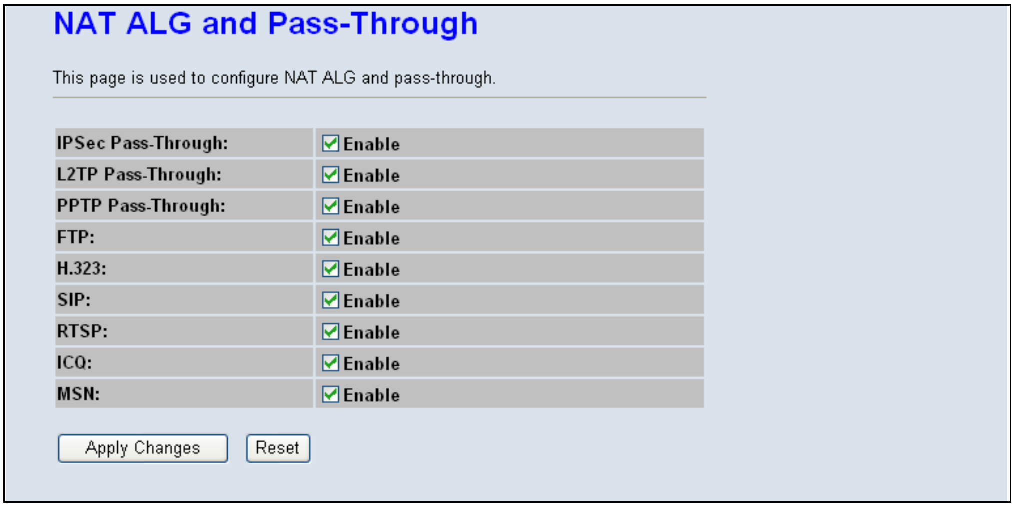
- **Remote IP Address** — Specifies the source IP address on the WAN to allow access from. Leaving this parameter blank allows access from all traffic.

- **Enable** — Checking this box activates the parameters configurated once added to the Current NAT Port Forwarding Table. (Default: Enabled)

NAT ALG AND PASS-THROUGH

Application Layer Gateway (ALG) and passthrough is a useful feature when a host computer or server on the Local Area Network must be accessible from the Internet using specific protocols. This can be necessary with certain software applications that do not function reliably through Network Address Translation.

Figure 53: NAT ALG and Pass-Through



NAT ALG and Pass-Through

This page is used to configure NAT ALG and pass-through.

IPSec Pass-Through:	☑ Enable
L2TP Pass-Through:	☑ Enable
PPTP Pass-Through:	☑ Enable
FTP:	☑ Enable
H.323:	☑ Enable
SIP:	☑ Enable
RTSP:	☑ Enable
ICQ:	☑ Enable
MSN:	☑ Enable

The following items are displayed on this page:

- **IPSec Pass Through** — Enables IPsec passthrough. (Default: Enabled)

- **L2TP Pass Through** — Enables L2TP passthrough. (default: Enabled)

- **PPTP Pass Through** — Enables PPTP passthrough. (Default: Enabled)

- **FTP** — Enables FTP passthrough. (Default: Enabled)

- **H.323** — Enables H.323 (Windows Netmeeting) passthrough. (Default: Enabled)

- **SIP** — Enables SIP passthrough. (Default: Enabled)

- **RTSP** — Enables RTSP passthrough. (Default: Enabled)

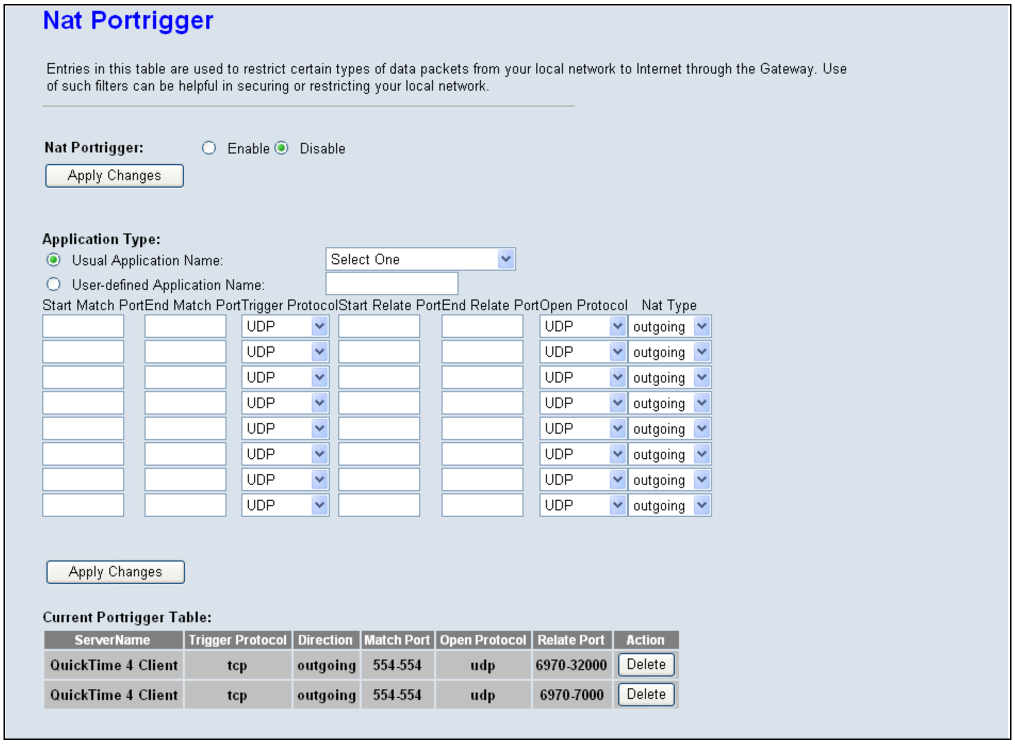
- **ICQ** — Enables ICQ passthrough. (Default: Enabled)

- **MSN** — Enables MSN passthrough. (Default: Enabled)

NAT PORT TRIGGER

Port triggering is a way to automate port forwarding in which outbound traffic on predetermined ports (“triggering ports”) causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host while the outbound ports are in use.

Figure 54: NAT — Port Trigger



Nat Portrigger

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Nat Portrigger: ○ Enable ● Disable

Apply Changes

Application Type:

● Usual Application Name: Select One

○ User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing

Apply Changes

Current Portrigger Table:

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
QuickTime 4 Client	tcp	outgoing	554-554	udp	6970-32000	Delete
QuickTime 4 Client	tcp	outgoing	554-554	udp	6970-7000	Delete

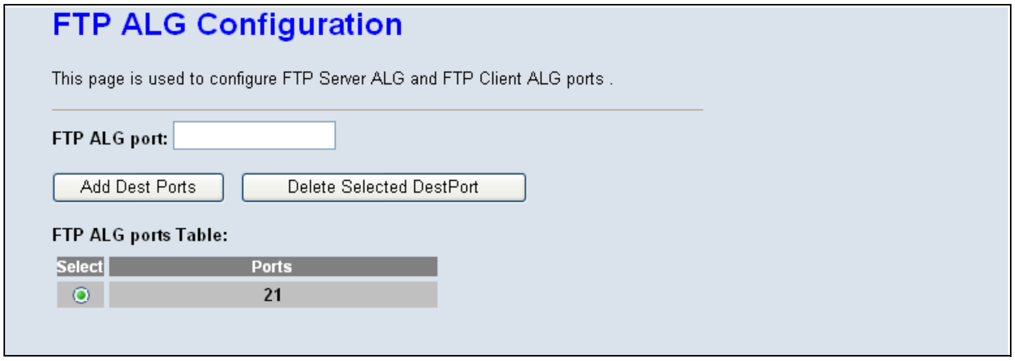
The following items are displayed on this page:

- **Port Trigger** – Enables the feature. (Default: Disabled)
- **Application Type** – Select a name from the list of common applications, or set a custom name to describe the service.
- **Start/End Match Port** — Specifies the trigger port range. (Range: 1-65535)
- **Trigger Protocol** — Specifies the trigger port type used, TCP, UDP, or both.
- **Start/End Relate Port** — Specifies the public port range. (Range: 1-65535).
- **Open Protocol** — Specifies the public port type used, TCP, UDP, or both.
- **NAT Type** — Specifies outgoing or incoming traffic.

FTP ALG CONFIGURATION

FTP ALG Configuration specifies a non-standard FTP port for passthrough traffic. The standard port for FTP connections is TCP port 21, and the router monitors port 21 to ensure the NAT passthrough of FTP. When the FTP server port is not 21, you must specify the TCP port to ensure NAT passthrough of FTP.

Figure 55: NAT — FTP ALG Configuration



FTP ALG Configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports .

FTP ALG port:

FTP ALG ports Table:

Select	Ports
●	21

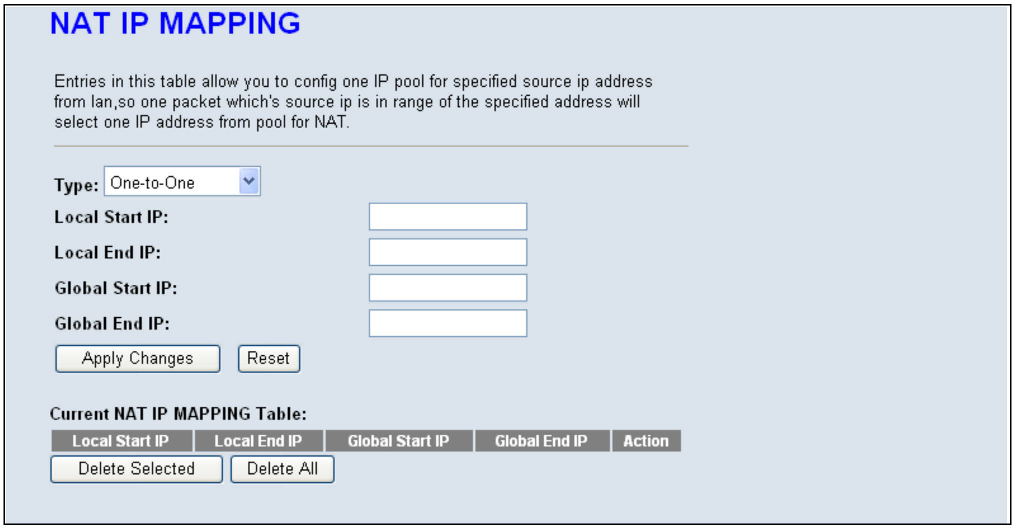
The following items are displayed on this page:

- **FTP ALG Port** – Specifies a non-standard FTP port for passthrough traffic. (Range: 0~65535)
- **Add Dest Ports** – Adds the specified port to the FTP ALG Ports Table.
- **Delete Selected Dest Port** – Removes the selected port from the FTP ALG Ports Table.

NAT IP MAPPING

IP Mapping enables a pool of local LAN IP addresses to be dynamically mapped to a pool of external (global) IP addresses.

Figure 56: NAT — IP Mapping



NAT IP MAPPING

Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

Type: One-to-One
Local Start IP:
Local End IP:
Global Start IP:
Global End IP:

Current NAT IP MAPPING Table:

Local Start IP	Local End IP	Global Start IP	Global End IP	Action

The following items are displayed on this page:

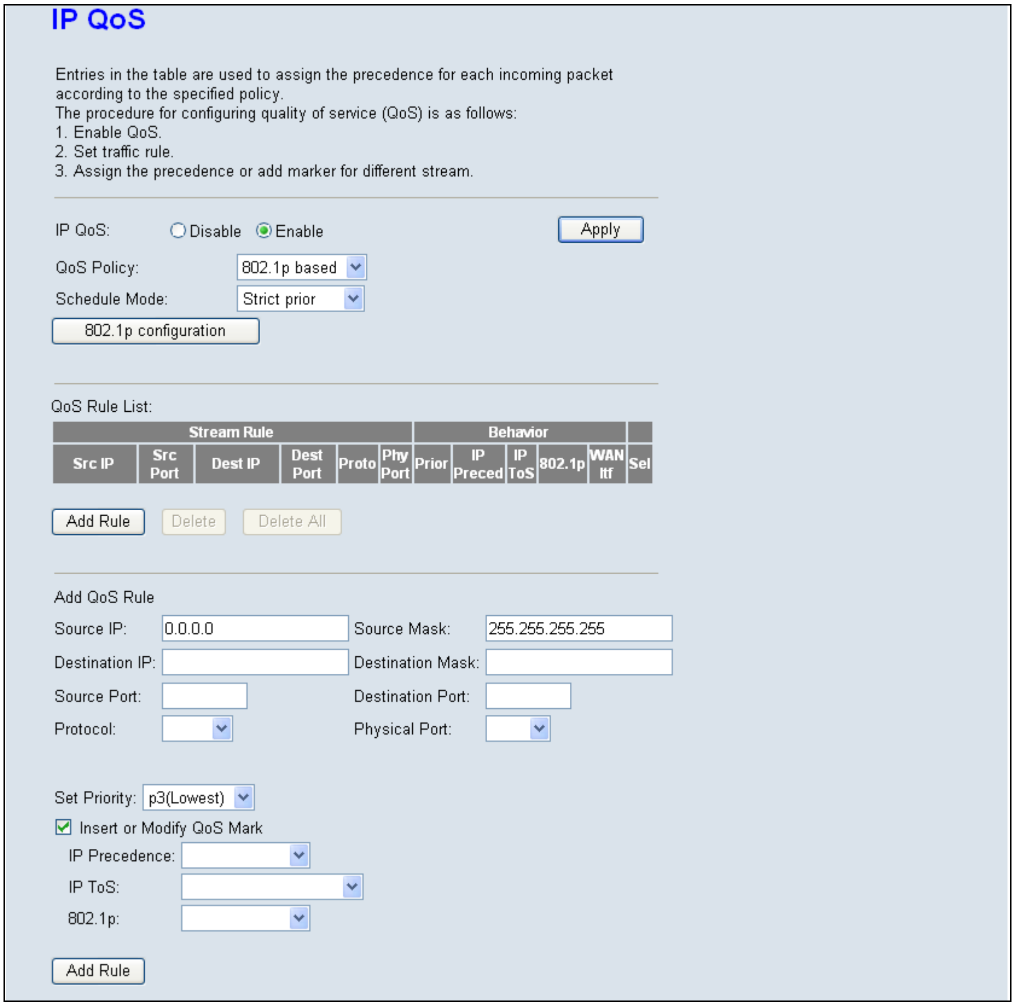
- **Type** – Selects the type of mapping to use. Either one-to-one, one-to-many, many-to-many, or many-to-one.
- **Local Start/End IP** – Defines a local IP address pool range.
- **Global Start/End IP** – Defines an external IP address pool range.

QUALITY OF SERVICE

The Quality of Service page is used to enable or disable QoS, and set the default priority for packets not matching any classification rules.

Click Services, IP QoS. If QoS is enabled, the default priority should also be set to an appropriate value. After setting any of the attributes on this page, click Apply.

Figure 57: Quality of Service



IP QoS

Entries in the table are used to assign the precedence for each incoming packet according to the specified policy.
The procedure for configuring quality of service (QoS) is as follows:
1. Enable QoS.
2. Set traffic rule.
3. Assign the precedence or add marker for different stream.

IP QoS: ○ Disable ● Enable

QoS Policy: 802.1p based

Schedule Mode: Strict prior

QoS Rule List:

Stream Rule							Behavior					
Src IP	Src Port	Dest IP	Dest Port	Proto	Phy Port	Prior	IP Preced	IP ToS	802.1p	WAN Itf	Sel

Add QoS Rule

Source IP: 0.0.0.0 Source Mask: 255.255.255.255

Destination IP: Destination Mask:

Source Port: Destination Port:

Protocol: Physical Port:

Set Priority: p3(Lowest)

☑ Insert or Modify QoS Mark

IP Precedence:

IP ToS:

802.1p:

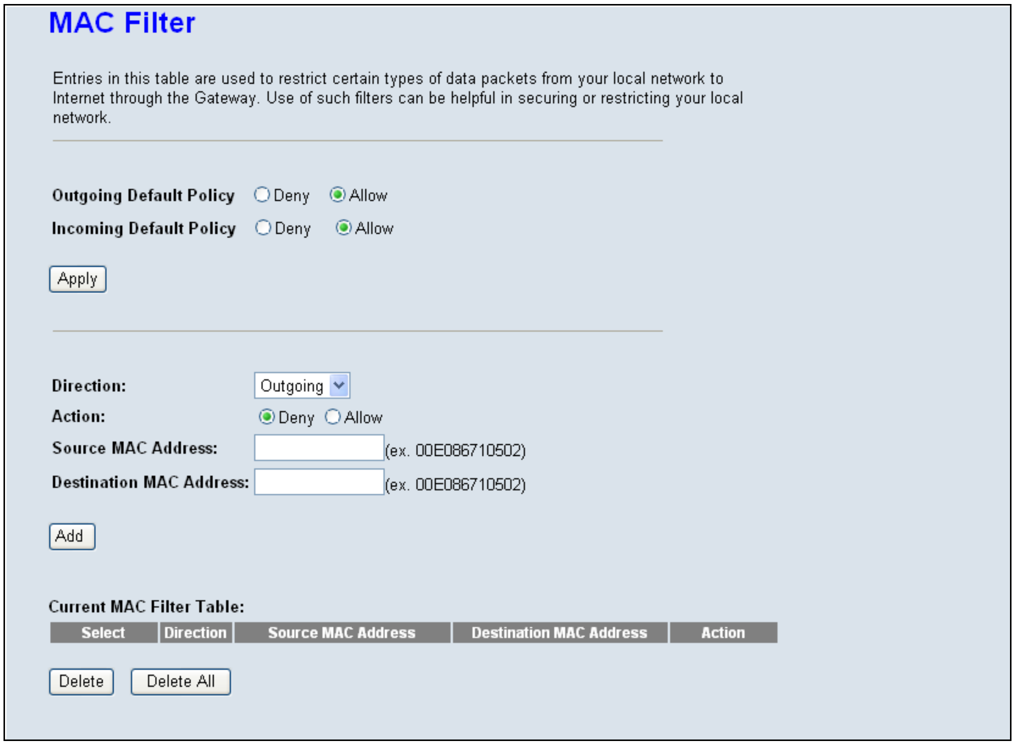
The following items are displayed on this page:

- **IP QoS** – If enabled, QoS rules will be applied to traffic entering the Gateway.
- **QoS Policy** – Selects Stream-based, 802.1p-based, or DSCP-based policy.
- **Schedule Mode** – Selects either Strict or Weighted Fair Queueing (WFQ) as the port priority mode.
- **802.1p Configuration** – When the QoS Policy is 802.1p-based, you can map the 802.1p values to port priority queues.
- **DSCP Configuration** – When the QoS Policy is DSCP-based, you can map the DSCP values to port priority queues
- **Add QoS Rule** – Specifies traffic classification rules based on protocol type and destination/source MAC address; and to set the resulting priority queue, re-marked IP Precedence, IP ToS, or 802.1p priority.
  - **Source IP/ Mask** – The source IP address and network mask.
  - **Destination IP/ Mask** – The destination IP address and network mask.
  - **Source Port** – The TCP/UDP source port.
  - **Destination Port** – The TCP/UDP destination port.
  - **Protocol** – The network protocol; TCP, UDP, or ICMP.
  - **Physical Port** – Select the physical interface; LAN or USB.
  - **Set Priority** – The port queue to which a matching packet is assigned.
  - **Insert or Modify QoS Mark** – Re-marks the matching packet with the selected IP Precedence, IP ToS, or 802.1p value.

MAC FILTERING

MAC based packet filtering enables the router to filter clients based on their physical layer address.

Figure 58: MAC Filtering Settings



MAC Filter

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy ○ Deny ● Allow

Incoming Default Policy ○ Deny ● Allow

Apply

Direction: Outgoing

Action: ● Deny ○ Allow

Source MAC Address: (ex. 00E086710502)

Destination MAC Address: (ex. 00E086710502)

Add

Current MAC Filter Table:

Select	Direction	Source MAC Address	Destination MAC Address	Action

Delete Delete All

The following items are displayed on this page:

- **Outgoing Default Policy** — A default action for MAC addresses not configured in the filter table. (Default: Allow, maximum 32 entries are allowed.)

- **Incoming Default Policy** — A default action for MAC addresses not configured in the filter table. (Default: Allow, maximum 32 entries.)

NOTE: The default outgoing and incoming defaults allow traffic from all MAC addresses.

- **Direction** — Specifies the packet destination. (Default: Outgoing)

- **Action** — Specifies if traffic should be permitted or denied. (Options: Deny, Allow; Default: Deny)

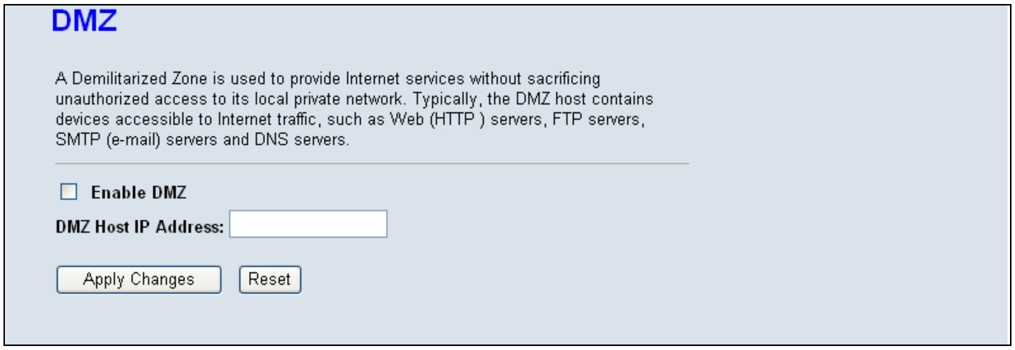
- **Source MAC Address** — Specifies a source MAC address.

- **Destination MAC Address** — Specifies a destination MAC address.

DMZ

DMZ enables a specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or videoconferencing, may not function properly behind the router's firewall. By specifying a Demilitarized Zone (DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned a static IP address.

Figure 59: DMZ Settings



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

□ **Enable DMZ**

DMZ Host IP Address:

The following items are displayed on this page:

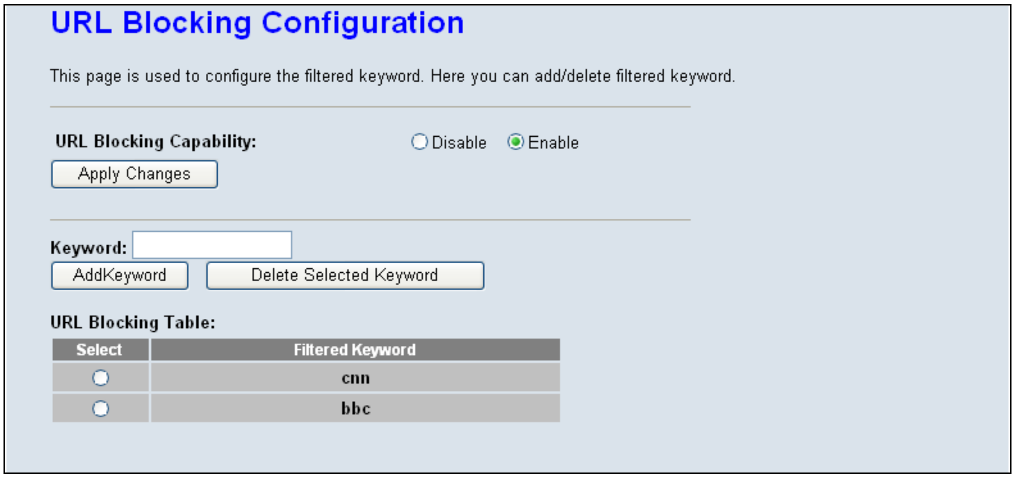
- **Enable DMZ** — Sets the DMZ status to enabled, but changes do not take affect until the Apply changes button has been pressed and changes are saved to the running configuration. (Default: disabled)

- **DMZ Host IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

URL BLOCKING

By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.

Figure 60: URL Blocking Settings



URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: ○ Disable ● Enable

Keyword:

URL Blocking Table:

Select	Filtered Keyword
○	cnn
○	bbc

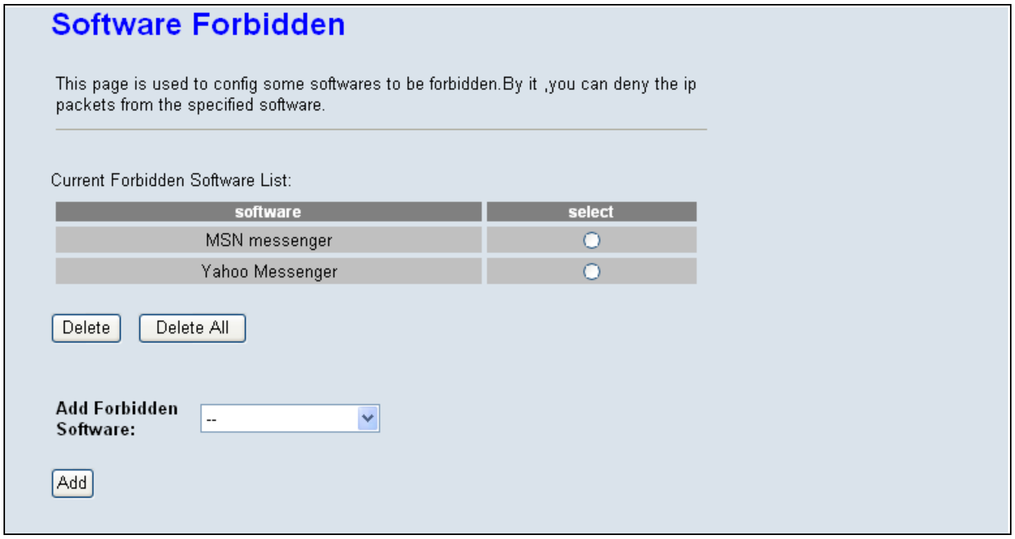
The following items are displayed on this page:

- **URL Blocking Capability** — Enables or disables URL blocking. (Default: Enabled)
- **Apply Changes** — Implements the selected URL blocking.
- **Keyword** — Specifies a string that traffic is to be blocked from. May be in the form of a text or number string with no spaces.
- **Add Keyword** — Adds a defined URL keyword to the blocking table.

SOFTWARE FORBIDDEN

The Software Forbidden page enables traffic from listed application software to be blocked by the router.

Figure 61: Software Forbidden Settings



Software Forbidden

This page is used to config some softwares to be forbidden.By it ,you can deny the ip packets from the specified software.

Current Forbidden Software List:

software	select
MSN messenger	○
Yahoo Messenger	○

Add Forbidden Software: --

The following items are displayed on this page:

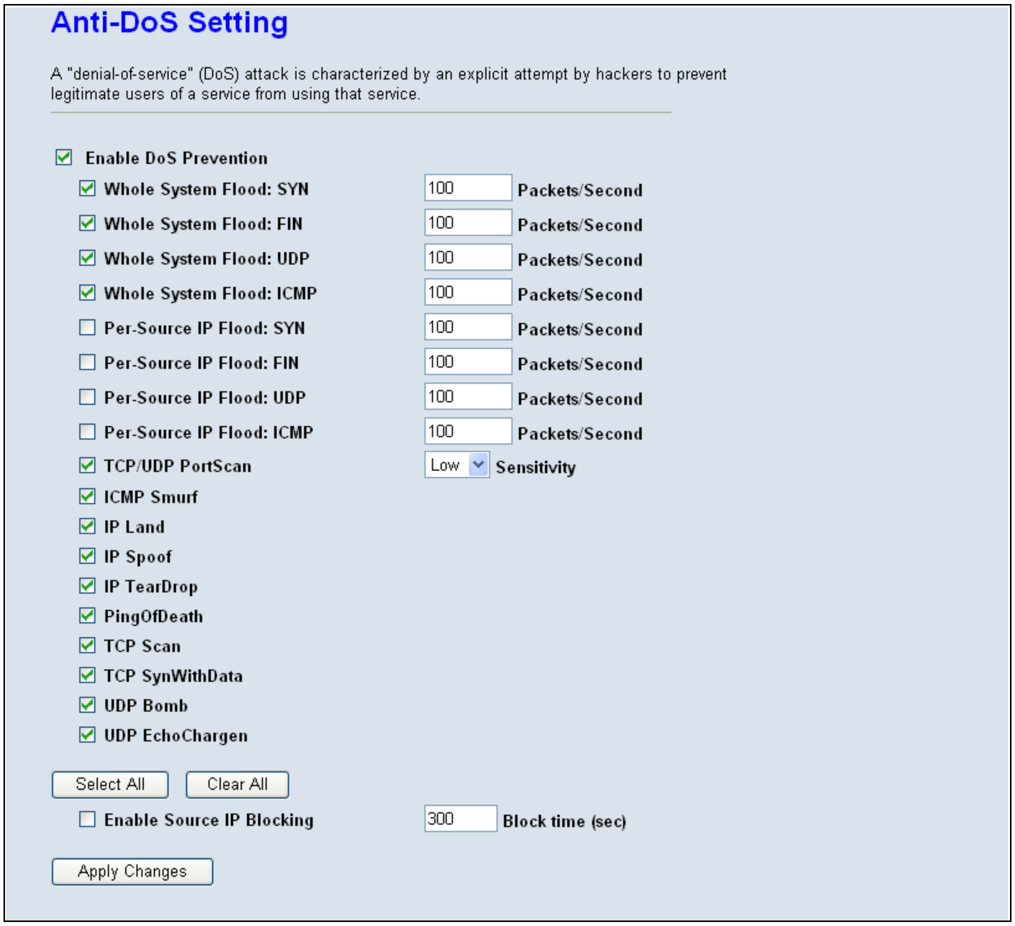
- **Current Forbidden Software List** — Software applications that are currently blocked by the router.
- **Add Forbidden Software** — Lists pre-defined software applications that can be added to the Forbidden Software table.

DoS

Denial of Service (DoS) is an attempt by a hacker to flood an IP address, domain, or server with repeated external communincation requests, effectively saturating the system with an information flood that renders it slow or effectively inoperable for genuine users to access it. DoS attacks are also referred to as non-intrusion attacks, the goal of which is to cripple your system but not steal data.

The DoS Settings on the router enable the user to block many of the common DoS attacks a network might suffer.

Figure 62: DoS Settings



Anti-DoS Setting

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☑ Enable DoS Prevention

☑ Whole System Flood: SYN	100	Packets/Second
☑ Whole System Flood: FIN	100	Packets/Second
☑ Whole System Flood: UDP	100	Packets/Second
☑ Whole System Flood: ICMP	100	Packets/Second
☐ Per-Source IP Flood: SYN	100	Packets/Second
☐ Per-Source IP Flood: FIN	100	Packets/Second
☐ Per-Source IP Flood: UDP	100	Packets/Second
☐ Per-Source IP Flood: ICMP	100	Packets/Second
☑ TCP/UDP PortScan	Low	Sensitivity
☑ ICMP Smurf		
☑ IP Land		
☑ IP Spoof		
☑ IP TearDrop		
☑ PingOfDeath		
☑ TCP Scan		
☑ TCP SynWithData		
☑ UDP Bomb		
☑ UDP EchoChargen		

☐ Enable Source IP Blocking 300 Block time (sec)

The following items are displayed on this page:

- **Enable DoS Blocking** — Activates the DoS check boxes and configurable parameters associated with them. (Default: Disabled)
  - **Whole System Flood: SYN:** Prevents a SYN (synchronise) attack in which the process of the common three way TCP handshake is interupted and the acknowledge response gets sent to a maicious IP address, or the system is flooded with false SYN requests.

- **Whole System Flood: FIN:** Prevents a FIN (no more data from sender) flood in which part of a TCP packet from an invalid (or spoofed) IP address floods the network with connection resets.
- **Whole System Flood: UDP:** Prevents a flood of large numbers of raw UDP (User Datagram Protocol) packets targeted at the unit.
- **Whole System Flood: ICMP:** Prevents a flood of ICMP (internet control message protocol) messages from an invalid IP address causing all TCP requests to be halted.
- **Per Source IP Flood: SYN:** Prevents a SYN attach on a specified IP address, usually that of the LAN port.
- **Per Source IP Flood: FIN:** Prevents a FIN attach on the LAN port IP address.
- **Per Source IP Flood: UDP:** Prevents a UDP attack on the LAN port IP address.
- **Per Source IP Flood: ICMP:** Prevents an ICMP attack on the LAN port IP address.
- **TCP/UDP Port Scan:** Prevents a situation whereby a hacker sends a series of systematic queries to the unit for open ports through which to route traffic.
- **TCMP Smurf:** Prevents a situation whereby a hacker forges the IP address of the unit and sends repeated ping requests to it flooding the network.
- **IP Land:** Prevents an attack that involves a synchronise request being sent as part of the TCP handshake to an open port specifying the port as both the source and destination effectively locking the port.
- **IP Spoof:** Prevents a situation where a hackerby a hacker creates an alias (spoof) of the units IP address to which all traffic is redirected.
- **IP Teardrop:** Prevents a Teardrop attack that involves sending mangled IP fragments with overlapping, over-sized, payloads to the unit. The fragmented packets are processed by the unit causing it to crash.
- **PingofDeath:** Prevents the receival of an oversized ping packet that the unit cannot handle. Normal ping packets are 56 bytes, or 84 bytes with the IP header attached. The Ping of Death will exceed the maximum IP packet size of 65,535 bytes.
- **TCP Scan:** Prevents the probing of the unit by a hacker for open TCP ports to then block.

- **TCP SynWithData:** Prevents the hacker sending a volume of requests for connections that cannot be completed.
- **UDP Bomb:** Also called a UDP Flood or packet storm. Prevents the hacker congesting the network by generating a flood of UDP packets between it and the unit using the UDP chargen service (a testing utility that generates a character string for every packet it receives).
- **UDP EchoChargen:** Prevents the hacker from sending a UDP packet to the echo server with a source port set to the chargen port.
- **packets/second:** Enter the number of packets per second that you want to scan for malicious activity.
- **Sensitivity:** Specifies the sensivity of the TCP/UDP port scan prevention. (Options: High, Low; Default: Low)

- **Select All** — Selects all DoS prevention measures listed.
- **Clear All** — Clears all fields.
- **Enable Source IP Blocking** — When multiple attacks are detected from each of the fields listed above, or the packet threshold has been exceeded - the IP address of the hacker is blocked.
- **Block Time (sec)** — Sets the length of time in seconds the IP address should remain blocked.

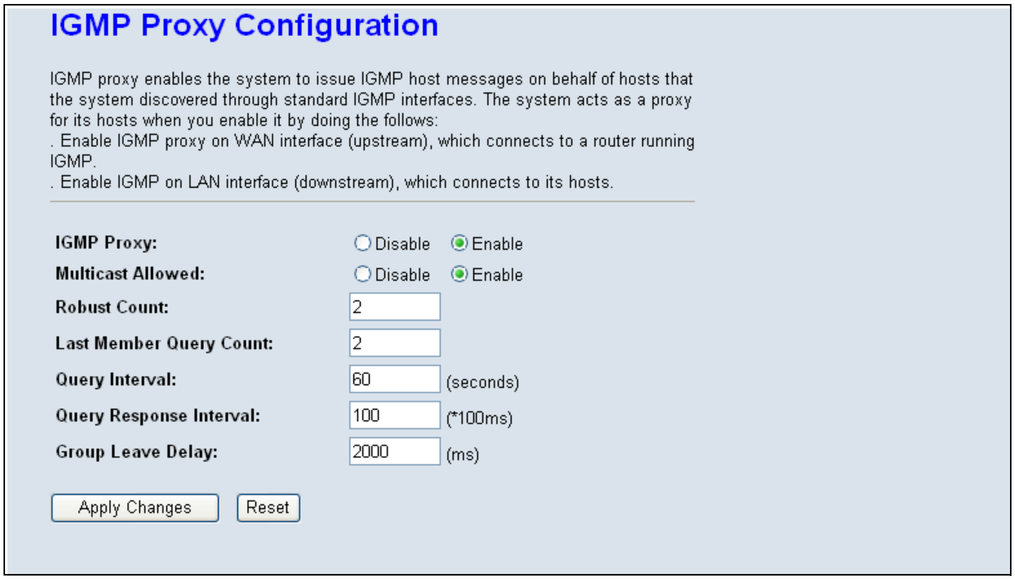
IGMP PROXY CONFIGURATION

Multicasting is useful when the same data needs to be sent to more than one host. Using multicasting as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. This device supports IGMP proxy that handles IGMP messages. When enabled, this device acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast group on the WAN side.

When you enable IGMP Proxy, make sure IGMP is also enabled on the WAN interface (upstream) that connects to a router running IGMP. You must also enable IGMP on the LAN interface (downstream) that is connected to hosts.

Figure 63: IGMP Proxy Configuration



IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:
. Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
. Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	○ Disable ● Enable	
Multicast Allowed:	○ Disable ● Enable	
Robust Count:	2	
Last Member Query Count:	2	
Query Interval:	60	(seconds)
Query Response Interval:	100	(*100ms)
Group Leave Delay:	2000	(ms)

The following items are displayed on this pages:

- **IGMP Proxy** — Enables IGMP proxy. When enabled, the upstream interface acts as a host interface, sending query messages periodically to the downstream interfaces, sending join and leave messages to the upstream multicast router when a first join or last leave message is received from a downstream interface, and sending membership reports in response to query messages from the multicast router.

- **Multicast Allowed** — Enables multicast forwarding. (Default: Enabled)

- **Robustness Count** — Specifies the robustness (or expected packet loss) for interfaces. The robustness value is used in calculating the appropriate range for other IGMP variables. (Range: 1-255; Default: 2)

- **Last Member Query Count** — The number of query messages sent before the router determines that there are no remaining members of the specific host group being queried on the interface. (Range: 1-255; Default: 2)

- **Query Interval** — The interval between sending IGMP general queries. (Range: 2-31744 seconds; Default: 60 seconds)

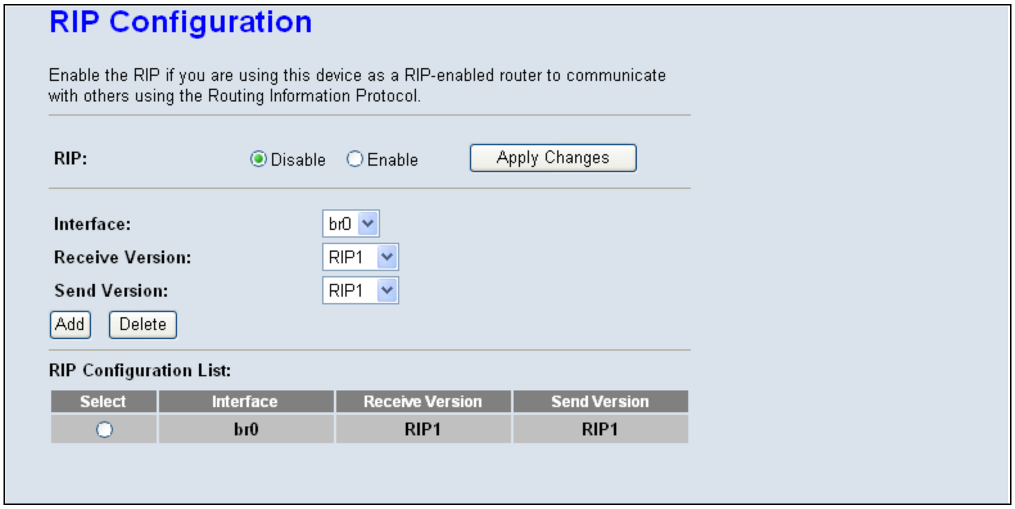
- **Query Response Interval** — The maximum time the system waits for a response to general queries. (Range: 10-31744 tenths of a second; Default: 10 seconds)

- **Group Leave Delay** — The time duration it takes a device to stop forwarding multicast frames after an IGMP Leave Group message has been successfully sent to the device. (Default: 2000 ms)

RIP CONFIGURATION

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Most small home or office networks do not need to use RIP; they have only one router, such as the router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

Figure 64: RIP Configuration



RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

RIP: ● Disable ○ Enable

Interface: br0

Receive Version: RIP1

Send Version: RIP1

RIP Configuration List:

Select	Interface	Receive Version	Send Version
○	br0	RIP1	RIP1

The following items are displayed on this pages:

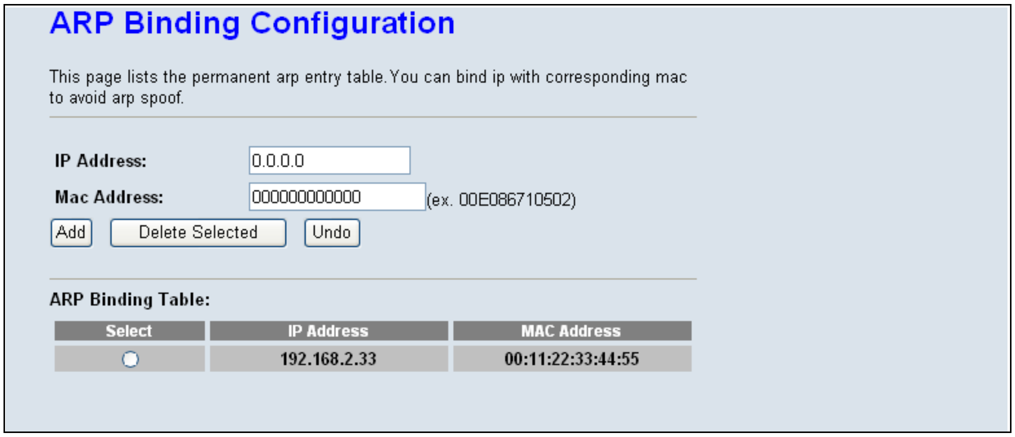
- **RIP** — Enables or disables RIP on the unit. (Default: Disabled)
- **Interface** — The name of the interface on which you want to enable RIP. (Default: br0)
- **Receive Version** — Indicate the RIP version in which information must be passed to the DSL device in order for it to be accepted into its routing table.
- **Send Version** — Indicate the RIP version this interface will use when it sends its route information to other devices.

ARP BINDING CONFIGURATION

The router uses its tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer MAC address. When an IP frame is received by the router, it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to its final destination.

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a MAC address. If this occurs, you can use ARP Binding to manually map an IP address to the corresponding MAC address in the ARP cache.

Figure 65: ARP Binding Configuration



ARP Binding Configuration

This page lists the permanent arp entry table. You can bind ip with corresponding mac to avoid arp spoof.

IP Address: 0.0.0.0

Mac Address: 000000000000 (ex. 00E086710502)

ARP Binding Table:

Select	IP Address	MAC Address
○	192.168.2.33	00:11:22:33:44:55

The following items are displayed on this pages:

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods, and must match a known network interface)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xxxxxxxxxxxx)

9 ADVANCED

The Advanced Configuration settings for the ADSL Router contain advanced system management configuration settings.

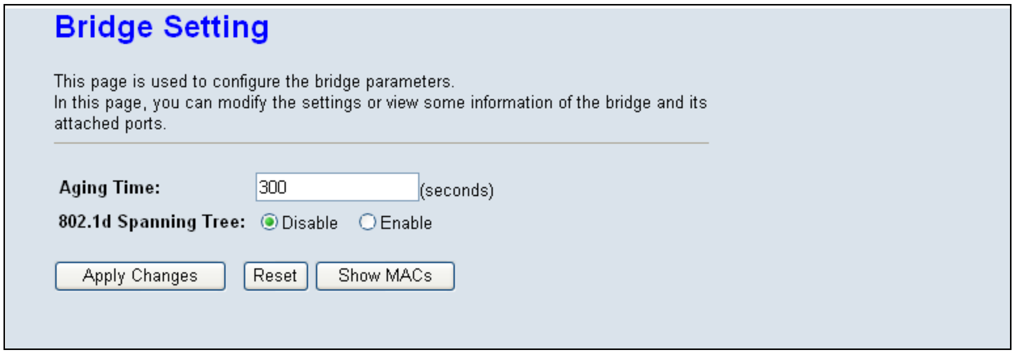
The following sections are contained in this chapter:

BRIDGE SETTING

This feature allows you to set the bridge aging time and to enable Spanning Tree.

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between bridges. This allows a wireless bridge to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Figure 66: Bridge Setting



Bridge Setting

This page is used to configure the bridge parameters.
In this page, you can modify the settings or view some information of the bridge and its attached ports.

Aging Time: 300 (seconds)

802.1d Spanning Tree: ● Disable ○ Enable

The following items are displayed on this page:

- **Ageing Time** — Sets the MAC address ageing time, in seconds. After the aging time has been reached with no traffic received, the unit will delete the address from the forwarding database. (Default: 300 seconds)

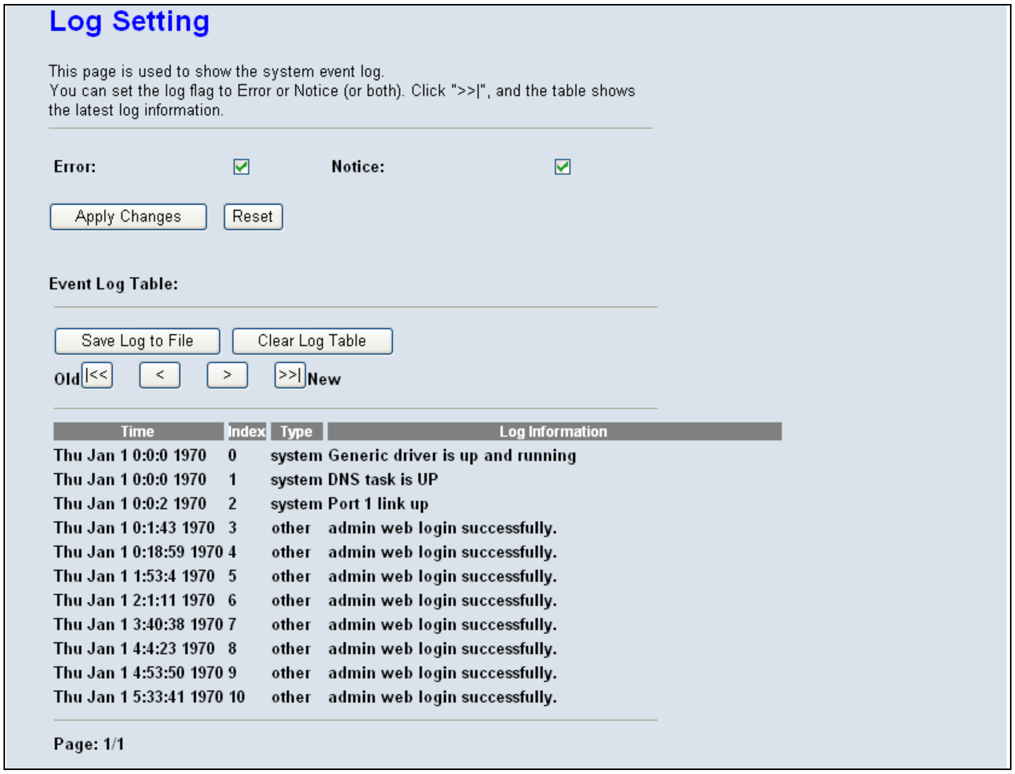
- **802.1d Spanning Tree** — Enables/disables the Spanning Tree Protocol on the ADSL Router. (Default: Disabled)

LOG SETTING

The ADSL Router supports a logging process that controls error messages saved to memory. The logged messages serve as a valuable tool for isolating ADSL Router and network problems.

The Log Setting page displays the latest messages logged in chronological order. Log messages saved in the ADSL Router's memory are erased when the device is rebooted.

Figure 67: Log Setting



Log Setting

This page is used to show the system event log.
You can set the log flag to Error or Notice (or both). Click ">>|", and the table shows the latest log information.

Error: ☑ Notice: ☑

Event Log Table:

Time	Index	Type	Log Information
Thu Jan 1 0:0:0 1970	0	system	Generic driver is up and running
Thu Jan 1 0:0:0 1970	1	system	DNS task is UP
Thu Jan 1 0:0:2 1970	2	system	Port 1 link up
Thu Jan 1 0:1:43 1970	3	other	admin web login successfully.
Thu Jan 1 0:18:59 1970	4	other	admin web login successfully.
Thu Jan 1 1:53:4 1970	5	other	admin web login successfully.
Thu Jan 1 2:1:11 1970	6	other	admin web login successfully.
Thu Jan 1 3:40:38 1970	7	other	admin web login successfully.
Thu Jan 1 4:4:23 1970	8	other	admin web login successfully.
Thu Jan 1 4:53:50 1970	9	other	admin web login successfully.
Thu Jan 1 5:33:41 1970	10	other	admin web login successfully.

Page: 1/1

The following items are displayed on this page:

- **Error:** Selects the Error level of messages to be displayed by the ADSL Router.
- **Notice:** Selects the Notice level of messages to be displayed by the ADSL Router.
- **Save Log to File** — Saves the currently recorded system logs to file.
- **Clear Log Table** — Clears the system log table.
- **Old/New** — Displays the previous or next page of log entries.

EVENT LOG TABLE

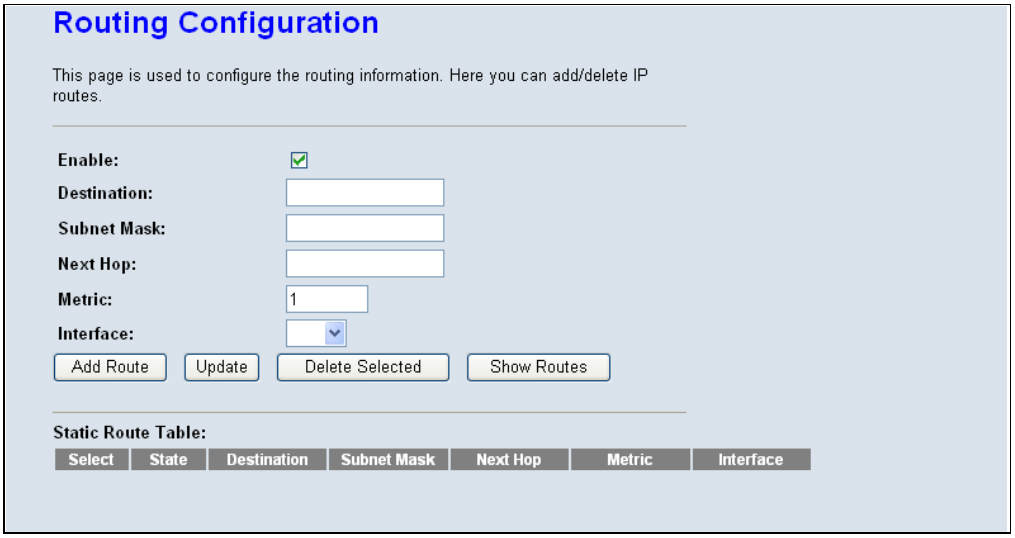
Displays the current entries in the System Log table.

- **Time** — Displays the date and time the log entry was created.
- **Index** — The number of the log entry.
- **Type** — Displays the source of the log message.
- **Log Information** — Information that identifies the cause of the event that prompted the system log message.

ROUTING CONFIGURATION

This page displays the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

Figure 68: Routing Configuration



Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	1
Interface:	

Static Route Table:

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

The following items are displayed on this page:

- **Enable** — Enables static routing on the ADSL Router. (Default: Enabled)
- **Destination** — The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined.

- **Subnet Mask** — The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
- **Next Hop** — The IP address of the next hop through which traffic will flow towards the destination subnet.
- **Metric** — Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
- **Interface** — The WAN interface to which a static routing subnet is to be applied.
- **Add Route** — Adds a static route to the Static Route Table.
- **Update** — Clears the above fields.
- **Delete Selected** — Deletes the specified static route.

STATIC ROUTE TABLE

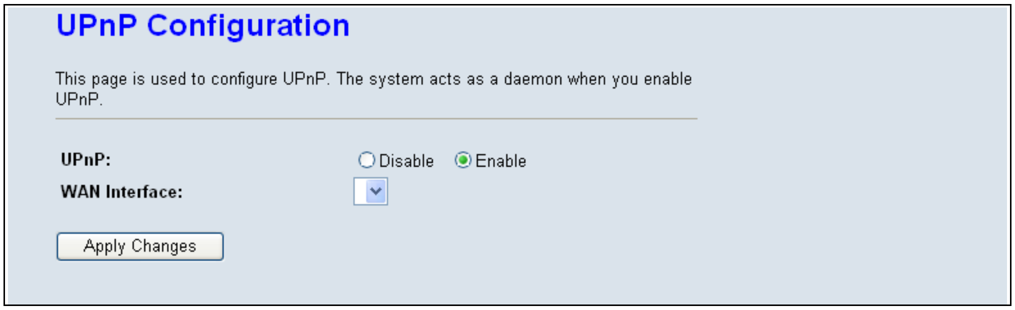
This table displays all the configured static routes.

- **Select** — Highlights an entry in the Static Route Table.
- **State** — Displays if the route is enabled or disabled.
- **Destination** — Displays the final destination of the routed packets.
- **Subnet Mask** — Displays the subnet mask.
- **Next Hop** — The next hop that the packets will be routed to on their way to their final destination.
- **Metric** — Displays the number of hops from router to router that the packets must make before reaching their final destination.
- **Interface** — Displays the interface the packets will be routed on.

UPNP

UPnP (Universal Plug and Play) provides inter-connectivity between devices supported by the same standard. UPnP is based on standard Internet protocols, such as TCP/IP, UDP, and HTTP.

Figure 69: UPnP



UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPnP: ○ Disable ● Enable

WAN Interface:

The following items are displayed on this page:

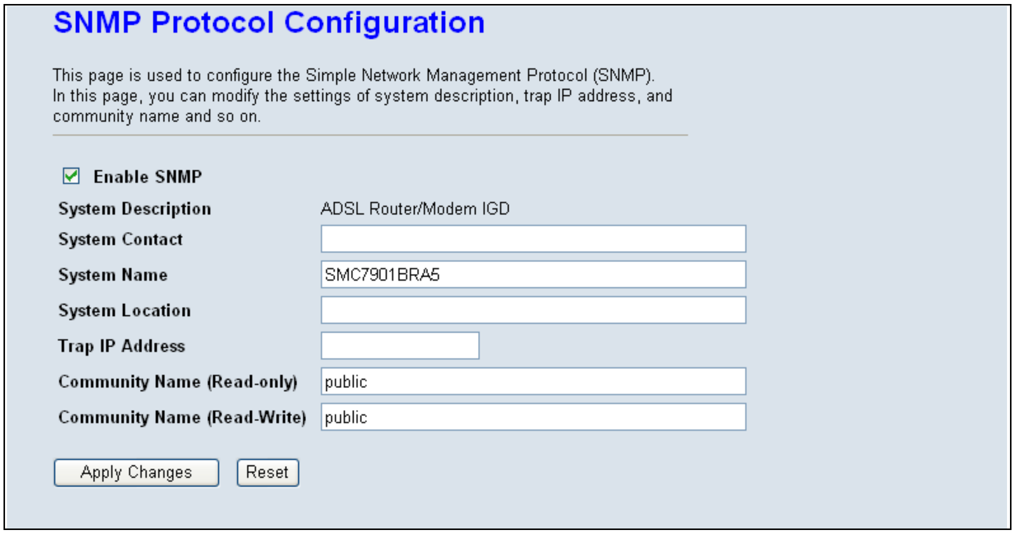
- **UPnP** — Enables UPnP on the ADSL Router. (Default: Enabled)
- **WAN Interface** — Selects the WAN interface for the UPnP service.

SNMP PROTOCOL CONFIGURATION

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. SNMP is typically used to configure devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The ADSL Router can be managed locally or remotely by SNMP.

Figure 70: SNMP Configuration



SNMP Protocol Configuration

This page is used to configure the Simple Network Management Protocol (SNMP). In this page, you can modify the settings of system description, trap IP address, and community name and so on.

☑ Enable SNMP

System Description	ADSL Router/Modem IGD
System Contact	
System Name	SMC7901BRA5
System Location	
Trap IP Address	
Community Name (Read-only)	public
Community Name (Read-Write)	public

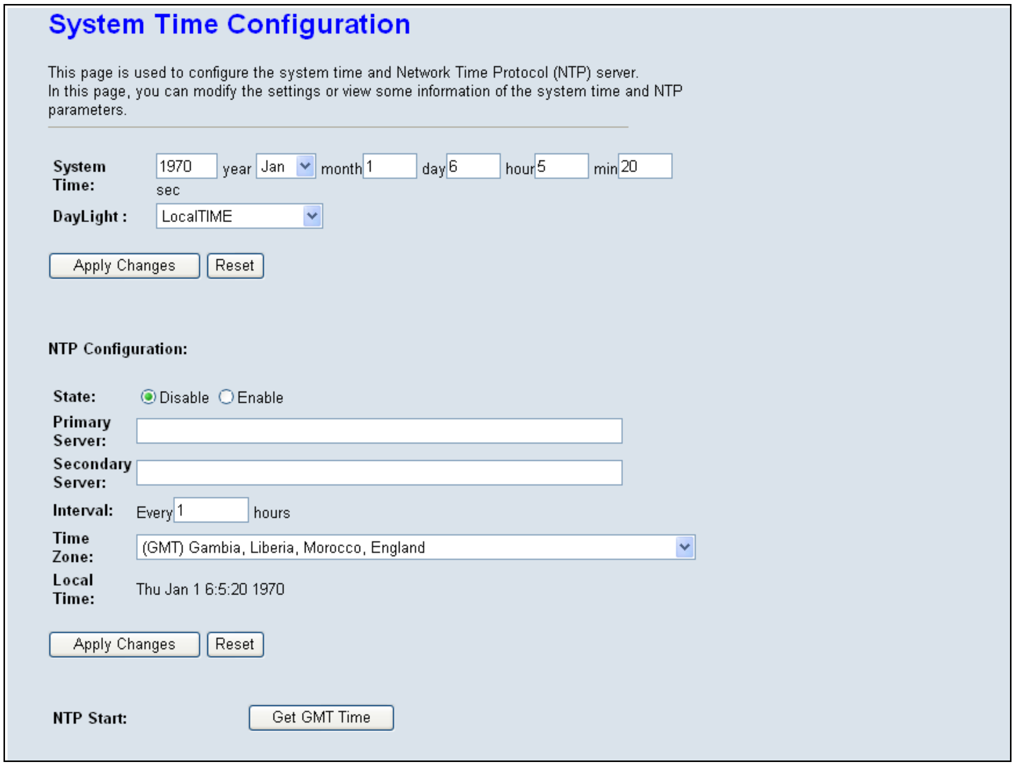
The following items are displayed on this pages:

- **SNMP** — Enables/disables SNMP. (Default: Enabled)
- **System Description** — A name given to identify the ADSL Router.
- **System Contact** — The name of the system contact person.
- **System Name** — A description of the unit. (Default: Wireless ADSL Modem/Router)
- **System Location** — The location of the ADSL Router.
- **Trap IP Address** — Destination IP address of the SNMP trap.
- **Community Name (Read-only)** — Name of the read-only community. This read-only community allows read operation to all objects in the Management Information Base (MIB).
- **Community Name (Read-Write)** — Name of the write-only community. This write-only community allows write operations to objects defined as read-writable in the MIB.

SYSTEM TIME CONFIGURATION

The System Time page allows you to manually configure time settings or enable the use of an NTP server.

Figure 71: System Time Configuration



System Time Configuration

This page is used to configure the system time and Network Time Protocol (NTP) server. In this page, you can modify the settings or view some information of the system time and NTP parameters.

System Time: 1970 year Jan month 1 day 6 hour 5 min 20 sec

DayLight : LocalTIME

NTP Configuration:

State: ● Disable ○ Enable

Primary Server:

Secondary Server:

Interval: Every 1 hours

Time Zone: (GMT) Gambia, Liberia, Morocco, England

Local Time: Thu Jan 1 6:5:20 1970

NTP Start:

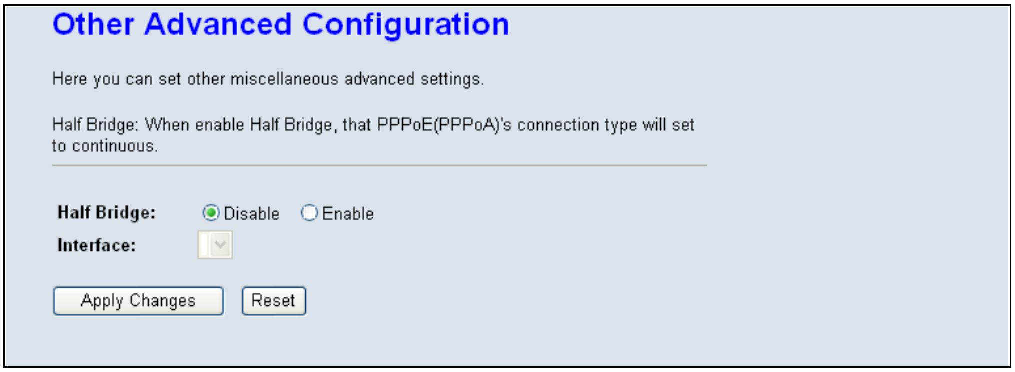
The following items are displayed on this page:

- **System Time** — Displays the current date and time and allows you to manually configure time settings.
- **DayLight** — Enables daylight saving time to be configured.
- **State** — Enables NTP (Network Time Protocol). (Default: Disabled)
- **Primary/Secondary Server** — Specifies NTP servers to poll for time updates.
- **Interval** — Specifies the interval to poll for time updates.
- **Time Zone** — Allows you to select your current location or nearest city. All time zones are given in Greenwich Mean Time (GMT).
- **Local Time** — Displays the current date and time and allows you to manually configure time settings.
- **NTP Start** — Initiates a time update from an NTP server.

OTHER ADVANCED CONFIGURATION

Enables the Half Bridge feature for PPPoE (PPPoA) connections. When the router is set to Half Bridge, it establishes the PPPoE/PPPoA connection with the ISP, then forwards all other traffic to DHCP clients connected to the router.

Figure 72: Other Advanced Configuration



Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to continuous.

Half Bridge: ● Disable ○ Enable

Interface:

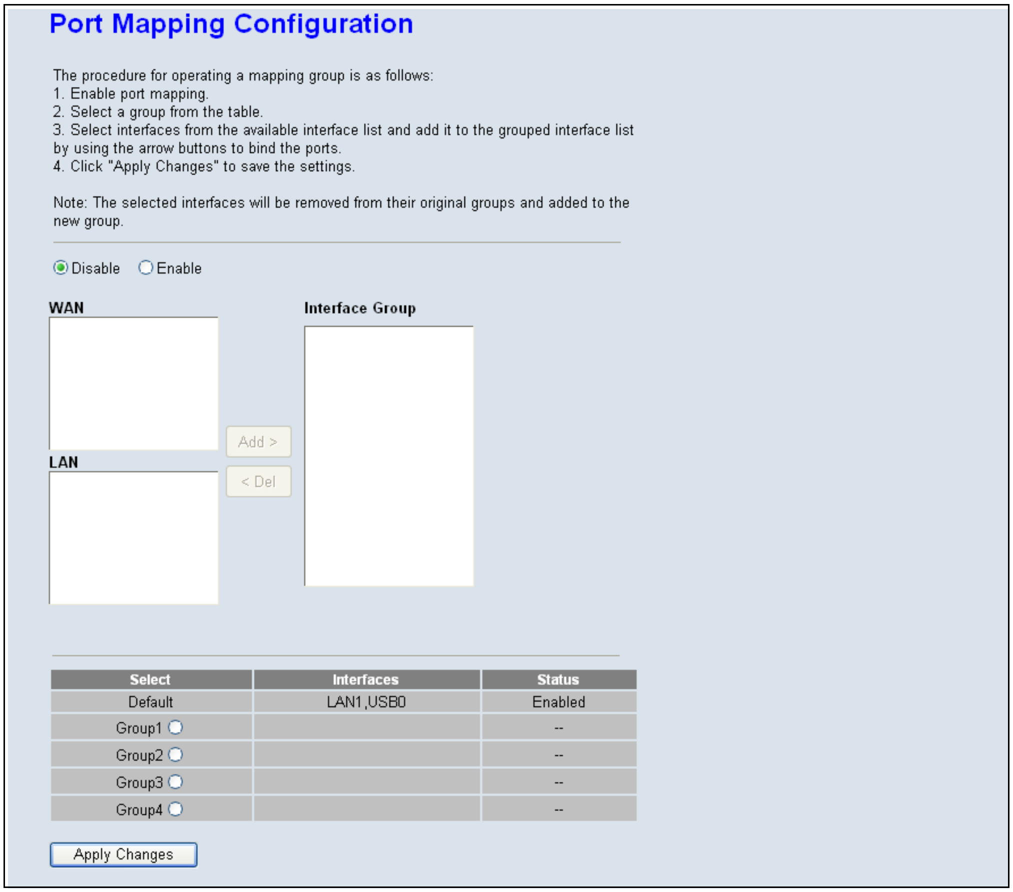
The following items are displayed on this page:

- **Half Bridge** — Displays the current date and time and allows you to manually configure time settings.
- **Interface** — Selects the WAN interface for the Half Bridge feature.

PORT MAPPING

Port Mapping supports multiple ports to WAN interfaces and bridging groups. Each group performs as an independent network. You can create up to four groups on the router.

Figure 73: Port Mapping Configuration



Port Mapping Configuration

The procedure for operating a mapping group is as follows:
1. Enable port mapping.
2. Select a group from the table.
3. Select interfaces from the available interface list and add it to the grouped interface list by using the arrow buttons to bind the ports.
4. Click "Apply Changes" to save the settings.

Note: The selected interfaces will be removed from their original groups and added to the new group.

● Disable ○ Enable

Select	Interfaces	Status
Default	LAN1,USB0	Enabled
Group1 ○		--
Group2 ○		--
Group3 ○		--
Group4 ○		--

The following items are displayed on this page:

- **WAN** – The WAN interfaces that can be grouped.
- **LAN** – The LAN interfaces that can be grouped.
- **Interfaces Group** — The grouped WAN and LAN interfaces.
- **Apply Changes** — Sets the Interfaces Group as the selected group in the table.

10 Diagnostics

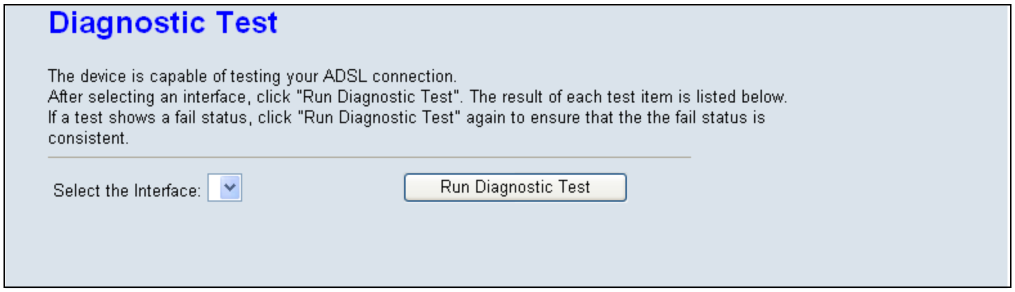
The Diagnostics page is used to test the local Ethernet connection, or the WAN connection for the DSL signal and the connection to DSL provider network.

This chapter contains the following sections:

DIAGNOSTIC TEST

The diagnostic test shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

Figure 74: Diagnostic Test



Diagnostic Test

The device is capable of testing your ADSL connection.
After selecting an interface, click "Run Diagnostic Test". The result of each test item is listed below.
If a test shows a fail status, click "Run Diagnostic Test" again to ensure that the the fail status is consistent.

The following items are displayed on this page:

- **Select the Interface** — Selects the WAN connection. (Default: vc0)
- **Run Diagnostic Test** — Performs a diagnostic test on the LAN and WAN side connections.

LAN CONNECTION CHECK

Displays the result of a test for connectivity on the LAN port.

- **Test Ethernet LAN Connection** — Displays the connectivity of the Ethernet LAN port.

ADSL CONNECTION TEST

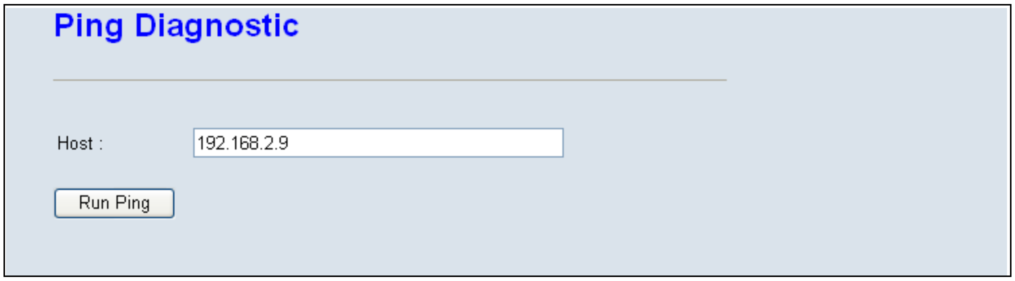
Displays the results of a test for connectivity on the WAN port.

- **Test ADSL Synchronization** — Displays the connectivity of the ADSL synchronisation.
- **Test ATM OAM F5 Segment Loopback** — Displays the connectivity of an F5 segment loopback of the permanent virtual circuit (PVC) connection with your service provider.
- **Test ATM OAM F5 End-to-end Loopback** — Displays the connectivity of an F5 end-to-end loopback integrity test of the permanent virtual circuit (PVC) connected to your service provider.
- **Test ATM OAM F4 Segment Loopback** — Displays the connectivity of an F4 segment loopback of the permanent virtual circuit (PVC) connection with your service provider.
- **Test ATM OAM F4 End-to-end Loopback** — Displays the connectivity of an F4 end-to-end loopback integrity test of the permanent virtual circuit (PVC) connected to your service provider.

PING

The ADSL Router provides the function of “pinging” its own IP address or URL to test for connectivity.

Figure 75: Ping



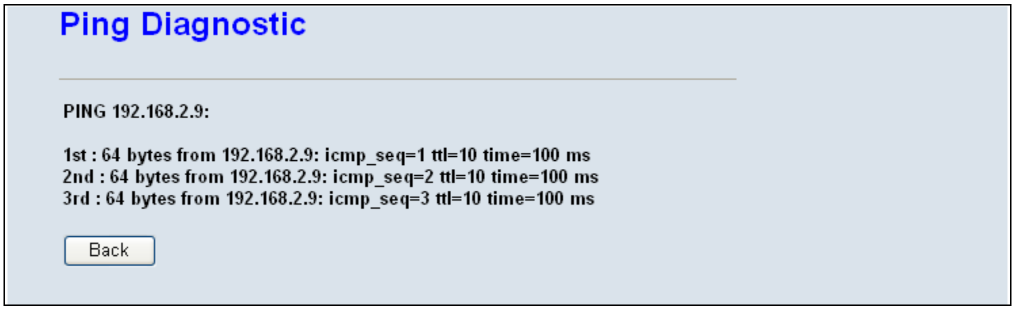
Ping Diagnostic

Host : 192.168.2.9

The following items are displayed on this page:

- **Host** — The host IP address or URL to test for connectivity.
- **Run Ping** — Sends the ping request, resulting in the the following page:

Figure 76: Ping Result



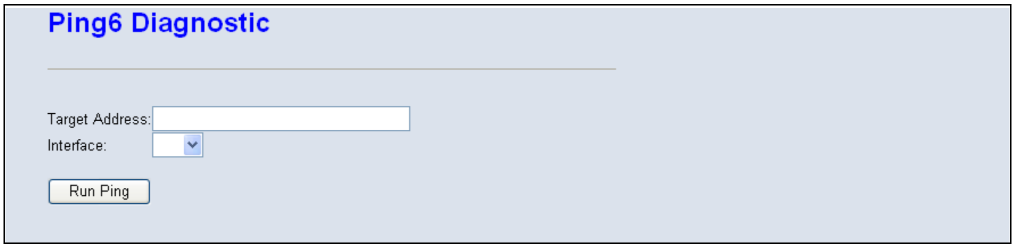
Ping Diagnostic

```
PING 192.168.2.9:

1st : 64 bytes from 192.168.2.9: icmp_seq=1 ttl=10 time=100 ms
2nd : 64 bytes from 192.168.2.9: icmp_seq=2 ttl=10 time=100 ms
3rd : 64 bytes from 192.168.2.9: icmp_seq=3 ttl=10 time=100 ms
```

PING6

The ADSL Router can also ping IPv6 addresses on specific interfaces to test for connectivity.

Figure 77: Ping6



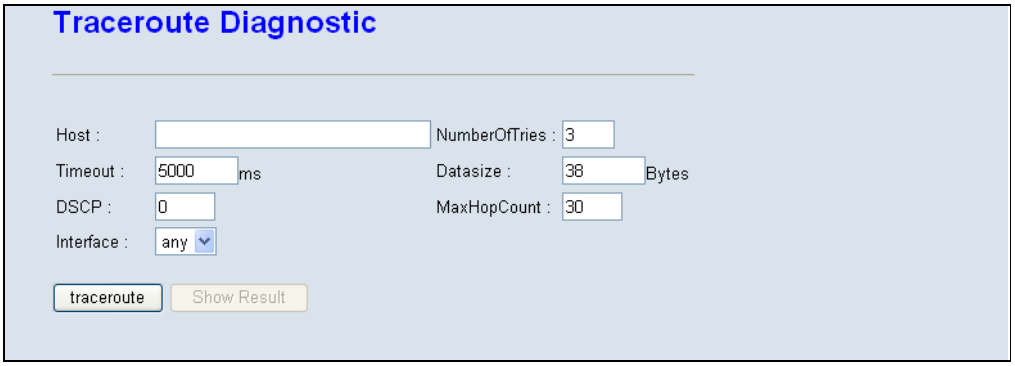
Ping6 Diagnostic

TRACEROUTE

Traceroute discovers the routes that packets take when traveling to a destination. Traceroute works by taking advantage of the error messages generated by routers when a packet exceeds its time-to-live (TTL) value.

The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the roundtrip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device. A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

Figure 78: Traceroute



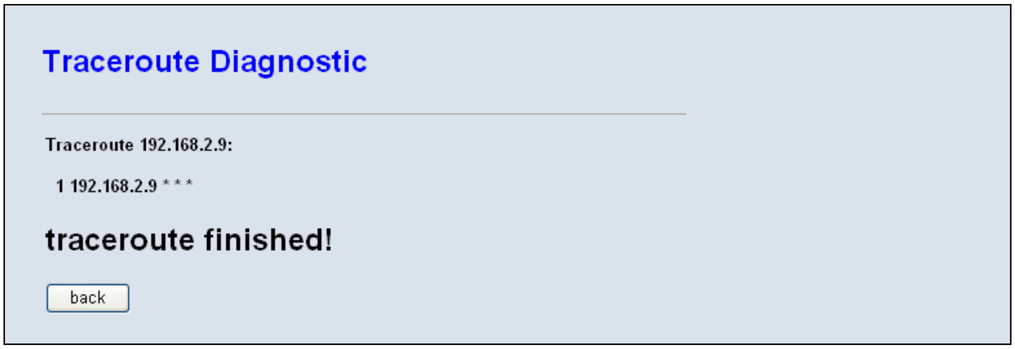
Traceroute Diagnostic

Host :
NumberOfTries : 3
Timeout : 5000 ms
Datasize : 38 Bytes
DSCP : 0
MaxHopCount : 30
Interface : any

The following items are displayed on this page:

- **Host** — The IP address of the destination host.
- **Number of Tries** — The number of datagrams to be sent at each TTL level. The default count is 3. (Range: 1–10)
- **Timeout** — The number of seconds to wait for a response to a probe packet. The default is 5000 ms. (Range: 1–65535)
- **Datasize** — Number of bytes in the packet. The default is 38 bytes. (Range: 64-1518)
- **DSCP** — The DSCP value in the IP Header of the packet. (Range: 0-63)
- **Max Hop Count** — The largest TTL value that can be used. The traceroute terminates when the destination is reached or when this value is reached. The default is 30. (Range: 1–255)
- **Interface** — Selects the interface on which to run the traceroute.

Figure 79: Traceroute Result



Traceroute Diagnostic

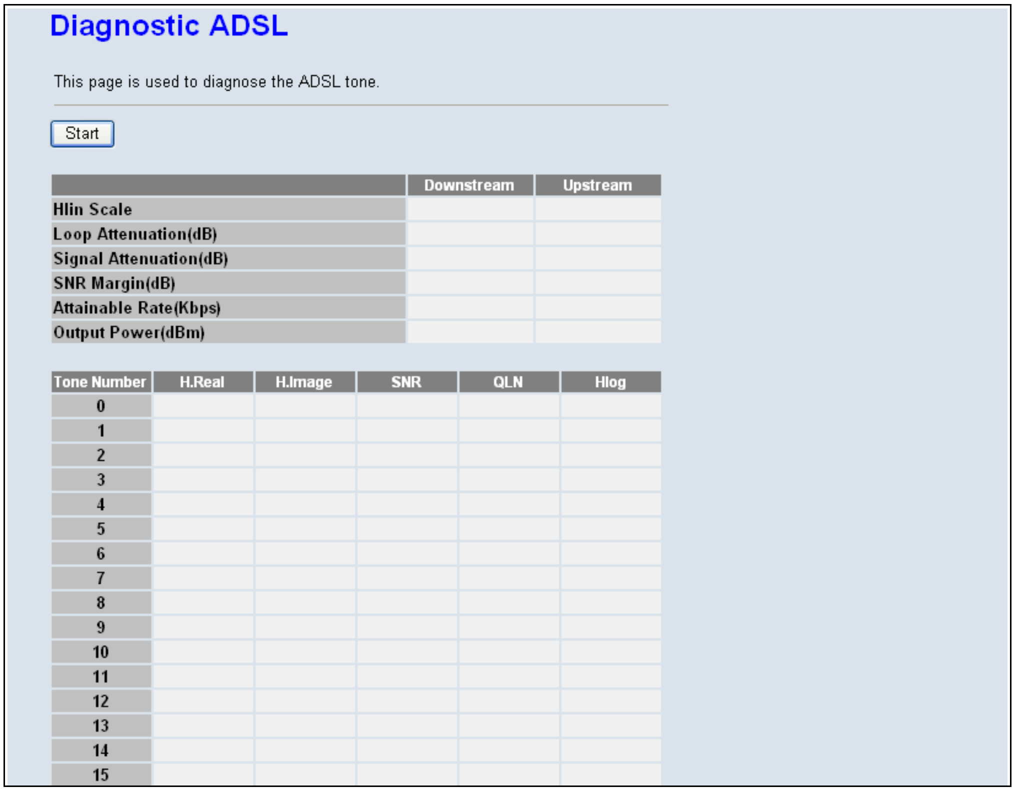
```
Traceroute 192.168.2.9:

 1 192.168.2.9 * * *
```

traceroute finished!

ADSL TONE DIAGNOSTICS

The ADSL page displays diagnostic testing for the ADSL connection.

Figure 80: ADSL Tone Diagnostics



Diagnostic ADSL

This page is used to diagnose the ADSL tone.

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

The following items are displayed on this page:

- **Start** — Starts the diagnostics test.
- **Downstream/Upstream** — Displays downstream and upstream traffic.
- **Hlin Scale** — Displays the scaling factor for H.Real and H.Image represented in fixed-point format.
- **Loop Attenuation (dB)** — Displays the attentuation of the link to the ADSL Router and the service provider in decibels.
- **Signal Attenuation (dB)** — Displays the signal attentuation of the link which determines the frequency in decibels.
- **SNR Margin (dB)** — Displays the signal-to-noise ratio of the link in dedibels.
- **Attainable Rate (Kbps)** — Displays the attainable rate of the link to the service provider in kilobits per second.

- **Output Power (dBm)** — Displays the output power of the unit in decibels per milliwatt.
- **Tone Number** — Displays the tone number of the ADSL signal. (Range: 0~255)
- **H.Real** — Displays the real part of channel transfer function of each subcarrier.
- **H.Image** — Displays the imaginary part of channel transfer function of each subcarrier.
- **SNR** — Displays the SNR (Singal to Noise Ratio) of each subcarrier expressed in decibels.
- **QLN** — Displays the Quite Line Noise of each subcarrier, expressed in dBm/Hz.
- **Hlog** — Displays the amplitude response of channel transfer function of each subcarrier, expressed in decibels.

11 Administration Settings

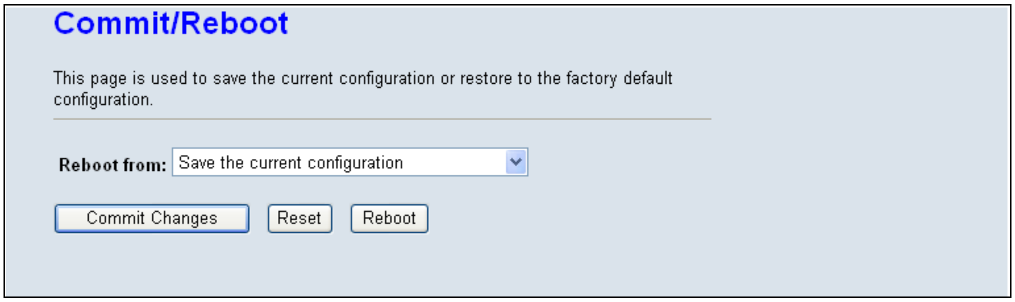
The Admin pages are used to manage configuration files, system logs, TR-069 ACS, passwords; and also to update software and reboot the system.

This chapter contains the following sections:

COMMIT/REBOOT

Use this page to save the current configuration and reboot the system.

Figure 81: Commit/Reboot



Commit/Reboot

This page is used to save the current configuration or restore to the factory default configuration.

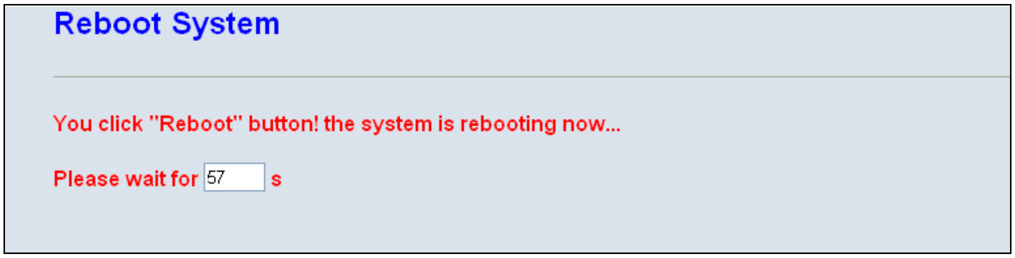
Reboot from: Save the current configuration

The following items are displayed on this page:

- **Reboot from** — Select the option for router's configuration:
  - **Save the current configuration** — Select this option if you want to save your changes for the next reboot.
  - **Restore to the factory default configuration** — Select this option if you want to return all changes to default values.
- **Commit Changes** — Sets the selected configuration option.
- **Reset** — Resets the selected option on the page.
- **Reboot** — Restarts the router.

When rebooting the system the following page displays and a countdown from 64 seconds begins.

Figure 82: Rebooting



Reboot System

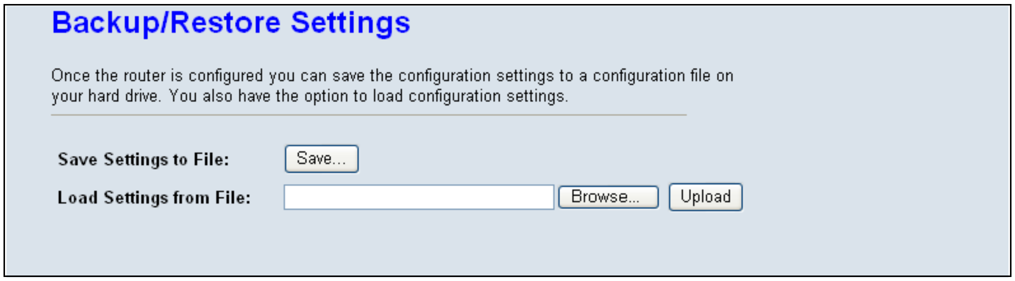
You click "Reboot" button! the system is rebooting now...

Please wait for 57 s

BACKUP/RESTORE SETTINGS

The Backup/Restore Settings page allows you to backup current settings to a local file, and load previously saved settings to the unit.

Figure 83: Backup/Restore Settings



Backup/Restore Settings

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.

The following items are displayed on this page:

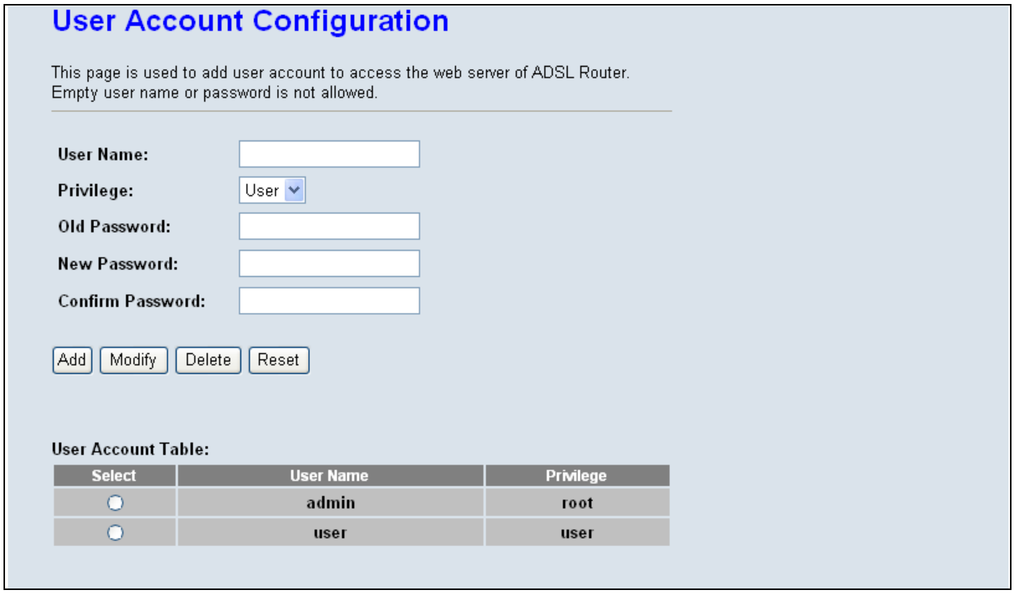
- **Save Settings to File** — Saves the current configuration to a file locally on the management PC.
- **Load Settings from File** — Allows the user to load previously saved configuration files from a local file on the management PC.

PASSWORD SETUP

Management access to the ADSL Router is controlled through different levels of user name and password.

To protect access to the management interface, you need to configure a new Administrator's password as soon as possible. If a new password is not configured, then anyone having access to the ADSL Router may be able to compromise the unit's security by entering the default values.

Figure 84: Password Setup



User Account Configuration

This page is used to add user account to access the web server of ADSL Router.
Empty user name or password is not allowed.

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

User Account Table:

Select	User Name	Privilege
○	admin	root
○	user	user

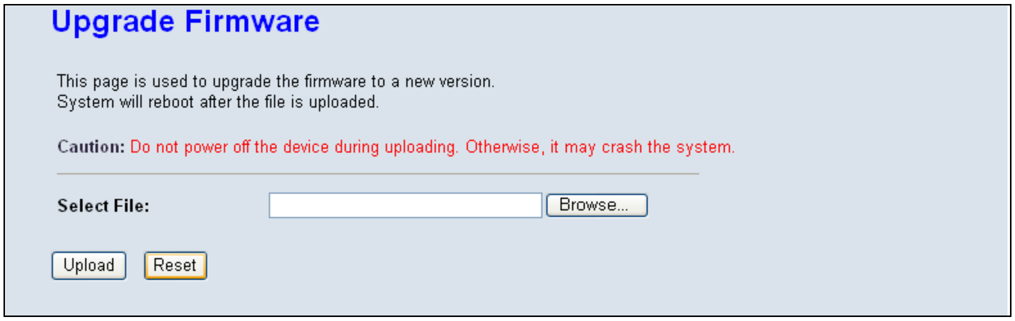
The following items are displayed on this page:

- **User Name** — Specifies the user name to configure:
- **Privilege** — Configures the access privileges that the user has. Select between:
  - **Admin:** Grants administrator level access, no restrictions.
  - **User:** Grants user level access, some configuration restrictions.
- **Old Password** — The password for management access. The default passwords preset for access to the unit is "smcadmin" for admin and user level. (Length: 3-16 characters, case sensitive)
- **New Password** — Enter a new password.
- **Confirmed Password** — Enter the new password again for verification.

UPGRADE FIRMWARE

You can update the ADSL Router's firmware by using the Upgrade Firmware facility which allows you to upload new firmware manually by specifying a file path. Make sure the firmware file you want to use is on the local computer by clicking Browse to search for the file to be used for the update.

Figure 85: Upgrade Firmware



Upgrade Firmware

This page is used to upgrade the firmware to a new version.
System will reboot after the file is uploaded.

Caution: Do not power off the device during uploading. Otherwise, it may crash the system.

Select File:

The following items are displayed on this page:

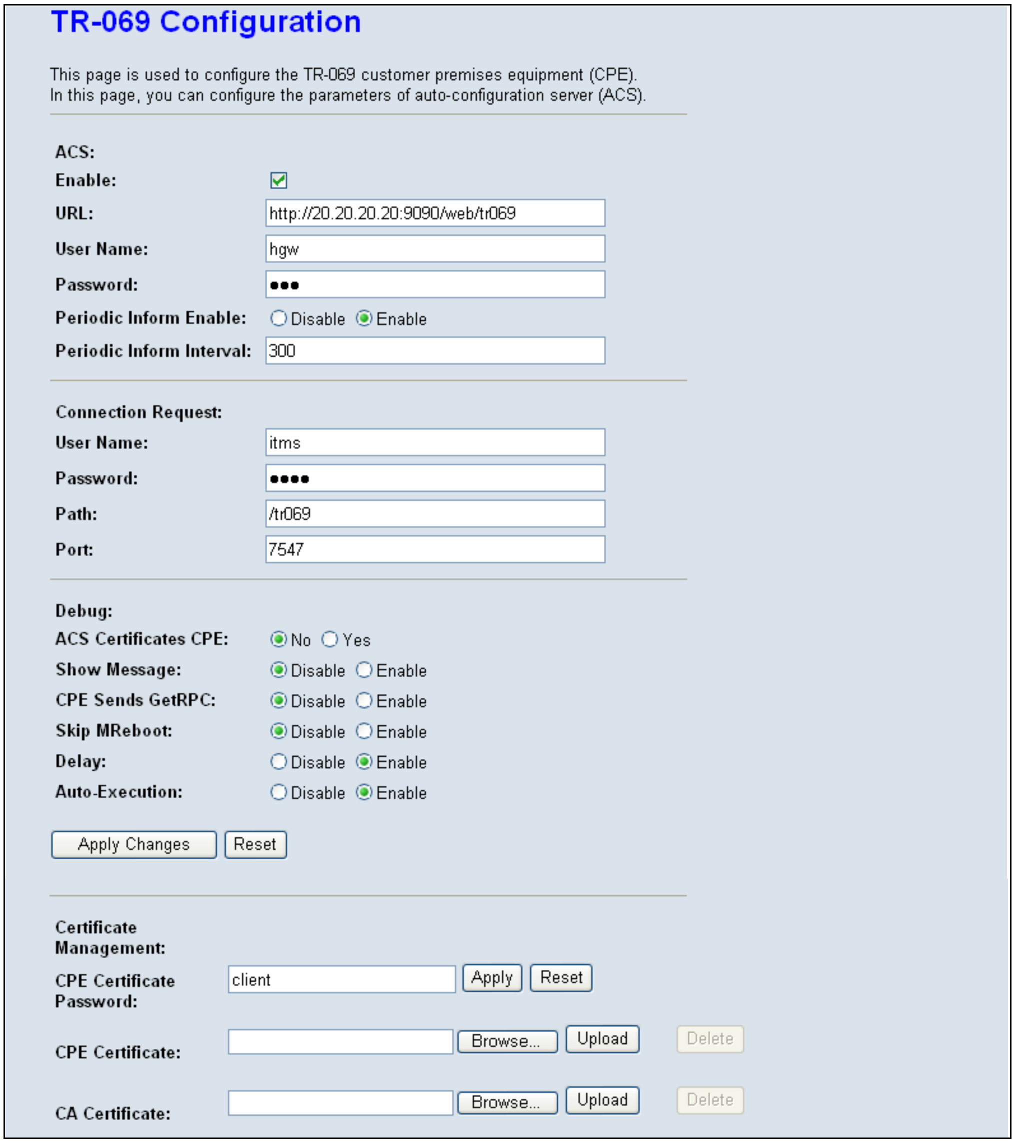
- **Select File** — Specifies the firmware file for the upgrade. The file location must be on the local management PC. You can use the Browse button to find the file.
- **Browse** — Opens a directory on the local hard drive for specifying the path of file required for uploading.
- **Upload** — Starts the upload procedure.
- **Reset** — Clears all file directory fields.

TR-069 CONFIGURATION

The Technical Report 069 (TR069) protocol defines a specification for remote management of CPE devices. The protocol uses HTTP for two-way communication between the CPE device and an Auto Configuration Server (ACS), allowing service providers to provide CPE configuration, software upgrades, and other service functions for end-users.

The ADSL Router's TR-069 parameters need to be defined to allow communication with the remote ACS.

Figure 86: TR-069 Configuration



TR-069 Configuration

This page is used to configure the TR-069 customer premises equipment (CPE).
In this page, you can configure the parameters of auto-configuration server (ACS).

ACS:	
Enable:	☑
URL:	http://20.20.20.20:9090/web/tr069
User Name:	hgw
Password:	●●●
Periodic Inform Enable:	○ Disable ● Enable
Periodic Inform Interval:	300
Connection Request:	
User Name:	itms
Password:	●●●●
Path:	/tr069
Port:	7547
Debug:	
ACS Certificates CPE:	● No ○ Yes
Show Message:	● Disable ○ Enable
CPE Sends GetRPC:	● Disable ○ Enable
Skip MReboot:	● Disable ○ Enable
Delay:	○ Disable ● Enable
Auto-Execution:	○ Disable ● Enable
Certificate Management:	
CPE Certificate Password:	client
CPE Certificate:	
CA Certificate:	

The following items are displayed on this pages:

ACS

Defines the Auto Configuration Server parameters.

- **Enable** — Enables/disables TR-069 support. (Default: Enabled)
- **URL** — Speceifies the URL required for the CPE to connect to the ACS.
- **User Name** — Enter the user name that the ADSL Router should use when connecting to the ACS.
- **Password** — Enter the password that the ADSL Router should use when connecting to the ACS.
- **Periodic Inform Enable** — When this field is enabled, the DSL device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the DSL device will only send Inform RPC to the ACS server once at the system startup. (Default: Enabled)
- **Periodic Inform Interval** — Time interval in seconds to send Inform RPC.

CONNECTION REQUEST

Defines the connection from the ADSL Router to the ACS.

- **User Name** — The user name the remote ACS should use when connecting to this device.
- **Password** — The password the remote ACS should use when connecting to this device.
- **Path** — The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path
- **Port** — The port of the device ConnectionRequestURL.

DEBUG

Sets options for displaying debug messages for the ACS connection.

- **ACS Certificates CPE** — Selects if digital certificates are used on the CPE.
- **Show Message** — Displays ACS SOAP messages on the serial console.
- **CPE sends GetRPC** — The router contacts the ACS to obtain Remote Procedure Call methods.

- **Skip MReboot** — Specifies whether to send an MReboot event code in the inform message.

- **Delay** — Specifies whether to start TR-069 after a short delay.

- **Auto-Execution** — Specifies whether to automatically start TR-069 after the router is powered on.

CERTIFICATE MANAGEMENT

Defines the digital certificate files used for authentication between the ADSL Router and the ACS.

- **CPE Certificate Password** — The password to use with the ADSL Router's digital certificate file.

- **CPE Certificate** — The unique digital security certificate used by the ADSL Router to authenticate with the ACS server. Click the "Browse" button to locate the file on your local PC and upload it to the unit using the "Upload" button.

- **CA Certificate** — The digital security certificate issued by a Certified Authority to be used by the unit when authenticating the ACS server. Click the "Browse" button to locate the file on your local PC and upload it to the unit using the "Upload" button.

SECTION III

APPENDICES

This section provides additional information and includes these items:

A Troubleshooting

Diagnosing Gateway Indicators

Gateway operation is easily monitored via the LED indicators to identify problems. The table below describes common problems you may encounter and possible solutions. If the solutions in the table fail to resolve the problem, contact technical support for advice.

Table 3: LED Troubleshooting Chart

Symptom	Cause	Solution
Power indicator does not light up after power on.	Power outlet, power cord, or external power adapter may be defective.	◆ Check the power outlet by plugging in another device that is functioning properly. ◆ Check the power adapter with another router.
Ethernet link indicator does not light up after making a connection.	Network interface (e.g., a network adapter card in the attached computer), network cable, or router LAN port may be defective.	◆ Verify that the router and computer are powered on. ◆ Be sure the cable is plugged into both the router and the computer. ◆ Verify that the proper cable type is used and its length does not exceed specified limits. ◆ Check the network adapter in the computer and cable connections for possible defects. Replace the defective adapter or cable if necessary.
Link indicator is off or does not stop blinking (i.e., synchronizing) after making a connection.	Cabling or router DSL port may be defective.	◆ Be sure the cable is plugged into both the router, ADSL Splitter, and an RJ-11 telephone jack. ◆ Verify that the cable length does not exceed specified limits. (Check with your service provider for this information.) ◆ Check the cable connections on the router, ADSL Splitter, and wall jack for possible defects. Replace the defective cable if necessary.

IF YOU CANNOT CONNECT TO THE INTERNET

- Check that your computer is properly configured for TCP/IP. For more information, see "Configuring the TCP/IP Protocols" on page 32.
- Make sure the correct network adapter driver is installed for your PC operating system. If necessary, try reinstalling the driver.
- Check that the network adapter's speed or duplex mode has not been configured manually. We recommend setting the adapter to auto-negotiation when installing the network driver.

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 4: Web Access Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	◆ Be sure the router is powered up. ◆ Check the network cabling between the management station and the router. ◆ Check that you have a valid network connection to the router and that the port you are using has not been disabled. ◆ Be sure the management station has an IP address in the same subnet as the router's IP interface to which it is connected.
Forgot or lost the password	◆ Press and hold down the Reset button for 3 seconds or more to restore the unit's factory default settings, then use the default password to access the web interface.

B HARDWARE SPECIFICATIONS

PHYSICAL CHARACTERISTICS

PORTS	1 RJ-11 DSL line (to phone jack in the wall) 4 RJ-45 10/100BASE-TX (Ethernet connection to PC)
ETHERNET INTERFACE	RJ-45 connector, auto MDI/X pinout detection 10BASE-T: 100-ohm, UTP cable; Category 3 or better 100BASE-TX: 100-ohm, UTP cable; Category 5 or better *Maximum Cable Length - 100 m (328 ft)
DSL INTERFACE	RJ-11 connector, using standard phone cable (26 AWG)
LED INDICATORS	Power, DSL, Internet, LAN, WLAN, WPS
INPUT POWER	12 VDC (via AC power adapter), 800 mA maximum
SIZE	140 x 104 x 28.5 mm (5.51 x 4.09 x 1.12 in.)
WEIGHT	177 g (6.2 oz)
TEMPERATURE	Operating: 0 °C to 40 °C (32 °F to 104 °F)
HUMIDITY	Operating: 10% to 95% (non-condensing)

WIRELESS CHARACTERISTICS

FREQUENCY BAND	2.4 ~ 2.484 GHz
RADIO DATA RATE	11b: 11/5.5/2/1M (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11n: HT40 up to 150 Mbps, HT20 up to 65 Mbps (Automatic)
CHANNELS	Up to 14 (depending on region)
MODULATION	802.11b: 64-QAM, 16-QAM, QPSK, BPSK, DSSS 802.11g: CCK, DQPSK, DBPSK 802.11n, HT20 and HT40: 64-QAM, 16-QAM, QPSK, BPSK
SECURITY	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK

SOFTWARE FEATURES

ATM FEATURES	Support up to 8 ATM PVCs Support ATM Forum UNI 3.1/4.0 PVC Support UBR, CBR, and rt-VBR and nrt-VBR service classes Provide ATM layer functionality Support up to 8 PVCs – traffic shaping (CBR, UBR, rt/nrt-VBR) Support PPPoA (RFC2364) Support MPoA functionality (RFC2684) Support IP over ATM (IPoA) Support ATM cell format ITU -T I.361 Support OAM F4/F5 loopback
PPP FUNCTIONS	Point-to-Point Protocol (RFC1661) PPP over ATM (RFC2364) PPP over Ethernet (RFC2516) User Authentication - CHAP (RFC1994) - PAP (RFC1334)

Bridge Features

Ethernet bridging
Support for transparent bridging
- MAC address learning
- MAC address filtering and protocol filtering for up-link

Routing Features

RIP v1/v2
Static routing
PPP/PPPoE (RFC 2516)
NAT with ALGs
NAPT
IGMP v1/v2
IGMP proxy and snooping
IPv4
IP pass-through
ARP binding
Port mapping

Security

Stateful Packet Inspection (SPI)
Management Access Control for WAN
User authentication for PPP (PAP/CHAP)
DDoS (Dynamic DoS) Protection

Firewall

NAT
DMZ
Filtering – IP Filtering, MAC Filtering, URL Filtering
ACL (Access Control List)
VPN (IPSec, PPTP, L2TP) pass-through
Software Forbidden

Management

Access administration
Web-based configuration - HTTP server
System configuration backup and restore
SNMP Support (V.1 and V.2C) – MIB I, MIB II (RFC1213)
Firmware upgrade by Web/TFTP
Remote firmware upgrade
UPnP
EZ Setup Wizard
TR069 remote management diagnostic
TR067 ensures product meets all ADSL IOT tests

QoS

IP ToS function (RFC 1349)

802.1p bit remarking
Traffic classification by port, 802.1p , ToS, and DSCP

STANDARDS

ETHERNET STANDARDS IEEE 802.3-2005 Ethernet Access
Ethernet, Fast Ethernet
Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.1D Spanning Tree Protocol
IEEE 802.1p priority tags

WIRELESS STANDARDS 802.11b
802.11g
802.11n

ADSL COMPLIANCE ANSI T1.413 Issue 2
G.992.1 (G.dmt) Annex A
G.992.2 (G.lite) Annex A
G.992.3 ADSL2 (G.dmt.bis) Annex A/J/K/L/M
G.992.4 ADSL2 (G.lite.bis)
G.992.5 ADSL2+

COMPLIANCES

EMISSIONS FCC Part 15B Class B
FCC Part 68
CE Mark
CCC Class B

ENVIRONMENTAL RoHS compliant

SAFETY UL

C CABLES AND PINOUTS

TWISTED-PAIR CABLE ASSIGNMENTS

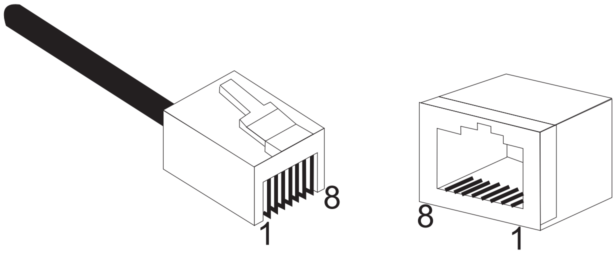
For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. For 1000BASE-T connections the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

NOTE: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

CAUTION: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

Figure 87: RJ-45 Connector



10/100BASE-TX PIN ASSIGNMENTS

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 port on the router supports automatic MDI/MDI-X operation, so you can use straight-through or crossover cables for all network connections to PCs, switches, or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable.

Table 5: 10/100BASE-TX MDI and MDI-X Port Pinouts

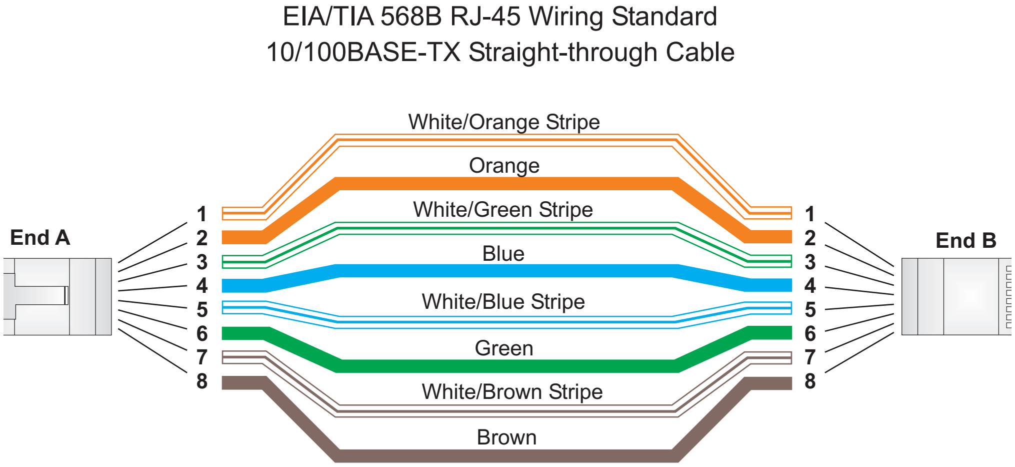
PIN	MDI Signal Name[a]	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4, 5, 7, 8	Not used	Not used

[a] The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

STRAIGHT-THROUGH WIRING

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on this gateway, you can use either straight-through or crossover cable to connect to any device type.)

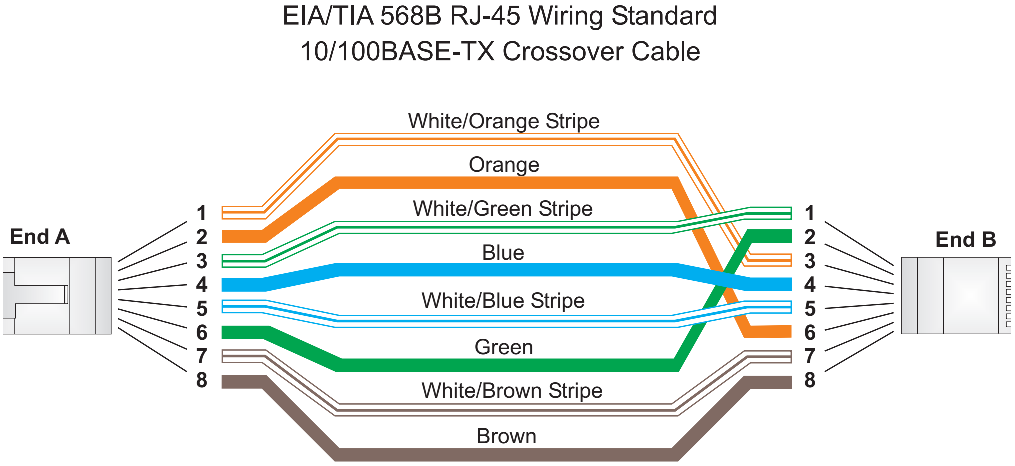
Figure 88: Straight-through Wiring



CROSSOVER WIRING

If the twisted-pair cable is to join two ports and either both ports are labeled with an "X" (MDI-X) or neither port is labeled with an "X" (MDI), a crossover must be implemented in the wiring. (When auto-negotiation is enabled for any RJ-45 port on this gateway, you can use either straight-through or crossover cable to connect to any device type.)

Figure 89: Crossover Wiring



RJ-11 PORT

Standard telephone RJ-11 connectors and cabling can be found in several common wiring patterns. These six-pin connectors can accommodate up to three wire-pairs (three telephone lines), but usually only one or two pairs of conductor pins and wires are implemented.

The RJ-11 port on this device contains one wire-pair, an inner pair on pins 3 and 4. This wire-pair carries the digital data.

Figure 90: RJ-11 Wiring

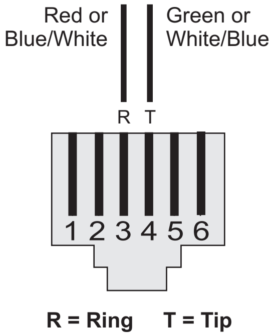


Table 6: RJ-11 Port Pinouts

Pin	Signal Name	Wire Color
1	Not used	
2	Not used	
3	Line 1 Ring	Red or Blue/White
4	Line 1 Tip	Green or White/Blue
5	Not used	
6	Not used	

Glossary

10BASE-T IEEE 802.3-2005 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX IEEE 802.3-2005 specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

1000BASE-T IEEE 802.3ab specification for 1000 Mbps Gigabit Ethernet over four pairs of Category 5 or better UTP cable.

Backbone The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

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.

Ethernet A popular local area data communications network, which accepts transmission from computers and terminals.

Firewall A firewall is designed to prevent unauthorized access to or from a private network.

FTP File Transfer Protocol: A TCP/IP protocol used for file transfer.

HTTP Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.

ISP Internet Service Provider. A company that provides access to the Internet. This may be your local telephone company, or a dedicated Internet service company.

ITU International Telecommunication Union

ITU-T Telecommunication Standardization Section of ITU

LAN Local Area Network: A group of interconnected computers and support devices.

MAC ADDRESS The physical layer address used to uniquely identify network nodes.

MTU Maximum Transfer Unit. The maximum transfer unit for traffic crossing this device. MTU should be set to a value that minimizes unnecessary fragmentation and maximizes the transfer of large sequential data streams.

NTP Network Time Protocol: NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

PING A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POTS Plain Old Telephone Service. One of the services using voice band. Sometimes used as a descriptor for all voice band services.

PPP Point-to-Point Protocol. A protocol for connecting remote hosts to the Internet using TCP/IP.

PPPOE PPP over Ethernet. A protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PSTN Public Switched Telephone Network.

QOS Quality of Service. A network protocol used to specify a guaranteed throughput level. This protocol is often used by Internet service providers to guarantee their customers a minimum end-to-end latency.

RATE ADAPTIVE A DSL service that automatically adjusts the transmission rate depending on line quality and loading to ensure data quality (such as, keeping within a maximum error rate).

RJ-45 Connector A connector for twisted-pair wiring.

Splitter A filter to separate DSL signals from POTS signals to prevent mutual interference.

SNTP Simple Network Time Protocol: SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TIA Telecommunications Industry Association

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UPnP Universal Plug-and-Play. A set of protocols that allows devices to connect seamlessly and simplifies the deployment of home and office networks, using auto-discovery of other network devices, acquiring information about device capabilities, and requests for services.

UTP Unshielded twisted-pair cable.

VPN Virtual Private Network. A secure tunnel used to protect data passing from one network to another over the Internet.

WAN Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

INDEX

Edge-corE NETWORKS | SMC Networks

Headquarters & Sub-Sahara Africa Office

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

Asia-Pacific Office

1 Coleman Street
#07-09, The Adelphi
Singapore 179803
Tel: +65-63387667
Fax: +65-63387767

Europe & N. Africa Office

C/Fructuós Gelabert 6-8, 2º, 2ª
Edificio Conata II
08970 Sant Joan Despí
Barcelona, Spain
Tel: +34 93 477 4920

Middle East Office

Office No. 416, Le Solarium Bldg
Dubai Silicon Oasis
Dubai, U.A.E.
Tel: +971-4-3564800
Fax:+971-4-3564801

North America Office

20 Mason
Irvine CA 92618 U.S.A.
Tel: +1 (949) 679-8000

SMC NETWORKS TECHNICAL SUPPORT

From Singapore in English and 中文 (Mon.-Fri. 9 AM to 5 PM)
Tel: +65-63387667, Ext. 4

From the United Arab Emirates in English (Sun.-Thu. 9 AM to 6 PM)
Tel: +971 800 222866/+971 4 3564810

From U.S.A. and Canada (24 hours a day, 7 days a week)
Tel: +1 (800) SMC-4-YOU/+1 (949) 679-8000 Fax: +1 (949) 679-1481

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

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

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

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

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

Français: Informations Support Technique sur www˙smc˙com

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

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

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

Nederlands: Technische ondersteuningsinformatie beschikbaar op www·smc·com

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

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

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

简体中文 : 技术支持讯息可通过www.smc-prc.com查询

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

ไทย: 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

SMC7904WBRAS-N2 v2

www.edge-core.com / www.smc.com