

**SMC®** | **USER MANUAL**

**ADSL2 Barricade™ N**  
**11n Wireless 4-Port ADSL2/2+ Modem Router**

**SMC7904WBRA-N2**

---

# **SMC7904WBRA-N2**

## **User Manual**

## Contents

1	Compliances .....	1
1.1	Europe – EU Declaration of Conformity .....	1
2	Safety Precautions .....	5
3	Précautions de sécurité.....	6
4	Sicherheitsmaßnahmen .....	7
5	Precauciones de seguridad.....	8
6	Precauções de Segurança.....	9
7	Overview .....	10
7.1	Packing List .....	10
7.2	Application .....	10
7.3	Features .....	11
7.4	Standards Compatibility and Compliance .....	12
8	Hardware Description and Installation .....	12
8.1	Hardware Description .....	12
8.1.1	Front Panel .....	12
8.1.2	Rear Panel.....	14
8.2	Hardware Installation .....	15
8.2.1	Choosing the Best Location for Wireless Operation.....	15
8.2.2	Connecting the Router.....	15
9	PC Network Configuration and Login.....	17
9.1	PC Network Configuration .....	17
9.2	Logging In to the DSL Router .....	19
10	Web-Based Management .....	20
10.1	Start .....	22
10.1.1	Wizard Setup .....	22
10.1.2	Wireless .....	26
10.1.3	LAN.....	40
10.1.4	LAN Configuration .....	40
10.2	Advanced Setup .....	45
10.2.1	Layer2 Interface.....	46
10.2.2	WAN Service .....	48
10.2.3	NAT.....	72

10.2.4	Security.....	76
10.2.5	Parental Control.....	80
10.2.6	Quality of Service .....	82
10.2.7	Routing .....	86
10.2.8	DNS .....	90
10.2.9	DSL.....	91
10.2.10	UPnP .....	92
10.2.11	DNS Proxy.....	93
10.2.12	Storage Service .....	94
10.2.13	Interface Grouping.....	95
10.2.14	Multicast .....	98
10.2.15	Wireless.....	98
10.3	Management.....	105
10.3.1	Passwords Settings.....	105
10.3.2	Internet Time.....	106
10.3.3	Diagnostics .....	107
10.3.4	Settings.....	108
10.3.5	System Log.....	109
10.3.6	SNMP Agent.....	110
10.3.7	TR-69 Client .....	111
10.3.8	Access Control- Services .....	112
10.3.9	Update Software.....	114
10.3.10	Reboot.....	114
10.4	Device Information.....	115
10.4.1	Summary .....	115
10.4.2	WAN .....	117
10.4.3	Statistics .....	117
10.4.4	LAN.....	117
10.4.5	WAN Service .....	118
10.4.6	xTM.....	118
10.4.7	xDSL.....	118
10.4.8	Route .....	120
10.4.9	ARP .....	120
10.4.10	DHCP .....	120
11	Q&A.....	122

## 1 Compliances

### 1.1 Europe – EU Declaration of Conformity

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

- EN 60950-1:2006 + A11: 2009  
Safety of Information Technology Equipment.
- EN 300 328 V1.7.1: 2006-10  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.
- EN 301 489-17 V1.8.1/ 2008-04  
EN 301 489-17 V2.1.1/ 2009-05  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 62311: 2008  
Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz).

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

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

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



This equipment may be operated in:



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

Български [Bulgarian]	С настоящето, SMC Networks декларира, че това безжично устройство е в съответствие със съществените изисквания и другите приложими разпоредби на Директива 1999/5/ЕС.
čs Česky [Czech]	SMC tímto prohlašuje, že tento Router je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede SMC erklærer herved, at følgende udstyr Router overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
nl Nederlands [Dutch]	Hierbij verklaart SMC dat het toestel Router in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
en English	Hereby, SMC, declares that this Router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian et Eesti	Käesolevaga kinnitab SMC seadme Router vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish fi Suomi	SMC vakuuttaa täten että Router tyypinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

## User Manual

<span style="border: 1px solid black; padding: 2px;">French</span> <span style="border: 1px solid black; padding: 2px;">fr</span> Français	Par la présente SMC déclare que l'appareil Router est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
<span style="border: 1px solid black; padding: 2px;">German</span> <span style="border: 1px solid black; padding: 2px;">de</span> Deutsch	Hiermit erklärt SMC, dass sich das Gerät Router in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
<span style="border: 1px solid black; padding: 2px;">Greek</span> <span style="border: 1px solid black; padding: 2px;">el</span> Ελληνικά	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣMC ΔΗΛΩΝΕΙ ΟΤΙ Router ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
<span style="border: 1px solid black; padding: 2px;">Hungarian</span> <span style="border: 1px solid black; padding: 2px;">hu</span> Magyar	Alulírott, SMC nyilatkozom, hogy a Router megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
<span style="border: 1px solid black; padding: 2px;">Italian</span> <span style="border: 1px solid black; padding: 2px;">it</span> Italiano	Con la presente SMC dichiara che questo Router è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabiliti dalla direttiva 1999/5/CE.
<span style="border: 1px solid black; padding: 2px;">Latvian</span> <span style="border: 1px solid black; padding: 2px;">lv</span> Latvian	Ar šo SMC deklarē, ka Router atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
<span style="border: 1px solid black; padding: 2px;">Lithuanian</span> <span style="border: 1px solid black; padding: 2px;">lt</span> Lietuvių	Šiuo SMC deklaruoja, kad šis Router atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
<span style="border: 1px solid black; padding: 2px;">Maltese</span> <span style="border: 1px solid black; padding: 2px;">mt</span> Malti	Hawnhekk, SMC, jiddikjara li dan Router jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
<span style="border: 1px solid black; padding: 2px;">Polish</span> <span style="border: 1px solid black; padding: 2px;">pl</span> Polski	Niniejszym SMC oświadcza, że Router jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
<span style="border: 1px solid black; padding: 2px;">Portuguese</span> <span style="border: 1px solid black; padding: 2px;">pt</span> Português	SMC declara que este Router está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

## User Manual

Romanian Romană	SMC Networks declară că acest dispozitiv fără să respectă cerințele esențiale precum și alte dispoziții relevante ale Directivei 1999/5/EC.
Slovak  Slovensky	SMC týmto vyhlasuje, že Router spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian  Slovencko	SMC izjavlja, da je ta Router v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Spanish  Español	Por medio de la presente SMC declara que el Router cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Swedish  Svenska	Härmed intygar SMC att denna Router står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Turkish Türk	SMC Networks bu kablosuz cihazın temel gereksinimleri ve 1999/5/EC yonergesindeki ilgili koşulları karşıladığı beyan eder.

## 2 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 exists 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.

### 3 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.

## 4 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.

## 5 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.

## 6 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.

## 7 Overview

The SMC7904WBRA-N2 Router is an ADSL2+ Integrated Access Device. It provides four 10/100Base-TX Ethernet interfaces at the user end. The Router provides a high-speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high-performance access to the Internet, with downstream speeds up to 24 Mbps.

The Router supports WLAN access. It complies with IEEE 802.11b/g and 802.11n standards, and WEP, WPA, and WPA2 security specifications. The WLAN of the Router supports a two-transmit, two-receive (2T2R) antenna configuration.

### 7.1 Packing List

- SMC7904WBRA-N2
- ADSL splitter
- Switching AC power adapter
- Ethernet cable (RJ-45)
- 2 Telephone cables (RJ-11)
- Quality Warranty Card
- Quick Installation Guide (QIG)
- GPL Notice
- CD; includes User Manual and GPL source code

### 7.2 Application

- Home gateway
- SOHOs
- Small enterprises
- High data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

## 7.3 Features

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game support and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry-standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVCs)
- Support for up to 8 PPPoE sessions
- Support for RIP v1 and RIP v2
- WLAN with high-speed data transfer rates of up to 130 Mbps, compatible with IEEE 802.11b/g/n, 2.4 GHz compliant equipment
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of Service (QoS)
- Wireless LAN security: WPA, 802.1X, RADIUS client
- Universal plug-and-play (UPnP)
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Command line interface (CLI)
  - TR-069 WAN management protocol
- Remote update
- USB mass-storage, SAMBA and DLNA
- System statistics and monitoring
- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.

## 7.4 Standards Compatibility and Compliance

- Supports application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

## 8 Hardware Description and Installation

### 8.1 Hardware Description

#### 8.1.1 Front Panel



Figure 1 Front Panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on and operating normally.
	Red	On	The device has detected a self-test failure or other malfunction.
	Off		The device is powered off.
DSL	Green	On	DSL link has been established.
		Slow Blink	No DSL link detected.
		Fast Blink	DSL link detected.
	Off		The device is powered off.

## User Manual

<b>Indicator</b>	<b>Color</b>	<b>Status</b>	<b>Description</b>
Internet	Green	On	There is a connection to the Internet (PPP is up).
		Blink	Data is being transmitted.
	Red	On	Authentication has failed.
	Off		No PPP connection or the PPP connection is down.
LAN 1/2/3/4	Green	On	An Ethernet link is established.
		Blink	Transmitting or receiving data over the Ethernet link.
	Off		No Ethernet link established.
WLAN	Green	On	The WLAN is enabled.
		Blink	Transmitting or receiving data over the WLAN.
	Off		The WLAN is disabled.
WPS	Green	On	A Wi-Fi Protected Setup connection has been successfully established.
		Blink	Wi-Fi Protected Setup is setting up a connection.
	Off		Wi-Fi Protected Setup is idle.
USB	Green	On	A USB device is connected.
	Off		No USB device is connected.

### 8.1.2 Rear Panel

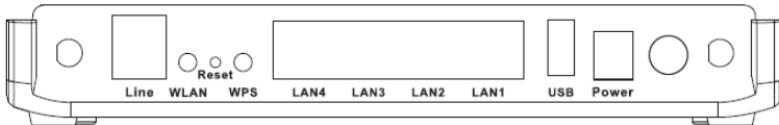


Figure 2 Rear panel

The following table describes the interfaces and buttons on the rear panel.

Interface	Description
Line	RJ-11 port for connecting to the ADSL interface or a splitter through a telephone cable.
WLAN	WLAN switch for enabling or disabling the WLAN function.
Reset	Press the button for at least 3 seconds and then release it. System restores the factory default settings.
WPS	Enables WPS PBC mode. When WPS is enabled, press this button for the wireless router to start the negotiation of PBC mode.
LAN 4~1	RJ-45 ports for connecting the router to PCs or other network devices.
USB	USB host port for connection to a USB device to support a specific value-added application.
Power	For connecting the AC power adapter to supply 12 V DC, 1 A.
○	Power on/off switch, next to the power socket.

 **Warning:**

*Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, press the **Reset** button for 3 seconds with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.*

*The power specification is 12V, 1A. If the power adapter does not match the specification, it may damage the device.*

## 8.2 Hardware Installation

### 8.2.1 Choosing the Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the DSL Router. If this is the first time that you have set up a wireless network device, read the following information:

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting. Designed to reach up to 100 meters indoors and up to 300 meters outdoors, the wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background radio frequency noise in your home or business.

### 8.2.2 Connecting the Router

**Step1** Connect the **Line** interface of the Router to the **MODEM** interface of the splitter through a telephone cable. Connect the phone to the **PHONE** interface of the splitter through a telephone cable. Connect the incoming line to the **LINE** interface of the splitter.

The splitter has three interfaces:

- **LINE:** Connect to a wall phone jack (RJ-11 jack).
- **MODEM:** Connect to the ADSL jack of the device.
- **PHONE:** Connect to a telephone set.

**Step2** Connect the **LAN** interface of the Router to the network interface card (NIC) of the computer through an Ethernet cable (MDI/MDIX).

**Step3** Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** interface of the device.

#### Connection 1

Figure 3 displays the application diagram for the connection of the router, computer, splitter and the telephone sets, when no telephone set is placed before the splitter.

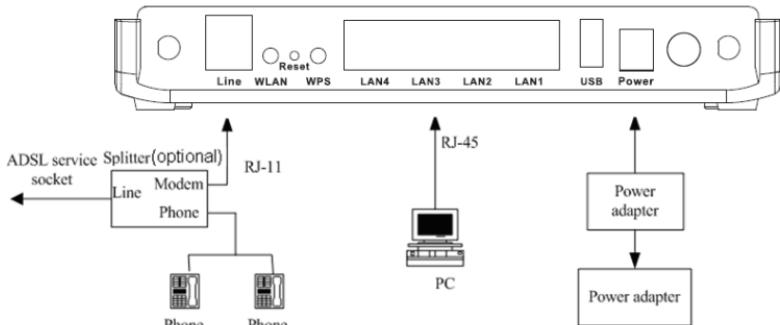


Figure 3 Connection diagram (Without connecting telephone sets before the splitter)

## Connection 2

Figure 4 displays the connection when the splitter is installed close to the router.

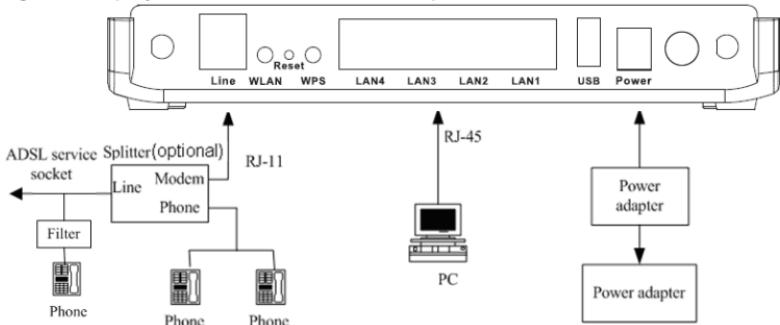


Figure 4 Connection diagram (Connecting a telephone set before the splitter)



### Note:

When connection 2 is used, the filter must be installed close to the telephone cable. See Figure 4. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

## 9 PC Network Configuration and Login

### 9.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

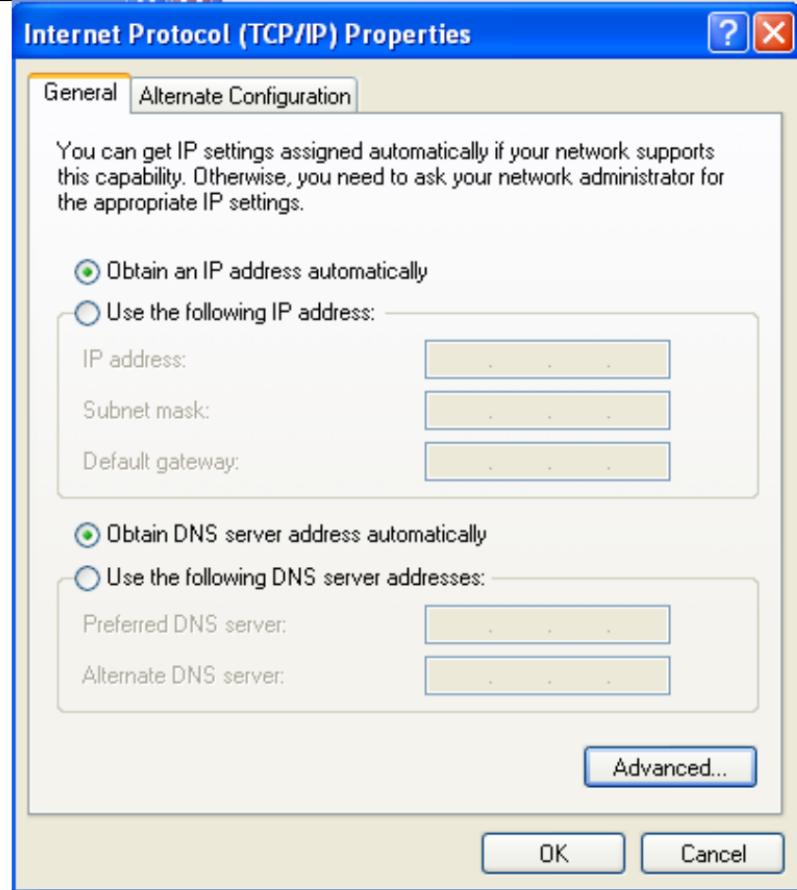


Figure 5 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

- Step1** Choose **Start > Control Panel > Network Connections**.
- Step2** Right-click the Ethernet connection icon and choose **Properties**.
- Step3** On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.
- Step4** The **Internet Protocol (TCP/IP) Properties** window appears.
- Step5** Select the **Obtain an IP address automatically** radio button.

**Step6** Select the **Obtain DNS server address automatically** radio button.

**Step7** Click **OK** to save the settings.

## 9.2 Logging In to the DSL Router

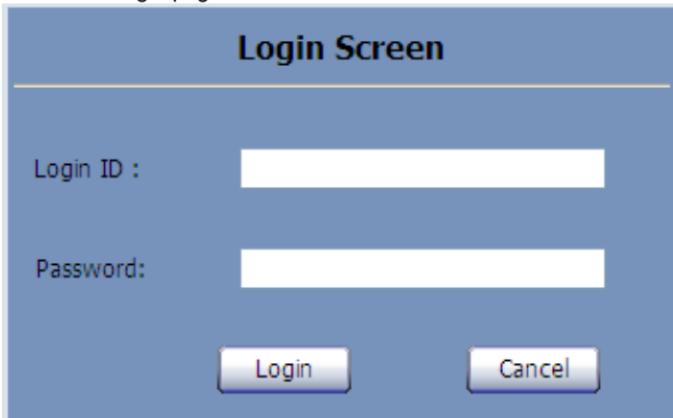
To log in to the DSL router, follow these steps:

**Step1** Open a Web browser on your computer.

**Step2** Enter **<http://192.168.2.1>** (the default IP address of the DSL router) in the address bar. The login page appears.

**Step3** Enter the Login ID and the password. The default Login ID is **admin** with default password **smcadmin**. It is recommended to change these default values after logging in to the DSL router for the first time.

**Step4** Click **Login** to log in to the Web page. Otherwise, please click **Cancel** to exit the login page.



## 10 Web-Based Management

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters through a user-friendly GUI.

After logging in to the DSL router successfully, the following page appears.



- **Setup Wizard:** Select this option to display the following page. For the wizard configuration, refer to 5.1.1 Wizard Setup.

## User Manual

**1.Getting Started**

**2.Wireless Settings**

**3.Time Zone**

**4. ADSL Settings**

**5.Summary**

**1.Getting Started**

Welcome!

Thank you for purchasing this SMC ADSL router product. After answering the following questiNs you will be online and free to enjor high-speed Internet Access with this SMC ADSL router.

First of all, please make sure this ADSL line is connected properly. You can refer to the detailed description in the user guide. If everything is OK, please click the Next button.

Note: If you select to apply the wizard setting, it will delete all layer2/3 interface that exist now.

[Next](#)

- **Advanced Setup:** Select this option to display the following page. For configuration details, refer to the following section.

**SMC Networks**

**ADSL2/2+ Barricade™ N SMC7904WBRA-N2**

[Home](#) [Logout](#)

**Wizard**

**Wireless**

**LAN**

**Device Info**

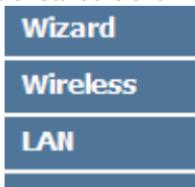
Board ID:	96328ang
Build Timestamp:	110111_1747
Software Version:	0.0.0.1
Bootloader (CFE) Version:	1.0.37-106.17
DSL PHY and Driver Version:	A2pD030l.d23a
Wireless Driver Version:	5.60.120.1.cpe4.06L02.2

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.2.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
Date/Time:	Thu Jan 1 01:26:53 1970

## 10.1 Start

Choose **Start** and the submenus of **Start** are shown as below:



### 10.1.1 Wizard Setup

**Wizard** helps you to fast and accurately configure Internet connection and other important parameters. The following sections describe these various configuration parameters.

**Step1** Choose **Wizard** in the main page and the page as shown in the following figure appears.



**Step2** In the **Getting Started** page, click **Next** and the following page appears. In this page, you can enable wireless, set the SSID, and enable or disable hide access point.

### 1.Wireless Settings

This page allows you to define SSID and Channel ID for wireless connection. In the wireless environment, the router can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.

Enable Wireless:	<input checked="" type="checkbox"/>
SSID:	SMC
Hide Access Point:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

[Back](#) [Next](#)

**Step3** After proper setting wireless, click **Next** and the **Times settings** page appears. In this page, you can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet.

### 3.Time settings

You can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet.

Automatically synchronize with Internet time servers

When you enable this option, you will need to configure two different time servers, use the options below to set the primary and secondary [NTP](#) servers in your area:

First NTP time server:	time.nist.gov	<input type="button" value=""/>
Second NTP time server:	clock.nyc.he.net	<input type="button" value=""/>
Set the time zone for the ADSL Modem. Use this setting to ensure the time-based client filtering feature and system log entries are based on the correct localized time.		
Time zone offset:	(GMT-05:00) Eastern Time <input type="button" value=""/>	

[Back](#) [Next](#)

**Step4** After proper setting time, click **Next** and the **ADSL settings** page appears.

#### 4. ADSL settings

Please select the network that your Network Provider/Internet Provider is using:

<b>Country:</b>	(Click to select) <input type="button" value="▼"/>
<b>ISP Provider:</b>	(Click to select) <input type="button" value="▼"/>
<b>Protocol:</b>	(Click to select) <input type="button" value="▼"/>
<b>Encapsulation Mode:</b>	(Click to Select) <input type="button" value="▼"/>
<b>VPI:</b>	8
<b>VCI:</b>	35

Select the country and ISP provider. Set the VPI and VCI. If you fail to find the country and ISP from the drop-down lists, select **Others**.

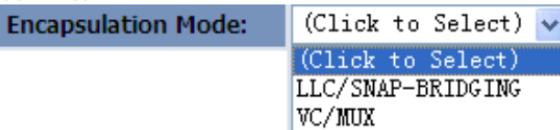
- **Protocol:** You can select the protocol from the drop-down list.

<b>Protocol:</b>	<div style="border: 1px solid #ccc; padding: 5px; width: 150px; display: inline-block;"> <div style="background-color: #0070C0; color: white; padding: 2px 5px; font-weight: bold;">PPPoA</div> <div style="margin-top: 2px;">(Click to select)</div> <div style="display: flex; justify-content: space-around; font-size: 0.8em;"> <span>PPPoE</span> <span>PPPoA</span> </div> <div style="display: flex; justify-content: space-around; font-size: 0.8em;"> <span>Dynamic IPoE</span> <span>Static IPoE</span> </div> <div style="display: flex; justify-content: space-around; font-size: 0.8em;"> <span>IPoA</span> <span>Bridge</span> </div> </div>
------------------	--

- **PPPoE/PPPoA:** When you select the PPPoE or PPPoA as the protocol, you need to set the correct user name and password provided by your ISP.
- **Static IPoE/IPoA:** When you select the static IPoE or IPoA as the protocol, you need to enter the IP address,

subnet mask, default gateway and DNS provided by your ISP.

- **Encapsulation Mode:** You can select the encapsulation mode from the drop-down list.



- **VPI (Virtual Path Identifier):** The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier):** The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).

**Step5** After proper setting ADSL, click **Next** and the **Summary** page appears. In this page, you can check whether the summary information matches the information provided by your ISP. Click **Back** to review or modify settings. Click **Finish** to apply current settings.

## 5.Summary

Wizard setup complete. Click Back to review or modify settings. Click Finish to apply current settings.

### Wireless Parameters:

Enable Wireless: ENABLE

Wireless SSID: SMC

SSID Broadcast: ENABLE

### Time Zone Parameters:

Enable NTP: ENABLE

Time Zone: Eastern Time

Primary Server: time.nist.gov

Secondary Server: clock.nyc.he.net

### ADSL Operation Mode(WAN):

ISP: Others

Protocol: PPPoE

### Network Layer Parameters(WAN):

WAN IP Address: 0.0.0.0

basefrm

Back

Finish

## 10.1.2 Wireless

### 10.1.2.1 Basic Settings

Choose **Start > Wireless > Basic** to display the following page.

## Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

<b>Enable Wireless</b>	<input checked="" type="checkbox"/>						
<b>Hide Access Point</b>	<input type="checkbox"/>						
<b>Clients Isolation</b>	<input type="checkbox"/>						
<b>Disable WMM Advertise</b>	<input type="checkbox"/>						
<b>SSID:</b>	SMC						
<b>BSSID:</b>	02:10:18:01:00:02						
<b>Country:</b>	UNITED STATES <input type="button" value="▼"/>						
<b>Max Clients:</b>	16						
<b>Enable Wireless Multicast Forwarding (WMF)</b> <input type="checkbox"/>							
<b>Wireless - Guest/Virtual Access Points:</b>							
Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	SMC_2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input type="checkbox"/>	SMC_3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input type="checkbox"/>	SMC_4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A

This page allows you to configure the basic features of the wireless LAN interface.

- **Enable Wireless:** Enable or disable the wireless function.
- **Hide Access Point:** if you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive scanning.
- **Clients Isolation:** When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
- **Disable WMM Advertise:** After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
- **BSSID:** Display the MAC address of the wireless interface.

- **Country:** The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max value, all other clients are refused.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After finishing setting, click **Apply/Save** to save the basic wireless settings and make the settings take effect.

#### 10.1.2.2 Security

Choose **Start > Wireless > Security** to display the following page.

### Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.

You may setup configuration manually

OR

through WiFi Protected Setup(WPS)

#### WPS Setup

Enable WPS

Disabled

#### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click "Apply/Save" when done.

Select SSID:

SMC

Network Authentication:

WPA-PSK

WPA Pre-Shared Key:

\*\*\*\*\*

[Click here to display](#)

WPA Group Rekey Interval:

0

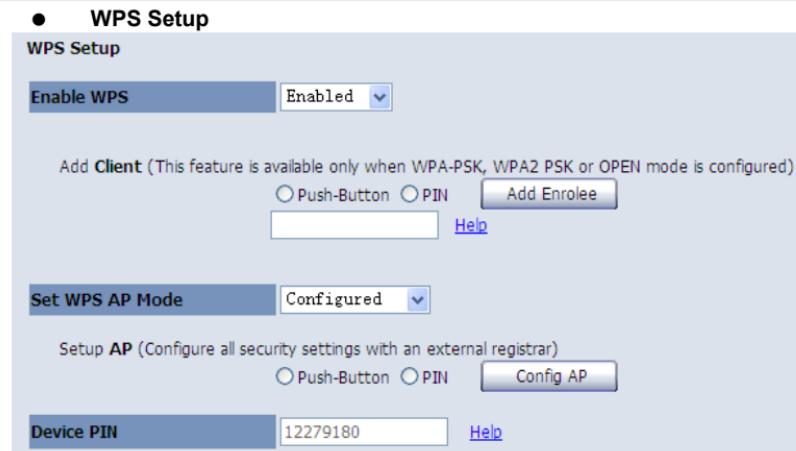
WPA Encryption:

AES

WEP Encryption:

Disabled

This page allows you to configure the security features of the wireless LAN interface. In this page, you can configure the network security settings by the Wi-Fi Protected Setup (WPS) method or setting the network authentication mode.



There are 2 primary methods used in the Wi-Fi Protected Setup:

- PIN entry, a mandatory method of setup for all WPS certified devices.
- Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router. (**Note:** The PBC method may also need a Registrar when used in a special case where the PIN is all zeros)

In order to use the push-button for WPS authentication, you must ensure that the network card support the function. if it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function.

#### ● Manual Setup AP

This page provides 9 types of network authentication modes, including Open, Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

## User Manual

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Select SSID: SMC

Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	Open Shared 802.1X WPA WPA-PSK
WPA Group Rekey Interval:	Click here to display
WPA Encryption:	WPA2 WPA2 -PSK
WEP Encryption:	Mixed WPA2/WPA Mixed WPA2/WPA -PSK

Apply/Save

- Open Mode

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	Open
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	1
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys	
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys	
<input type="button" value="Apply/Save"/>	

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the Open mode.
- **WEP Encryption:** Enable or disable WEP encryption. After enabling this function, you can set the encryption strength, current network key, and network keys.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.
- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- Shared Mode

## User Manual

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	Shared
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	1
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys	
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys	
<input type="button" value="Apply/Save"/>	

The parameters' description of shared mode, please refer to the **Open Mode**.

- 802.1x

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

<b>Select SSID:</b>	SMC
<b>Network Authentication:</b>	802.1X
<b>RADIUS Server IP Address:</b>	0.0.0.0
<b>RADIUS Port:</b>	1812
<b>RADIUS Key:</b>	
<b>WEP Encryption:</b>	Enabled
<b>Encryption Strength:</b>	128-bit
<b>Current Network Key:</b>	2
<b>Network Key 1:</b>	1234567890123
<b>Network Key 2:</b>	1234567890123
<b>Network Key 3:</b>	1234567890123
<b>Network Key 4:</b>	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

**Apply/Save**

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the 802.1X in the drop-down list.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WEP Encryption:** You can only select **Enabled**.
- **Encryption Strength:** You can set 64-bit or 128-bit key.
- **Current Network Key:** The current key that you use.

- **Network Key1/2/3/4:** Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- WPA Mode

#### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	WPA
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA-PSK Mode

## Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	WPA-PSK
WPA Pre-Shared Key:	*****
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA-PSK mode.
- **WPA/WAPI passphrase:** The key for WPA encryption. Click the **Click here to display** button to display the current key. The default key is 87654321.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA2 Mode

**Manual Setup AP**

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

<b>Select SSID:</b>	SMC
<b>Network Authentication:</b>	WPA2
<b>WPA2 Preauthentication:</b>	Disabled
<b>Network Re-auth Interval:</b>	36000
<b>WPA Group Rekey Interval:</b>	0
<b>RADIUS Server IP Address:</b>	0.0.0.0
<b>RADIUS Port:</b>	1812
<b>RADIUS Key:</b>	
<b>WPA Encryption:</b>	AES
<b>WEP Encryption:</b>	Disabled

**Apply/Save**

- **Select SSID:** Select a SSID for configuring the security settings.
- **Network Authentication:** Select the WPA2 mode.
- **WPA2 Preauthentication:** Enable or disable pre-authentication.
- **Network Re-auth Interval:** Set the network re-auth interval.
- **WPA Group Rekey Interval:** Setting the interval for renewing key.
- **RADIUS Server IP Address:** Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
- **RADIUS Port:** The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
- **RADIUS Key:** Set the RADIUS key for accessing the RADIUS server.
- **WPA/WAPI Encryption:** You may select AES, or TKIP+AES.

- WPA2-PSK

## User Manual

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	SMC <input type="button" value="▼"/>
Network Authentication:	WPA2 -PSK <input type="button" value="▼"/>
WPA Pre-Shared Key:	***** <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	AES <input type="button" value="▼"/>
WEP Encryption:	Disabled <input type="button" value="▼"/>

The parameters' description of WPA2-PSK mode, please refer to the [WPA-PSK mode](#).

#### - Mixed WPA2/WPA

### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	Mixed WPA2/WPA
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled

The parameters' description of Mixed WPA2/WPA mode, please refer to the [WPA2 mode](#).

- Mixed WPA2/WPA-PSK

**Manual Setup AP**

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click "Apply/Save" when done.

Select SSID:	SMC
Network Authentication:	Mixed WPA2/WPA -PSK
WPA Pre-Shared Key:	***** <a href="#">Click here to display</a>
WPA Group Rekey Interval:	0
WPA Encryption:	TKIP+AES
WEP Encryption:	Disabled
<input type="button" value="Apply/Save"/>	

The parameters' description of Mixed WPA2/WPA-PSK mode, please refer to the **WPA-PSK mode**.

### 10.1.3 LAN

#### 10.1.4 LAN Configuration

Choose **Advanced Setup > LAN**, and the following page appears.

## User Manual

### Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address:   
Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:   
End IP Address:   
Leased Time (hour):

Port 1  Port 2  Port 3  Port 4

Static IP Lease List: (A maximum 32 entries can be configured)

Configure the second IP Address and Subnet Mask   
for LAN interface

### Ethernet Media Type

Port 1	<input type="button" value="Auto"/>
Port 2	<input type="button" value="Auto"/>
Port 3	<input type="button" value="Auto"/>
Port 4	<input type="button" value="Auto"/>

In this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, and edit the DHCP option.

## Configuring the Private IP Address for the DSL Router

<b>IP Address:</b>	192.168.2.1
<b>Subnet Mask:</b>	255.255.255.0

In this page, you can modify the IP address of the device. The preset IP address is 192.168.2.1.

## Enabling IGMP Snooping

IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

<b>Enable IGMP Snooping</b>	<input checked="" type="checkbox"/>
<input checked="" type="radio"/> Standard Mode	
<input type="radio"/> Blocking Mode	

## Enabling the LAN Side Firewall

Firewall can prevent unexpected traffic on the Internet from your host in the LAN.

<b>Enable LAN side firewall</b>	<input checked="" type="checkbox"/>
---------------------------------	-------------------------------------

In this page, you can enable or disable the LAN side firewall.

## Configuring the DHCP Server

Enable DHCP Server

Start IP Address: 192.168.2.2

End IP Address: 192.168.2.254

Leased Time (hour): 72

Port 1  Port 2  Port 3  Port 4

If you enable the DHCP sever, the clients will automatically acquire the IP address from the DHCP server. If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.

## Editing the DHCP Option

Click the **DHCP Option** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option Setup** page.

DHCP Option Setup

This page allows you to configurate the DHCP OPTION. These options will be sent to DHCP client.

You can define at most 30 options.

State Code Value Pool

Add Edit Delete Return

In this page, you can add, edit or delete the DHCP options, and these options will be sent to the DHCP client.

## Editing the DHCP Option60

Click the **DHCP Option60** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Option60 Setup** page.

DHCP OPTION 60 SETUP

This page allow you to setup dhcp option 60, the dhcp server will assign one ip address based on you setting to dhcp client.

DHCP OPTION 60 TABLE:

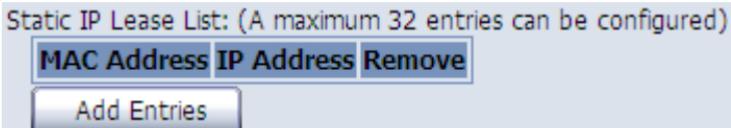
device	className	vendorId	minAddress	maxAddress	dnsPrimary	dnsSecondary	subnetMask	gateWay	dhcpLeaseTime
--------	-----------	----------	------------	------------	------------	--------------	------------	---------	---------------

Add Edit Delete Return

In this page, you can add, edit or delete the DHCP60 options.

### Configuring the DHCP Static IP Lease List

The lease list of static IP address can reserve the static IP addresses for the hosts with the specific MAC addresses. When a host whose MAC address is in the lease list of static IP address requests the DHCP server for an IP address, the DHCP server assigns the reserved IP address to the host.



Click the **Add Entries** button in the **Local Area Network (LAN) Setup** page to display the **DHCP Static IP Lease** page.

#### DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save".

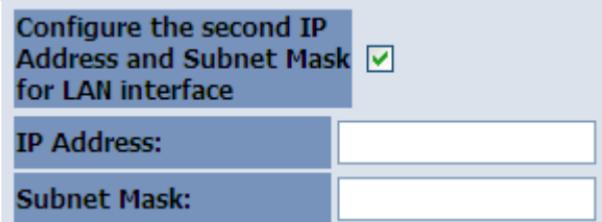
MAC Address:	<input type="text"/>
IP Address:	<input type="text"/>

**Apply/Save**

In this page, enter the MAC address of the LAN host and the static IP address that is reserved for the host, and then click the **Apply/Save** button to apply the settings.

### Configuring the Second IP Address and Subnet Mask for a LAN Interface

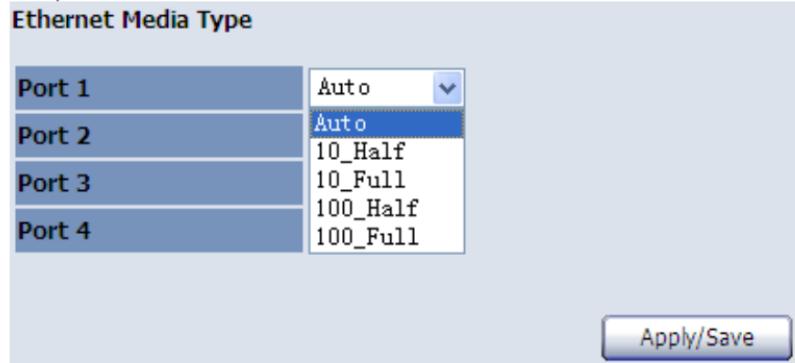
In the **Local Area Network (LAN) Setup** page, you are allowed to set the second IP address and the subnet mask for a LAN interface.



After enabling **Configure the second IP Address and Subnet Mask for LAN interface**, enter an IP address and a subnet mask for the LAN interface.

### Ethernet Media Type

In the **Local Area Network (LAN) Setup** page, you can select the media type from the drop-down list.



After finishing setting, click the **Apply/Save** button to apply the settings.

## 10.2 Advanced Setup

Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown as below:

<b>ATM Interface</b>
<b>WAN Service</b>
<b>NAT</b>
<b>Security</b>
<b>Parental Control</b>
<b>Quality of Service</b>
<b>Routing</b>
<b>DNS</b>
<b>DSL</b>
<b>UPnP</b>
<b>DNS Proxy</b>
<b>Storage Service</b>
<b>Interface Grouping</b>
<b>Multicast</b>
<b>Wireless</b>

### 10.2.1 Layer2 Interface

#### ATM Interface

Choose **Advanced Setup > ATM Interface** , and the following page appears.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
-----------	-----	-----	-------------	----------	-----------	-----------------	--------	---------------	--------------	------------------	--------

Add

## User Manual

In this page, you can add or remove the DSL ATM Interfaces.

Click the **Add** button to display the following page.

### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Latency

Path0

Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Select Connection Mode

Default Mode - Single service over one connection

VLAN MUX Mode - Multiple Vlan service over one connection

Encapsulation Mode:

Service Category:

Select IP QoS Scheduler Algorithm

Strict Priority

Precedence of the default queue:

Weighted Fair Queuing

Weight Value of the default queue: [1-63]

MPAAL Group Precedence:

In this page, you can set the VPI and VCI values, and select the DSL latency, link type (EoA is for PPPoE, IPoE, and Bridge.), connection mode, encapsulation mode, service category, and IP QoS scheduler algorithm.

- **VPI (Virtual Path Identifier):** The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
- **VCI (Virtual Channel Identifier):** The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Select DSL Latency:** You may select **Path0** and **Path1**.

- **Select DSL Link Type:** You may select **EoA** (it is for PPPoE, IPoE, and Bridge), **PPPoA**, or **IPoA**.
- **Select Connection Mode:** You may select the **Default Mode** or the **VLAN MUX Mode**.
- **Encapsulation Mode:** You may select **LLC/SNAP-BRIDGING** or **VC/MUX** in the drop-down list.
- **Service Category:** you may select **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR** or **Realtime VBR** in the drop-down list.
- **Select IP QoS Scheduler Algorithm:** You may select **Strict Priority** and **Weighted Fair Queuing**.

**Note:**

QoS cannot be set for CBR and Realtime VBR.

After finishing setting, click the **Apply/Save** button to make the settings take effect.

See the following figure:

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

**Add** **Remove**

If you want to remove this Interface, please select the **Remove** check box that is corresponding to the selected interface and then click the **Remove** button.

## 10.2.2 WAN Service

Choose **Advance Setup > WAN Service**, and the following page appears.

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit	Action
										<b>Add</b>

In this page, you are allowed to add, remove, or edit a WAN service.

## Adding a PPPoE WAN Service

This section describes the steps for adding the PPPoE service.

**Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.)

### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

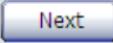
low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm0/(0\_0\_35) 

 Back

 Next

**Step2** In this page, you can select a ATM Interface for the WAN service. After selecting the ATM interface, click **Next** to display the following page.

## WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

pppoe\_0\_0\_35

Back

Next

**Step3** In this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to display the following page.

## User Manual

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:	<input type="text"/>
PPP Password:	<input type="text"/>
PPPoE Service Name:	<input type="text"/>
Authentication Method:	AUTO <input type="button" value="▼"/>
Enable Fullcone NAT	<input type="checkbox"/>
Dial on demand (with idle timeout timer)	<input type="checkbox"/>
PPP IP extension	<input type="checkbox"/>
Use Static IPv4 Address	<input type="checkbox"/>
Enable PPP Debug Mode	<input type="checkbox"/>
Bridge PPPoE Frames Between WAN and Local Ports	<input type="checkbox"/>
Multicast Proxy	
Enable IGMP Multicast Proxy	<input type="checkbox"/>

**Step4** In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.

- **Enable Fullcone NAT:** NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPOE dialup. If this function is disabled, the modem performs PPPOE dial-up all the time. The PPPOE connection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it first.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPOE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Bridge PPPOE Frames Between WAN and Local Ports:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** if you want PPPOE mode to support IPTV, enable it.

**Step5** After setting the parameters, click **Next** to display the following page.

### Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

#### Selected Default Gateway Interfaces

ppp0



#### Available Routed WAN Interfaces

Back

Next

**Step6** In this page, select a preferred WAN interface as the system default gateway, and then click **Next** to display the following page.

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

#### Selected DNS Server

ppp0

#### Available WAN Interfaces



**Use the following Static DNS IP address:**

**Primary DNS server:**

**Secondary DNS server:**

Back

Next

**Step7** In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must manually enter the static DNS server addresses. Click **Next**, and the following page appears.

#### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	PPPoE
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)

[Apply/Save](#)

**Step8** In this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

### Adding a MER (IPoE) WAN service

This section describes the steps for adding the MER WAN service.

**Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a ATM configuration for this WAN service.)

## WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vc)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm1/(0\_0\_36) 

Back

Next

**Step2** Select an ATM Interface, for example, atm1/(0\_0\_36), and then click **Next** to display the following page.

## WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

ipoe\_0\_0\_36

Back

Next

**Step3** In this page, select the WAN service type to be IP over Ethernet and enter the service description. After finishing setting, click **Next** to display the following page.

**WAN IP Settings**

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:	
Option 61 IAID:	(8 hexadecimal digits)
Option 61 DUID:	(hexadecimal digit)
Option 125:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input type="radio"/> Use the following Static IP address:	
WAN IP Address:	
WAN Subnet Mask:	
WAN gateway IP Address:	

**Back** **Next**

**Step4** In this page, you can select obtain an IP address automatically or manually enter the IP address provided by your ISP. Click **Next** and the following page appears.

**Note:**

*If selecting Obtain an IP address automatically, DHCP will be enabled for PVC in MER mode.*

*If selecting Use the following Static IP address, please enter the WAN IP address, subnet mask and gateway IP address.*

### Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

**Enable NAT**

**Enable Firewall**

#### IGMP Multicast

**Enable IGMP Multicast**

**Back**

**Next**

**Step5** In this page, you can set the network address translation settings, for example, enabling NAT, enabling firewall, and enabling IGMP multicast. After finishing setting, click **Next** and the following page appears.

### Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

#### Selected Default Gateway Interfaces

ppp0

#### Available Routed WAN Interfaces

atm1

**>**  
**<**

**Back**

**Next**

**Step6** In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server  
Interfaces

Available WAN Interfaces



**Use the following Static DNS IP address:**

Primary DNS server:	<input type="text"/>
Secondary DNS server:	<input type="text"/>

Back

Next

**Step7** In this page, you may obtain the DNS server addresses from the selected WAN interface or manually enter static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	IPoE
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)

[Apply/Save](#)

**Step8** In this page, it displays the information about the IPoE settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

### **Adding a PPPoA WAN service**

This section describes the steps for adding the PPPoA WAN service.

**Step1** Choose **Advanced Setup > ATM Interface** to display the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for PPPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

## User Manual

### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0

VCI: [32-65535] 37

Select DSL Latency

Path0

Path1

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA

PPPoA

IPoA

Encapsulation Mode: VC/MUX

Service Category: UBR Without PCR

Select IP QoS Scheduler Algorithm

Strict Priority

Precedence of the default queue: 8 (lowest)

Weighted Fair Queuing

Weight Value of the default queue: [1-63] 1

MPAAL Group Precedence: 8

Back

Apply/Save

**Step2** Select the DSL link type to be **PPPoA**, and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the settings, and the following page appears.

### DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm1	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm2	0	37	Path0	UBR	PPPoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

Add

Remove

**Step3** Choose **WAN Service** and click **Add** to display the following page.

### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

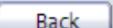
low =0 --> Low PTM Priority not set

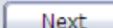
low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm2/ (0\_0\_37) 

 Back

 Next

**Step4** Select the proper interface for the WAN service, and then click **Next** to display the following page.

### WAN Service Configuration

Enter Service Description:

 Back

 Next

**Step5** In this page, you may modify the service description. Click **Next** to display the following page.

## User Manual

### PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:	<input type="text" value="test"/>
PPP Password:	<input type="password" value="****"/>
Authentication Method:	<input type="text" value="AUTO"/>
Enable Fullcone NAT	<input type="checkbox"/>
Dial on demand (with idle timeout timer)	<input type="checkbox"/>
PPP IP extension	<input type="checkbox"/>
Use Static IPv4 Address	<input type="checkbox"/>
Enable PPP Debug Mode	<input type="checkbox"/>
Multicast Proxy	<input type="checkbox"/>
Enable IGMP Multicast Proxy	<input type="checkbox"/>

[Back](#) [Next](#)

- **PPP Username:** The correct user name provided by your ISP.
- **PPP Password:** The correct password provided by your ISP.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Enable Fullcone NAT:** NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoA connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoA dialup. If this function is disabled, the modem performs PPPoA dial-up all the time. The PPPoA connection

does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.

- **PPP IP extension:** If you want to configure DMZ Host, you should enable it first.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
- **Enable PPP Debug Mode:** Enable or disable this function.
- **Enable IGMP Multicast Proxy:** If you want PPPoA mode to support IPTV, enable it.

**Step6** In this page, you can enter the PPP username and PPP password provided by your ISP. Select the authentication method according to your requirement. After finishing setting, click **Next** to display the following page.



**Step7** In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

## User Manual

## DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

**DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

- Select **DNS Server Interface** from available WAN interfaces:

## Selected DNS Server Interfaces

### Available WAN Interfaces

The diagram illustrates a connection between two network interfaces. On the left, a white box contains the text 'ppp0'. On the right, a white box contains the text 'ppp0al' on top and 'atm1' below it. Two blue rectangular boxes with arrows are positioned between them: the top one has a right-pointing arrow labeled '=>', and the bottom one has a left-pointing arrow labeled '<='.

- Use the following Static DNS IP address:

### Primary DNS server:

### Secondary DNS server:

[Back](#) [Next](#)

**Step8** In this page, you can obtain the DNS server addresses from the selected WAN interface or manually enter the static DNS server addresses. If only a PVC with IPoA or static MER protocol is configured, you must enter the static DNS server addresses. After finishing setting, click **Next** to display the following page.

## WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	PPPoA
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back

Apply/Save

**Step9** In this page, it displays the information about the PPPoA settings. Click **Apply/Save** to apply the settings. You can modify the settings by clicking the **Back** button if necessary.

## Adding an IPoA WAN service

This section describes the steps for adding the IPoA WAN service.

**Step1** Choose **Advanced Setup > ATM Interface** to display the **DSL ATM Interface Configuration** page. In this page, you need to add a PVC for IPoA mode. Click the **Add** button in the **DSL ATM Interface Configuration** page to display the following page.

**ATM PVC Configuration**

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]	0
VCI: [32-65535]	38
Select DSL Latency	
Path0	<input checked="" type="checkbox"/>
Path1	<input type="checkbox"/>
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)	
<input type="radio"/> EoA	
<input type="radio"/> PPPoA	
<input checked="" type="radio"/> IPoA	
Encapsulation Mode:	LLC/SNAP-ROUTING
Service Category:	UBR Without PCR
Select IP QoS Scheduler Algorithm	
<input checked="" type="radio"/> Strict Priority	
Precedence of the default queue:	8 (lowest)
<input type="radio"/> Weighted Fair Queuing	
Weight Value of the default queue: [1-63]	1
MPAAL Group Precedence:	8
<input type="button" value="Back"/> <input type="button" value="Apply/Save"/>	

**Step2** Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After

finishing setting, click the **Apply/Save** button to display the following page.

#### DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm1	0	36	Path0	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm2	0	37	Path0	UBR	PPPoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
ipoa0	0	38	Path0	UBR	IPoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

[Add](#) [Remove](#)

**Step3** Choose **WAN Service** and click **Add** to display the following page.

#### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)

For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

low =0 --> Low PTM Priority not set

low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

ipoa0/(0\_0\_38) [▼](#)

[Back](#)

[Next](#)

**Step4** Select the proper interface for the WAN service ,and then click **Next** to display the following page.

## WAN Service Configuration

Enter Service Description:

[Back](#)

[Next](#)

**Step5** In this page, you may modify the service description. Click **Next** to display the following page.

### WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

[Back](#)

[Next](#)

**Step6** In this page, enter the WAN IP address and the WAN subnet mask provided by your ISP and then click **Next** to display the following page.

### Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

### IGMP Multicast

Enable IGMP Multicast

[Back](#)

[Next](#)

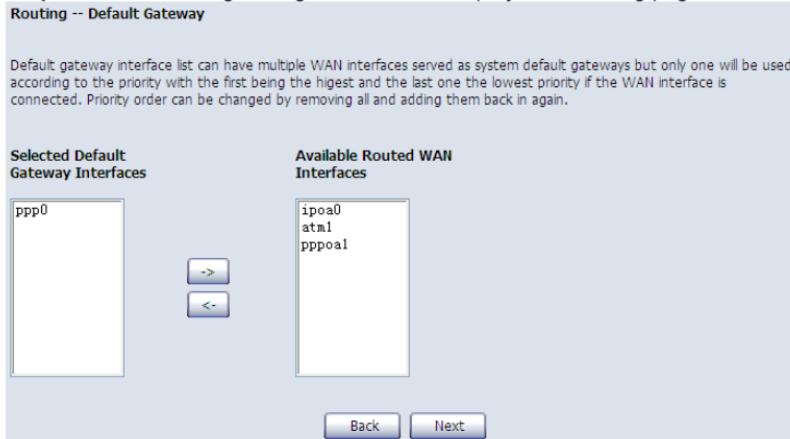
In this page, Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

If you do not want to enable NAT, and wish the user of modem to access the Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, please enable the NAT function.

**Step7** After finishing setting, click **Next** to display the following page.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.



**Step8** In this page, select a preferred WAN interface as the system default gateway and then click **Next** to display the following page.

## User Manual

### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server  
Interfaces

Available WAN Interfaces



**Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

[Back](#)

[Next](#)

**Step9** In this page, you can select DNS server interface from available WAN interface or enter static DNS server IP addresses fro the system. Click **Next** to display the following page.

### WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	IPoA
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)

[Apply/Save](#)

**Step10** In this page, it displays the information about the IPoA settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

## Adding a Bridge WAN service

This section describes the steps for adding the Bridge WAN service.

**Step1** In the **Wide Area Network (WAN) Service Setup** page, click the **Add** button to display the following page. (At first, you must add a proper ATM configuration for this WAN service.) Click the **Add** button to display the following page.

### WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)  
For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0

portId=1 --> DSL Latency PATH1

portId=4 --> DSL Latency PATH0&1

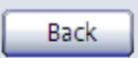
low =0 --> Low PTM Priority not set

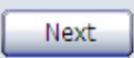
low =1 --> Low PTM Priority set

high =0 --> High PTM Priority not set

high =1 --> High PTM Priority set

atm3/(0\_0\_39) 

 Back

 Next

**Step2** Select the proper ATM Interface, for example atm3/(0\_0\_39) and then click **Next** to display the following page.

**WAN Service Configuration**

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

**Enter Service Description:**

br\_0\_0\_39

**Back****Next**

**Step3** In this page, you can select the WAN service type, and modify the service description. After finishing setting, click **Next** to display the following page.

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>Connection Type:</b>	Bridge
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Not Applicable
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

**Back****Apply/Save**

**Step4** In this page, it displays the information about the bridge settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

### 10.2.3 NAT

#### Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Choose **Advanced Setup > NAT > Virtual Servers**, and the following page appears.

##### NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
<input type="button" value="Add"/>								

In this page, you are allowed to add or remove a virtual server entry.

To add a virtual server, do as follows:

Click the **Add** button to display the following page.

## User Manual

## NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start". Remaining number of entries that can be configured: 22.**

Remaining number of entries that can be configured:32

- **Use interface:** Select an interface that you want to configure.
- **Select a Service:** Select a proper service in the drop-down list.
- **Custom Server:** Enter a new service name to establish a user service type.
- **Server IP Address:** Assign an IP address to virtual server.
- **External Port Start:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **External Port End:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

- **Protocol:** You may select TCP/UDP, TCP, or UDP in the drop-down list.
- **Internal Port Start:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
- **Internal Port End:** When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

After finishing setting, click **Save/Apply** to save and apply the settings.

## Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

Choose **Advanced Settings > NAT > Port Triggering**, and the following page appears.

### NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range Start	Port Range End	Protocol	Port Range Start	Port Range End		

Add

In this page, you may add or delete an entry of port triggering.

Click the **Add** button to display the following page.

## User Manual

## NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

- **Use interface:** Select an interface that you want to configure.
- **Select an application:** Select a proper application in the drop-down list.
- **Custom application:** Manually define an application.
- **Trigger port Start:** The start port number that LAN uses to trigger the open port.
- **Trigger port End:** The end port number that LAN uses to trigger the open port.
- **Trigger Protocol:** Select the application protocol. You may select TCP/UDP, TCP, or UDP.
- **Open Port Start:** The start port number that is opened to WAN.
- **Open Port End:** The end port number that is opened to WAN.
- **Open Protocol:** Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click **Save/Apply** to apply the settings.

**Note:**

*You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.*

## DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ host** to display the following page.

### NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

**DMZ Host IP Address:**

**Apply/Save**

In this page, enter the IP address of the DMZ host.

After finishing the settings, click the **Apply/Save** button to apply the settings.

If you want to clear the DMZ function of the host, please delete the IP address of the host in the field of **DMZ Host IP Address**, and then click the **Apply/Save** button.

## 10.2.4 Security

### Firewall

Choose **Security > Firewall** and the following page appears.

## User Manual

### Firewall Setup

Incoming/Outgoing traffic can be ACCEPTED/DROPPED/REJECTED by setting up firewall rules.

Choose Add or Remove to configure firewall or firewall rules.

Firewall Name	Interface	Type	Default action	Remove
---------------	-----------	------	----------------	--------

[Add Firewall](#)

### Firewall Rule Setup

Firewall Name	Protocol	ICMP type	Action	Reject type	SrcIP/PrefixLength	SrcPort	DstIP/PrefixLength	DstPort	Remove
---------------	----------	-----------	--------	-------------	--------------------	---------	--------------------	---------	--------

[Add Rule](#)

Click **Add Firewall**, and the following page appears.

#### Add firewall

The screen allows you to create a firewall. All of the specified conditions in this firewall must be satisfied for the firewall to take effect. Click 'Apply/Save' to save and activate the firewall.

Name:	<input type="text"/>
Interface:	<input type="text"/> pppoe_0_0_35/ppp0
Type:	<input type="text"/> In
Default action:	<input type="text"/> Permit

[Back](#)

[Apply/Save](#)

- **name:** The name of firewall.
- **Interface:** You can select the interface from the drop-down list.
- **Type:** You can select **In** or **Out** from the drop-down list.
- **Default action:** You can select **Permit** or **Drop** from the drop-down list.

Click **Add Rule**, and the following page appears.

### Add firewall rule

The screen allows you to create a firewall rule. All of the specified conditions in this firewall rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Firewall Name:	Firewall11
Protocol:	<input type="button" value="▼"/>
Action:	Permit
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address [/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Apply/Save"/>	

- **Firewall Name:** Select it from the drop-down list.
- **Protocol:** You can select **UDP**, **TCP**, or **ICMP** from the drop-down list.
- **Action:** You can select **Permit**, **Drop**, or **Reject** from the drop-down list.

After finishing setting, click **Save/Apply** to save and activate the rule.

### MAC Filtering Setup

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the DSL router serves as a firewall that works at layer 2.

#### Note:

*MAC filtering is only effective on ATM PVCs configured in bridge mode.*

Choose **Security > MAC Filtering** and the following page appears.

### MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
atm3	FORWARD	<input type="checkbox"/>

[Change Policy](#)

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<a href="#">Add</a>					

In this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from **FORWARDED** to **BLOCKED** by clicking the **Change Policy** button.

Click the **Add** button to display the following page.

#### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Source MAC Address:	<input type="text"/>
Frame Direction:	<input type="text" value="LAN&lt;=&gt;WAN"/>
WAN Interfaces (Configured in Bridge mode only)	
<input type="text" value="br_0_0_39/atm3"/>	
<a href="#">Save/Apply</a>	

- **Protocol Type:** Select the proper protocol type.
- **Destination MAC Address:** Enter the destination MAC address.

- **Source MAC Address:** Enter the source MAC address.
- **Frame Direction:** The direction of transmission frame.
- **WAN Interface (Configured in bridge mode only):** Select the proper WAN interface in the drop-down list.

After finishing setting, click **Apply/Save** to save and apply the filtering rule.

## DoS

Choose **Security > DoS** and the following page appears.

**DoS Settings**

Select the protection below.

<b>SYN Flood Attack</b>	<input type="checkbox"/>
<b>FIN/URG/PSH Attack</b>	<input type="checkbox"/>
<b>Ping Attack</b>	<input type="checkbox"/>
<b>Xmas Tree Attack</b>	<input type="checkbox"/>
<b>TCP reset Attack</b>	<input type="checkbox"/>
<b>Null scanning Attack</b>	<input type="checkbox"/>
<b>Ping of Death Attack</b>	<input type="checkbox"/>
<b>SYN/RST SYN/FIN Attack</b>	<input type="checkbox"/>
<b>LAND Attack</b>	<input type="checkbox"/>

**Apply/Save**

After selecting the protection, click **Apply/Save** to apply the settings.

### 10.2.5 Parental Control

#### Time Restriction

Choose **Advanced Setup > Parental Control > Time Restriction**, and the following page appears.

## User Manual

### Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
----------	-----	-----	-----	-----	-----	-----	-----	-----	-------	------	--------

Add

Click the **Add** button to display the following page.

#### Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name	<input type="text"/>						
<input checked="" type="radio"/> Browser's MAC Address	<input type="text"/>						
<input type="radio"/> Other MAC Address (xx:xx:xx:xx:xx:xx)	<input type="text"/>						
Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>						
Start Blocking Time (hh:mm)	<input type="text"/>						
End Blocking Time (hh:mm)	<input type="text"/>						

**Apply/Save**

This page is used to control the time restriction to a special LAN device that connects to the DSL router. In this page, set the user name and configure the time settings. After finishing setting, click the **Apply/Save** to save and apply the settings.

### Url Filter

Click **Advanced Setup > Parental Control > Url Filter**, and the following page appears.

## User Manual

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type:  Exclude  Include

**Address** **Port** **Remove**

**Add**

This page is used to prevent the LAN users from accessing some Websites in the WAN.

In this page, you may select the **Exclude** URL list type or the **Include** URL list type. If you select the **Exclude** URL list type, it means that the URLs in the list are not accessible. If you select the **Include** URL list type, you are allowed to access the URLs in the list.

Click the **Add** button to display the following page.

**Parental Control -- URL Filter Add**

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

**URL Address:**

**Port Number:**  (Default 80 will be applied if leave blank.)

**Apply/Save**

In this page, enter the URL address and its corresponding port number.

### 10.2.6 Quality of Service

#### Enabling QoS

Choose **Advance Setup > Quality of Service** and the following page appears.

## User Manual

### QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note:** If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

**Note:** The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS



Apply/Save

Select **Enable QoS** to enable QoS and configure the default DSCP mark.

### QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note:** If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

**Note:** The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS



Select Default DSCP Mark

No Change (-1)

Apply/Save

In this page, enable the QoS function and select the default DSCP mark.

After finishing setting, click **Apply/Save** to save and apply the settings.

#### **Note:**

If the **Enable QoS** checkbox is not selected, all QoS will be disabled for all interfaces.

The default DSCP mark is used to mark all egress packets that do not match any classification rules.

## Queue Configuration

Choose **Advanced Setup > Quality of Service > Queue Configuration**, and the following page appears.

### QoS Queue Setup

In ATM mode, maximum 16 queues can be configured. 8 queues are reserved for Wireless WMM. If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	Enable	Remove
Default Queue 35		atm0	SP	8		Path0	<input type="checkbox"/>	
Default Queue 36		atm1	SP	8		Path0	<input type="checkbox"/>	
Default Queue 37		atm2	SP	8		Path0	<input type="checkbox"/>	
Default Queue 38		ipoa0	SP	8		Path0	<input type="checkbox"/>	
Default Queue 39		atm3	SP	8		Path0	<input type="checkbox"/>	

**Add**

In this page, you can enable, add or remove a QoS rule.

#### Note:

*The lower integer value for precedence indicates the higher priority.*

Click the **Add** button to display the following page.

### QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

**Note:** For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others.

Click 'Apply/Save' to save and activate the queue.

**Name:**

**Enable:**

**Interface:**

**Apply/Save**

- **Name:** Enter the name of QoS queue.

- **Enable:** Enable or disable the QoS queue.
- **Interface:** Select the proper interface for the QoS queue.

After finishing setting, click **Apply/Save** to save and apply the settings.

## QoS Classification

Choose **Advanced Setup > Quality of Service > Qos Classification** and the following page appears.

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

The QoS function has been disabled. Classification rules would not take effects.

CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS							
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove

In this page, you can enable, add or remove a QoS classification rule.

Click the **Add** button to display the following page.

### Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:	<input type="text"/>
Rule Order:	Last <input type="button" value="▼"/>
Rule Status:	Disable <input type="button" value="▼"/>

#### Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:	<input type="text" value="LAN"/>
Ether Type:	<input type="text"/>
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>

#### Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:	<input type="text"/>
Mark Differentiated Service Code Point (DSCP):	<input type="text"/>
Mark 802.1p priority:	<input type="text"/>
Tag VLAN ID [0-4094]:	<input type="text"/>

In this page, enter the traffic name, select the rule order and the rule status, and specify the classification criteria and the classification results.

After finishing setting, click **Apply/Save** to save and apply the settings.

## 10.2.7 Routing

### Default Gateway

Choose **Advanced Setup > Routing > Default Gateway**, and the following page appears.

### Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0	atm1 ipoa0 ppp0al

**Apply/Save**



In this page, you can modify the default gateway settings.

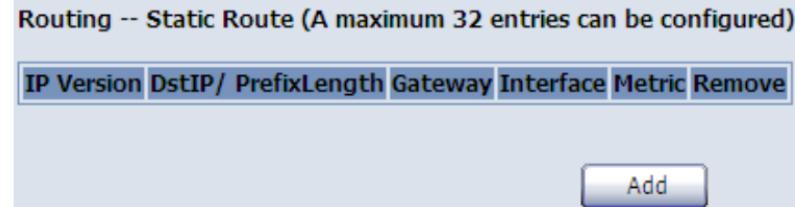
After finishing setting, click **Apply/Save** to save and apply the settings.

### Static Route

Choose **Advanced Setup > Routing > Static Route** and the following page appears.

### Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	Metric	Remove
					<b>Add</b>



Click the **Add** button to display the following page.

### Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:	IPv4
Destination IP address/prefix length:	<input type="text"/>
Interface:	<input type="text"/>
Gateway IP Address:	<input type="text"/>
(optional: metric number should be greater than or equal to zero)	
Metric:	<input type="text"/>

- **IP Version:** Select the IP version to be IPv4.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

After finishing setting, click **Apply/Save** to save and apply the settings.

### Policy Routing

Choose **Advanced Setup > Routing > Policy Routing** and the following page appears.

**Policy Routing Setting -- A maximum 8 entries can be configured.**

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
					<input type="button" value="Add"/>

In this page, you can add or remove a static policy rule.

Click the **Add** button to display the following page.

## User Manual

### Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.  
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:	<input type="text"/>
Physical LAN Port:	<input type="text"/>
Source IP:	<input type="text"/>
Use Interface:	<input type="text"/> ipoe_0_0_36/atm1
Default Gateway IP:	<input type="text"/>

In this page, enter the policy name, source IP and default gateway, and select the physical LAN port and interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

### RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.

Routing -- RIP Configuration

**NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).**

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to start/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm1	2	Passive	<input type="checkbox"/>
ipoa0	2	Passive	<input type="checkbox"/>
atm3	2	Passive	<input type="checkbox"/>

In this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

## 10.2.8 DNS

### DNS Server

Choose **Advanced Setup > DNS > DNS Server** and the following page appears.

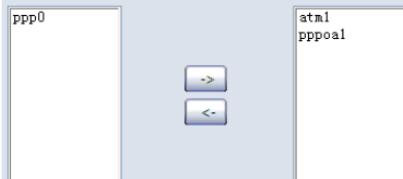
#### DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

**Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server  
Interfaces

Available WAN Interfaces



**Use the following Static DNS IP address:**

Primary DNS server:   
Secondary DNS server:

**Apply/Save**

In this page, you can select a DNS server interface from the available interfaces, or manually enter the DNS server addresses.

After finishing setting, click **Apply/Save** to save and apply the settings.

### Dynamic DNS

Choose **Advanced Setup > DNS > Dynamic DNS** and the following page appears.

#### Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

**Hostname** **Username** **Service** **Interface** **Remove**

**Add**

In this page, you are allowed to modify the DDNS settings.

Click the **Add** button to display the following page.

**Add Dynamic DNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

<b>D-DNS provider</b>	<input style="width: 100px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="DynDNS.org"/>
<b>Hostname</b>	<input type="text"/>
<b>Interface</b>	<input style="width: 100px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="ipoe_0_0_36/atm1"/>
<b>DynDNS Settings</b>	
<b>Username</b>	<input type="text"/>
<b>Password</b>	<input type="text"/>

- **D-DNS provider:** Select a proper DDNS server in the drop-down list.
- **Hostname:** It is the domain name and it can be modified.
- **Interface:** The interface that the packets pass through on the DSL router.
- **Username:** Enter the username for accessing the DDNS management interface.
- **Password:** Enter the password for accessing the DDNS management interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

### 10.2.9 DSL

Choose **Advanced Setup > DSL** and the following page appears.

**DSL Settings**

Select the modulation below.

G.Dmt Enabled	<input checked="" type="checkbox"/>
G.lite Enabled	<input checked="" type="checkbox"/>
T1.413 Enabled	<input checked="" type="checkbox"/>
ADSL2 Enabled	<input checked="" type="checkbox"/>
AnnexL Enabled	<input checked="" type="checkbox"/>
ADSL2+ Enabled	<input checked="" type="checkbox"/>
AnnexM Enabled	<input type="checkbox"/>

Select the phone line pair below.

Inner pair	<input checked="" type="radio"/>
Outer pair	<input type="radio"/>

**Capability**

Bitswap Enable	<input checked="" type="checkbox"/>
SRA Enable	<input type="checkbox"/>

**Apply/Save**

**Advanced Settings**

In this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings.

After finishing setting, click **Apply/Save** to save and apply the settings.

### 10.2.10 UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

**UPnP Configuration**

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

**Enable UPnP**

**Apply/Save**

In this page, you can enable or disable the UPnP function.

After finishing setting, click **Apply/Save** to save and apply the settings.

### 10.2.11 DNS Proxy

Choose **Advanced Setup > DNS Proxy** and the following page appears.

**DNS Proxy Configuration**

**Enable DNS Proxy**

**Host name of the Broadband Router:**

**Domain name of the LAN network:**

**Apply/Save**

In this page, you can enable or disable the DNS proxy function.

After enabling the DNS proxy function, enter the host name of the broadband router and the domain name of the LAN network, and then click **Apply/Save** to save and apply the settings.

## 10.2.12 Storage Service

### Storage Device Info

Choose **Advanced Setup > Storage Service > Storage Device Info** and the following page appears.

**Storage Service**

The Storage service allows you to use Storage devices with modem to be more easily accessed.

Volume Name	File System	Total Space	Used Space	Actions
-------------	-------------	-------------	------------	---------

This page is used to display the information of the storage device that connects to the DSL router.

### FTP Configuration

Choose **Advanced Setup > Storage Service > FTP Configuration** and the following page appears. In this page, you can set the password for the ftp user account.

**FTP Configuration for Storage Service**

Access to the storage devices via FTP can be configured in the following ways.

- Setting password for the FTP user account.

**Password for ftp user account(ftpuser):**  [Click here to display](#)

**Apply/Save**

Click [Click here to display](#) to view the password for ftp user account.



### Samba Configuration

Choose **Advanced Setup > Storage Service > Samba Configuration** and the following page appears.

### Samba Configuration for Storage Service

Access to your USB storage devices via Samba is always active. You can access them in the following ways.

- Simply open your File Explore and go to \\Accton-Router. Then click on "Storage" where you will see your devices.
- On Windows, you can use "Tools->Map network driver..." to create a shortcut to \\Accton-Router\Storage.
- Or simply click [here](#).

Samba setting to enables or disables write operation from WAN or LAN side.

Services	WAN	LAN
Samba Writable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Apply/Save**

In this page, you can enable or disable writing operation from WAN or LAN side. After proper configuration, click **Apply/Save** to apply the settings.

### 10.2.13 Interface Grouping

Choose **Advanced Setup > Interface Grouping** and the following page appears.

**Interface Grouping -- A maximum 16 entries can be configured**

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP	Vendor IDs
Default		ppp0	eth0		
		atm1	eth1		
		atm3	eth2		
			eth3		
			wlan0		

**Add**

**Remove**

Interface grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with the appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the default group. Only the default group has IP interface.

## User Manual

---

Click the **Add** button to display the following page.

### Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses.**
4. Click Apply/Save button to make the changes effective immediately.

**IMPORTANT: If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.**

**Group Name:**

Group Name:

**WAN Interface used in the grouping**

#### Grouped LAN Interfaces

#### Available LAN Interfaces

eth0  
eth1  
eth2  
eth3  
wlan0

**Automatically Add  
Clients With the  
following DHCP Vendor  
IDs**

In this page, please follow the on-screen configuration steps to configure the parameters of the interface grouping.

After finishing setting, click **Apply/Save** to save and apply the settings.

### 10.2.14 Multicast

Choose **Advanced Setup > Multicast** and the following page appears.

**IGMP Configuration**

Enter IGMP protocol configuration fields if you want modify default values shown below.

<b>Default Version:</b>	3
<b>Query Interval:</b>	125
<b>Query Response Interval:</b>	10
<b>Last Member Query Interval:</b>	10
<b>Robustness Value:</b>	2
<b>Maximum Multicast Groups:</b>	25
<b>Maximum Multicast Data Sources (for IGMPv3 : (1 - 24)):</b>	10
<b>Maximum Multicast Group Members:</b>	25
<b>Fast Leave Enable:</b>	<input checked="" type="checkbox"/>
<b>LAN to LAN (Intra LAN) Multicast Enable:</b>	<input checked="" type="checkbox"/>

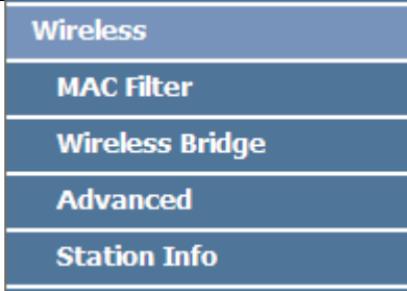
**Apply/Save**

In this page, you can configure the multicast parameters.

After finishing setting, click **Apply/Save** to save and apply the settings.

### 10.2.15 Wireless

Choose **Advanced Setup > Wireless** and the submenus of **Wireless** are shown as below:



### 10.2.15.1 MAC Filter

Choose **Wireless > MAC Filter** to display the following page.

Wireless -- MAC Filter

Select SSID:	SMC
MAC Restrict Mode:	<input checked="" type="radio"/> Disabled <input type="radio"/> Allow <input type="radio"/> Deny
<b>MAC Address</b> <b>Remove</b>	
<b>Add</b>	

This page is used to allow or reject the wireless clients to access the wireless network of the wireless router.

In this page, you can add or remove the MAC filters.

The MAC restrict modes include **Disabled**, **Allow**, and **Deny**.

- **Disabled**: Disable the wireless MAC address filtering function.
- **Allow**: Allow the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

- **Deny:** Reject the wireless clients with the MAC addresses in the **MAC Address** list to access the wireless network of the wireless router.

Click the **Add** button to display the following page.

**Wireless -- MAC Filter**

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

Apply/Save

In this page, enter the MAC address of the wireless client, and then click the **Apply/Save** button to add the MAC address to the MAC address list.

### 10.2.15.2 Wireless Bridge

Choose **Wireless > Wireless Bridge** to display the following page.

**Wireless -- Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled, Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:	Access Point
Bridge Restrict:	Enabled
Remote Bridges MAC Address:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

Refresh Apply/Save

This page allows you to configure the wireless bridge features of the wireless LAN interface.

- **AP mode:** you may select Access Point or Wireless Bridge.
- **Bridge Restrict:** Enable or disable the bridge restrict function.
- **Remote Bridges MAC Address:** Enter the remote bridge MAC address.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

### **10.2.15.3 Advanced Settings**

Choose **Wireless > Advanced** to display the following page. This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings in this page.

## Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in Both Bands	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existance:	Enable	
RX Chain Power Save:	Disable	
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Disabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

- **Band:** The radio frequency remains at 2.4GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer(min):** Specifies the timer of auto channelling.
- **802.11n/EWC:** Select **disable** 802.11n or **Auto**.
- **Bandwidth:** Select the bandwidth for the network. You can select **20MHz in Both Bands** or **40MHz in Both Bands**.
- **Control Sideband:** If you select **20MHz in Both Bands** the service of control sideband does not work. When you select **40MHz in Both Bands** as the bandwidth, you can select **Lower** or **Upper** as the value of sideband.
- **802.11n Rate/54g Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **802.11n Protection:** The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.
- **Support 802.11n Client Only:** Only stations that are configured in 802.11n mode can associate.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving

an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.

- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **XPress Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default is Disabled.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
- **WMM (Wi-Fi Multimedia):** Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
- **WMM No Acknowledgement:** Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledgement packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
- **WMM APSD:** APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

**Note:**

*The advanced wireless setting is only for the advanced user. For the common user, do not change any settings in this page.*

#### **10.2.15.4 Station Info**

Choose **Wireless > Station Info** to display the following page.

## Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

**MAC Associated Authorized SSID Interface**

**Refresh**

This page shows the authenticated wireless stations and their status.

## 10.3 Management

Choose **Management** and the submenus of **Management** are shown as below:



### 10.3.1 Passwords Settings

Choose **Management > Passwords Settings**, and the following page appears.

### Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords.  
Note: Password cannot contain a space.

User Name:	<input type="text" value="admin"/>
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

In the page, you can modify the password of different users. The default password of the admin user is **smcadmin**. After finishing setting, click the **Apply/Save** button to save and apply the settings.

### 10.3.2 Internet Time

Choose **Management > Internet Time** to display the following page.

**Time settings**

This page allows you to the modem's time configuration.

**Automatically synchronize with Internet time servers**

First NTP time server:	time.nist.gov	<input style="width: 20px; height: 20px;" type="button" value="..."/>	<input style="width: 150px; height: 20px;" type="text"/>
Second NTP time server:	clock.nyc.he.net	<input style="width: 20px; height: 20px;" type="button" value="..."/>	<input style="width: 150px; height: 20px;" type="text"/>
Third NTP time server:	None	<input style="width: 20px; height: 20px;" type="button" value="..."/>	<input style="width: 150px; height: 20px;" type="text"/>
Fourth NTP time server:	None	<input style="width: 20px; height: 20px;" type="button" value="..."/>	<input style="width: 150px; height: 20px;" type="text"/>
Fifth NTP time server:	None	<input style="width: 20px; height: 20px;" type="button" value="..."/>	<input style="width: 150px; height: 20px;" type="text"/>

Time zone offset: (GMT-05:00) Eastern Time

In this page, you may configure the router to synchronize its time with the Internet time servers, and then click the **Apply/Save** button to save and apply the settings.

### 10.3.3 Diagnostics

Choose **Management > Diagnostics**, and the following page appears.

**pppoe\_0\_0\_35 Diagnostics**

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your eth0 Connection:	FAIL	<a href="#">Help</a>
Test your eth1 Connection:	PASS	<a href="#">Help</a>
Test your eth2 Connection:	FAIL	<a href="#">Help</a>
Test your eth3 Connection:	FAIL	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

**Test the connection to your DSL service provider**

Test xDSL Synchronization:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	DISABLED	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	DISABLED	<a href="#">Help</a>

**Test the connection to your Internet service provider**

Test PPP server connection:	DISABLED	<a href="#">Help</a>
Test authentication with ISP:	DISABLED	<a href="#">Help</a>
Test the assigned IP address:	DISABLED	<a href="#">Help</a>
Ping default gateway:	FAIL	<a href="#">Help</a>
Ping primary Domain Name Server:	FAIL	<a href="#">Help</a>

[Next Connection](#)[Test](#)[Test With OAM F4](#)

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button.

### 10.3.4 Settings

#### Backup

Choose **Management > Settings > Backup** to display the following page.

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

[Backup Settings](#)

In this page, click the **Backup Settings** button to save your router's settings to your local PC.

## Update

Choose **Management > Settings > Update**, and the following page appears.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

In this page, click the **Browse...** button to select the correct new settings file, and then click the **Update Settings** button to update the router's settings.

## Restore Default

Choose **Management > Settings > Restore Default** to display the following page.

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

In this page, click the **Restore default settings** button, and then system returns to the default settings.

### 10.3.5 System Log

Choose **Management > System Log** to display the following page.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "View Firewall Log" to view the Firewall Log.

Click "Configure System Log" to configure the System Log options.

- **View System Log:** Click this button to view the system log.
- **View Firewall Log:** Click this button to view the firewall log.
- **Configuring the System Log:** Click this button to display the following page.

#### System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Log Level:	Debugging
Display Level:	Error
Mode:	Error

Log Level: Debugging

Display Level: Error

Mode: Error

Error  
Emergency  
Alert  
Critical  
Warning  
Notice  
Informational  
Debugging

Apply/Save

In this page, you can set 3 types of system log modes, including **Local**, **Remote**, and **Both**.

- **Local:** When selecting **Local**, the events are recorded in the local memory.
- **Remote:** When selecting **Remote**, the events are sent to the specified IP address and UDP port of the remote system log server.
- **Both:** When selecting **Both**, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

**Note:**

*If you want to log all the events, you need to select the **Debugging** log level.*

#### 10.3.6 SNMP Agent

Choose **Management > SNMP Agent**, and the following page appears.

### SNMP - Configuration

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

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent  Disable  Enable

Read Community:	public
Set Community:	private
System Name:	Aciton
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

**Apply/Save**

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

In this page, you may enable or disable the SNMP agent and set the parameters such as the read community, system name and trap manager IP.

After finishing setting, click the **Save/Apply** button to save and apply the settings.

### 10.3.7 TR-69 Client

Choose **Management > TR-069Client** to display the following page.

**TR-069 client - Configuration**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

<b>Inform</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Inform Interval:</b>	300
<b>ACS URL:</b>	
<b>ACS User Name:</b>	admin
<b>ACS Password:</b>	*****
<b>WAN Interface used by TR-069 client:</b>	Any_WAN
 <b>Display SOAP messages on serial console</b> <input checked="" type="radio"/> Disable <input type="radio"/> Enable	
 <b>Connection Request Authentication</b> <input checked="" type="checkbox"/>	
<b>Connection Request User Name:</b>	admin
<b>Connection Request Password:</b>	*****
<b>Connection Request URL:</b>	

**Apply/Save**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

In this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

### 10.3.8 Access Control- Services

Choose **Management > Access Control** and the following page appears.

## Access Control -- Services

A Service control List ("SCL") enables or disables services from being used.

Services	LAN	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	80
TELNET	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	23
SSH	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	22
FTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	21
TFTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	69
ICMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	0
SNMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	161
SAMBA	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	139

Enable IP Limit for Management Service:

**Apply/Save**

In this page, you can enable or disable the different types of services.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

### 10.3.9 Update Software

Choose **Management > Update Software**, and the following page appears.

Tools -- **Update Software**

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name:	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Update Software"/>		

If you want to upload the software, click the **Browse...** button to choose the new software, and then click the **Update Software** button.

**Note:**

*When software update is in progress, do not shut down the router. After software update completes, the router automatically reboots.*

*Please make sure that the new software for updating is correct, and do not use other software to update the router.*

### 10.3.10 Reboot

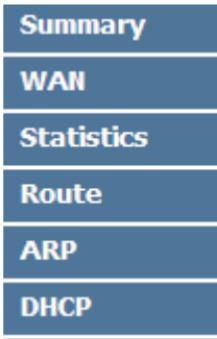
Choose **Management > Reboot** and the following page appears.

**Click the button below to reboot the router.**

In this page, click the **Reboot** button, and then the router reboots.

## 10.4 Device Information

Choose **Device Info**, and the submenus of **Device Info** are shown as below:



### 10.4.1 Summary

Choose **Device Info > Summary**, and the following page appears.

**Device Info**

<b>Board ID:</b>	96328ang
<b>Build Timestamp:</b>	110111_1747
<b>Software Version:</b>	0.0.0.1
<b>Bootloader (CFE) Version:</b>	1.0.37-106.17
<b>DSL PHY and Driver Version:</b>	A2pD030i.d23a
<b>Wireless Driver Version:</b>	5.60.120.1.cpe4.06L02.2

This information reflects the current status of your WAN connection.

<b>Line Rate - Upstream (Kbps):</b>	0
<b>Line Rate - Downstream (Kbps):</b>	0
<b>LAN IPv4 Address:</b>	192.168.2.1
<b>Default Gateway:</b>	
<b>Primary DNS Server:</b>	0.0.0.0
<b>Secondary DNS Server:</b>	0.0.0.0
<b>Date/Time:</b>	Thu Jan 1 02:08:38 1970

This page displays the device information such as the board ID, software version, and the information of your WAN connection such as the upstream rate and the LAN IPv4 address.

## 10.4.2 WAN

Choose **Device Info > WAN** and the following page appears.

### WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address
atm1	ipoe_0_0_36	IPoE	Disabled	Disabled	Disabled	Disabled	Unconfigured	0.0.0.0
ipoa0	ipoa_0_0_38	IPoA	Disabled	Disabled	Disabled	Disabled	Unconfigured	12.12.12.21
atm3	br_0_0_39	Bridge	Disabled	Disabled	Disabled	Disabled	Unconfigured	0.0.0.0
ppp0	pppoe_0_0_35	PPPoE	Disabled	Disabled	Enabled	Enabled	Unconfigured	(null)
pppoa1	ppoa_0_0_37	PPPoA	Disabled	Disabled	Enabled	Enabled	Unconfigured	(null)

This page displays the information of the WAN interface, such as the connection status, and IPv4 address.

## 10.4.3 Statistics

### 10.4.4 LAN

Choose **Device Info > Statistics > LAN** and the following page appears.

### Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	0	0	0	0
eth1	724818	7345	0	0	8599071	8734	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	4	0	0	0	18	0

**Reset Statistics**

In this page, you can view the statistical information about the received and transmitted data packets of the Ethernet and wireless interfaces.

Click **Reset Statistics** to restore the values to zero and recount them.

### 10.4.5 WAN Service

Choose **Device Info > Statistics > WAN Service** and the following page appears.

Statistics -- WAN

Interface	Description	Received				Transmitted				Up Time
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	
atm1	ipoe_0_0_36	0	0	0	0	0	0	0	0	0
ipoa0	ipoa_0_0_38	0	0	0	0	0	0	0	0	0
atm3	br_0_0_39	0	0	0	0	0	0	0	0	0
ppp0	pppoe_0_0_35	0	0	0	0	0	0	0	0	0
pppoa1	pppoa_0_0_37	0	0	0	0	0	0	0	0	0

**Reset Statistics**

In this page, you can view the statistical information about the received and transmitted data packets of the WAN interface.

Click **Reset Statistics** to restore the values to zero and recount them.

### 10.4.6 xTM

Choose **Device Info > Statistics > xTM** and the following page appears.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
<b>Reset</b>										

In this page, you can view the statistical information about the received and transmitted data packets at the xTM interfaces.

Click the **Reset** button to restore the values to zero and recount them.

### 10.4.7 xDSL

Choose **Device Info > Statistics > xDSL** and the following page appears.

## Statistics -- xDSL

Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		
	xDSL BER Test	Reset Statistics

In this page, you can view the statistical information about the received and transmitted data packets of the xDSL interfaces.

Click **xDSL BER Test** to test the xDSL Bit Error Rate.

Click **Reset Statistics** to restore the values to zero and recount them.

#### 10.4.8 Route

Choose **Device Info > Route** and the following page appears.

##### Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate  
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.2.0	0.0.0.0	255.255.255.0	U	0		br0

In this page, you can view the route table information.

#### 10.4.9 ARP

Choose **Device Info > ARP** and the following page appears.

##### Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.2.12	Complete	00:1d:0f:19:91:c1	br0

In this page, you can view the MAC address and IP address information of the device connected to the router.

#### 10.4.10 DHCP

Choose **Device Info > DHCP** and the following page appears.

##### Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

## User Manual

---

In this page, you can view the host name, the IP address assigned by the DHCP server, the MAC address which is corresponding to the IP address, and the DHCP lease time.

## 11 Q&A

(1) **Q:** Why all the indicators are off?

**A:** Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.

(2) **Q:** Why the **LAN** indicator is off?

**A:** Check the following:

- The connection between the ADSL router and your computer, hub, or switch.
- The running status of your PC, hub, or switch.

(3) **Q:** Why the **DSL** indicator is off?

**A:** Check the connection between the “Line” port of router and the wall jack.

(4) **Q:** Why Internet access fails while the **DSL** indicator is on?

**A:** Check whether the VPI, VCI, user name, and password are correctly entered.

(5) **Q:** Why I fail to access the web configuration page of the DSL router?

**A:** Choose **Start > Run** from the desktop, and ping **192.168.2.1** (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.

(6) **Q:** How to load the default settings after incorrect configuration?

**A:** To restore the factory default settings, turn on the device, and press the reset button for about 1 second, and then release it. The default IP address and the subnet mask of the DSL router are **192.168.2.1** and **255.255.255.0**, respectively.

- User/password of super user: **admin/smcadmin**

U.S.A Office  
20 Mason  
Irvine CA 92618  
Phn: (949) 679-8000

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

#### TECHNICAL SUPPORT

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

**English:** Technical Support information available at [www.smc.com](http://www.smc.com)

**English (For Asia Pacific):** Technical Support information available at [www.smc-asia.com](http://www.smc-asia.com)

**Deutsch:** Technischer Support und weitere Information unter [www.smc.com](http://www.smc.com)

**Español:** En [www.smc.com](http://www.smc.com) Ud. podrá encontrar la información relativa a servicios de soporte técnico

**Français:** Informations Support Technique sur [www.smc.com](http://www.smc.com)

**Português:** Informações sobre Suporte Técnico em [www.smc.com](http://www.smc.com)

**Italiano:** Le informazioni di supporto tecnico sono disponibili su [www.smc.com](http://www.smc.com)

**Svenska:** Information om Teknisk Support finns tillgängligt på [www.smc.com](http://www.smc.com)

**Nederlands:** Technische ondersteuningsinformatie beschikbaar op [www.smc.com](http://www.smc.com)

**Polski:** Informacje o wsparciu technicznym sa dostepne na [www.smc.com](http://www.smc.com)

**Čeština:** Technicka podpora je dostupna na [www.smc.com](http://www.smc.com)

**Magyar:** Műszaki támogat informacio elérhető -on [www.smc.com](http://www.smc.com)

**简体中文:** 技术支持讯息可通过[www.smc-prc.com](http://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](http://www.smcnetworks.com.tw)

**ไทย:** สามารถดาวน์โหลดทุกหัวข้อแม่พกพาได้ที่ [www.smc-asia.com](http://www.smc-asia.com)

**한국어:** 기술지원관련 정보는 [www.smc-asia.com](http://www.smc-asia.com)을 참고하시기 바랍니다

#### INTERNET

E-mail address: [www.smc.com](http://www.smc.com)→ Support→ By email  
Driver updates: [www.smc.com](http://www.smc.com)→ Support→ Downloads

World Wide Web: [http://www.smc.com/](http://www.smc.com)

