SMC® Networks

USER GUIDE

Barricade™ N
150 Mbps 4-Port Wireless Broadband Router

SMCWBR14S-N4

Barricade™ SMCWBR14S-N4 User Guide

SMC® Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

August 2009
Pub. # 149100000034W
E082009-DT-R01

Warranty and Product Registration

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

COMPLIANCES

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

IC STATEMENT

This Class B digital apparatus complies with Canadian ICES-003.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

TAIWAN NCC

根據交通部低功率管理辦法規定：

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

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

EC CONFORMANCE DECLARATION CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety

This device is intended for use in the following European Community and EFTA countries:

- Austria
- Belgium
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Kingdom

NOTE: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

DECLARATION OF CONFORMITY IN LANGUAGES OF THE EUROPEAN COMMUNITY

Czech Česky	Manufacturer tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Estonian Eesti	Käesolevaga kinnitab Manufacturer seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Manufacturer, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish Suomi	Valmistaja Manufacturer vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch Nederlands	Hierbij verklaart Manufacturer dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze Manufacturer dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French Français	Par la présente Manufacturer déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Swedish Svenska	Härmed intygar Manufacturer att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish Dansk	Undertegnede Manufacturer erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF

German Deutsch	Hiermit erklärt Manufacturer, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt Manufacturer die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek Ελληνική	με την παρουσα Manufacturer δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ.
Hungarian Magyar	Alulírott, Manufacturer nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Italian Italiano	Con la presente Manufacturer dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian Latviski	Ar šo Manufacturer deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo Manufacturer deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Maltese Malti	Hawnhekk, Manufacturer, jiddikjara li dan Radio LAN device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Spanish Español	Por medio de la presente Manufacturer declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Polish Polski	Niniejszym Manufacturer oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	Manufacturer declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak Slovensky	Manufacturer týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	Manufacturer izjavlja, da je ta radio LAN device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

About This Guide

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

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

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

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

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

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

Related Publications As part of the Wireless Broadband Router's software, there is an online web-based help that describes all management related features.

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

August 2009 Revision
This is the first revision of this guide. It is valid for software release v.0.0.3.0.

CONTENTS

WARRANTY AND PRODUCT REGISTRATION 4

COMPLIANCES 5

ABOUT THIS GUIDE 10

CONTENTS 11

FIGURES 16

TABLES 19

SECTION I GETTING STARTED 20

1 INTRODUCTION 21

Key Hardware Features 21

Description of Capabilities 21

Applications 22

Package Contents 23

Hardware Description 23

LED Indicators 25

Ethernet WAN Port 26

Ethernet LAN Ports 26

Power Connector 26

Reset Button 27

WPS Button 27

2 NETWORK PLANNING 29

Internet Gateway Router 29

LAN Access Point 30

Wireless Bridge 31

3 INSTALLING THE GATEWAY ROUTER 33

System Requirements 33

Location Selection 33
Mounting on a Wall 34
Mounting on a Horizontal Surface 35
Gateway Mode Connections 35
Bridge Mode Connections 36

4 INITIAL CONFIGURATION 38
ISP Settings 38
Connecting to the Login Page 38
Home Page and Main Menu 39
Common Web Page Buttons 40
Setup Wizard 40
Step 1 - Language Selection 40
Step 2 - SNTP Settings 41
Step 3 - WAN Settings - DHCP 42
Step 3 - WAN Settings - Static IP 43
Step 3 - WAN Settings - PPPoE 44
Step 3 - WAN Settings - PPTP 45
Step 4 - Wireless Security 46
Completion 46

SECTION II WEB CONFIGURATION 47

5 OPERATION MODE 49
Logging In 50
Operation Mode 52

6 INTERNET SETTINGS 53
WAN Setting 53
DHCP 53
Static IP 55
PPPoE 56
PPTP 57
LAN Setting 59
Advanced Routing 61
Advanced Routing Settings 61
Routing Table 62

Dynamic Route 63

7 WIRELESS CONFIGURATION 65
Wireless Settings 65
Basic Settings 66
HT Physical Mode Settings 68
Wireless Distribution System (WDS) 69
Wi-Fi Protected Setup (WPS) 71
Station List 74

8 FIREWALL CONFIGURATION 75
MAC/IP/Port Filtering 75
Current Filter Rules 77
Virtual Server Settings (Port Forwarding) 78
Current Virtual Servers in system 79
DMZ 79
System Security 80
Content Filtering 81

9 ADMINISTRATION SETTINGS 83
System Management 84
Language Settings 84
Web Interface Settings 84
SNTP Settings 85
DDNS Settings 86
Upgrade Firmware 87
Configuration Settings 88
System Status 89
Statistics 91
System Log 92

SECTION III APPENDICES 94

A TROUBLESHOOTING 95
Diagnosing LED Indicators 95
If You Cannot Connect to the Internet 95
Before Contacting Technical Support 95

B HARDWARE SPECIFICATIONS 98

C CABLES AND PINOUTS 100

Twisted-Pair Cable Assignments 100

10/100BASE-TX Pin Assignments 101

Straight-Through Wiring 101

Crossover Wiring 102

D LICENSE INFORMATION 103

The GNU General Public License 103

GLOSSARY 107

INDEX 111

FIGURES

Figure 1: Top Panel 24
Figure 2: Rear Panel 25
Figure 3: LEDs 25
Figure 4: Operating as an Internet Gateway Router 30
Figure 5: Operating as an Access Point 31
Figure 6: Operating as a Wireless Bridge 32
Figure 7: Wall Mounting 34
Figure 8: Gateway Mode Connection 35
Figure 9: Bridge Mode Connection 36
Figure 10: Login Page 39
Figure 11: Home Page 39
Figure 12: Wizard Step 1 - Language Selection 40
Figure 13: Wizard Step 2 - Time and SNTP Settings 41
Figure 14: Wizard Step 3 - WAN Settings - DHCP 42
Figure 15: Wizard Step 3 - WAN Settings - Static IP 43
Figure 16: Wizard Step 3 - WAN Settings - PPPoE 44
Figure 17: Wizard Step 3 - WAN Settings - PPTP 45
Figure 18: Wizard Step 4 - Wireless Security 46
Figure 19: Logging On 50
Figure 20: Home Page 51
Figure 21: Operation Mode (Gateway) 52
Figure 22: DHCP Configuration 54
Figure 23: Static IP Configuration 55
Figure 24: PPPoE Configuration 56
Figure 25: PPTP Configuration 57
Figure 26: LAN Configuration 59
Figure 27: Advanced Routing (Gateway Mode) 61
Figure 28: Basic Settings 66
Figure 29: HT Physical Mode Settings 68
Figure 30: Enabling WPS 72
Figure 31: WPS Configuration 72

Figure 32: Station List 74
Figure 33: MAC/IP/Port Filtering 76
Figure 34: Virtual Server 78
Figure 35: DMZ 79
Figure 36: System Security 80
Figure 37: Content Filtering 81
Figure 38: System Management 84
Figure 39: SNTP Settings 85
Figure 40: DDNS Settings (Gateway Mode) 86
Figure 41: Upgrade Firmware 87
Figure 42: Configuration Settings 88
Figure 43: System Status (Gateway Mode) 89
Figure 44: Statistics 91
Figure 45: System Log 92
Figure 46: RJ-45 Connector 100
Figure 47: Straight-through Wiring 102
Figure 48: Crossover Wiring 102

TABLES

Table 1: Key Hardware Features 21
Table 2: LED Behavior 26
Table 3: LED Indicators 95
Table 4: 10/100BASE-TX MDI and MDI-X Port Pinouts 101

SECTION I

GETTING STARTED

This section provides an overview of the Wireless Broadband Router, and describes how to install and mount the unit. It also describes the basic settings required to access the management interface and run the setup Wizard.

This section includes these chapters:

- "Introduction" on page 21
- "Network Planning" on page 29
- "Initial Configuration" on page 38
- "Installing the Gateway Router" on page 33

1 INTRODUCTION

The Barricade Wireless Broadband Router (SMCWBR14S-N4) supports routing from an Internet Service Provider (ISP) connection (DSL or cable modem) to a local network. It is simple to configure and can be up and running in minutes.

KEY HARDWARE FEATURES

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

Table 1: Key Hardware Features

Feature	Description
WAN Port	One 100BASE-TX RJ-45 port for connecting to the Internet.
4 LAN Ports	Four 100BASE-TX RJ-45 ports for local network connections.
WPS Button	To set up a secure connection to a wireless device.
Reset Button	For resetting the unit and restoring factory defaults.
LEDs	Provides LED indicators for Power, WAN port, and LAN ports status.
Mounting Options	Can be mounted on any horizontal surface such as a desktop or shelf, or on a wall using two screws.

DESCRIPTION OF CAPABILITIES

- Internet connection through an RJ-45 WAN port.
- Local network connection through four 10/100 Mbps Ethernet ports.
- DHCP for dynamic IP configuration.
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT.
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, e-mail, and Telnet).
- VPN pass-through (PPTP).
- User-definable application sensing tunnel supports applications requiring multiple connections.

- Easy setup through a Web browser on any operating system that supports TCP/IP.
- Compatible with all popular Internet applications.

In addition, the Gateway Router offers full network management capabilities through an easy-to-configure web interface.

APPLICATIONS

Many advanced networking features are provided by the Barricade:

- **Wired LAN** — The Barricade provides connectivity to wired 10/100 Mbps devices, making it easy to create a network in small offices or homes.
- **Internet Access** — This device supports Internet access through a WAN connection. Since many DSL providers use PPPoE to establish communications with end users, the Barricade includes built-in clients for these protocols, eliminating the need to install these services on your computer.
- **Shared IP Address** — The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the Web at the same time.
- **Virtual Server** — If you have a fixed IP address, you can set the Barricade to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Barricade can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.
- **DMZ Host Support** — Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.
- **Security** — The Barricade supports security features that deny Internet access to specified users, or filter all requests for specific services the administrator does not want to serve. WPA (Wi-Fi Protected Access) and MAC filtering provide security over the wireless network.
- **Virtual Private Network (VPN)** — The Barricade supports one of the most commonly used VPN protocols – PPTP. This protocol allows remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network). The VPN protocols supported by the Barricade are briefly described below.

- **Point-to-Point Tunneling Protocol** — Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.

PACKAGE CONTENTS

The Barricade Wireless Broadband Router package includes:

- Barricade Wireless Broadband Router
- RJ-45 Category 5 network cable
- AC power adapter
- Quick Installation Guide
- EZ Installation & Documentation CD

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

HARDWARE DESCRIPTION

The Barricade Wireless Broadband Router, from herein refered to as Gateway Router, connects to the Internet using its RJ-45 WAN port. It connects directly to your PC or to a local area network using its RJ-45 Fast Ethernet LAN ports.

The Gateway Router includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting.

Figure 1: Top Panel

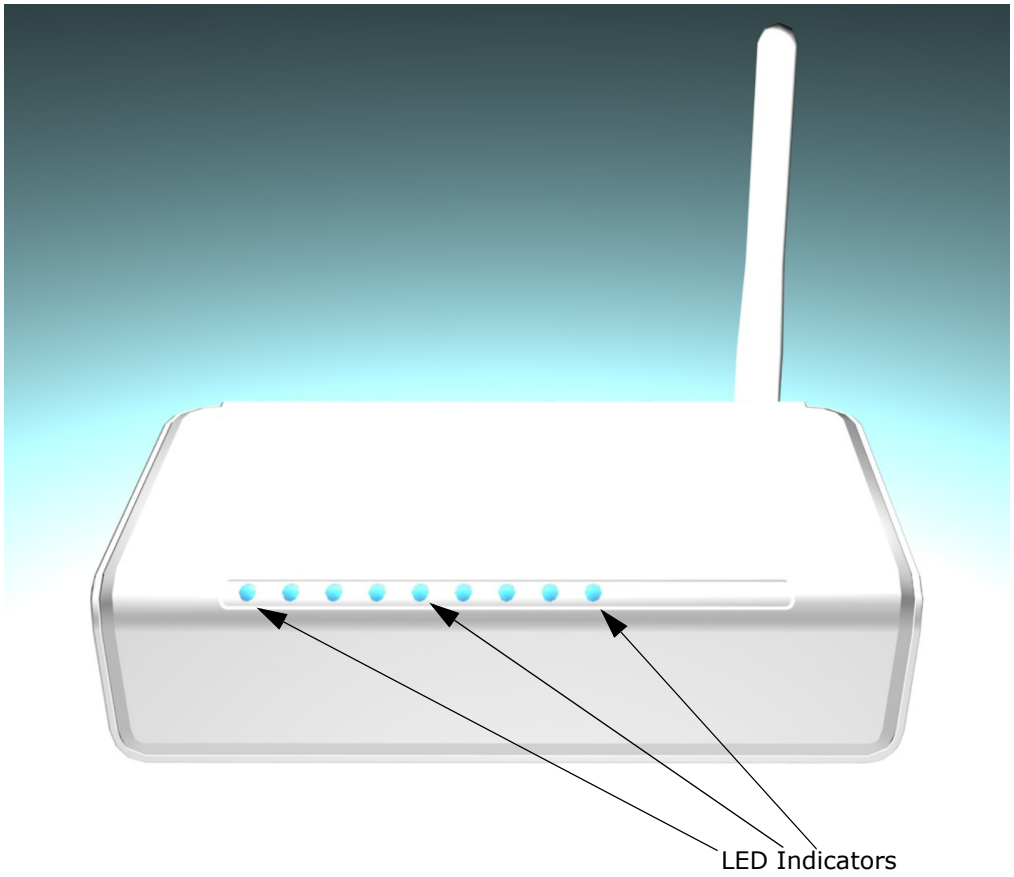
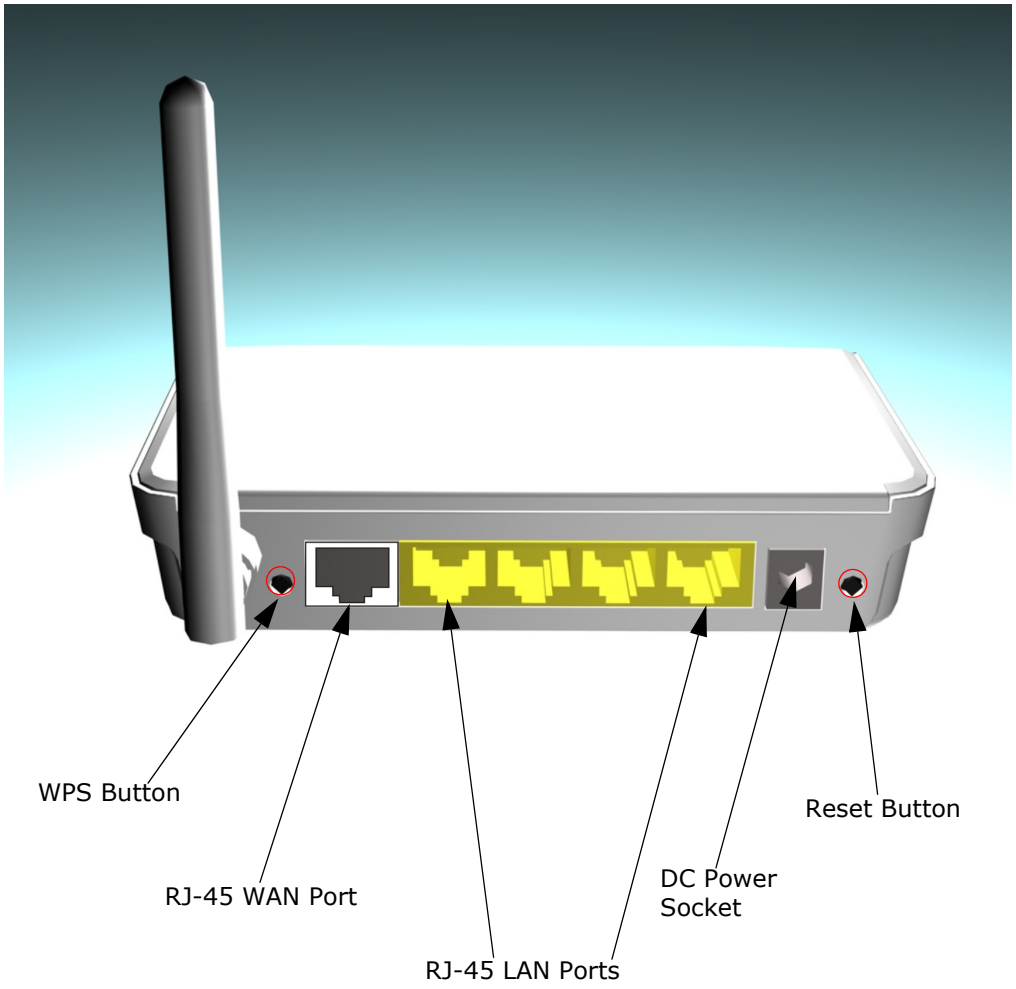


Figure 2: Rear Panel



LED INDICATORS

The Wireless Broadband Router includes seven status LED indicators, as described in the following figure and table.

Figure 3: LEDs

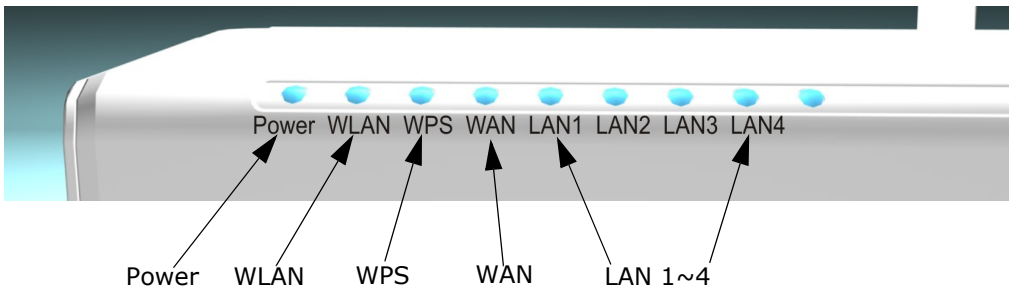


Table 2: LED Behavior

LED	Status	Description
Power	On Blue	The unit is receiving power and is operating normally.
	Off	There is no power currently being supplied to the unit.
WLAN	On/Blinking Blue	The 802.11n radio is enabled and transmitting or receiving data through wireless links.
	Off	The 802.11n radio is disabled.
WPS	Blinking	WPS authentication is in progress.
	Off	WPS authentication is not in progress.
WAN	On Blue	The Ethernet WAN port is aquiring an IP address.
	Blinking	The Ethernet WAN port is connected and is transmitting/receiving data.
	Off	The Ethernet WAN port is disconnected or has malfunctioned.
LAN1~LAN4	On Blue	The Ethernet LAN port is connected to a PC or server.
	Blinking	The Ethernet port is connected and is transmitting/receiving data.
	Off	The Ethernet port is disconnected or has malfunctioned.

ETHERNET WAN PORT

A 100BASE-TX RJ-45 port that can be attached to an Internet access device, such as a DSL or Cable modem.

ETHERNET LAN PORTS

The Wireless Broadband Router has four 100BASE-TX RJ-45 ports that can be attached directly to 10BASE-T/100BASE-TX LAN segments.

These port support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

POWER CONNECTOR

The Wireless Broadband Router must be powered with its supplied power adapter. Failure to do so results in voiding of any warrantly supplied with the product. The power adapter automatically adjusts to any voltage between 100~240 volts at 50 or 60 Hz, and supplies 5 volts DC power to the unit. No voltage range settings are required.

RESET BUTTON This button is used to restore the factory default configuration. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the Gateway Router.

WPS BUTTON Press to automatically configure the Wireless Broadband Router with other WPS devices in the WLAN.

2 NETWORK PLANNING

The Wireless Broadband Router is designed to be very flexible in its deployment options. It can be used as an Internet gateway for a small network, or as an access point to extend an existing wired network to support wireless users. It also supports use as a wireless bridge to connect up to four wired LANs.

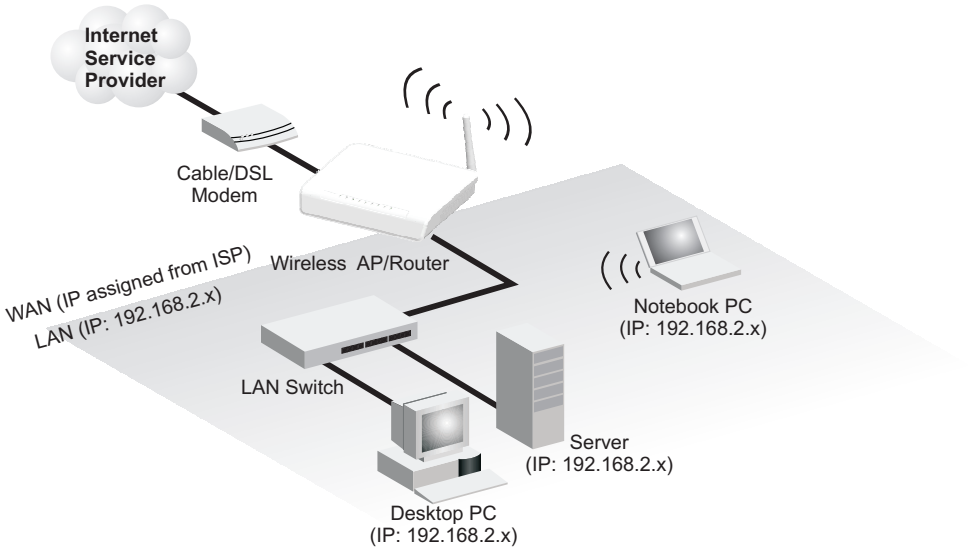
This chapter explains some of the basic features of the Wireless Broadband Router and shows some network topology examples in which the device is implemented.

INTERNET GATEWAY ROUTER

The Wireless Broadband Router can connect directly to a cable or DSL modem to provide an Internet connection for multiple users through a single service provider account. Users connect to the Wireless Broadband Router either through a wired connection to a LAN port, or though the device's own wireless network. The Wireless Broadband Router functions as an Internet gateway when set to Gateway Mode.

An Internet gateway employs several functions that essentially create two separate Internet Protocol (IP) subnetworks; a private internal network with wired and wireless users, and a public external network that connects to the Internet. Network traffic is forwarded, or routed, between the two subnetworks.

Figure 4: Operating as an Internet Gateway Router



The private local network, connected to the LAN port or wireless interface, provides a Dynamic Host Configuration Protocol (DHCP) server for allocating IP addresses to local PCs and wireless clients, and Network Address Translation (NAT) for mapping the multiple "internal" IP addresses to one "external" IP address.

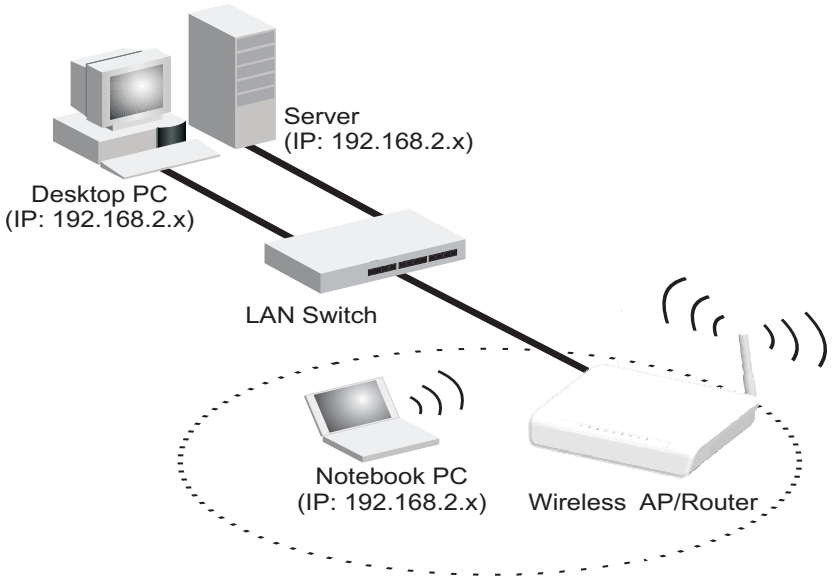
The public external network, connected to the WAN port, supports DHCP client, Point-to-Point Protocol over Ethernet (PPPoE) and static IP for connection to an Internet service provider (ISP) through a cable or DSL modem.

LAN ACCESS POINT

The Wireless Broadband Router can provide an access point service for an existing wired LAN, creating a wireless extension to the local network. The Wireless Broadband Router functions as purely an access point when set to Bridge Mode. When used in this mode, there are no gateway functions between the WAN port and the LAN and wireless interface.

A Wi-Fi wireless network is defined by its Service Set Identifier (SSID) or network name. Wireless clients that want to connect to a network must set their SSID to the same SSID of the network service.

Figure 5: Operating as an Access Point



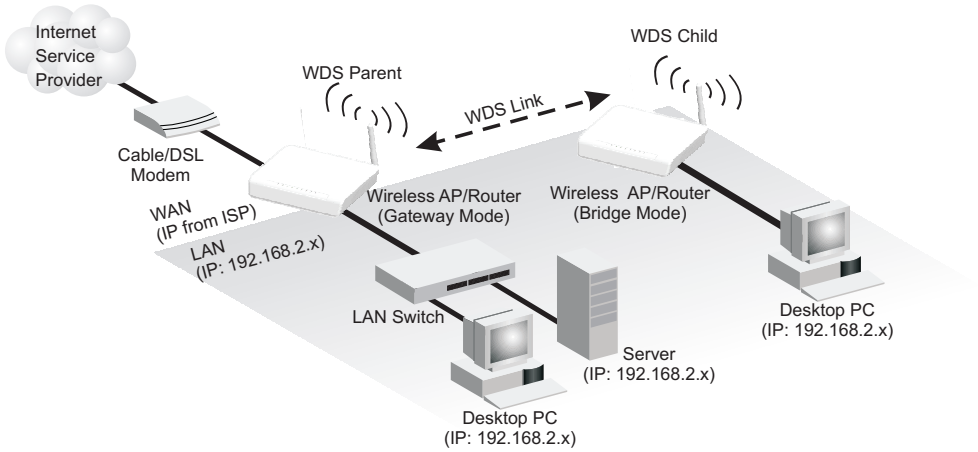
WIRELESS BRIDGE

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for bridge connections between access points. The Wireless Broadband Router can use WDS to forward traffic on links between units.

Up to four WDS links can be specified for the Wireless Broadband Router. One end of a link must be configured as the "WDS Parent" and the other as the "WDS Child."

NOTE: The network domain of WDS child has to be the same as WDS parent.

Figure 6: Operating as a Wireless Bridge



3 INSTALLING THE GATEWAY ROUTER

The Wireless Broadband Router has two basic operating modes that can be set through the web-based management interface. For information on setting the mode suitable for your network environment. See "Operation Mode" on page 52.

- Gateway Mode — A gateway mode that connects a wired LAN and wireless clients to an Internet access device, such as a cable or DSL modem. This is the factory set default mode.
- Bridge Mode — An access point mode that extends a wired LAN to wirelessclients.

In addition to these basic operating modes, the wireless interface supports a Wireless Distribution System (WDS) link to another Wireless Broadband Router. These advanced configurations are not described in this section. See "Network Planning" on page 29 for more information.

In a basic configuration, how the Wireless Broadband Router is connected depends on the operating mode. The sections in this chapter describe connections for basic Gateway Mode and Bridge Mode operation.

SYSTEM REQUIREMENTS

You must meet the following minimum requirements:

- An Internet access device (DSL or Cable modem) with an Ethernet port connection.
- An up-to-date web browser: Internet Explorer 6.0 or above or Mozilla Firefox 2.0 or above.

LOCATION SELECTION

The Wireless Broadband Router can be mounted on any horizontal surface, or on a wall. The following sections describe the mounting options.

MOUNTING ON A WALL

The Wireless Broadband Router should be mounted only to a wall or wood surface that is at least 1/2-inch plywood or its equivalent. To mount the unit on a wall, always use its wall-mounting bracket. The unit must be mounted with the RJ-45 cable connector oriented upwards to ensure proper operation.

Figure 7: Wall Mounting

To mount on a wall, follow the instructions below.

1. Mark the position of the two screw holes on the wall. For concrete or brick walls, you will need to drill holes and insert wall plugs for the screws.

2. Insert the included screws into the holes, leaving about 0.08~0.12 inches (2-3 mm) clearance from the wall.

3. Line up the two mounting points on the unit with the screws in the wall, then slide the unit down onto the screws until it is in a secured position.

MOUNTING ON A HORIZONTAL SURFACE

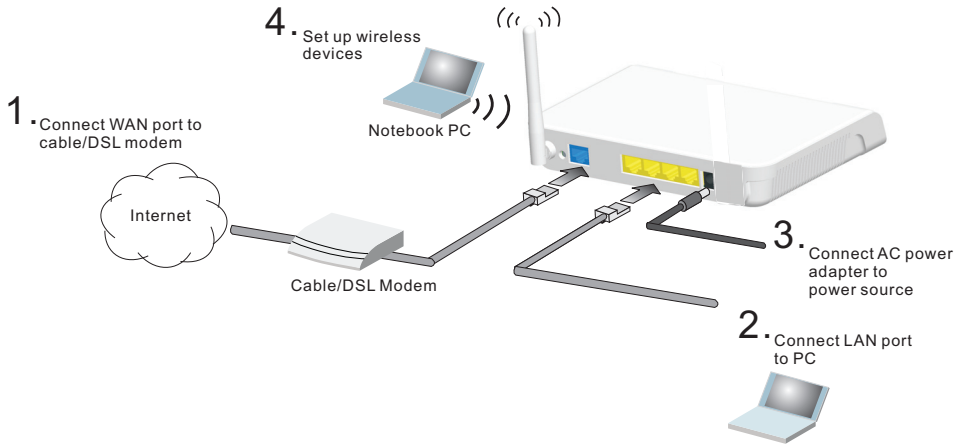
To keep the Wireless Broadband Router from sliding on the surface, the Wireless Broadband Router has four rubber feet on the bottom of the unit.

It is recommended to select an uncluttered area on a sturdy surface, such as a desktop or table. The unit can also be protected by securing all attached cables to a table leg or other nearby fixed structure.

GATEWAY MODE CONNECTIONS

In its default Gateway Mode, the Wireless Broadband Router forwards traffic between an Internet connected cable or ADSL modem, and wired or wireless PCs or notebooks. The basic connections are illustrated in the figure below.

Figure 8: Gateway Mode Connection



To connect the Wireless Broadband Router in Gateway Mode for use as an Internet gateway, follow these steps:

1. Connect an Ethernet cable from the Wireless Broadband Router's WAN port to your Internet connected cable or ADSL modem.

2. Connect an Ethernet cable from the Wireless Broadband Router's LAN ports to your PCs. Alternatively, you can connect to a workgroup switch to support more wired users. The Wireless Broadband Router can support up to 253 wired and wireless users.

3. Power on the Wireless Broadband Router by connecting the AC power adapter and plugging it into a power source.

CAUTION: Use ONLY the power adapter supplied with the Wireless Broadband Router. Otherwise, the product may be damaged.

When you power on the Wireless Broadband Router, verify that the Power LED turns on and that the other LED indicators start functioning as described under see "LED Indicators" on page 25.

4. Set up wireless devices by pressing the WPS button on the Wireless Broadband Router or by using the web interface. See "Initial Configuration" on page 38 for more information on accessing the web interface.

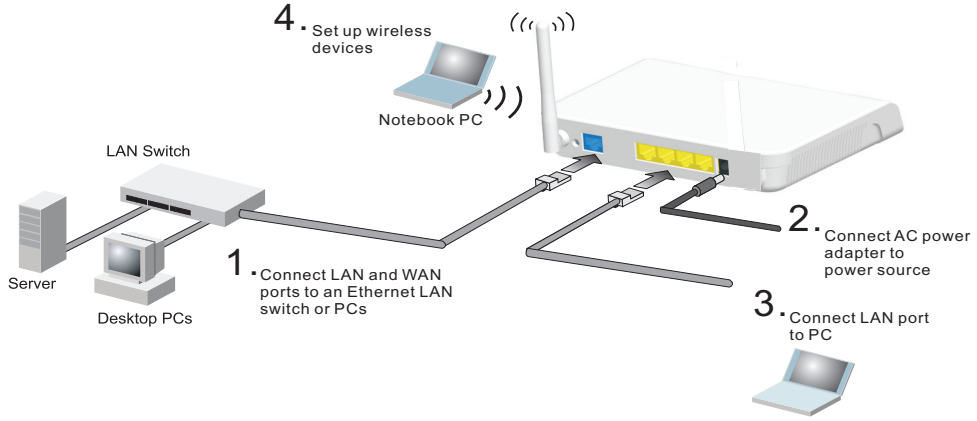
BRIDGE MODE CONNECTIONS

In Bridge Mode, the Wireless Broadband Router operates as a wireless access point, extending a local wired network to associated wireless clients (PCs or notebooks with wireless capability). From any nearby location, you can then make a wireless connection to the Wireless Broadband Router and access the wired network resources, including local servers and the Internet.

In Bridge Mode, the Wireless Broadband Router does not support gateway functions on its WAN port. Both the LAN port and the WAN ports can be connected to a local Ethernet LAN.

NOTE: Bridge Mode is not the factory default mode and must be manually set using the web management interface.

Figure 9: Bridge Mode Connection



To connect the Wireless Broadband Router for use as an access point, follow these steps:

1. Using Ethernet cable connect the Wireless Broadband Router's LAN and WAN ports to PCs or a LAN switch.

2. Power on the Wireless Broadband Router by connecting the AC power adapter and plugging it into a power source.

CAUTION: Use ONLY the power adapter supplied with the Wireless Broadband Router. Otherwise, the product may be damaged.

When you power on the Wireless Broadband Router, verify that the Power LED turns on and that the other LED indicators start functioning as described under "LED Indicators" on page 25.

3. Connect an Ethernet cable from the Wireless Broadband Router's LAN ports to your PCs. Alternatively, you can connect to a workgroup switch to support more wired users. The Wireless Broadband Router can support up to 253 wired and wireless users

4. Set up wireless devices by pressing the WPS button on the Wireless Broadband Router or by using the web interface. See "Initial Configuration" on page 38 for more information on accessing the web interface.

4 INITIAL CONFIGURATION

The Wireless Broadband Router offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

ISP SETTINGS

If you are not sure of your connection method, please contact your Internet Service Provider. There are several connection types to choose from: Static IP, DHCP (cable connection), PPPoE (DSL connection), and PPTP.

NOTE: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

CONNECTING TO THE LOGIN PAGE

It is recommended to make initial configuration changes by connecting a PC directly to one of the Wireless Broadband Router's LAN ports. The Wireless Broadband Router has a default IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the Gateway Router (that is, the PC and Gateway Router addresses must both start 192.168.2.x).

To access the Wireless Broadband Router's management interface, follow these steps:

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

2. Log into the interface by entering the default username "admin" and password "smcadmin," then click Login.

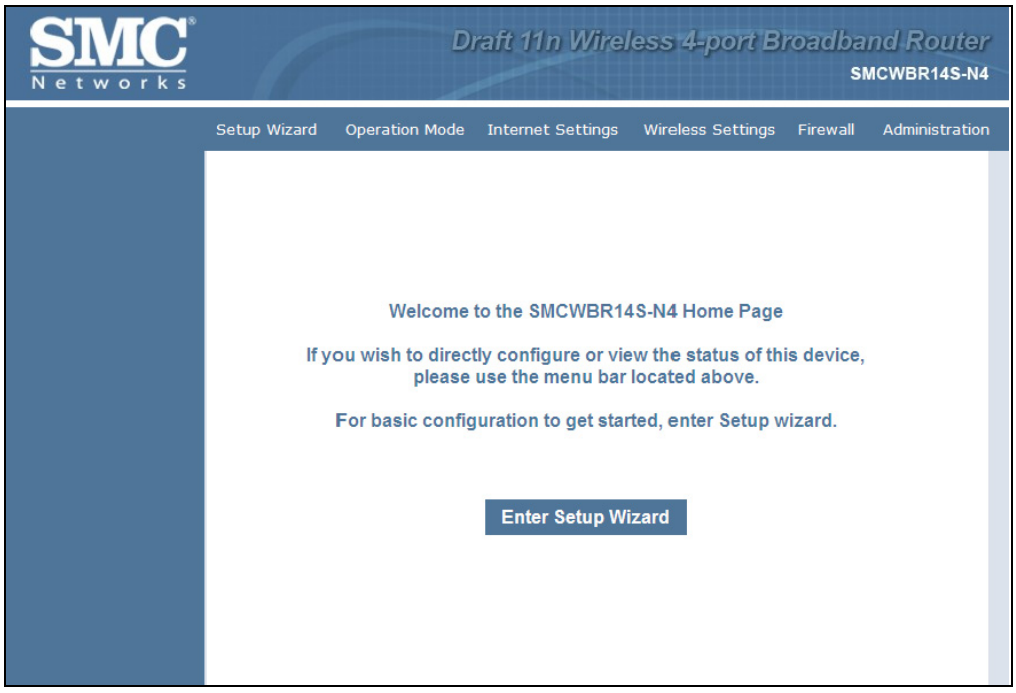
NOTE: It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, See "System Management" on page 84.

Figure 10: Login Page

HOME PAGE AND MAIN MENU

After logging in to the web interface, the Home page displays. The Home page shows the main menu and the method to access the Setup Wizard.

Figure 11: Home Page



COMMON WEB PAGE BUTTONS

The list below describes the common buttons found on most web management pages:

- **Apply** – Applies the new parameters and saves them to memory. Also displays a screen to inform you when it has taken affect. Clicking 'Apply' returns to the home page.
- **Cancel** – Cancels the newly entered settings and restores the previous settings.
- **Next** – Proceeds to the next step.
- **Back** – Returns to the previous screen.

SETUP WIZARD

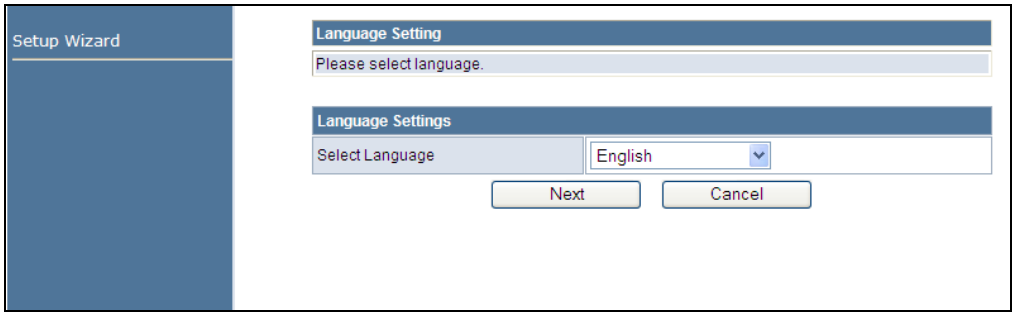
The Wizard is designed to help you configure the basic settings required to get the the Wireless Broadband Router up and running. There are only a few basic steps you need to set up the the Wireless Broadband Router and provide a connection.

Follow these steps:

STEP 1 - LANGUAGE SELECTION

Select between English or Traditional Chinese. Click Next to proceed to the next step of the wizard.

Figure 12: Wizard Step 1 - Language Selection



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

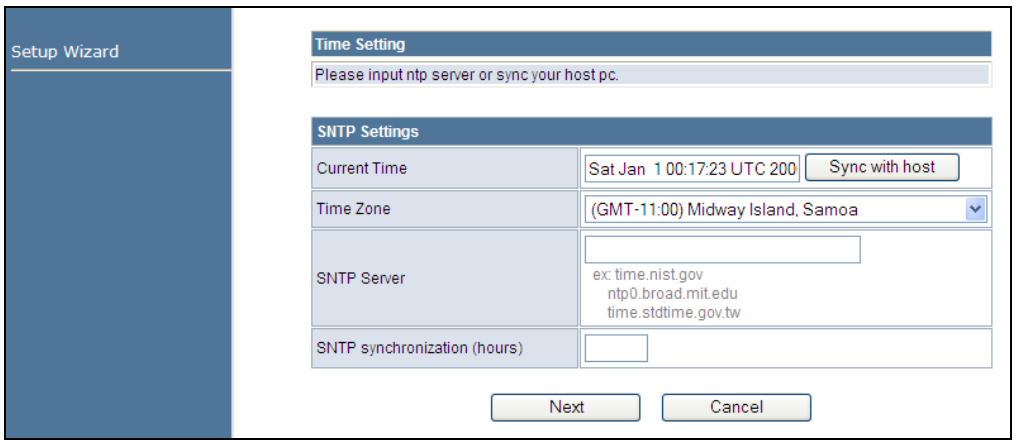
- **Select Language** — Toggles between English or Traditional Chinese as the interface language.
- **Next** — Proceeds to the next step.

STEP 2 - SNTP SETTINGS

The Step 2 page of the Wizard configures time zone and SNTP settings.

Select a time zone according to where the device is operated. Click Next after completing the setup.

Figure 13: Wizard Step 2 - Time and SNTP Settings



The following items are displayed on this page:

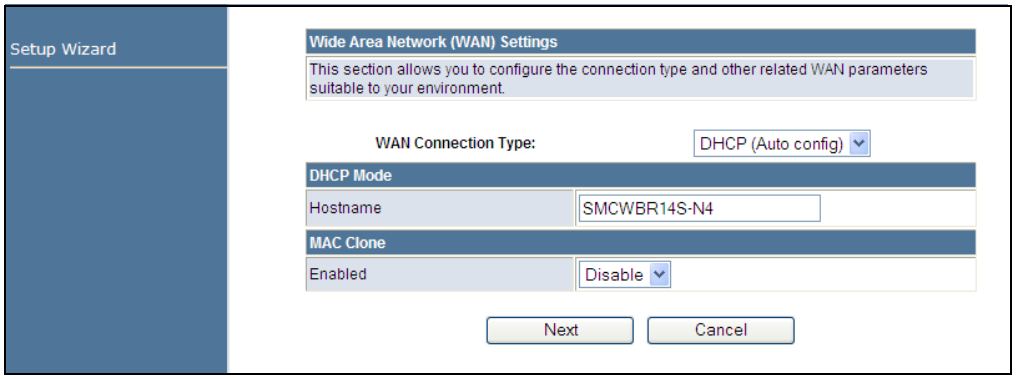
- **Current Time** — Receives a time and date stamp from an SNTP server.
- **Time Zone** — Select the time zone that is applicable to your region.
- **SNTP Server** — Enter the address of an SNTP server to receive time updates.
- **SNTP synchronization (hours)** — Specify the interval between SNTP server updates.

STEP 3 - WAN SETTINGS - DHCP

The Step 3 page of the Wizard specifies the Internet connection parameters for the Wireless Broadband Router's WAN port. Click Next after completing the setup.

By default, the access point WAN port is configured with DHCP enabled. The options are Static IP, DHCP, PPPoE (ADSL), and PPTP. Each option changes the parameters that are displayed on the page. (Default: DHCP)

Figure 14: Wizard Step 3 - WAN Settings - DHCP



The following items are displayed on this page:

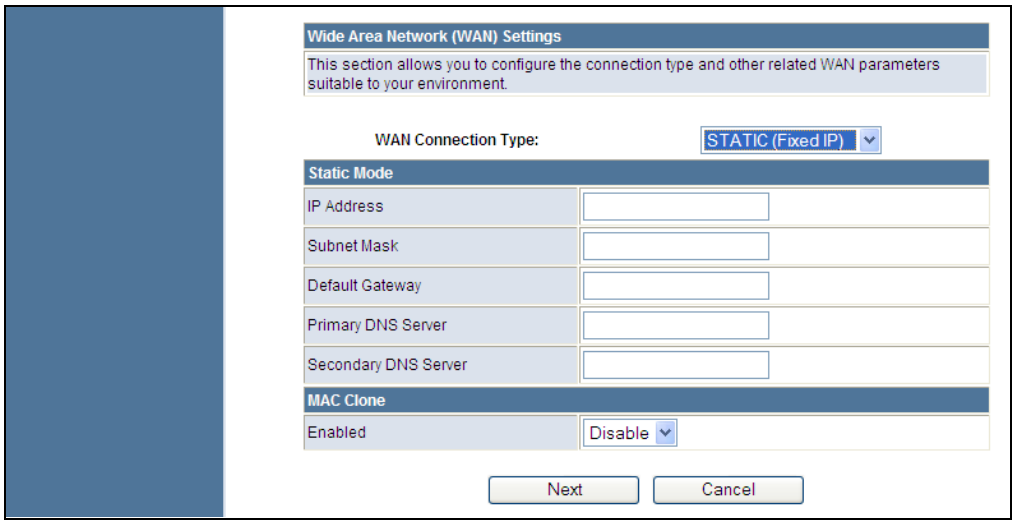
- **WAN Connection Type** — Select the connection type for the WAN port from the drop down list. (Default: DHCP)
- **DHCP Mode** — Specifies the hostname of the DHCP client. (Default: SMCWBR14S-N4)
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC, which is registered with the ISP. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address". (Default: Disabled)

NOTE: If you are unsure of the PC MAC address originally registered by your ISP, call your ISP and request to register a new MAC address for your account. Register the default MAC address of the Wireless Broadband Router.

STEP 3 - WAN SETTINGS - STATIC IP

Configures a static IP for the WAN port.

Figure 15: Wizard Step 3 - WAN Settings - Static IP



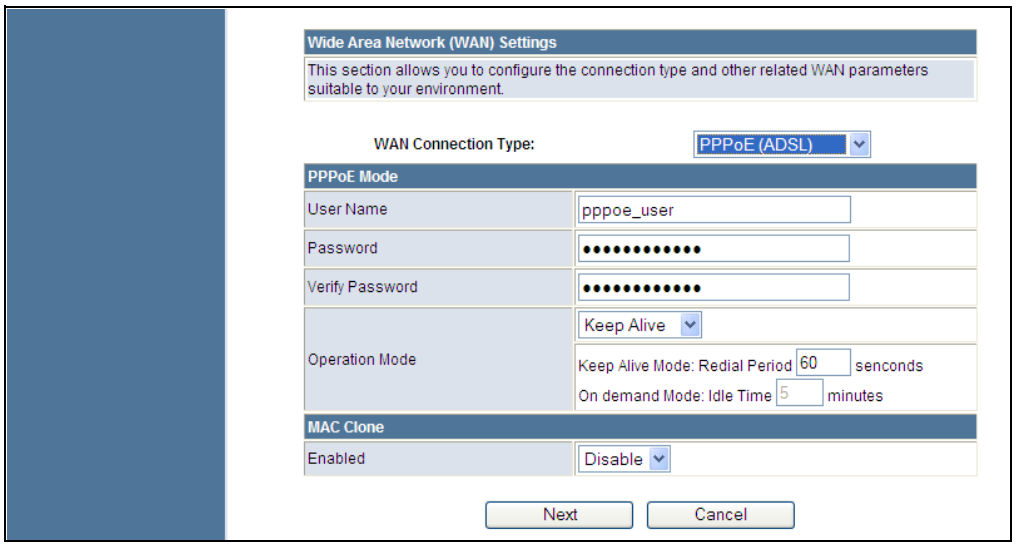
The following items are displayed on this page:

- **WAN Connection Type** — Select the connection type for the WAN port from the drop down list. (Default: DHCP)
- **IP Address** — The IP address of the Wireless Broadband Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** — The mask that identifies the host address bits used for routing to specific subnets.
- **Default Gateway** — The IP address of the gateway router for the Wireless Broadband Router, which is used if the requested destination address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

STEP 3 - WAN SETTINGS - PPPOE

Enable the Wireless Broadband Router IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using Point-to-Point Protocol over Ethernet (PPPoE).

Figure 16: Wizard Step 3 - WAN Settings - PPPoE



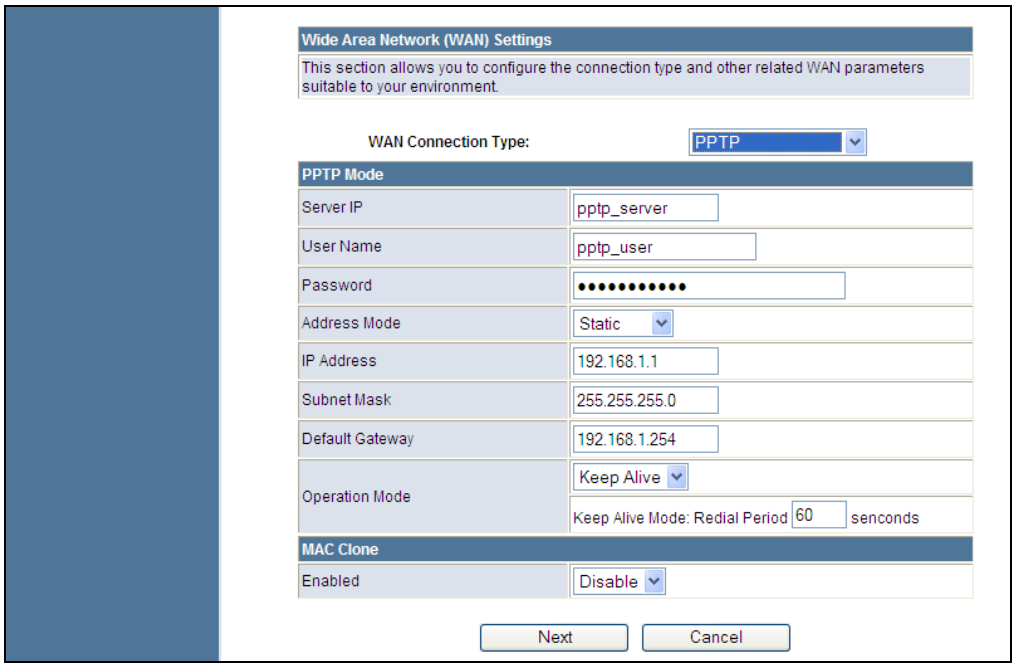
The following items are displayed on this page:

- **User Name** — Sets the PPPoE user name for the WAN port. (Default: pppoe_user; Range: 1~32 characters)
- **Password** — Sets a PPPoE password for the WAN port. (Default: pppoe_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

STEP 3 - WAN SETTINGS - PPTP

Enables the Point-to-Point Tunneling Protocol (PPTP) for implementing virtual private networks. The service is provided in many European countries.

Figure 17: Wizard Step 3 - WAN Settings - PPTP



The following items are displayed on this page:

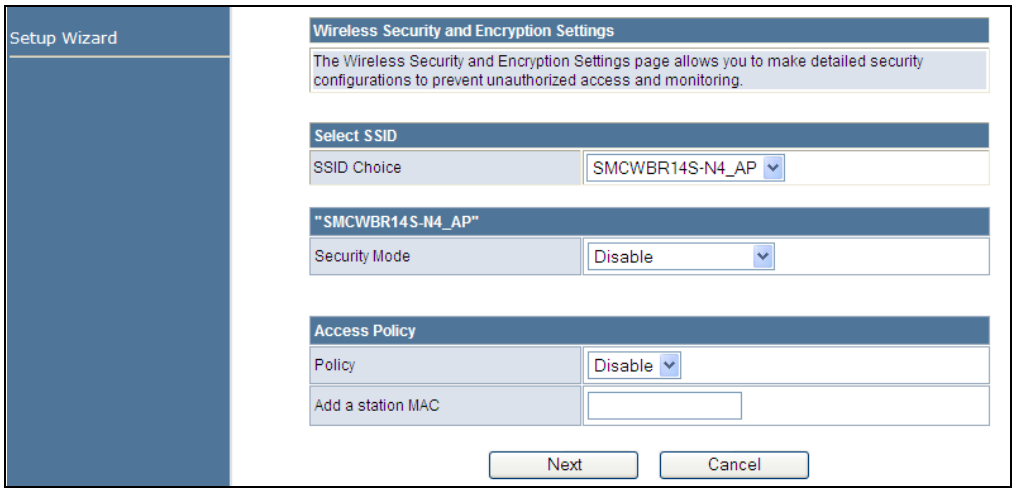
- **Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)
- **User Name** — Sets the PPTP user name for the WAN port. (Default: pptp_user; Range: 1~32 characters)
- **Password** — Sets a PPTP password for the WAN port. (Default: pptp_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Address Mode** — Sets a PPTP network mode. (Default: Static)
- **IP Address** — Sets the static IP address. (Default: 0.0.0.0, available when PPTP Network Mode is set to static IP.)
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0, available when PPTP Network Mode is set to static IP.)
- **Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.
- **Operation Mode —** Enables and configures the keep alive time.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC

address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

STEP 4 - WIRELESS SECURITY

The Step 4 page of the Wizard configures the wireless security.

Figure 18: Wizard Step 4 - Wireless Security



The following items are displayed on this page:

- **SSID Choice** — Selects the SSID (network name) interface to configure. The Gateway Router supports three SSID interfaces.
- **Security Mode** — Specifies the security mode for the SSID.
- **Policy** — Enables an allow or deny rule for a specified MAC address.
- **Add a station MAC** — Specify a MAC address to be filtered in the format: xx:xx:xx:xx:xx:xx.

COMPLETION

After completion of the Wizard, the screen returns to the Home Page.

SECTION II

WEB CONFIGURATION

This section provides details on configuring the Wireless Broadband Router using the web browser interface.

This section includes these chapters:

- "Operation Mode" on page 49
- "Internet Settings" on page 53
- "Wireless Configuration" on page 65
- "Firewall Configuration" on page 75
- "Administration Settings" on page 83

5 OPERATION MODE

The Wireless Broadband Router offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

The following sections are contained in this chapter:

- "Logging In" on page 50
- "Operation Mode" on page 52

LOGGING IN

It is recommended to make initial configuration changes by connecting a PC directly to one of the Wireless Broadband Router's LAN ports. The Wireless Broadband Router has a default IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. If your PC is set to "Obtain an IP address automatically" (that is, set as a DHCP client), you can connect immediately to the web interface. Otherwise, you must set your PC IP address to be on the same subnet as the Wireless Broadband Router (that is, the PC and Wireless Broadband Router addresses must both start 192.168.2.x).

To access the configuration menu, follow these steps:

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

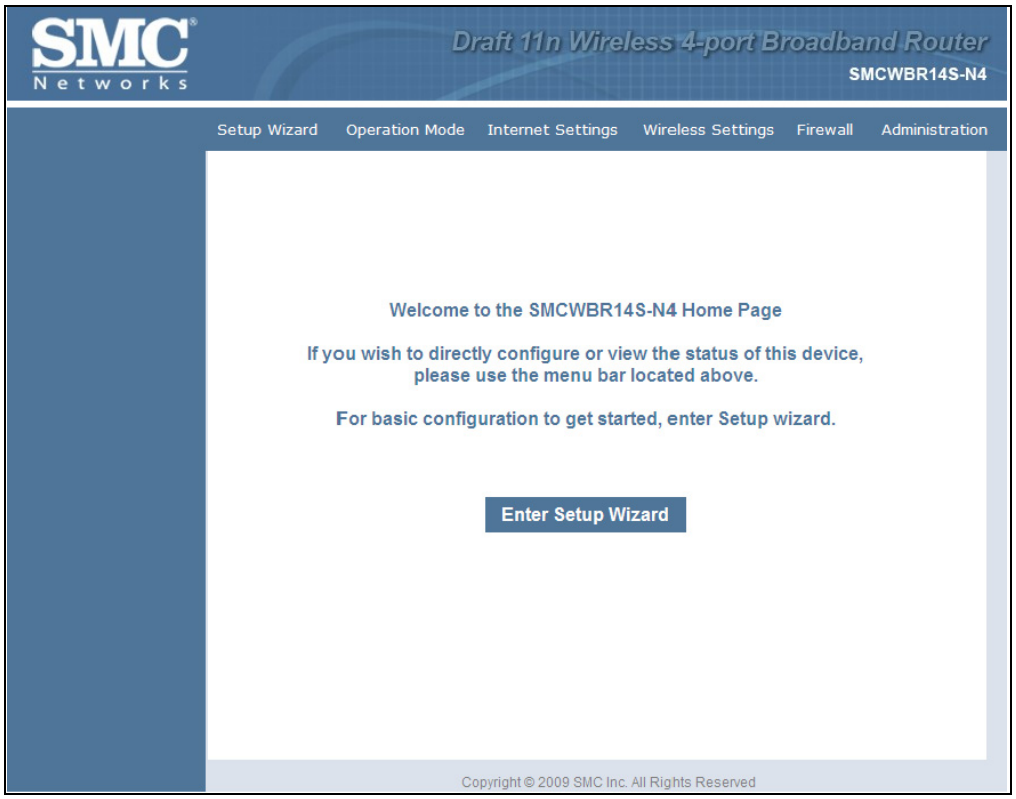
2. Log into the Wireless Broadband Router management interface by entering the default user name "admin" and password "smcadmin," then click Login.

NOTE: It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, see "Administration Settings" on page 83.

Figure 19: Logging On

The home page displays the main menu items at the top of the screen and the Setup Wizard. See "Setup Wizard" on page 40.

Figure 20: Home Page

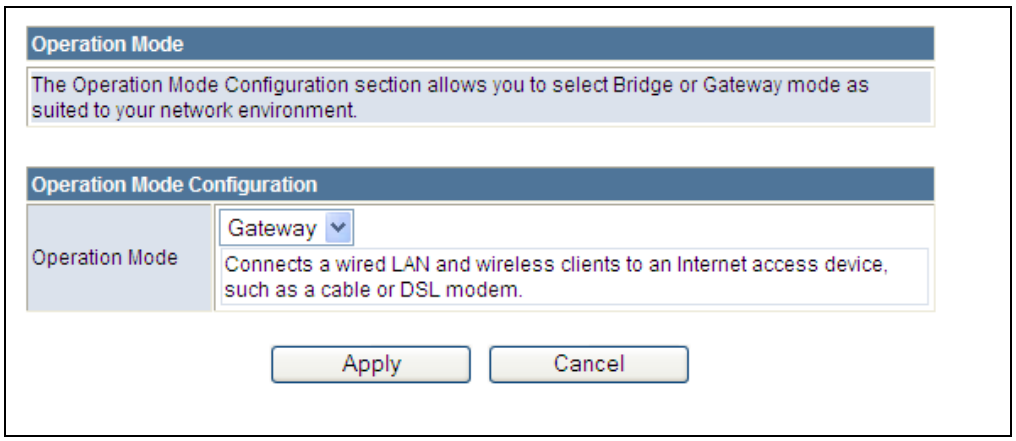


NOTE: The displayed pages and settings may differ depending on whether the unit is in Gateway or Bridge Mode. See "Operation Mode" on page 52.

OPERATION MODE

The Operation Mode Configuration page allows you to set up the mode suitable for your network environment.

Figure 21: Operation Mode (Gateway)



- **Bridge Mode** — An access point mode that extends a wired LAN to wireless clients.
- **Gateway Mode** — Normal gateway mode that connects a wired LAN and wireless clients to an Internet access device, such as a cable or DSL modem. This is the factory set default mode.

6 INTERNET SETTINGS

The Internet Settings pages allow you to manage basic system configuration settings. It includes the following sections:

- "WAN Setting" on page 53
  - "DHCP" on page 53
  - "Static IP" on page 55
  - "PPPoE" on page 56
  - "PPTP" on page 57
- "LAN Setting" on page 59
- "Advanced Routing" on page 61

NOTE: In Bridge mode, the Wireless Broadband Router's Internet Settings options are significantly reduced, with only LAN Settings and the Client List being available to the user.

WAN SETTING

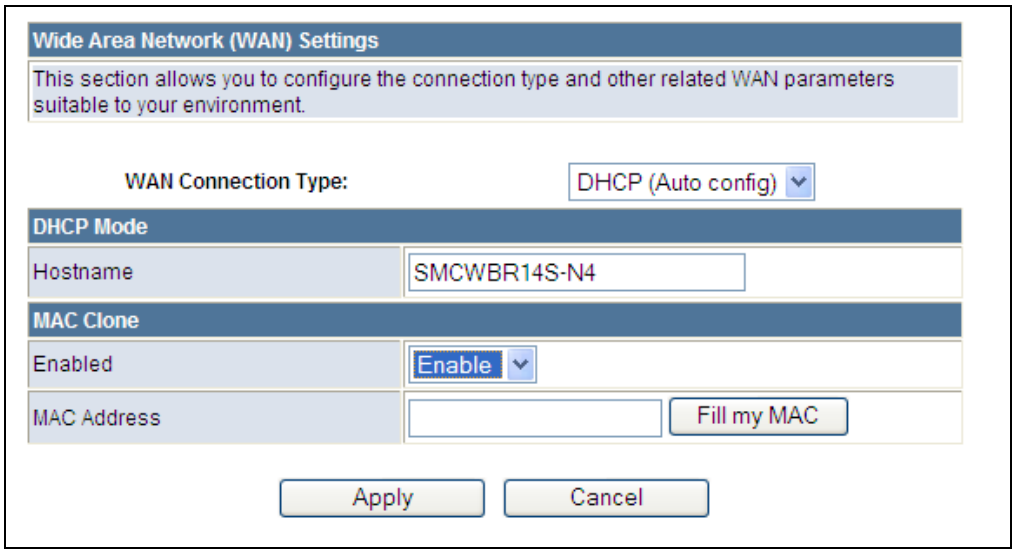
The WAN Setting page specifies the Internet connection parameters. Click on "Internet Settings" followed by "WAN".

- **WAN Connection Type** — By default, the access point WAN port is configured with DHCP enabled. After you have network access to the access point, you can use the web browser interface to modify the initial IP configuration, if needed. The options are Static IP, DHCP, PPPoE (ADSL), and PPTP. Each option changes the parameters displayed below it. (Default: DHCP).

DHCP

Enables Dynamic Host Configuration Protocol (DHCP) for the WAN port. This setting allows the Wireless Broadband Router to automatically obtain an IP address from a DHCP server normally operated by the Internet Service Provider (ISP).

Figure 22: DHCP Configuration



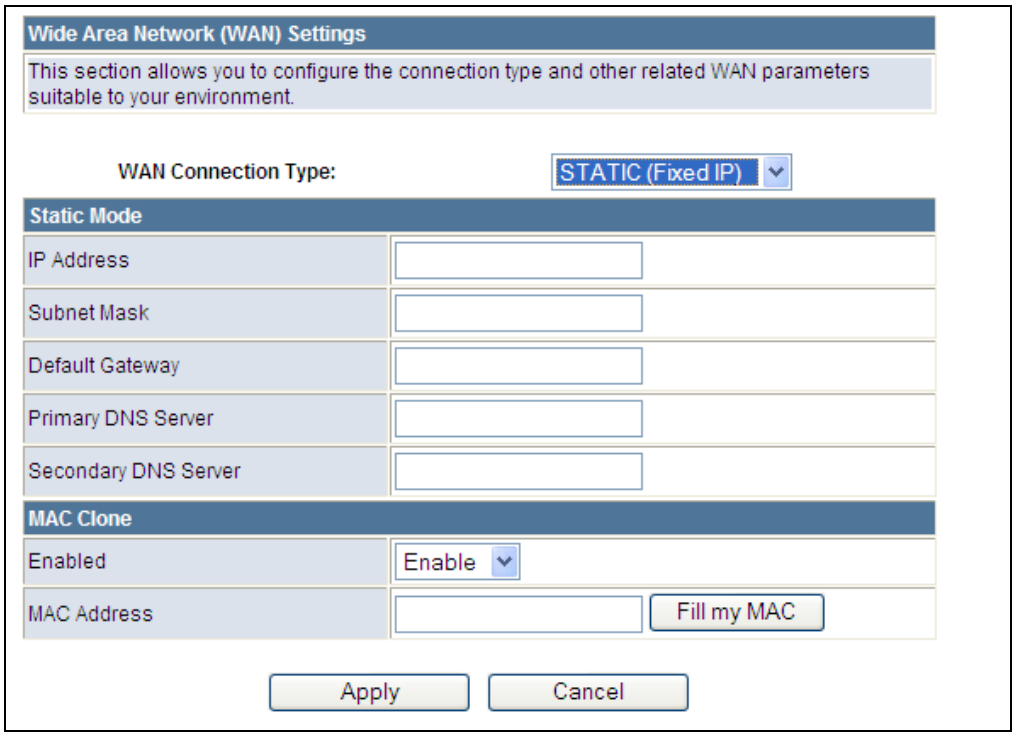
The following items are displayed on this page:

- **Hostname** (Optional) — The hostname of the DHCP client.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

NOTE: If you are unsure of the PC MAC address originally registered by your ISP, call your ISP and request to register a new MAC address for your account. Register the default MAC address of the Wireless Broadband Router.

STATIC IP Configures a static IP for the WAN port.

Figure 23: Static IP Configuration



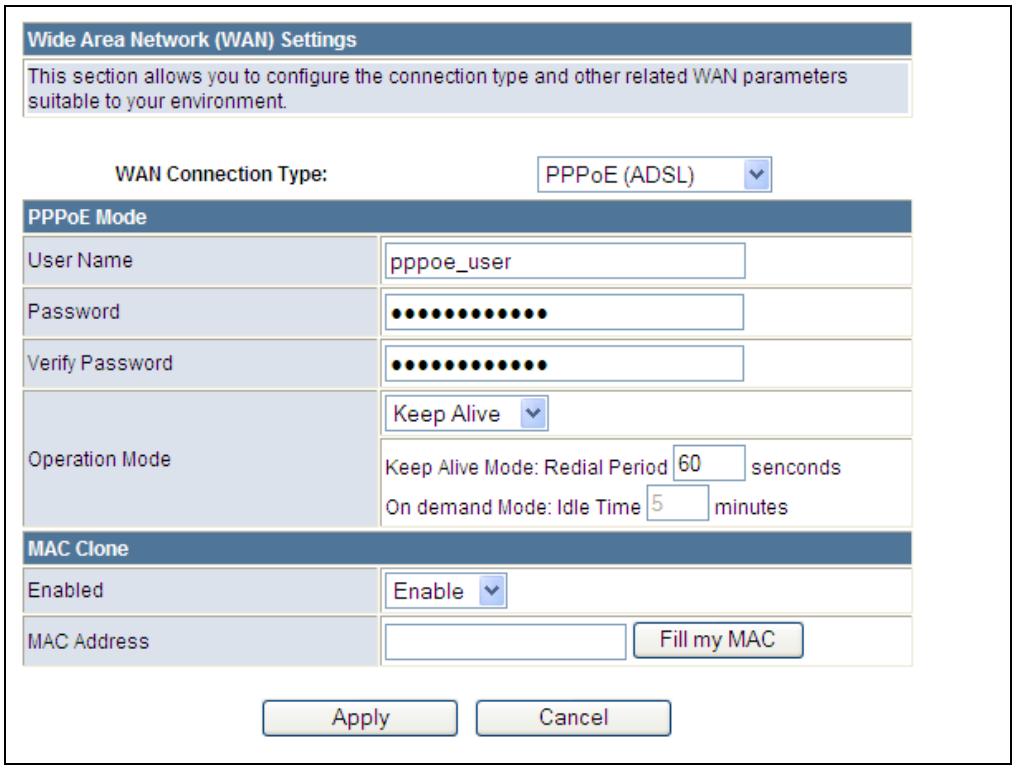
- **IP Address** — The IP address of the Wireless Broadband Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** — The mask that identifies the host address bits used for routing to specific subnets.
- **Default Gateway** — The IP address of the gateway router for the Wireless Broadband Router, which is used if the requested destination address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0).
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server on the network.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes

provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

PPPoE

Enables the Wireless Broadband Router IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using Point-to-Point Protocol over Ethernet (PPPoE).

Figure 24: PPPoE Configuration



- **PPPoE User Name** — Sets the PPPoE user name for the WAN port. (Default: pppoe_user; Range: 1~32 characters)
- **PPPoE Password** — Sets a PPPoE password for the WAN port. (Default: pppoe_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Operation Mode** — Selects the operation mode as Keep Alive, On Demand or Manual. (Default: Keep Alive)
  - **Keep Alive Mode**: The Wireless Broadband Router will periodically check your Internet connection and automatically re-establish your connection when disconnected. (Default: 60 seconds)

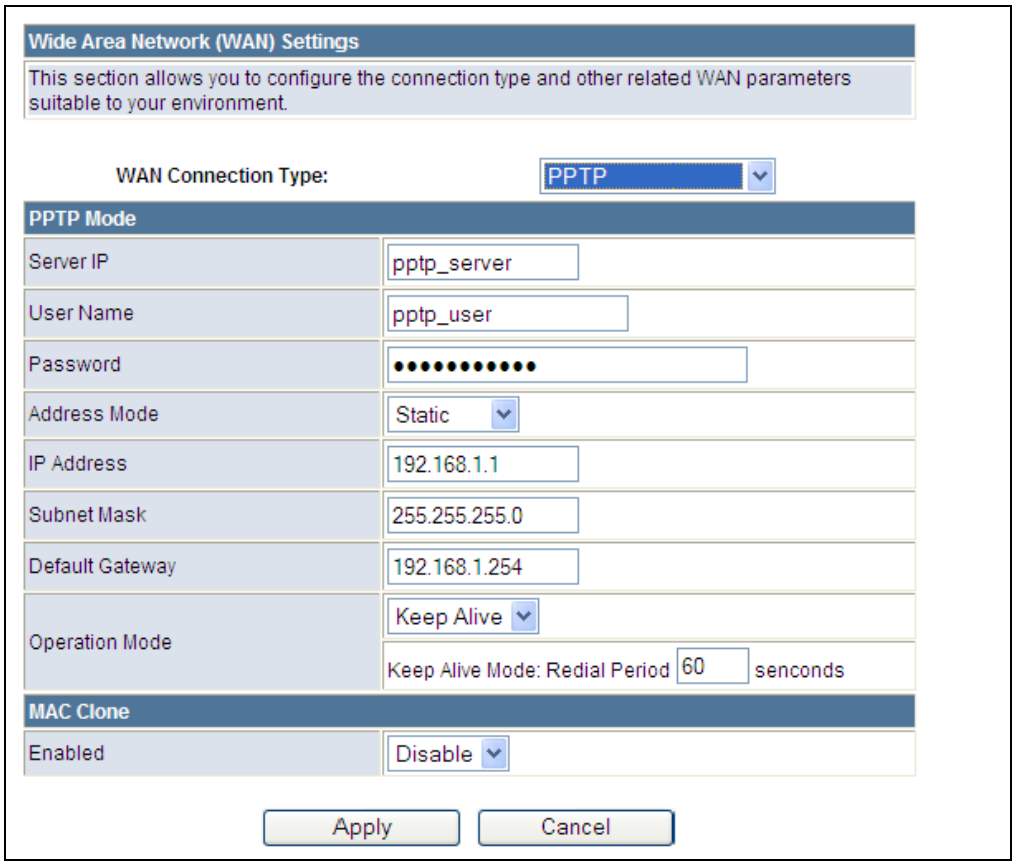
- **On Demand Mode**: The maximum length of inactive time the unit will stay connected to the DSL service provider before disconnecting. (Default: 5 minutes)

- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the "Clone your PC's MAC Address" (Default: Disable)

PPTP

Enables the Point-to-Point Tunneling Protocol (PPTP) for implementing virtual private networks. The service is provided in many European countries.

Figure 25: PPTP Configuration



- **Server IP** — Sets a PPTP server IP Address. (Default: pptp_server)

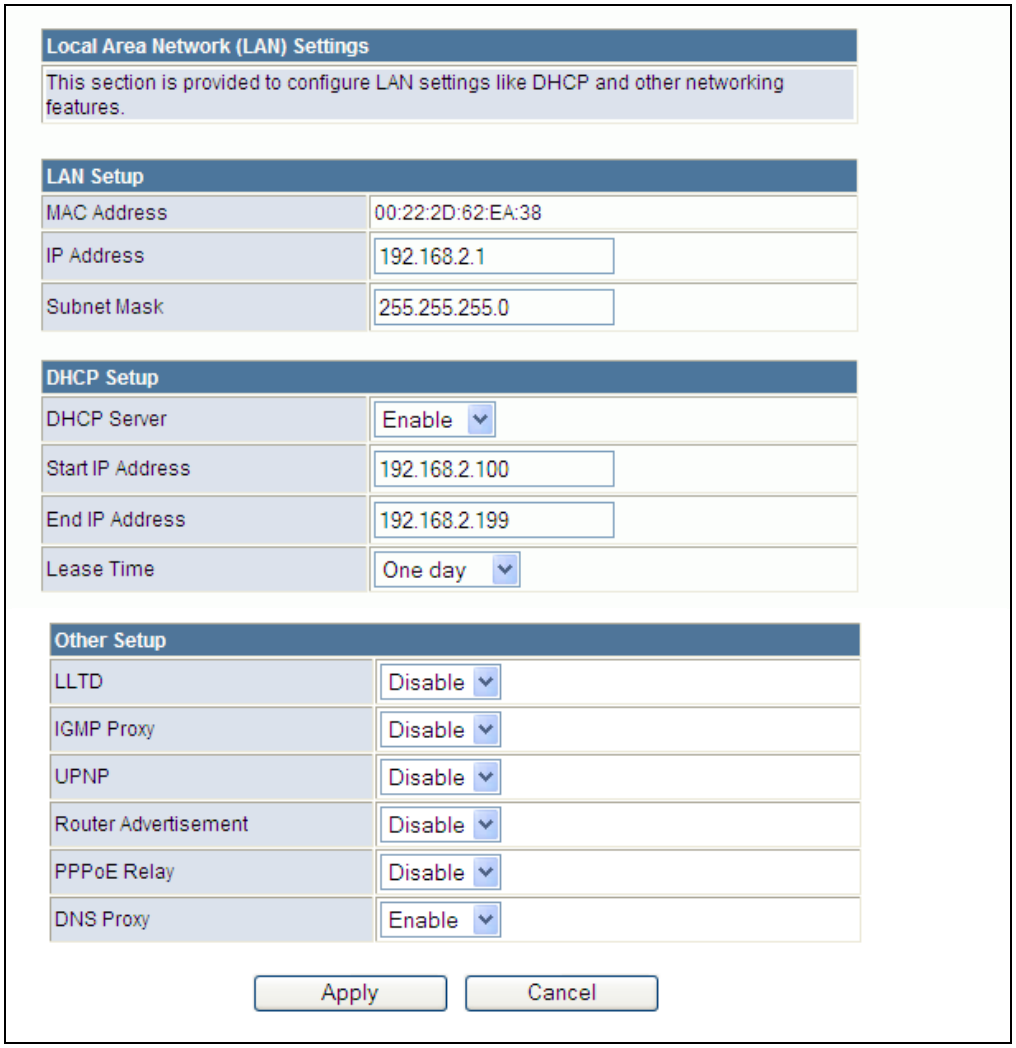
- **User Name** — Sets the PPTP user name for the WAN port. (Default: pptp_user; Range: 1~32 characters)

- **Password** — Sets a PPTP password for the WAN port. (Default: pptp_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Address Mode** — Sets a PPTP network mode. (Default: Static)
- **IP Address** — Sets the static IP address. (Default: 0.0.0.0, available when PPTP Network Mode is set to static IP.)
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0, available when PPTP Network Mode is set to static IP.)
- **Default Gateway** — The IP address of the gateway router for the Wireless Broadband Router, which is used if the requested destination address is not on the local subnet.
- **Operation Mode** — Selects the operation mode as Keep Alive, or Manual. (Default: Keep Alive)
  - **Keep Alive Mode**: The Wireless Broadband Router will periodically check your Internet connection and automatically re-establish your connection when disconnected. (Default: 60 seconds)
  - **Manual Mode**: The unit will remain connected to the Internet without disconnecting.
- **MAC Clone** — Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Wireless Broadband Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Wireless Broadband Router, then click the “Clone your PC’s MAC Address” (Default: Disable)

LAN SETTING

The Wireless Broadband Router must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.2.1. You can use this IP address or assign another address that is compatible with your existing local network. Click on "Internet Settings" followed by "LAN."

Figure 26: LAN Configuration



- **LAN IP Address** — Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.2.1.
- **Subnet Mask** — Indicate the local subnet mask. (Default: 255.255.255.0.)
- **MAC Address** — The shared physical layer address for the Wireless Broadband Router's LAN ports.

- **DHCP Server** — Enable this feature to assign IP settings to wired and wireless clients connected to the Gateway Router. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to clients. (Options: Enable, Disable; Default: Enable)

- **Start/End IP Address** — Specify the start and end IP addresses of a range that the DHCP server can allocate to DHCP clients. Note that the address pool range is always in the same subnet as the unit's IP setting. The maximum clients that the unit can support is 253.

- **Primary DNS Server** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server on the network.

- **Default Gateway** — The default gateway is the IP address of the router for the Wireless Broadband Router, which is used if the requested destination address is not on the local subnet.

- **Lease Time** — Select a time limit for the use of an IP address from the IP pool. When the time limit expires, the client has to request a new IP address. The lease time is expressed in seconds. (Options: One day, Half day, Two hours, One hour, Half hour; Default: One day)

- **Statically Assigned** — Up to three devices with specific MAC addresses can be assigned static IP addresses. That is, the DHCP server always assigns these devices the same IP addresses.

- **LLTD** — Link Layer Topology Discovery (LLTD) is a Microsoft proprietary discovery protocol which can be used for both wired and wireless networks. (Options: Disable/Enable, Default: Disable)

- **IGMP Proxy** — Enables IGMP proxy on the Wireless Broadband Router. (Options: Disable/Enable, Default: Disable)

- **UPNP** — Allows the device to advertise its UPnP capabilities. (Default: Disable)

- **Router Advertisement** — Enables the sending and receiving of routing advertisements to discover the existence of neighboring routers. (Options: Disable/Enable, Default: Disable)

- **PPPoE Relay** — When enabled, the Wireless Broadband Router will forward PPPoE messages to clients. Clients are then able to connect to the PPPoE service through the WAN port. (Options: Disable/Enable, Default: Disable)

- **DNS Proxy** — Enables DNS proxy on the LAN port. DNS Proxy receives DNS queries from the local network and forwards them to an Internet DNS server. (Default: Enable)

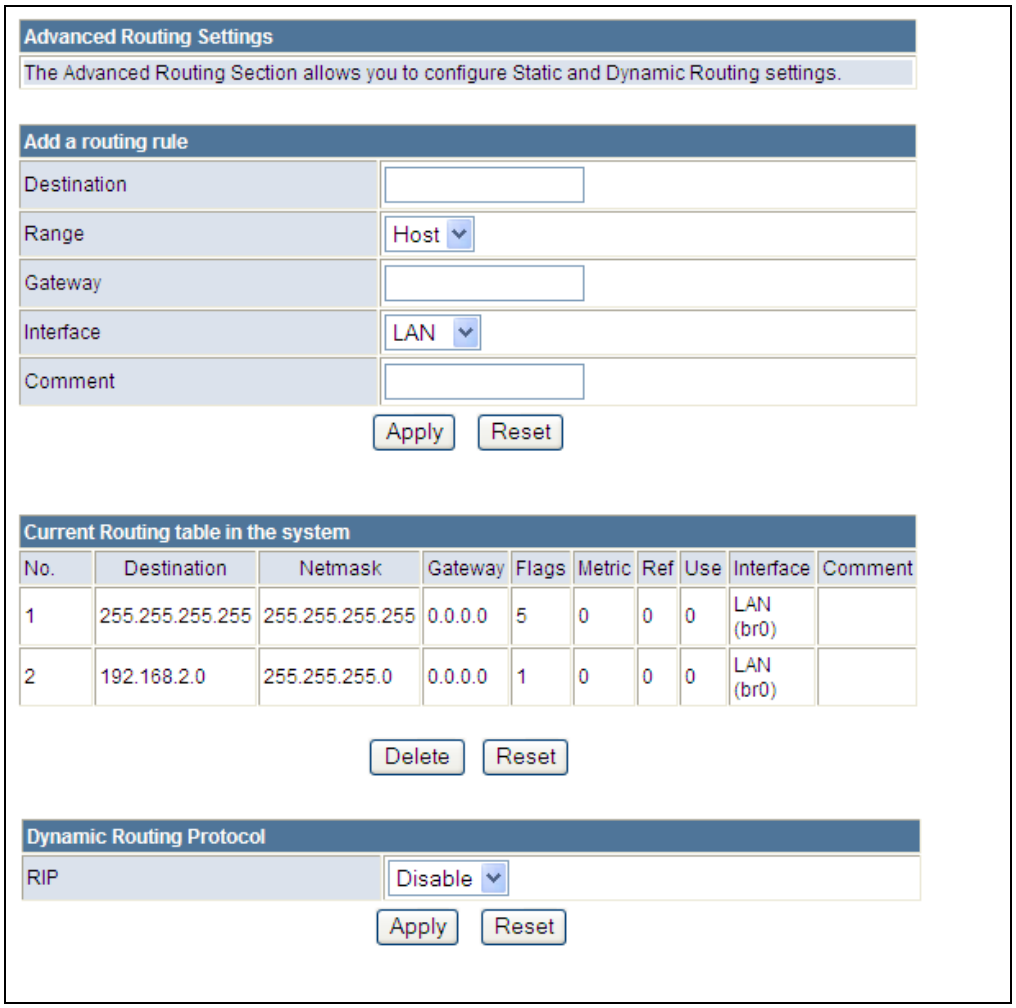
ADVANCED ROUTING

Routing setup allows a manual method to set up routing between networks. The network administrator configures static routes by entering routes directly into the routing table. Static routing has the advantage of being predictable and easy to configure.

ADVANCED ROUTING SETTINGS

This screen is used to manually configure static routes to other IP networks, subnetworks, or hosts. Click "Internet Settings" followed by "Advanced Routing". (Maximum 32 entries are allowed.)

Figure 27: Advanced Routing (Gateway Mode)



- **Destination** — A destination network or specific host to which packets can be routed.
- **Type** — Defines the type of destination. (Options: Host/Net, Default: Host)

- **Gateway** — The IP address of the router at the next hop to which matching frames are forwarded.
- **Interface** — The selected interface to which a static routing subnet is to be applied.
- **Comment** — Enters a useful comment to help identify this route.

ROUTING TABLE

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

NOTE: The Routing Table is only available when the Wireless Broadband Router is set to Gateway Mode.

- **Destination** — Displays all destination networks or specific hosts to which packets can be routed.
- **Netmask** — Displays the subnetwork associated with the destination.
- **Gateway** — Displays the IP address of the router at the next hop to which matching frames are forwarded.
- **Flags** — Flags – Possible flags identify as below
  - - 0: reject route
  - - 1: route is up
  - - 3: route is up, use gateway
  - - 5: route is up, target is a host
  - - 7: route is up, use gateway, target is a host
  - (Definition: U: route is up, H: target is a host, G: use gateway and !: Reject route.)
- **Metric** — A number used to indicate the cost of the route so that the best route, among potentially multiple routes to the same destination, can be selected.
- **Ref** — Number of references to this route.
- **Use** — Count of lookups for the route.

- **Interface** — Interface to which packets for this route will be sent.
- **Comment** — Displays a useful comment to identify the routing rules.

DYNAMIC ROUTE

- The Wireless Broadband Router supports RIP 1 and RIP 2 dynamic routing protocol. Routing Information Protocol (RIP) is the most widely used method for dynamically maintaining routing tables. RIP uses a distance vector-based approach to routing. Routes are chosen to minimize the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to build consistent tables of next hop links which lead to relevant subnets.
- **RIP** — Enables or disable the RIP protocol for the WAN or LAN interface. (Options: Disable/v1/v2, Default: Disable)

7 WIRELESS CONFIGURATION

The wireless settings section displays configuration settings for the access point functionality of the Wireless Broadband Router. It includes the following sections:

- "Wireless Settings" on page 65
- "Basic Settings" on page 66
- "Wireless Distribution System (WDS)" on page 69
- "Wi-Fi Protected Setup (WPS)" on page 71
- "Station List" on page 74

WIRELESS SETTINGS

The IEEE 802.11n interfaces include configuration options for radio signal characteristics and wireless security features.

The Wireless Broadband Router can operate in four modes, mixed 802.11b/g/n, mixed 802.11b/g, 802.11b only, or 802.11g only. Also note that 802.11g is backward compatible with 802.11b, and 802.11n is backward compatible with both 802.11b/g at slower data transmit rates.

NOTE: The radio channel settings for the access point are limited by local regulations, which determine the number of channels that are available.

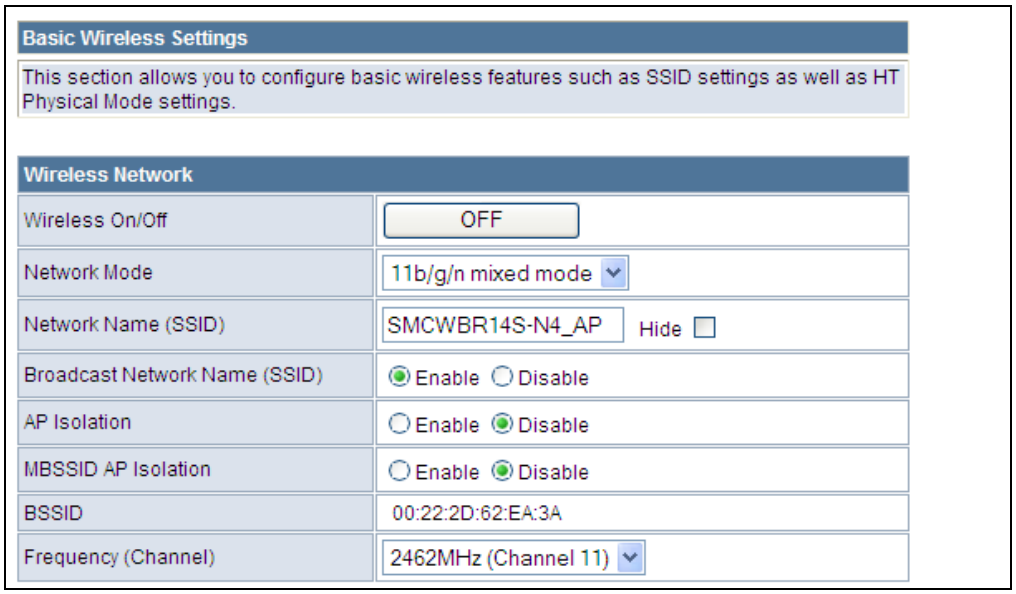
BASIC SETTINGS

The Basic Setting page allows you to enable the wireless interface, select which radio mode to use, choose the transmit frequency and configure the SSID.

Click on “Wireless Settings,” followed by “Basic”.

NOTE: There are several variables to consider when selecting a radio mode that make it fully functional. Simply selecting the mode you want is not enough to ensure full compatibility for that mode. Information on these variables may be found in the HT Physcial Mode Setting section.

Figure 28: Basic Settings



The following items are displayed on this page:

- **Wireless On/Off** — Enables or Disable the radio. (Default: Enable)
- **Network Mode** — Defines the radio mode for the VAP interface. (Default: 802.11b/g/n Mixed)

NOTE: Enabling the Wireless Broadband Router to communicate with 802.11b/g clients in 802.11b/g/n Mixed mode also requires that HT Operation in the HT Physical Mode Setting menu be set to Mixed. Setting HT Operation to Green Field is exclusive for 802.11n client communication only and prevents 802.11 b/g communication.

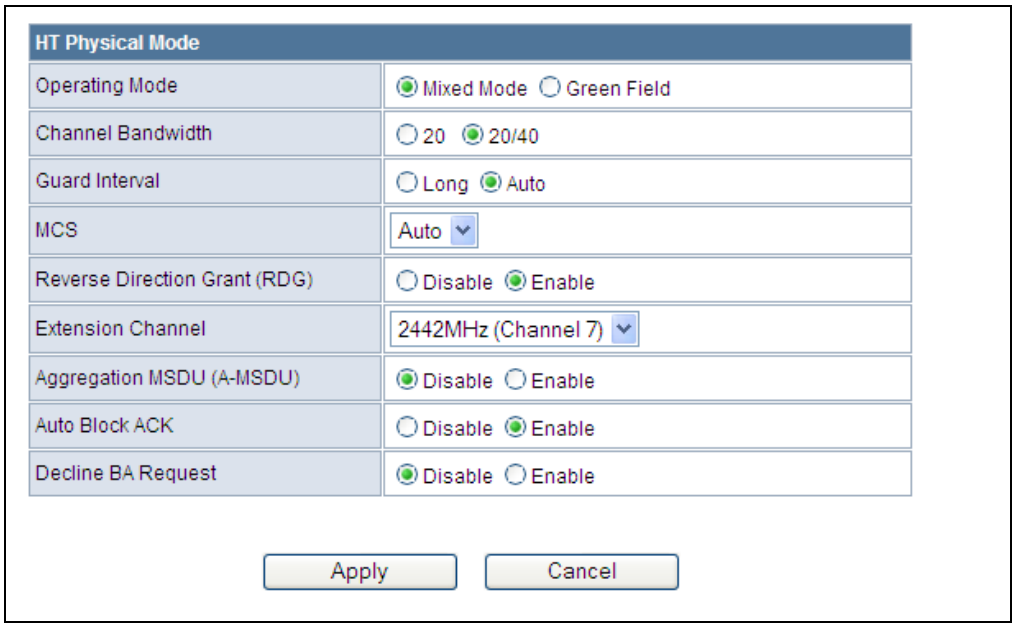
- **802.11b/g Mixed**: Both 802.11b and 802.11g clients can communicate with the Wireless Broadband Router (up to 108 Mbps), but data transmission rates may be slowed to compensate for 802.11b clients. Any 802.11n clients will also be able to communicate with the Wireless Broadband Router, but they will be limited to 802.11g protocols and data transmission rates.
- **802.11b only**: All 802.11b, 802.11g, and 802.11n clients will be able to communicate with the Wireless Broadband Router, but the 802.11g and 802.11n clients will be limited to 802.11b protocols and data transmission rates (up to 11 Mbps).
- **802.11g only**: Both 802.11g and 802.11n clients will be able to communicate with the Wireless Broadband Router, but the 802.11n clients will be limited to 802.11g protocols and data transmission rates (up to 54 Mbps). Any 802.11b clients will not be able to communicate with the Wireless Broadband Router.
- **802.11b/g/n Mixed**: All 802.11b/g/n clients can communicate with the Wireless Broadband Router (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11b/g clients.

- **Network Name (SSID)** — The name of the wireless network service provided by the Wireless Broadband Router. Clients that want to connect to the network must set their SSID to the same as that of the Wireless Broadband Router. (Default: “SMCWBR14S-N4_AP”; Range: 1-32 characters)
- **Broadcast Network Name (SSID)** — The Wireless Broadband Router will broadcast the SSID name in its beacon signal. When set to disable, the Network Name SSID is automatically set to "Hide."
- **AP Isolation** — The Wireless Broadband Router will isolate communincation between all clients in order to protect them. Normally for users who are at hotspots.
- **MBSSID AP Isolation** — The Wireless Broadband Router will isolate wireless clients from different SSID.
- **BSSID** — The identifier (MAC address) of a Wireless Broadband Router in a Basic Service Set (BSS) network.
- **WLAN Frequency** — The radio channel that the Wireless Broadband Router uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid

interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the Wireless Broadband Router to which it is linked. Selecting Auto Select enables the Wireless Broadband Router to automatically select an unoccupied radio channel.

HT PHYSICAL MODE SETTINGS

Figure 29: HT Physical Mode Settings



- **HT Operation Mode** — Packets from 802.11n clients are referred to as High Throughput (HT) Greenfield packets, in other words packets that can be transmitted at rates of up to 150 Mbps assuming that HT Channel Bandwidth is set to 20/40Mhz, see HT Channel Bandwidth next page.

NOTE: Some 802.11n wireless clients may be capable of transmission rates of up to 600 Mbps, however the Wireless Broadband Router will only be able to connect to them at a maximum transmission rate of 150 Mbps.

802.11b/g packets are referred to as non-HT packets, being transmitted at lower throughput rates. HT mixed format frames contain a preamble compatible with the non-HT receivers. HT Greenfield frames do not contain a non-HT compatible part. Support for HT Greenfield format is optional. An HT station that does not support the reception of an HT Greenfield format frame must be able to detect that an HT Greenfield format frame is an HT transmission (as opposed to a non-HT transmission). In this case the receiver must decode the high throughput signal (HT-SIG) in the packet header and determine if the HT-SIG cyclic redundancy check (CRC) passes. (Default: Mixed)

- **HT Channel Bandwidth** — The Wireless Broadband Router provides a channel bandwidth of 40 MHz by default giving an 802.11g connection speed of 108 Mbps (sometimes referred to as Turbo Mode) and a 802.11n connection speed of up to 150 Mbps. Setting the HT Channel Bandwidth to 20 MHz slows connection speed for 802.11g and 802.11n to 54 Mbps and 74 Mbps respectively and ensures backward compliance for slower 802.11b devices. (Default: 20/40MHz)

- **Guard Interval** — The guard interval between symbols helps receivers overcome the effects of multipath delays. When you add a guard time, the back portion of useful signal time is copied and appended to the front. (Default: Auto)

- **MCS** — The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels. (Options: value [range] = 0~7 (1 Tx Stream), 8~15 (2 TxStream), 32 and auto (33). Default: auto)

- **Reverse Direction Grant (RDG)** — When enables Reverse Direction Grant, the Wireless Broadband Router can reduce the transmitted data packet collision by using the reverse direction protocol. During TXOP (Transmission Opportunity) period, the receiver could use remaining transmission time to transmit data to a sender. The RDG improves transmission performance and scalability in a wireless environment.

- **Extension Channel** — When 20/40MHz channel bandwidth has been set, the extension channel option will be enabled. The extension channel will allow you to get extra bandwidth. (Options: 2417MHz/ Channel 2, 2457MHz/Channel 10. Default: 2457MHz/Channel 10.)

- **Aggregate MSDU (A-MSDU)** — This option enables Mac Service Data Unit (MSDU) aggregation. (Default: Disable)

- **Auto Block ACK** — Select to block ACK (Acknowledge Number) or not during data transferring.

- **Decline BA Request** — Select to reject peer BA-Request or not.

WIRELESS DISTRIBUTION SYSTEM (WDS)

The radio interface can be configured to operate in a mode that allows it to forward traffic directly to other Wireless Gateway Router units. To set up links between units, you must configure the Wireless Distribution System (WDS) forwarding table by specifying the wireless MAC address of all units to which you want to forward traffic.

Traffic forwarded to WDS links is automatically converted to 802.11 four-address format frame. This uses the MAC addresses of the station and that of the AP connected to it on the transmitting LAN, and the MAC addresses of the AP functioning as a wireless repeater/bridge and that of the station connected to it on a neighboring LAN in the 802.11 frame header. Ethernet traffic follows a three-address format that is reconstructed for WDS

transmission. The Wireless Broadband Router will reconstruct the frame format upon receival and transmission using the criteria of the receiving and forwarding port location and whether it is Ethernet or wireless in type.

NOTE: The Wireless Broadband Router does not support the spanning tree algorithm. WDS links should be configured appropriately to avoid causing loops on the network.

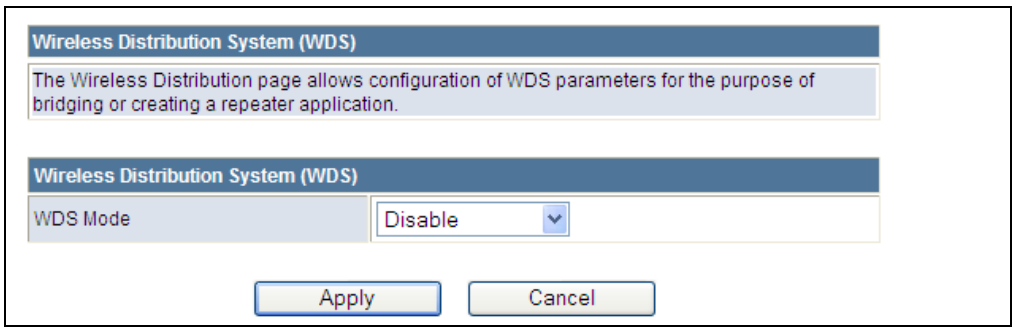
Up to four WDS links can be specified for each unit in the WDS network.

The WDS link can be configured in the following combinations:

1. Both two units are configured as Gateway Mode
2. One unit is Gateway Mode and one unit is Bridge Mode
3. Both two units are configured as Bridge Mode

When both units are set to Gateway Mode, be sure to check these settings:

- Be sure each unit is configured with a different LAN IP address.
- Be sure that only one unit has Internet access on its WAN port.
- Be sure the DHCP server is enabled only on one unit. If one unit is providing Internet access, enable the DHCP server on that unit.WDS Configuration



The WDS settings configures WDS related parameters. Up to four MAC addresses can be specified for each unit in the WDS network. WDS links may either be manually configured (Bridge and Repeater modes) or auto-discovered (Lazy mode).

- **WDS Mode** — Selects the WDS mode of the SSID. (Options: Disable/ Lazy/Bridge/Repeater. Default: Disable)
  - **Disable**: WDS is disabled.
  - **Lazy**: Operates in an automatic mode that detects and learns WDS peer addresses from received WDS four-address format frame packets, without the need to configure a WDS MAC list entry. This feature allows the Wireless Broadband Router to associate with other Wireless Broadband Routers in the network and use their WDS MAC list. In Lazy mode the Wireless Broadband Router sends a beacon.
  - **Bridge**: Operates as a standard bridge that forwards traffic between WDS links (links that connect to other AP/wireless bridges, or units in Repeater or Lazy mode) and an Ethernet port. Only data destined for stations which are known to be on the peer Ethernet link, multicast data or data with unknown destinations, need to be forwarded through the WDS link. The Bridge mode does not transmit a beacon, unlike the other three modes. In this mode the Wireless Broadband Router may also function as a repeater.
  - **Repeater**: Operates as a wireless repeater, extending the range for remote wireless clients and connecting them to an AP connected to the wired network. WDS peers must be registered with the Wireless Broadband Router. Repeater mode also supports the dual capability of the VAP functioning as an AP. In this mode, traffic is not forwarded to the Ethernet port from the radio interface. In Repeater mode the Wireless Broadband Router transmits a beacon.

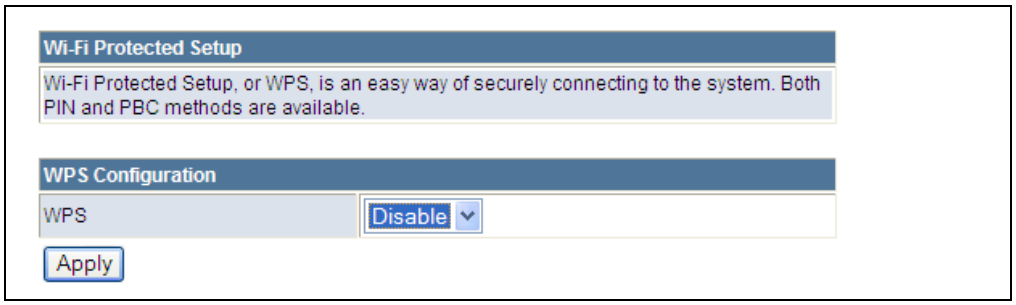
WI-FI PROTECTED SETUP (WPS)

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

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

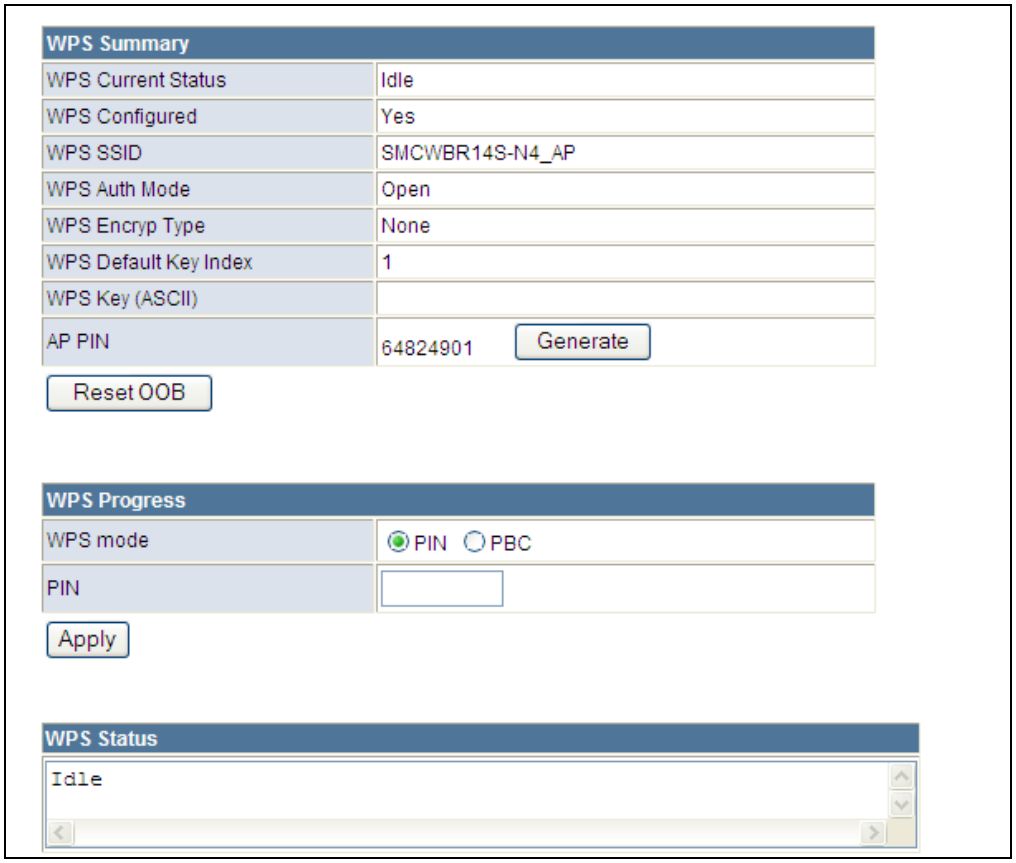
Click on “Wireless Settings,” followed by “WPS”.

Figure 30: Enabling WPS



- **WPS** — Enables WPS, locks security settings, and refreshes WPS configuration information. (Default: Enabled)

Figure 31: WPS Configuration



WPS Summary — Provides detailed WPS statistical information.

- **WPS Current Status** — Displays if there is currently any WPS traffic connecting to the Wireless Broadband Router. (Options: Start WSC Process; Idle)

- **WPS Configured** — States if WPS for wireless clients has been configured for this device.

- **WPS SSID** — The service set identifier for the unit.
- **WPS Auth Mode** — The method of authentication used.
- **WPS Encryp Type** — The encryption type used for the unit.
- **WPS Default Key Index** — Displays the WEP default key (1~4).
- **WPS Key (ASCII)** — Displays the WPS security key (ASCII) which can be used to ensure the security of the wireless network.
- **AP PIN** — Displays the PIN Code for the Wireless Broadband Router. The default is exclusive for each unit. (Default: 64824901)

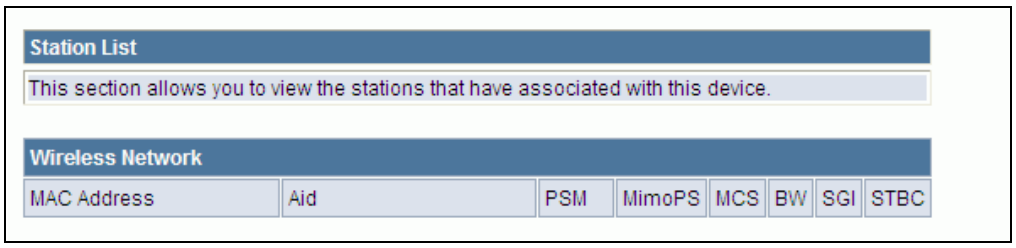
WPS Config — Configures WPS settings for the Wireless Broadband Router.

- **WPS Mode** — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:
  - **PIN**: The Wireless Broadband Router, along with other WPS devices, such as notebook PCs, cameras, or phones, all come with their own eight-digit PIN code. When one device, the WPS enrollee, sends a PIN code to the Wireless Broadband Router, it becomes the WPS registrar. After configuring PIN-Code information you must press "Apply" to send the beacon, after which you have up to two minutes to activate WPS on devices that need to join the network.
  - **PBC**: This has the same effect as pressing the physical WPS button that is located on the front of the Wireless Broadband Router. After checking this option and clicking "Apply" you have up to two minutes to activate WPS on devices that need to join the network.

STATION LIST

Displays the station information which associated to this Wireless Broadband Router.

Figure 32: Station List



8 FIREWALL CONFIGURATION

The Wireless Broadband Router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks.

Firewall Configuration contains the following sections:

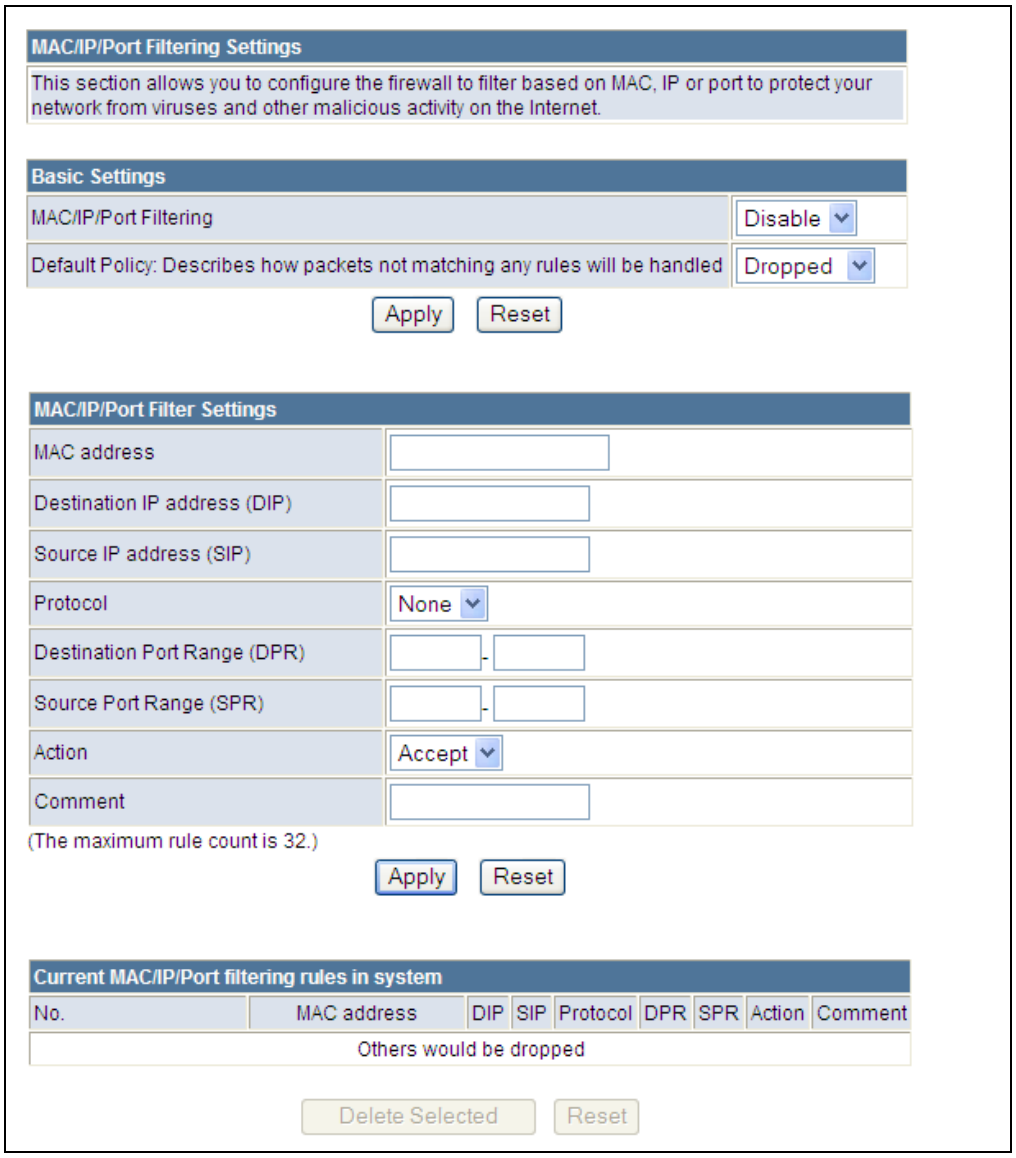
- "MAC/IP/Port Filtering" on page 75
- "Virtual Server Settings (Port Forwarding)" on page 78
- "DMZ" on page 79
- "System Security" on page 80
- "Content Filtering" on page 81

MAC/IP/PORT FILTERING

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

The Wireless Broadband Router allows you define a sequential list of permit or deny filtering rules (up to 32). This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.

Figure 33: MAC/IP/Port Filtering



- **MAC/IP/Port Filtering** — Enables or disables MAC/IP/Port Filtering. (Default: Disable)
- **Default Policy** — When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to “Dropped”, all incoming packets that don’t match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)
- **MAC Address** — Specifies the MAC address to block or allow traffic from.
- **Destination IP Address** — Specifies the destination IP address to block or allow traffic from.

- **Source IP Address** — Specifies the source IP address to block or allow traffic from.
- **Protocol** — Specifies the destination port type, TCP, UDP or ICMP. (Default: None).
- **Destination Port Range** — Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.
- **Source Port Range** — Specifies the range of source port to block traffic from the specified LAN IP address from reaching.
- **Action** — Specifies if traffic should be accepted or dropped. (Default: Accept)
- **Comment** — Enter a useful comment to help identify the filtering rules.

CURRENT FILTER RULES

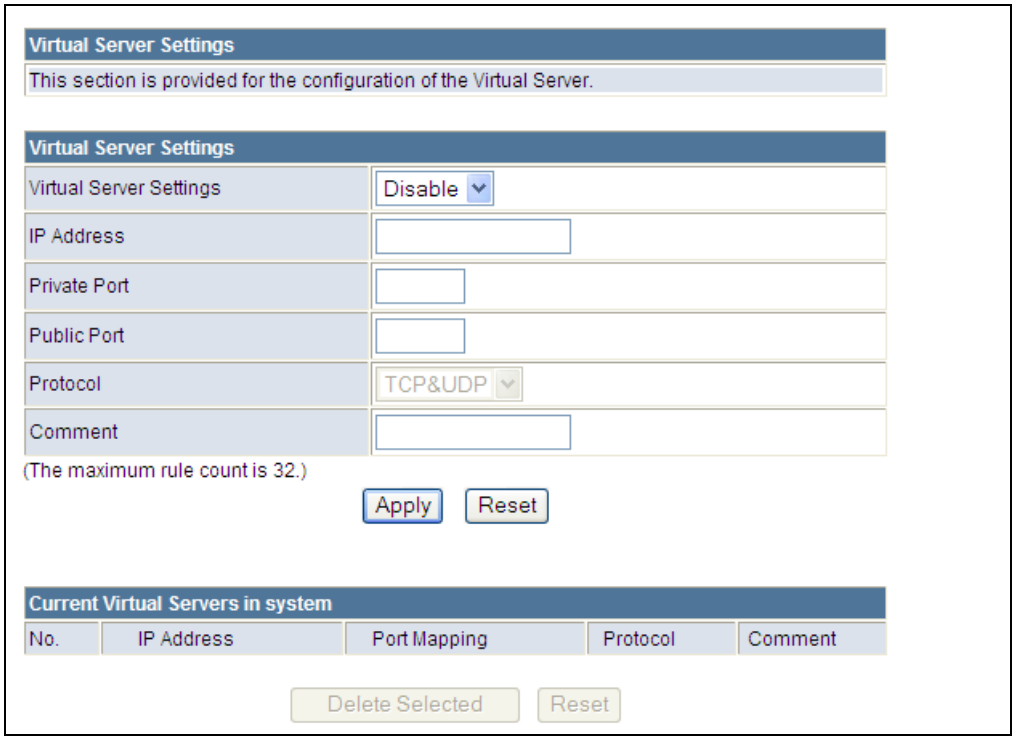
The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from the ADSL/Router.

- **Select** — Selects a table entry.
- **MAC Address** — Displays a MAC address to filter.
- **Destination IP Address** — Displays the destination IP address.
- **Source IP Address** — Displays the source IP address.
- **Protocol** — Displays the destination port type.
- **Destination Port Range** — Displays the destination port range.
- **Source Port Range** — Displays the source port range.
- **Action** — Displays if the specified traffic is accepted or dropped.
- **Comment** — Displays a useful comment to identify the routing rules.

VIRTUAL SERVER SETTINGS (PORT FORWARDING)

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding a network port from one network node to another. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NAT-enabled router. (Maximum 32 entries are allowed.)

Figure 34: Virtual Server



- **Virtual Server Settings** — Selects between enabling or disabling port forwarding the virtual server. (Default: Disable)
- **IP Address** — Specifies the IP address on the local network to allow external access.
- **Port Range** — Specifies the port range through which traffic is forwarded.
- **Protocol** — Specifies a protocol to use for port forwarding, either TCP, UDP or TCP&UDP.
- **Comment** — Enter a useful comment to help identify the forwarded port service on the network.

CURRENT VIRTUAL SERVERS IN SYSTEM

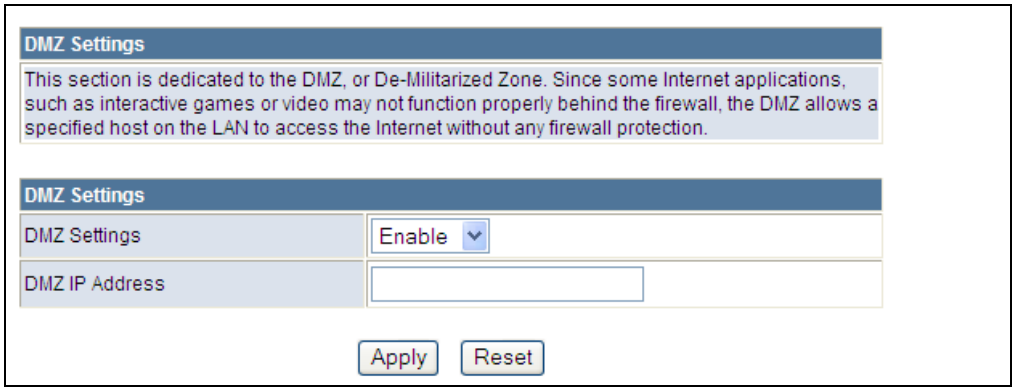
The Current Port Forwarding Table displays the entries that are allowed to forward packets through the Wireless Broadband Router's firewall.

- **No.** — The table entry number.
- **IP Address** — Displays an IP address on the local network to allow external access to.
- **Port Mapping** — Displays the port the server is mapped.
- **Protocol** — Displays the protocol used for forwarding of this port.
- **Comment** — Displays a useful comment to identify the nature of the port to be forwarded.

DMZ

Enables a specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the Wireless Broadband Router's firewall. By specifying a Demilitarized Zone (DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned a static IP address (which is mapped to its MAC address) and this must be configured as the DMZ IP address.

Figure 35: DMZ

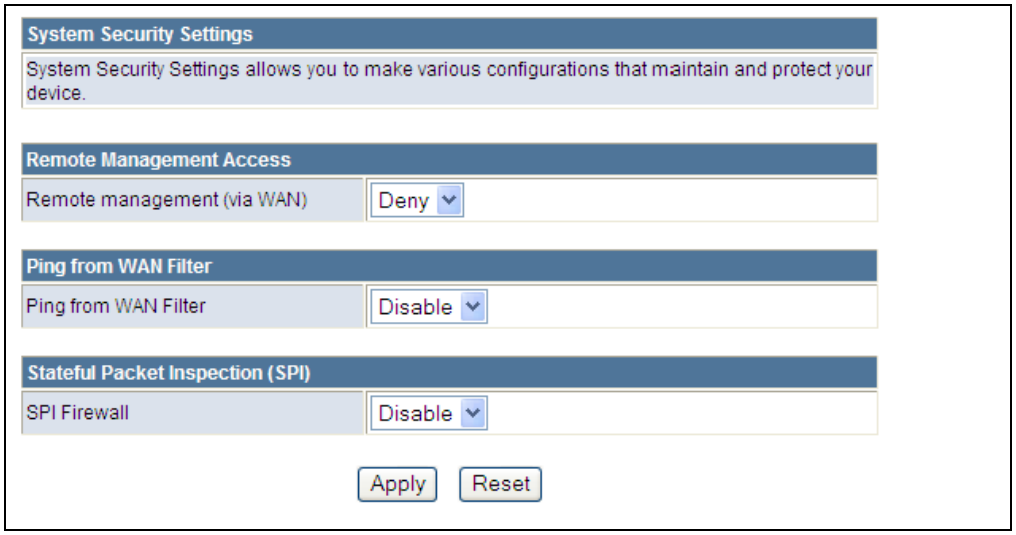


- **DMZ Settings** — Sets the DMZ status. (Default: Disable)
- **DMZ IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

SYSTEM SECURITY

The Wireless Broadband Router includes the facility to manage it from a remote location. The unit can also be sent a ping message from a remote location.

Figure 36: System Security

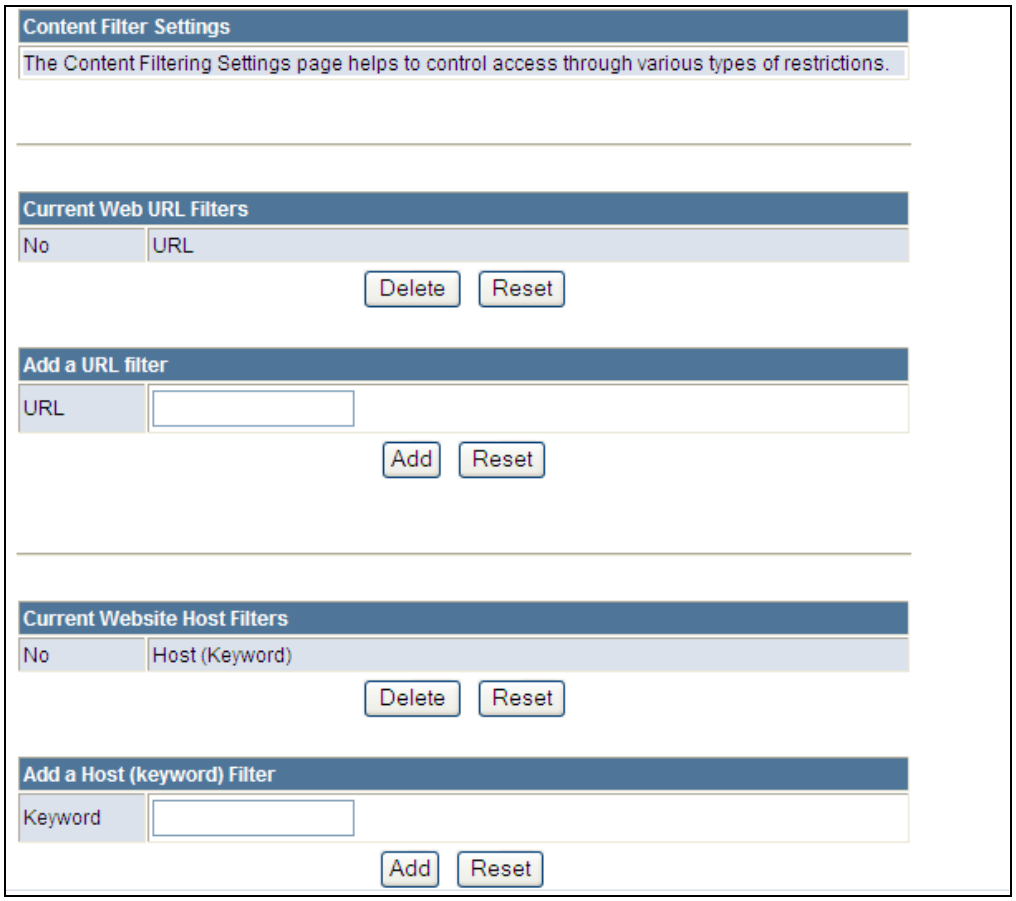


- **Remote Management** — Denies or allows management access to the Gateway Router through the WAN interface. (Default: Deny)
- **Ping from WAN Filter** — When enabled, the Gateway Router does not respond to ping packets received on the WAN port. (Default: Disable)
- **Stateful Packet Inspection (SPI)** — The Stateful Packet Inspection (SPI) firewall protects your network and computers against attacks and intrusions. A stateful packet firewall looks at packet contents to check if the traffic may involve some type of security risk. (Default: Disable)

CONTENT FILTERING

The Wireless Broadband Router provides a variety of options for blocking Internet access based on content, URL and host name.

Figure 37: Content Filtering



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

- **Current URL Filters** — Displays current URL filter.
- **Add a URL Filter** — Adds a URL filter to the settings. For example, myhost.example.com.

Web Host Filter Settings — The Wireless Broadband Router allows Internet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.FUNGAMES.com, the domain name is FUNGAMES.com. Enter the Keyword then click "Add".

- **Current Host Filters** — Displays current Host filter.

- **Add a Host Filter** — Enters the keyword for a host filtering.

9 ADMINISTRATION SETTINGS

The Wireless Broadband Router's Administration Settings menu provides the same configuration options in both Gateway and Bridge Mode. These settings allow you to configure a management access password, set the system time, upgrade the system software, display the system status and statistics.

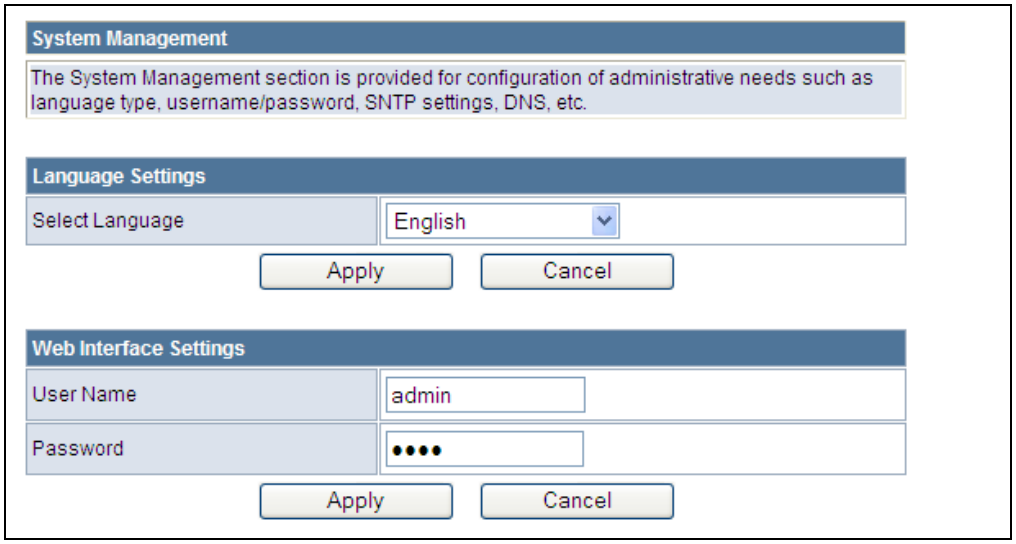
Administration Settings contains the following sections:

- "System Management" on page 84
- "SNTP Settings" on page 85
- "DDNS Settings" on page 86
- "Upgrade Firmware" on page 87
- "Configuration Settings" on page 88
- "System Status" on page 89
- "Statistics" on page 91
- "System Log" on page 92

SYSTEM MANAGEMENT

The System Management commands allow you to change the language settings displayed in the interface, and change the user name and password.

Figure 38: System Management



LANGUAGE SETTINGS

You can change the language displayed in web interface. Chooses the appropriate language of your choice from the drop-down list, then click "Apply". (Options: English, Traditional Chinese. Default: English)

WEB INTERFACE SETTINGS

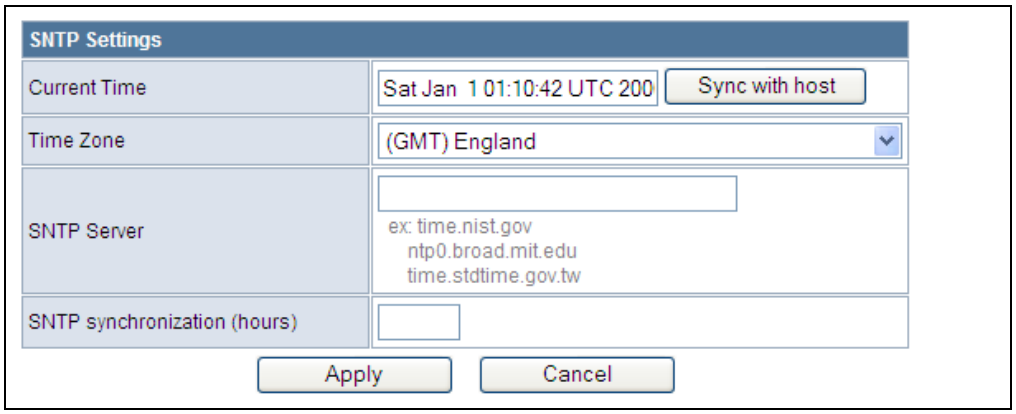
To protect access to the management interface, you need to configure a new Administrator's user name and password as soon as possible. If a new user name and password are not configured, then anyone having access to the Wireless Broadband Router may be able to compromise the unit's security by entering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

- **User Name** — The name of the user. The default name for access to the unit is "admin". (Length: 3-16 characters, case sensitive)
- **Password** — The password for management access. The default password preset for access to the unit is "smcadmin" (Length: 3-16 characters, case sensitive)
- **Confirm Password** — Prompts you to enter the password again for verification.

SNTP SETTINGS

The System Management page allows you to manually configure time settings or enable the use of a Simple Network Time Protocol (SNTP) or NTP server.

Figure 39: SNTP Settings



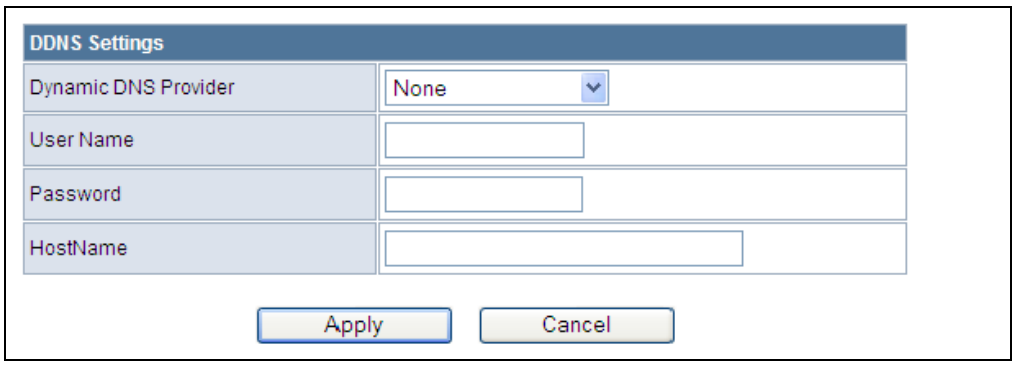
- **Current Time** — Displays the current system time on the unit.
- **Sync with host —** Updates the unit's time from the web management PC's system time.
- **Time Zone** — Specifies the time zone in relation to Greenwich Mean Time (GMT).
- **SNTP Server** — The IP address or URL of the NTP server to be used.
- **SNTP synchronization —** Sets the SNTP sycnronization in hours.

DDNS SETTINGS

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

The Wireless Broadband Router provides access to three DDNS service providers, DynDns.org, Non-IP.com and ZoneEdit.com. To set up an DDNS account, visit the websites of these service providers at www.dyndns.org, www.non-ip.com, or www.zoneedit.com.

Figure 40: DDNS Settings (Gateway Mode)

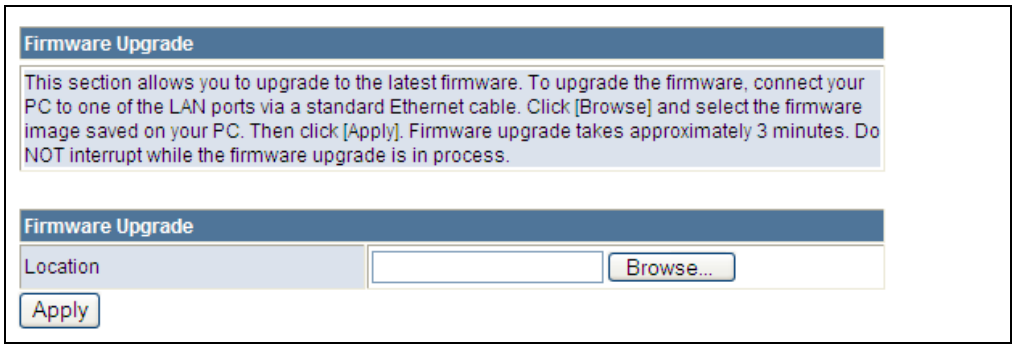


- **Dynamic DNS Provider** — Specifies the DDNS service provider, DynDns.org, Freedns.afraid.org, ZoneEdit.com or Non-IP.com. (Default: none)
- **User Name —** Specifies your user name for the DDNS service.
- **Password** — Specifies your password for the DDNS service.
- **HostName** — Specifies the URL of the DDNS service.

UPGRADE FIRMWARE

You can update the Wireless Broadband Router firmware by using the Firmware Update facility.

Figure 41: Upgrade Firmware



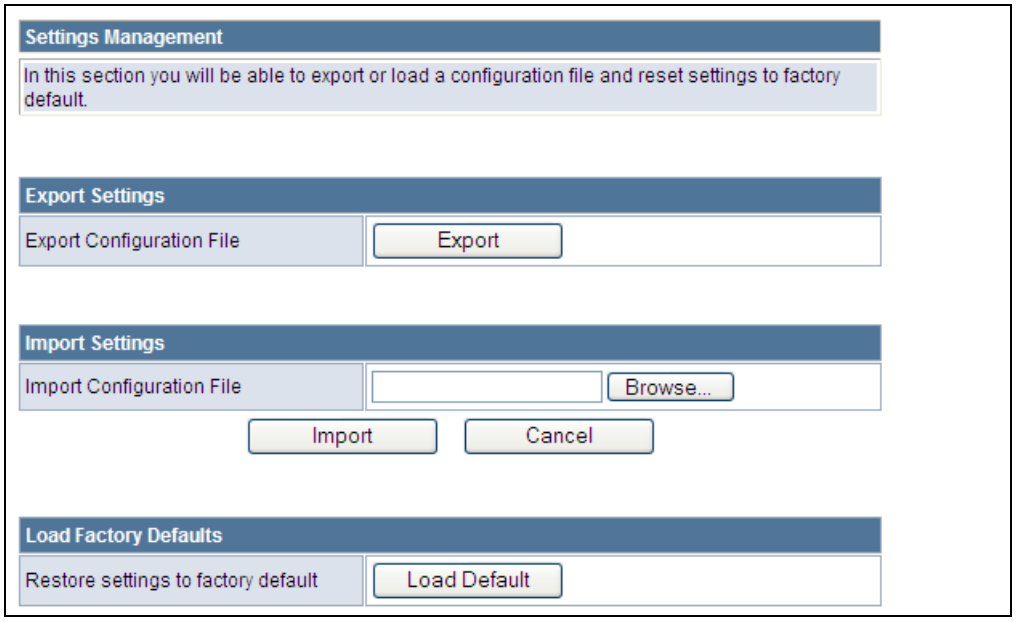
Firmware Upgrade — Allows you to upload new firmware manually by specifying a file path. Make sure the firmware you want to use is on the local computer by clicking Browse to search for the firmware to be used for the update.

- **Browse** — Opens a directory on the local hard drive for specifying the path of the file to upload.
- **Apply** — Starts the upload procedure.

CONFIGURATION SETTINGS

The Configuration Setting page allows you to save the Wireless Broadband Router's current configuration or restore a previously saved configuration back to the device.

Figure 42: Configuration Settings

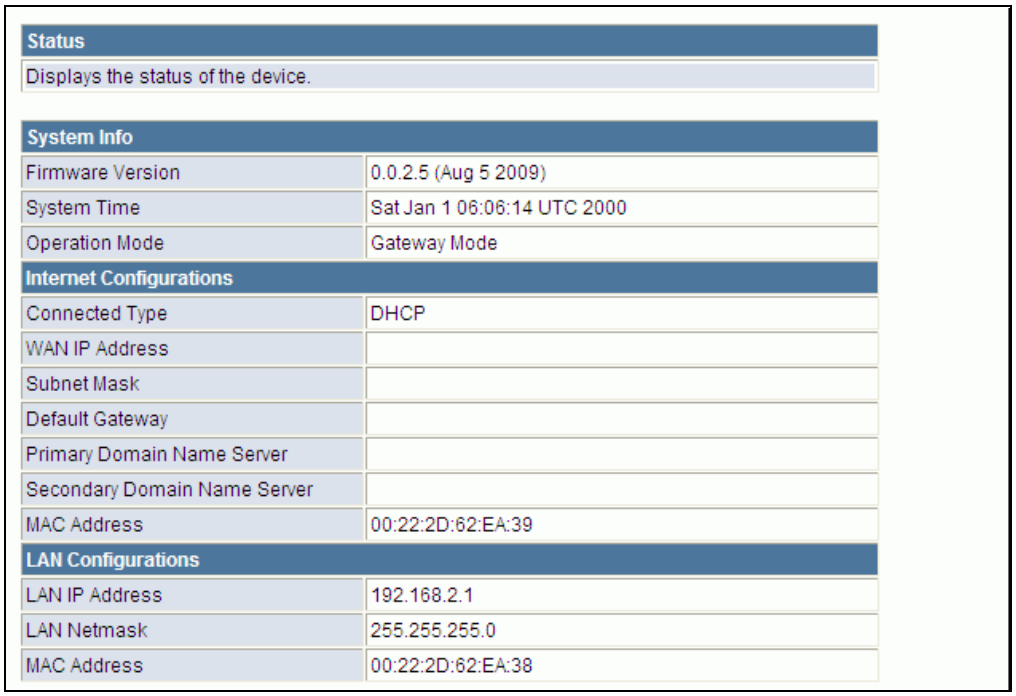


- **Export Settings** — Saves the current configuration to a file locally.
- **Import Settings** — Allows the user to load previously saved configuration files from a local source.
- **Load Factory Defaults** — Restores the factory defaults.

SYSTEM STATUS

The System Information page displays basic system information and the displayed settings are for status information only and are not configurable on this page. This information is split into the three sections that follow.

Figure 43: System Status (Gateway Mode)



Status	
Displays the status of the device.	
System Info	
Firmware Version	0.0.2.5 (Aug 5 2009)
System Time	Sat Jan 1 06:06:14 UTC 2000
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:22:2D:62:EA:39
LAN Configurations	
LAN IP Address	192.168.2.1
LAN Netmask	255.255.255.0
MAC Address	00:22:2D:62:EA:38

System Info — Displays the basic system information in both Bridge and Gateway Modes:

- **Firmware Version** — The version number of the current Wireless Broadband Router software.
- **System Time** — Length of time the management agent has been up, specified in hours and minutes.
- **Operation Mode** — Displays the mode setting of the unit.

Internet Configurations — Displays the basic WAN information:

- **Connected Type** — Displays the WAN connected mode. (Default: DHCP)
- **WAN IP Address** — IP address of the WAN port for this device.
- **Subnet Mask** — The mask that identifies the host address bits used for routing to the WAN port.

- **Default Gateway** — The default gateway is the IP address of the router for the Wireless Broadband Router, which is used if the requested destination address is not on the local subnet.

- **Primary DNS Server / Secondary DNS Server** — The IP address of Domain Name Servers. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

- **MAC Address** — The shared physical layer address for the Wireless Broadband Router's LAN ports.

Local Network — Displays the basic LAN information:

- **LAN IP Address** — The IP address configured on the Wireless Broadband Router.

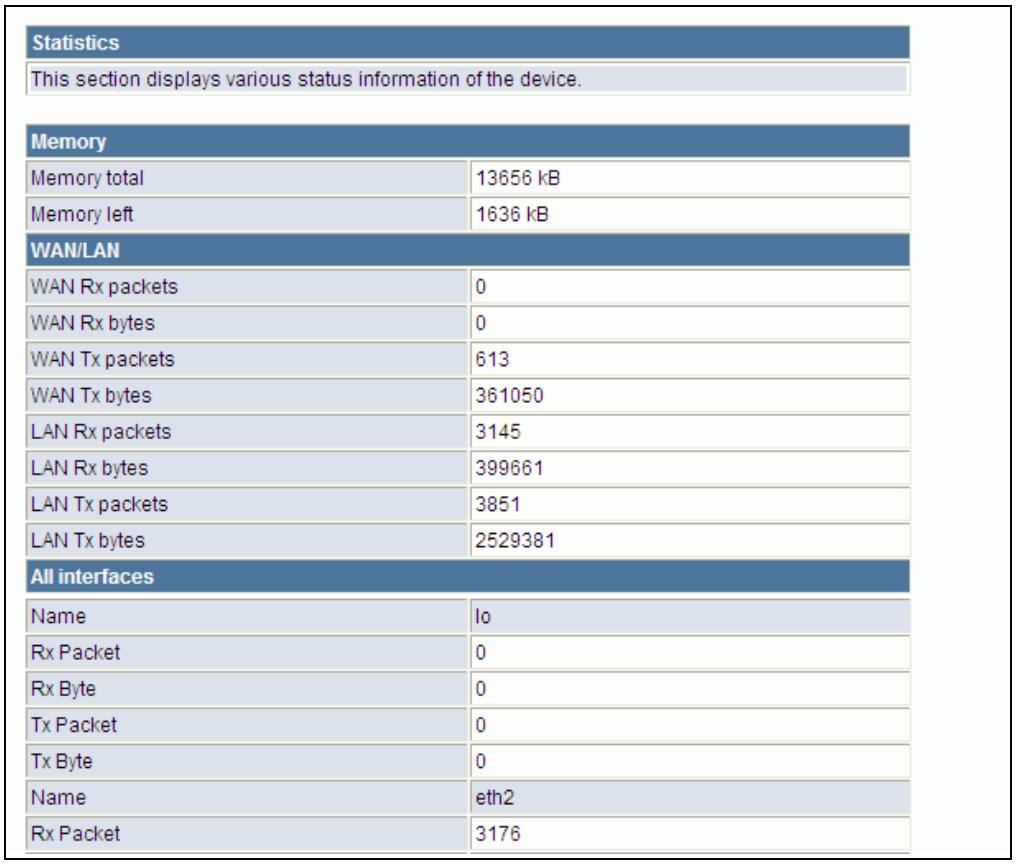
- **LAN Netmask** — The mask that identifies the host address bits used for routing to the LAN port.

- **MAC Address** — The shared physical layer address for the Wireless Broadband Router's LAN ports.

STATISTICS

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

Figure 44: Statistics



Statistics	
This section displays various status information of the device.	
Memory	
Memory total	13656 kB
Memory left	1636 kB
WAN/LAN	
WAN Rx packets	0
WAN Rx bytes	0
WAN Tx packets	613
WAN Tx bytes	361050
LAN Rx packets	3145
LAN Rx bytes	399661
LAN Tx packets	3851
LAN Tx bytes	2529381
All interfaces	
Name	lo
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	eth2
Rx Packet	3176

The following items are displayed on this page:

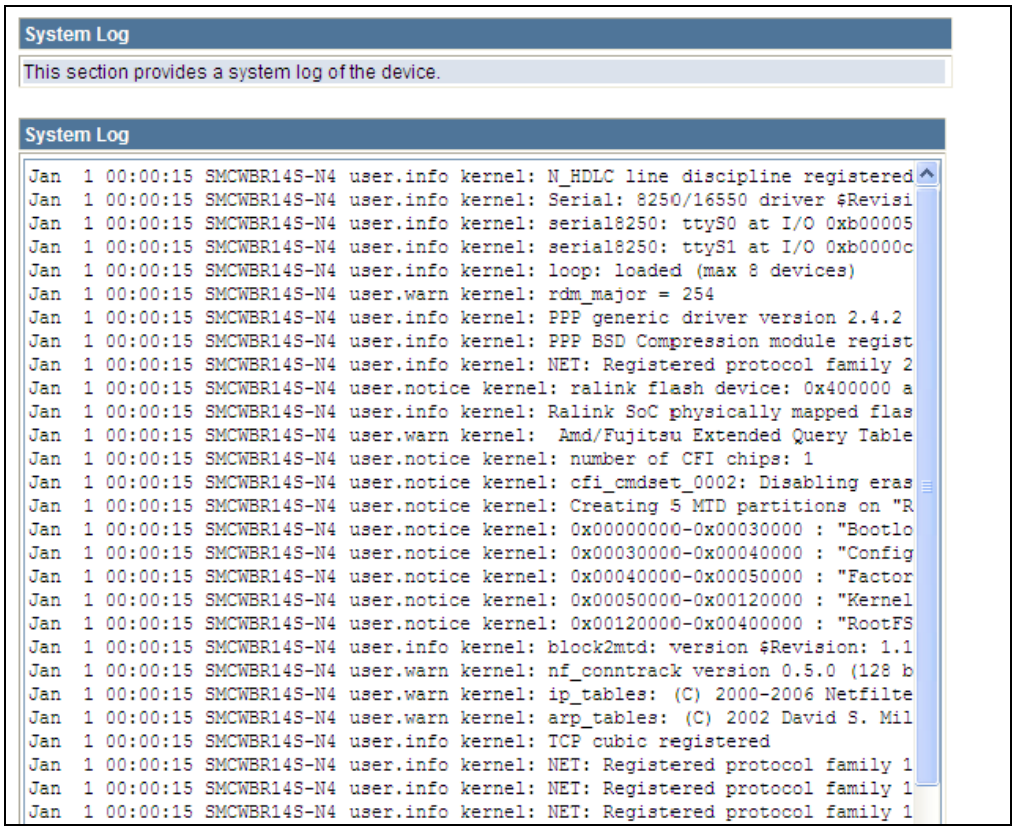
- **Memory total** — The total memory of this Wireless Broadband Router.
- **Memory left** — The available memory of this Wireless Broadband Router.
- **WAN/LAN/All Interfaces** — Displays the interface on which traffic is being monitored.
- **Rx packets** — Displays the total number of packets received by the specified interface.
- **Rx bytes** — Displays the total number of bytes transmitted by the specified interface.

- **Tx packets** — Displays the total number of packets transmitted by the specified interfaces.
- **Tx bytes** — Displays the total number of bytes transmitted by the specified interface.

SYSTEM LOG

The Wireless Broadband Router supports a logging process that controls error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating Wireless Broadband Router and network problems. The System Log page displays the latest messages logged in chronological order, from the newest to the oldest. Log messages saved in the Wireless Broadband Router's memory are erased when the device is rebooted.

Figure 45: System Log



- **Refresh** — Sends a request to add the latest entries to the System Log Table.
- **Clear** — Removes the current system log messages from the System Log Table.

SECTION III

APPENDICES

This section provides additional information and includes these items:

- "Troubleshooting" on page 95
- "Hardware Specifications" on page 98
- "Cables and Pinouts" on page 100
- "Glossary" on page 107
- "Index" on page 111

A TROUBLESHOOTING

DIAGNOSING LED INDICATORS

Table 3: LED Indicators

Symptom	Action
Power/LAN LEDs are off	◆ The AC power adapter may be disconnected. Check connections between the Gateway Router, the power adapter, and the wall outlet.
WLAN LED is off	◆ The access point radio has been disabled through it's web management interface. Access the management interface using a web browser to enable the radio.
LAN LEDs are off (when port connected)	◆ Verify that the Gateway Router is powered on. ◆ Be sure cables are plugged into both the Gateway Router and corresponding PC. ◆ Verify that the proper cable type is used and its length does not exceed specified limits. ◆ Check the cable connections for possible defects. Replace the defective cable if necessary.
WAN LED is off	◆ There is no detected signal from WAN port. Check connections and the management interface.

IF YOU CANNOT CONNECT TO THE INTERNET

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

BEFORE CONTACTING TECHNICAL SUPPORT

Check the following items before you contact local Technical Support.

1. If the Gateway Router cannot be configured using a web browser:
    - Be sure to have configured the Gateway Router with a valid IP address, subnet mask and default gateway.

- Check that you have a valid network connection to the Gateway Router and that the Ethernet port or the wireless interface that you are using has not been disabled.

- If you are connecting to the Gateway Router through the wired Ethernet interface, check the network cabling between the management station and the Gateway Router. If you are connecting to Gateway Router from a wireless client, ensure that you have a valid connection to the Gateway Router.

2. If you forgot or lost the password:

   - Set the Gateway Router to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default user name "admin" and password "smcadmin" to access the management interface.

3. If all other recovery measure fail, and the Gateway Router is still not functioning properly, take any of these steps:

   - Reset the Gateway Router's hardware using the web interface, or through a power reset.

B HARDWARE SPECIFICATIONS

PORT INTERFACES	WAN: 1 10/100BASE-TX port, RJ-45 connector, auto MDI/X (100-ohm, UTP cable; Category 5 or better) LAN 1~4: 1 10/100BASE-TX port, RJ-45 connector, auto MDI/X (100-ohm, UTP cable; Category 5 or better)
AC POWER ADAPTER	Input: 100~240 VAC, 50/60 Hz Output: 5 V/ 1 A
LED INDICATORS	Power, WLAN (Wireless Local Area Network), WPS (Wi-Fi Protected Setup), WAN (Wide Area Network), LAN 1~4 (Local Area Network).
NETWORK MANAGEMENT	Web-browser
TEMPERATURE	Operating: 0 to 40 °C (32 to 104 °F) Storage: -20 to 70 °C (32 to 158 °F)
HUMIDITY	20% to 85% (non-condensing)
RADIO	EN300 328, FCC Part 15c, LP0002
EMC	EN55022/24, EN301 489-1-17, FCC Part15b
SAFETY	EN60950-1
STANDARDS	UL60950-1/CSA22.2 No. 60950-1; EN60950-1/IEC60950-1 ETSI EN300 019-2-1 Class 1.2 (Storage) ETSI EN300 019-2-2 Class 2.3 (Packaged) ETSI EN300 019-2-3 Class 3.2 (Operating)
PHYSICAL SIZE	136 X 90.8 X 28.5 mm

WEIGHT 157 g (5.54 oz)

C CABLES AND PINOUTS

TWISTED-PAIR CABLE ASSIGNMENTS

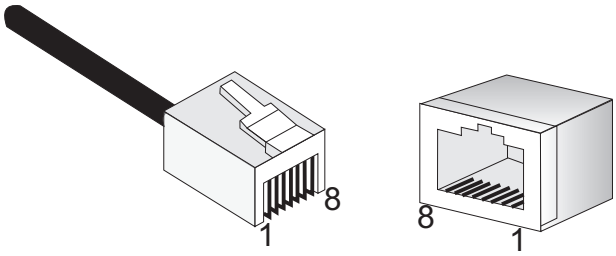
For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. For 1000BASE-T connections the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also,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

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

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

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

Figure 46: RJ-45 Connector



10/100BASE-TX PIN ASSIGNMENTS

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

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

Table 4: 10/100BASE-TX MDI and MDI-X Port Pinouts

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

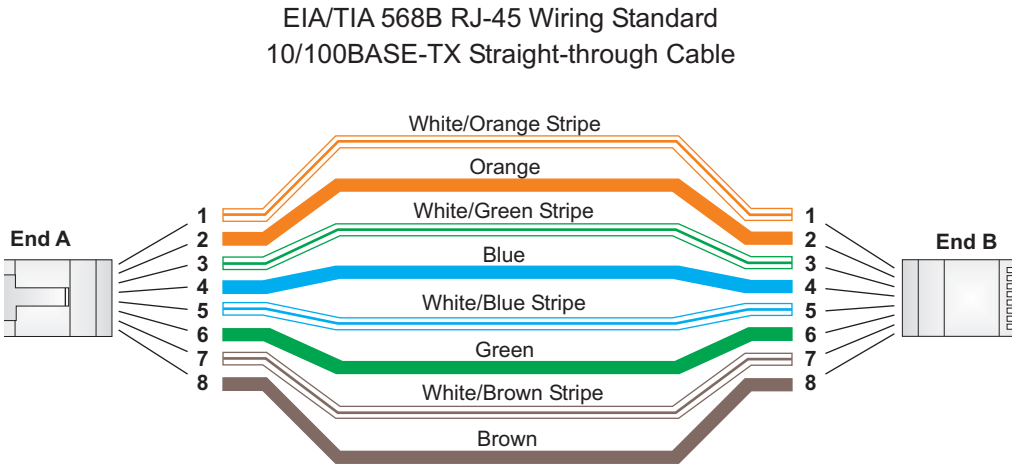
a. The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

STRAIGHT-THROUGH WIRING

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

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

Figure 47: Straight-through Wiring

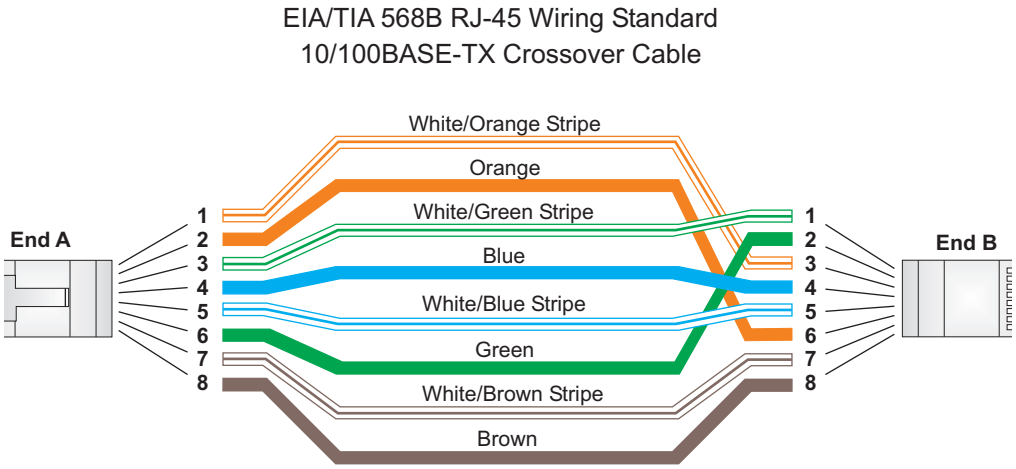


CROSSOVER WIRING

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

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

Figure 48: Crossover Wiring



D LICENSE INFORMATION

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GLOSSARY

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

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

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

ACCESS POINT An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

AES Advanced Encryption Standard: An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

AUTHENTICATION The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

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

BEACON A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

BROADCAST KEY Broadcast keys are sent to stations using dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on

the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

ENCRYPTION Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

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

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

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

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

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

INFRASTRUCTURE An integrated wireless and wired LAN is called an infrastructure configuration.

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

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

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

OPEN SYSTEM A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the

beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

ODFM Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

SSID Service Set Identifier: An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

SESSION KEY Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

SHARED KEY A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

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

TKIP Temporal Key Integrity Protocol: A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

TFTP Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

VAP Virtual Access Point: Virtual AP technology multiplies the number of Access Points present within the RF footprint of a single physical access device. With Virtual AP technology, WLAN users within the device.s footprint can associate with what appears to be different access points and their associated network services. All the services are delivered using a single radio channel, enabling Virtual AP technology to optimize the use of limited WLAN radio spectrum.

WI-FI PROTECTED ACCESS WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

WEP Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA-PSK WPA Pre-shared Key: WPA-PSK can be used for small office networks with a limited number of users that may not need a high level of security. WPA-PSK provides a simple security implementation that uses just a pre-shared password for network access.

INDEX

A

Applications 22

E

Ethernet port 26

H

hardware capabilities 21
hardware description 23

I

initial configuration 38
installing the access point 33
introduction 21, 29
ISP settings 38

K

key features 21

L

LED indicators 25
location selection 33
login page 38

M

mounting on a wall 34

P

package contents 23
power connector 26

R

reset button 27

S

system requirements 33

T

troubleshooting 103

SMC®
Networks

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

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

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

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

Français: Informations Support Technique sur www.smc.com

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

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

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

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

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

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

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

简体中文：技术支持讯息可通过www.smc-prc.com查询

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

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smc-asia.com을 참고하시기 바랍니다

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

World Wide Web: http://www.smc.com/

SMCWBR14S-N4

20 Mason • Irvine, CA 92618 • Phn: (949) 679-8000 • www.smc.com