USER GUIDE

Pareto Networks BG-100 Branch Services Gateway

BG-100

pareto networks™

USER GUIDE

BG-100

Pareto Networks BG-100 Branch Services Gateway
with one RJ-45 WAN Port,
One RJ-45 LAN Port,
and IEEE 802.11n Wi-Fi

BG-100
E022010-CS-R01
****

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.

The following three 3G cards have passed the co-located EMC/RF exposure test with this device and can be used with this device. Other 3G cards may or may not comply with FCC rules, please consult the manufacturer before purchase.

Interface	Brand	Product Name	Model	FCC ID	NCC ID
USB Port	HUAWEI	HSDPA USB Stick	E169	QISE169	CCAD083G0060T5
	ZTE	HSDPA USB Modem	MF626	Q78-ZTEMF622	N/A
	Huawei	HSDPA USB Modem	E220	QISE220	N/A

IC Statement

This device complies with RSS-210 of the Industry Canada Rules. 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.

This device has been designed to operate with an antenna having a maximum gain of 2.35 dBi. Antennas having a higher gain are strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

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 and your body.

Australia/New Zealand AS/NZS 4268

ACN 066 352010

TAIWAN NCC

根據國家通信傳播委員會低功率電波輻射性電機管理辦法規定：

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

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

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: 2006 (IEC 60950-1) — Product Safety
- EN 55022:2006 + A1:2007, Class B — ITE EMC
- EN 55024:1998 + A1:2001 + A2:2003 — ITE EMC
- EN 300 328 V1.7.1 (2006-10) — Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 V1.8.1 (2008-04) — EMC requirements for radio equipment
- EN 301 489-17 V1.3.2 (2008-04) — EMC requirements for radio equipment
- 50385 (2002) — Country-specific SAR requirements

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

- Austria
- Belgium
- Bulgaria
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- 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 gateway and its physical and performance related characteristics. It also gives information on how to operate and use the management functions of the gateway.

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 gateway’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.

February 2010 Revision

This is the first revision of this guide.

Contents

FIGURES

TABLES

SECTION I

GETTING STARTED

This section provides an overview of the gateway, 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:

1 Introduction

The Pareto Networks BG-100 Branch Services Gateway (BG-100) 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.

Table 1: Key Hardware Features

Feature	Description
WAN Port	One 100BASE-TX RJ-45 port for connecting to the Internet.
LAN Port	One 100BASE-TX RJ-45 port for local network connections.
USB Port	One USB slot for a 3G or 3.5G modem.
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, LAN port, and WLAN 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 one 10/100 Mbps Ethernet port.
- DHCP for dynamic IP configuration.
- Firewall with Stateful Packet Inspection, client privileges, 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 passthrough (IPsec, PPTP, or L2TP).

- User-definable application sensing tunnel supports applications requiring multiple connections.
- Easy setup and management through an easy-to-use web browser interface on any operating system that supports TCP/IP.
- Compatible with all popular Internet applications.

APPLICATIONS

Many advanced networking features are provided by the Gateway:

- **Wired LAN** — The Gateway provides connectivity to wired Ethernet 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, PPTP, or L2TP to establish communications with end users, the Gateway includes built-in clients for these protocols, eliminating the need to install these services on your computer.
- **Shared IP Address** — The Gateway provides Internet access for up to 253 users using a single shared IP address account.
- **Virtual Server** — If you have a fixed IP address, you can set the Gateway to act as a virtual host for network address translation. Remote users access various services at your site using a static IP address. Then, depending on the requested service (or port number), the Gateway 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 Gateway supports security features that deny Internet access to specified users, or filter all requests for specific services. WPA (Wi-Fi Protected Access) and MAC filtering provide security over the wireless network.
- **Virtual Private Network (VPN) Passthrough** — The Gateway supports the passthrough of three of the most commonly used VPN protocols – IPsec, PPTP, and L2TP. These protocols allow remote users to establish a secure connection to another 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 (that is, a traditionally shared data network). The VPN-passthrough protocols supported by the Barricade are briefly described below.

- **IPsec (Internet Protocol Security) —** Encrypts and authenticates entire IP packets and encapsulates them into new IP packets for secure communications between networks.

- **PPTP (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.

- **L2TP (Layer 2 Tunneling Protocol)** — Merges the best features of PPTP and the Layer 2 Forwarding (L2F) protocol. Like PPTP, L2TP requires that the ISP's routers support the protocol.

PACKAGE CONTENTS

The Pareto Networks BG-100 Branch Services Gateway package includes:

- BG-100 Branch Services Gateway
- 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 Pareto Networks BG-100 Branch Services Gateway, from herein refered to as the Gateway, connects to the Internet through its RJ-45 WAN port. It connects directly to your PC or to a local area network using its RJ-45 Fast Ethernet LAN port.

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

Figure 1: Top Panel

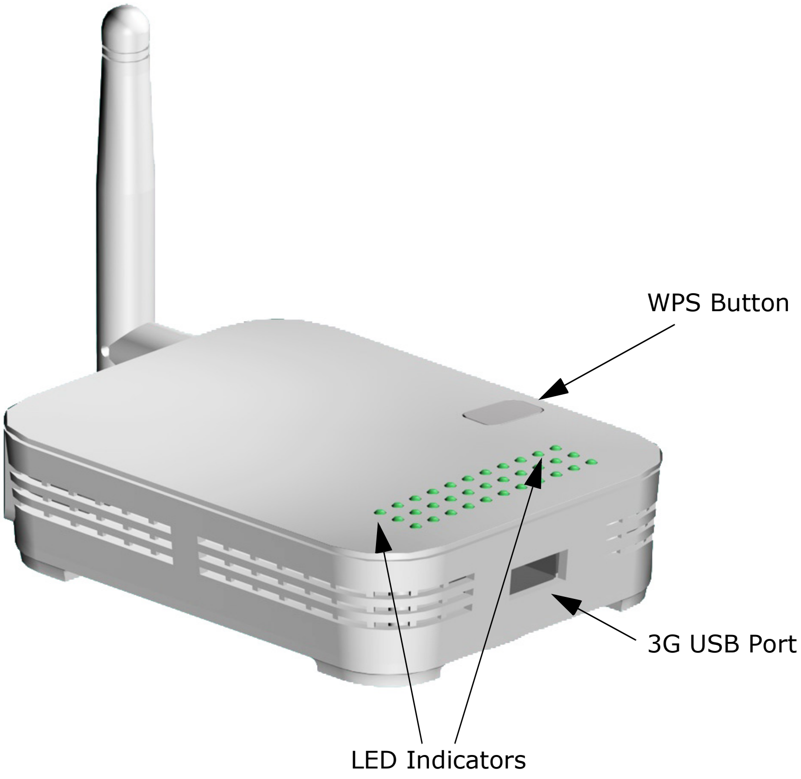
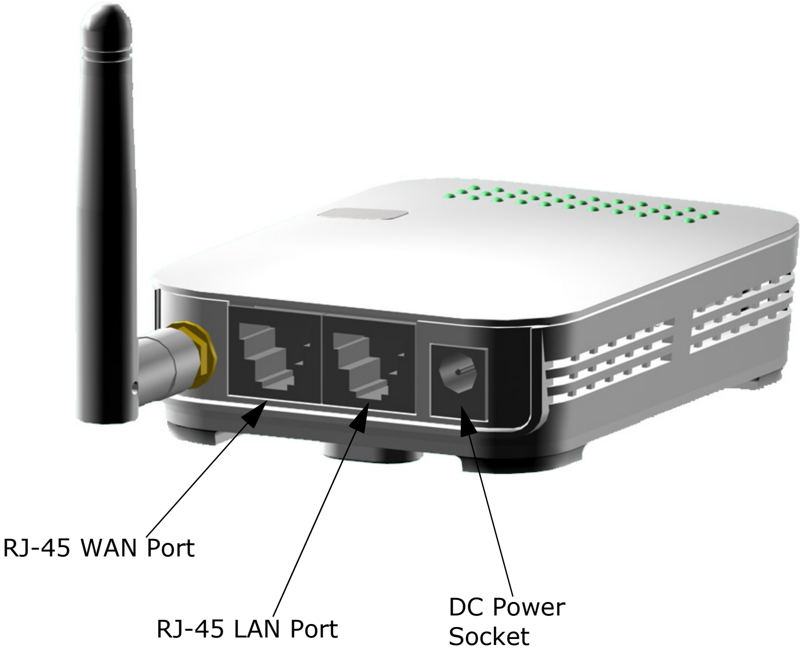


Figure 2: Rear Panel



LED INDICATORS

The Gateway includes four status LED indicators, as described in the following figure and table.

Figure 3: LEDs

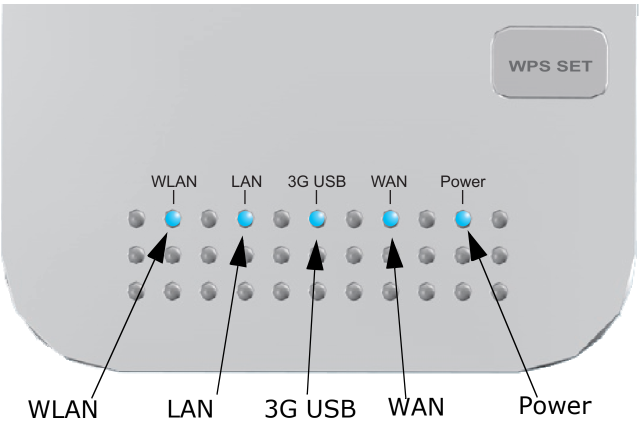


Table 2: LED Behavior

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.
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.
LAN	On Blue	The Ethernet LAN port is connected to a PC or server.
	Blinking	The Ethernet port is connected and is transmitting or receiving data.
	Off	The Ethernet port is disconnected or has malfunctioned.
3G USB	On Blue	The unit has established a 3G connection.
	Blinking	The unit is transmitting or receiving data on the 3G link.
	Off	There is no connection on the 3G USB port.

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 PORT

The Gateway has one 100BASE-TX RJ-45 port that can be attached directly to a PC or 10BASE-T/100BASE-TX LAN segments.

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

3G MODEM USB PORT

The 3G Modem USB Port supports connection to a wireless cellular 3G or 3.5G modem for broadband Internet access.

POWER CONNECTOR

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

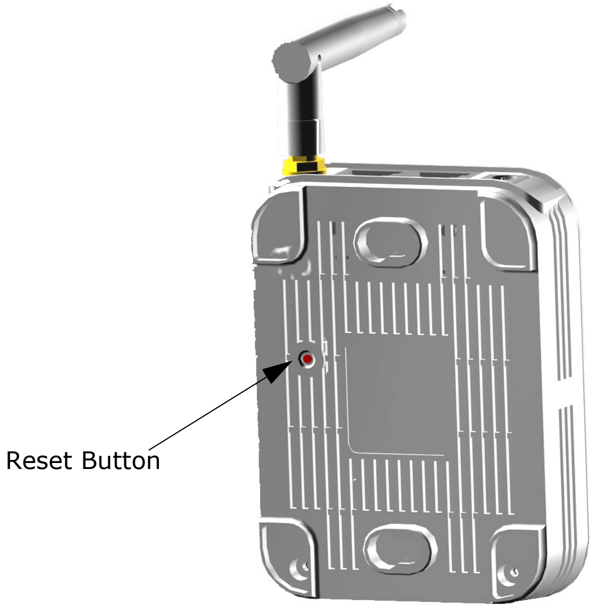
WPS BUTTON

Press the WPS button to automatically configure the Gateway with other WPS devices in the WLAN.

RESET BUTTON

The Reset 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.

Figure 4: Bottom Panel



2 Network Planning

The Gateway 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.

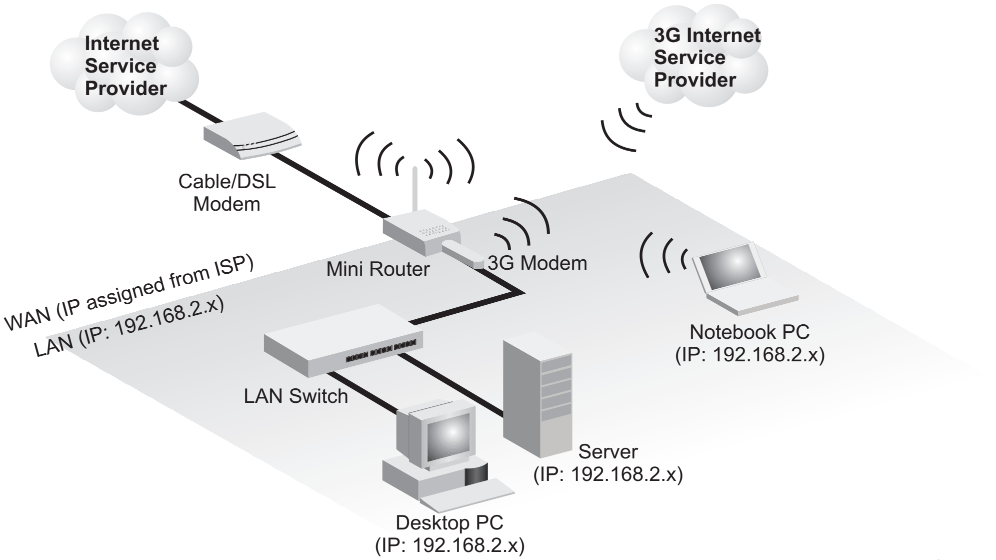
This chapter explains some of the basic features of the Gateway and shows some network topology examples in which the device is implemented.

Internet Gateway Router

The Gateway 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 Gateway either through a wired connection to a LAN port, or though the device's own wireless network. The Gateway functions as an Internet gateway when set to Router 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 5: Operating as an Internet Gateway Router


Internet Service Provider
3G Internet Service Provider
Cable/DSL Modem
Mini Router
3G Modem
WAN (IP assigned from ISP)
LAN (IP: 192.168.2.x)
Notebook PC (IP: 192.168.2.x)
LAN Switch
Server (IP: 192.168.2.x)
Desktop PC (IP: 192.168.2.x)

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), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and static IP for connection to an Internet service provider (ISP) through a cable or DSL modem.

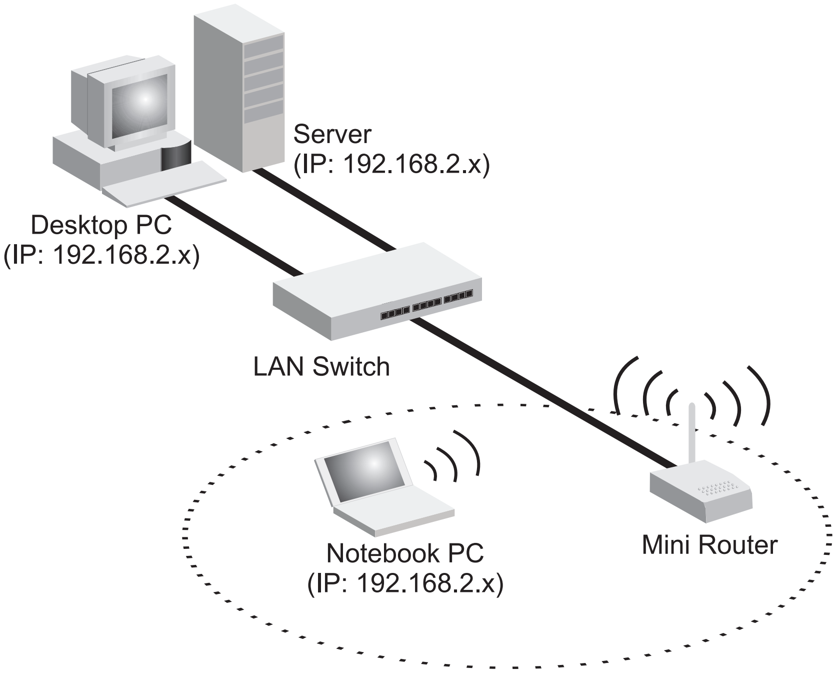
The 3G Modem link can provide a backup Internet connection with automatic failover and fallback to the primary WAN connection.

LAN ACCESS POINT

The Gateway can provide an access point service for an existing wired LAN, creating a wireless extension to the local network. The Gateway 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 6: 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 Gateway can use WDS to forward traffic on links between units.

Up to four WDS links can be specified for the Gateway.

The WDS feature enables two basic functions to be configured in the wireless network. Either a repeater function that extends the range of the wireless network, or a bridge function that connects a remote LAN segment to an Internet connection.

Figure 7: Operating as a Wireless Bridge

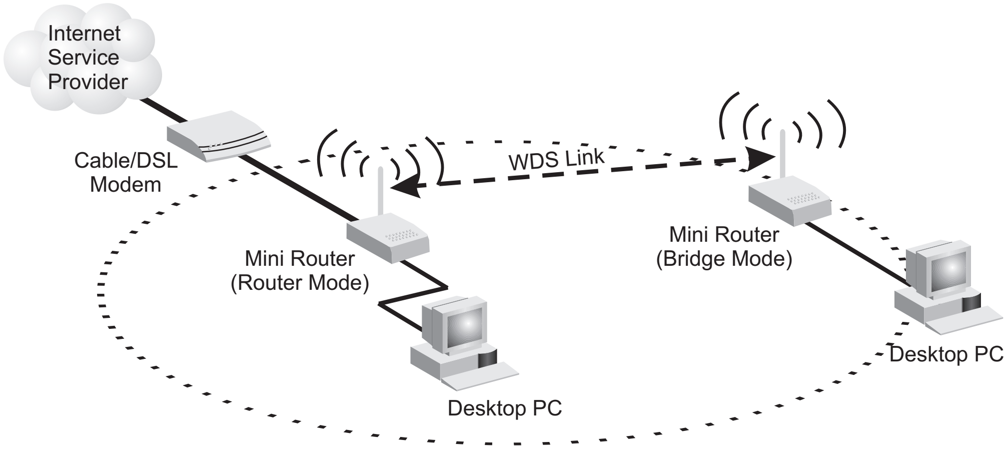
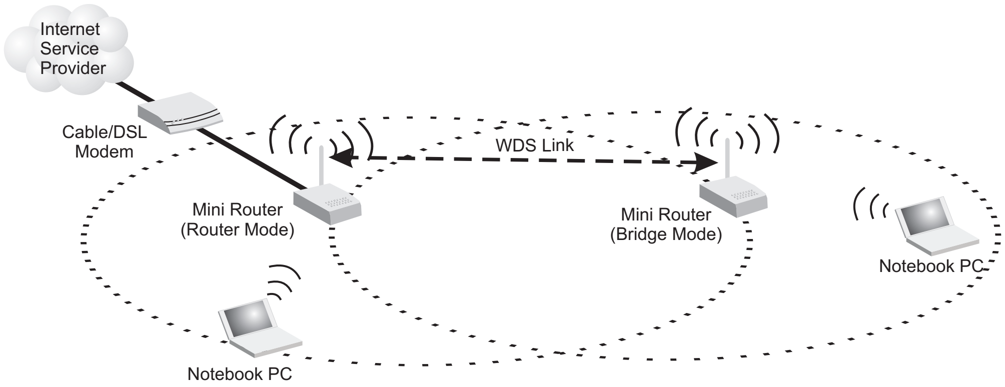

Internet Service Provider
Cable/DSL Modem
WDS Link
Mini Router (Router Mode)
Mini Router (Bridge Mode)
Desktop PC
Desktop PC

Figure 8: Operating as a Wireless Repeater


Internet Service Provider
Cable/DSL Modem
WDS Link
Mini Router (Router Mode)
Mini Router (Bridge Mode)
Notebook PC
Notebook PC

3 INSTALLING THE MINI 3G ROUTER

The Gateway 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 50.

- Router 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 wireless clients.

In addition to these basic operating modes, the wireless interface supports Wireless Distribution System (WDS) links to other Gateways. These advanced configurations are not described in this section. See "Network Planning" on page 23 for more information.

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

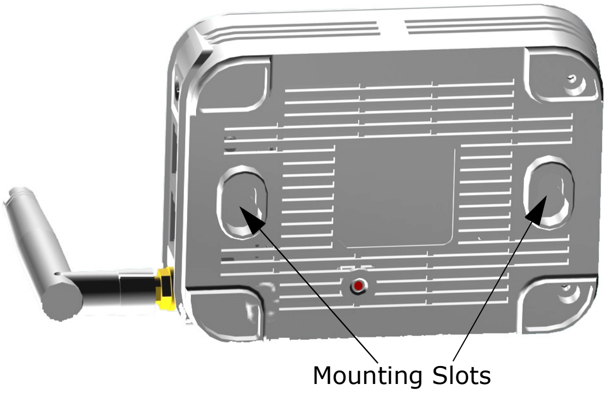
MOUNTING THE DEVICE

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

MOUNTING ON A WALL

The Gateway 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 slots.

Figure 9: 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 two 20-mm M4 tap screws (not included) into the holes, leaving about 2~3 mm (0.08~0.12 inches) 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

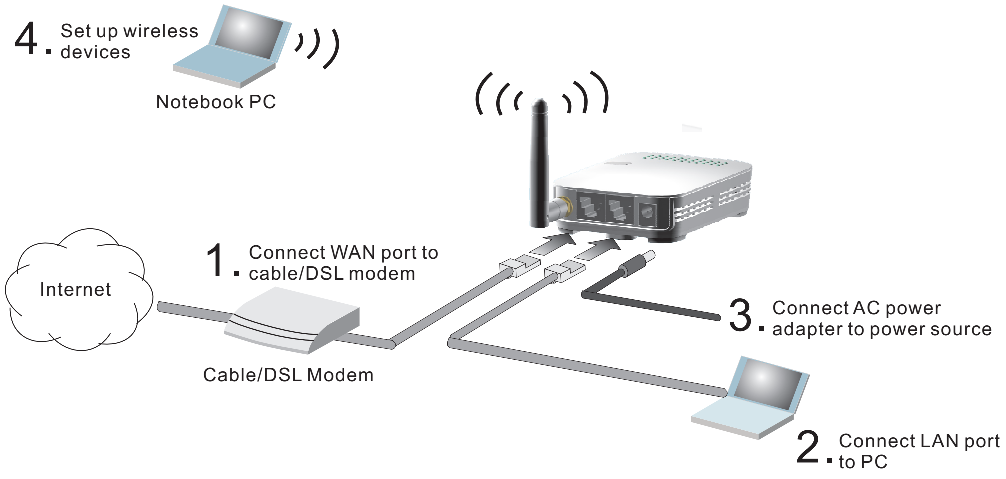
To keep the Gateway from sliding on the surface, the unit has four rubber feet on its base.

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.

ROUTER MODE CONNECTIONS

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

Figure 10: Router Mode Connection


4. Set up wireless devices
Notebook PC
Internet
1. Connect WAN port to cable/DSL modem
Cable/DSL Modem
3. Connect AC power adapter to power source
2. Connect LAN port to PC

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

1. Connect an Ethernet cable from the Gateway's WAN port to your Internet connected cable or DSL modem.

2. Connect an Ethernet cable from the Gateway's LAN port to your PC. Alternatively, you can connect to a workgroup switch to support more wired users. The Gateway can support up to 253 wired and wireless users.

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

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

When you power on the Gateway, verify that the Power LED turns on and that the other LED indicators start functioning as described under see "LED Indicators" on page 21.

4. Set up wireless devices by pressing the WPS button on the Gateway or by using the web interface. See "Initial Configuration" on page 31 for more information on accessing the web interface.

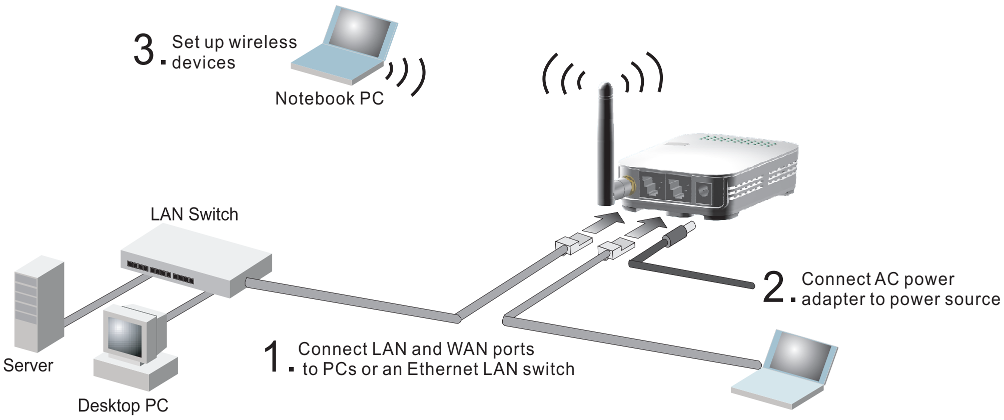
BRIDGE MODE CONNECTIONS

In Bridge Mode, the Gateway 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 Gateway and access the wired network resources, including local servers and the Internet.

In Bridge Mode, the Gateway 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 11: Bridge Mode Connection


3. Set up wireless devices
Notebook PC
LAN Switch
2. Connect AC power adapter to power source
Server
Desktop PC
1. Connect LAN and WAN ports to PCs or an Ethernet LAN switch

To connect the Gateway for use as an access point, follow these steps:

1. Using Ethernet cable connect the Gateway’s LAN and WAN ports to PCs. Alternatively, you can connect to a workgroup switch to support more wired users.

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

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

When you power on the Gateway, verify that the Power LED turns on and that the other LED indicators start functioning as described under “LED Indicators” on page 21.

3. Set up wireless devices by pressing the WPS button on the Gateway or by using the web interface. See “Initial Configuration” on page 31 for more information on accessing the web interface.

4 Initial Configuration

The Gateway 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), PPTP, L2TP and 3G.

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 the Gateway's LAN port. The Gateway 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 (that is, the PC and Gateway addresses must both start 192.168.2.x).

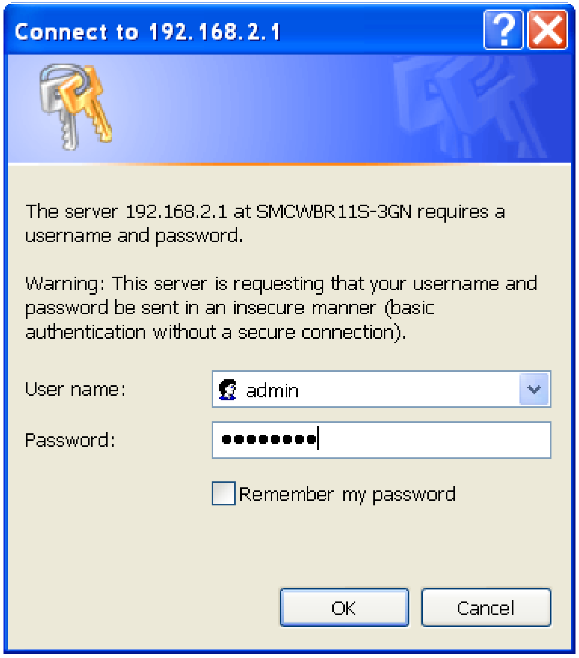
To access the Gateway's management interface, follow these steps:

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 OK.

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 102.

Figure 12: Login Page



Connect to 192.168.2.1

The server 192.168.2.1 at SMCWBR11S-3GN requires a username and password.

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

User name: admin

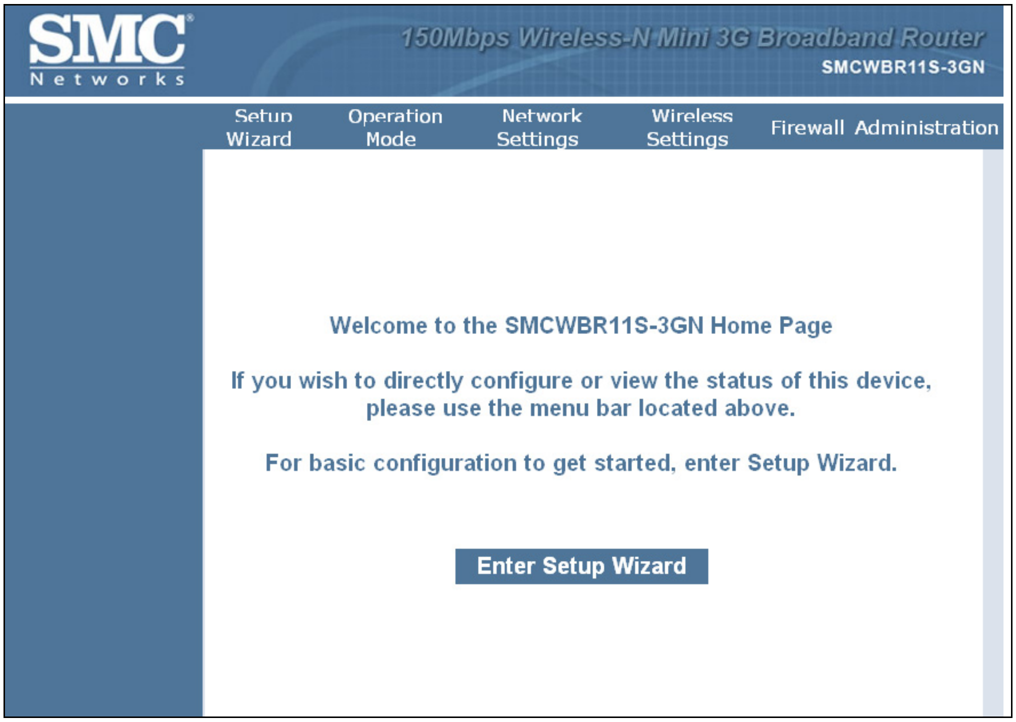
Password: ●●●●●●●●●

□ Remember my password

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 13: Home Page



Welcome to the SMCWBR11S-3GN Home Page

If you wish to directly configure or view the status of this device, please use the menu bar located above.

For basic configuration to get started, enter Setup Wizard.

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.
- **Previous** – Returns to the previous screen.

SETUP WIZARD

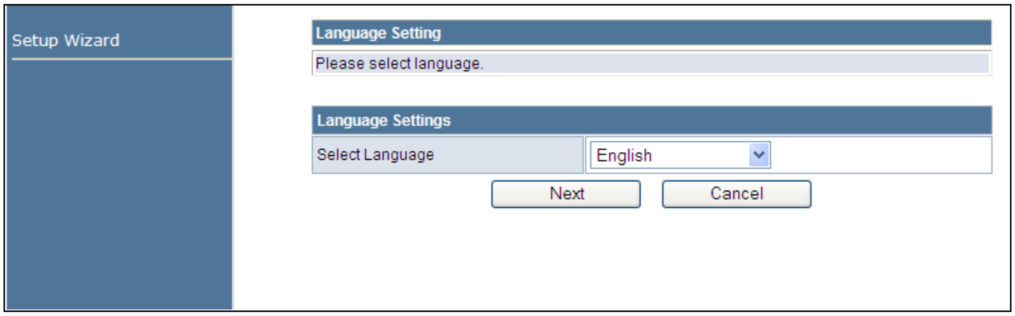
The Wizard is designed to help you configure the basic settings required to get the the Gateway up and running. There are only a few basic steps you need to set up the the Gateway and provide a connection.

Follow these steps:

STEP 1 - LANGUAGE SELECTION

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

Figure 14: Wizard Step 1 - Language Selection



Language Setting

Please select language.

Language Settings

Select Language: English

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

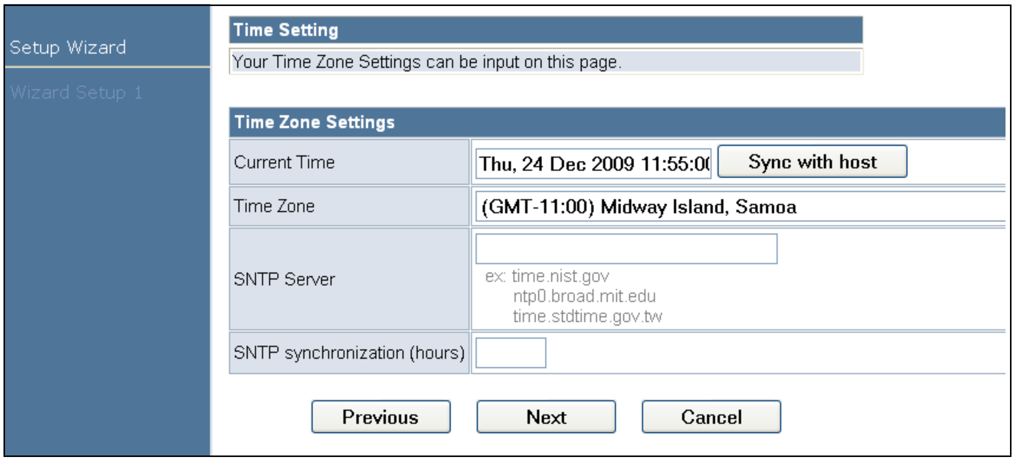
- **Select Language** — Selects English or Traditional Chinese as the interface language.

STEP 2 - TIME 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 15: Wizard Step 2 - Time and SNTP Settings



Time Setting

Your Time Zone Settings can be input on this page.

Time Zone Settings

Current Time	Thu, 24 Dec 2009 11:55:0(
Time Zone	(GMT-11:00) Midway Island, Samoa
SNTP Server	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
SNTP synchronization (hours)	

The following items are displayed on this page:

- **Current Time** — Receives a time and date stamp from an SNTP server.
- **Sync with host —** Updates the unit's time from the web management PC's system time.
- **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.

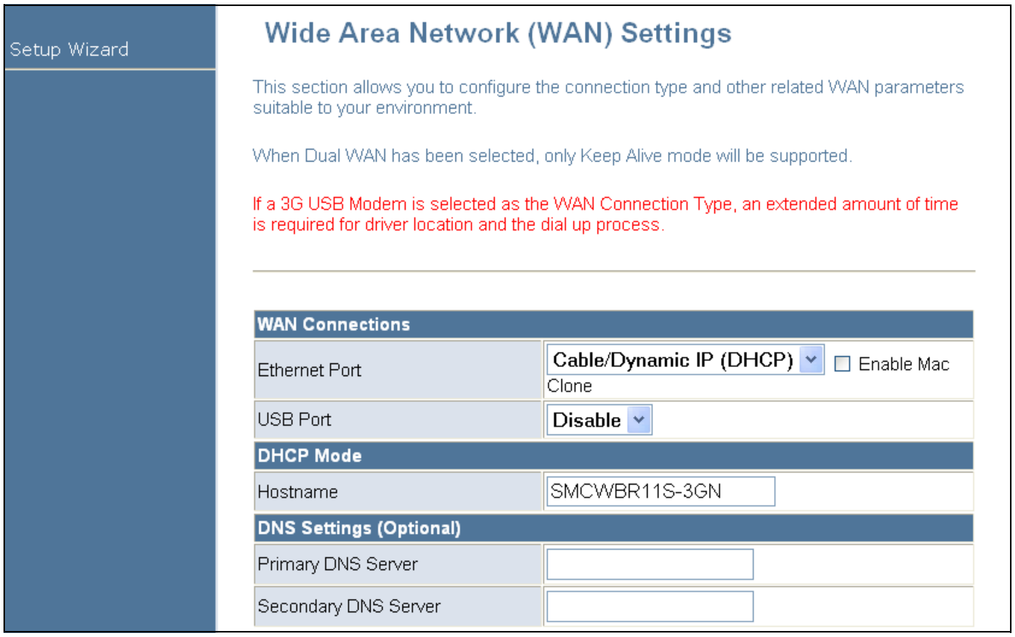
STEP 3 - WAN SETTINGS - DHCP

The Step 3 page of the Wizard specifies the Internet connection parameters for the Gateway’s WAN port. Click Next after completing the setup.

By default, the WAN port is configured with DHCP enabled. The options are Static IP, DHCP (cable modem), PPPoE (DSL modem), PPTP, and L2TP. Each option changes the parameters that are displayed on the page.

You can also enable support for a USB 3G modem as a WAN connection, either as a primary (Master) link, or as a backup to the WAN port link.

Figure 16: Wizard Step 3 - WAN Settings - DHCP



Wide Area Network (WAN) Settings

This section allows you to configure the connection type and other related WAN parameters suitable to your environment.

When Dual WAN has been selected, only Keep Alive mode will be supported.

If a 3G USB Modem is selected as the WAN Connection Type, an extended amount of time is required for driver location and the dial up process.

WAN Connections	
Ethernet Port	Cable/Dynamic IP (DHCP) ▾ □ Enable Mac Clone
USB Port	Disable ▾
DHCP Mode	
Hostname	SMCWBR11S-3GN
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **Ethernet Port** — Select "Cable/Dynamic IP (DHCP)" for the WAN port connection from the drop-down list. (Default: DHCP)
  - **Enable 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 Gateway's WAN port to match the PC MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the box provided. Otherwise, connect only the PC with the registered MAC address to the Gateway, 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 MAC address of the Gateway.

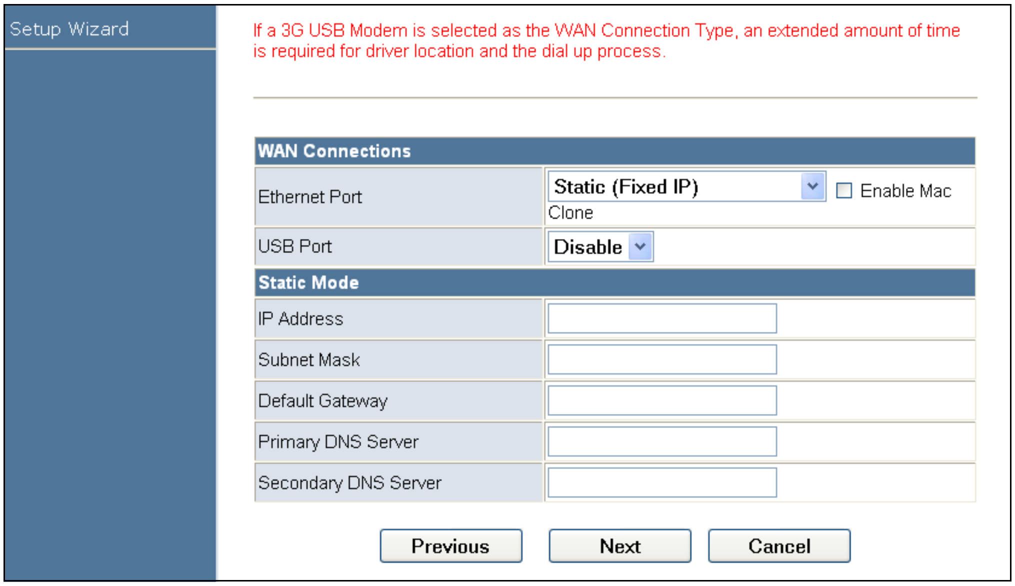
- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see "Step 3 - WAN Settings - 3G" on page 42. (Default: Disabled)
- **Hostname** — Specifies the host name of the DHCP client. (Default: SMCWBR11S-3GN)
- **Primary DNS Server** — The IP address of the Primary 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.

STEP 3 - WAN SETTINGS - STATIC IP

Configures a static IP for the WAN port.

Figure 17: Wizard Step 3 - WAN Settings - Static IP



If a 3G USB Modem is selected as the WAN Connection Type, an extended amount of time is required for driver location and the dial up process.

WAN Connections	
Ethernet Port	Static (Fixed IP) ☐ Enable Mac Clone
USB Port	Disable
Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **Ethernet Port** — Select "Static (Fixed IP)" for the WAN port connection from the drop-down list.
  - **Enable MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Gateway'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 Gateway, then click the "Clone your PC's MAC Address." (Default: Disable)
- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see "Step 3 - WAN Settings - 3G" on page 42. (Default: Disabled)
- **IP Address** — The IP address of the Gateway. 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 Gateway, which is used if the requested destination address is not on the local subnet.

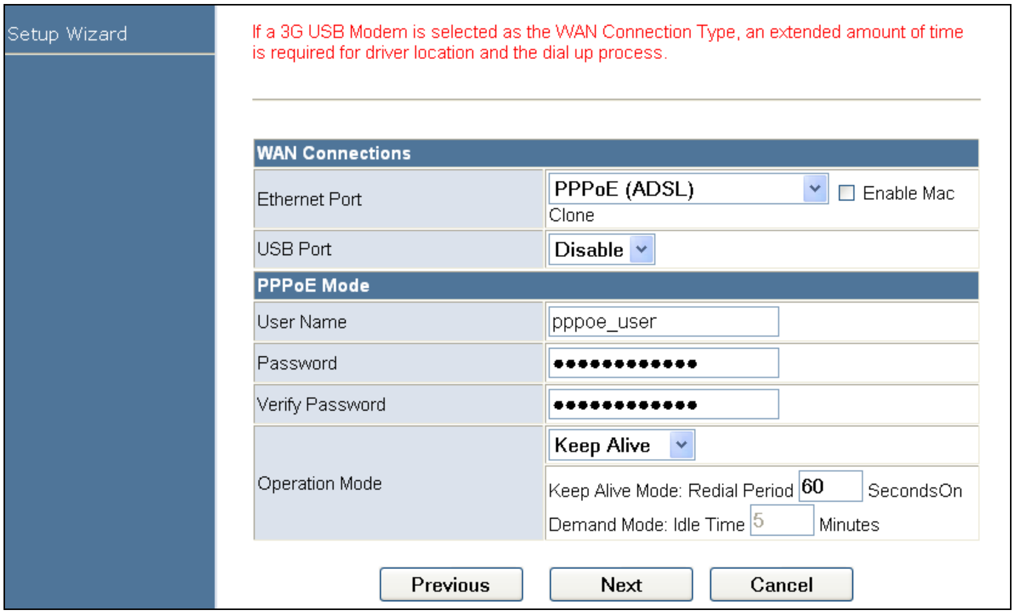
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

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

STEP 3 - WAN SETTINGS - PPPOE

Enable the Gateway IP address to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).

Figure 18: Wizard Step 3 - WAN Settings - PPPoE



If a 3G USB Modem is selected as the WAN Connection Type, an extended amount of time is required for driver location and the dial up process.

WAN Connections	
Ethernet Port	PPPoE (ADSL) □ Enable Mac Clone
USB Port	Disable
PPPoE Mode	
User Name	pppoe_user
Password	●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 SecondsOn Demand Mode: Idle Time 5 Minutes

The following items are displayed on this page:

- **Ethernet Port** — Select "PPPoE (ADSL)" for the WAN port connection from the drop-down list.
  - **Enable MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Gateway'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 Gateway, then click the "Clone your PC's MAC Address." (Default: Disable)

- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see "Step 3 - WAN Settings - 3G" on page 42. (Default: Disabled)

- **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)

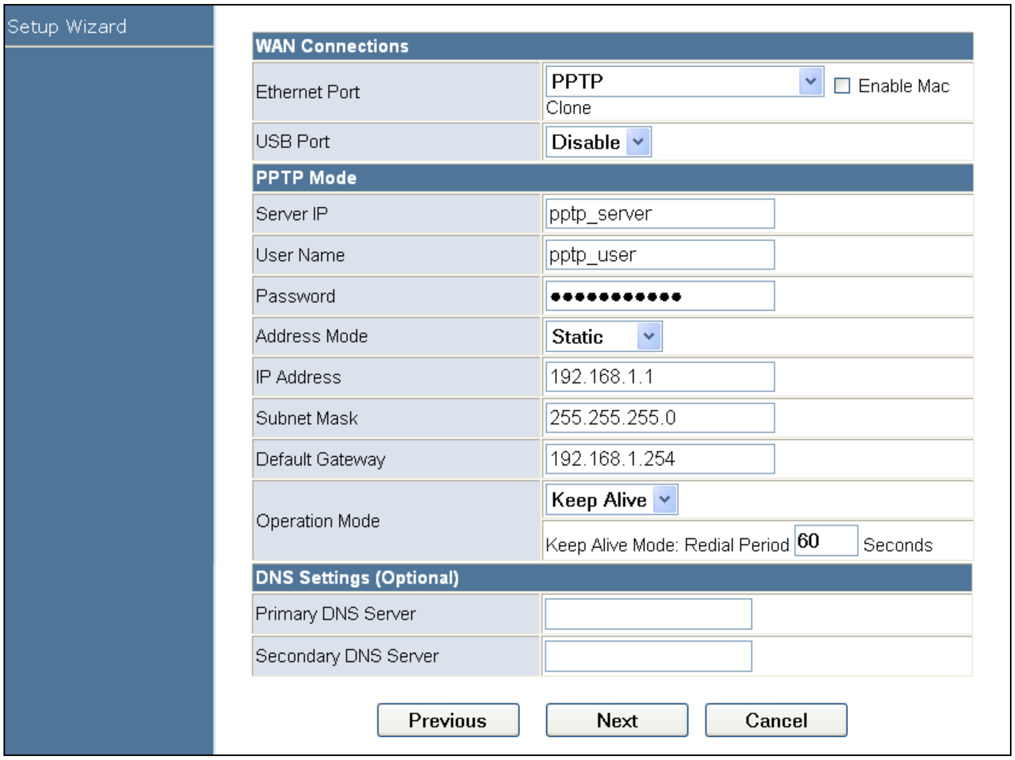
- **Verify Password** — Prompts you to re-enter your chosen password.

- **Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.

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 19: Wizard Step 3 - WAN Settings - PPTP



Setup Wizard

WAN Connections	
Ethernet Port	PPTP ☐ Enable Mac Clone
USB Port	Disable
PPTP Mode	
Server IP	pptp_server
User Name	pptp_user
Password	●●●●●●●●●●●
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 Seconds
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **Ethernet Port** — Select "PPTP" for the WAN port connection from the drop-down list.

  - **Enable MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Gateway'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 Gateway, then click the “Clone your PC’s MAC Address.” (Default: Disable)

- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see “Step 3 - WAN Settings - 3G” on page 42. (Default: Disabled)

- **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.

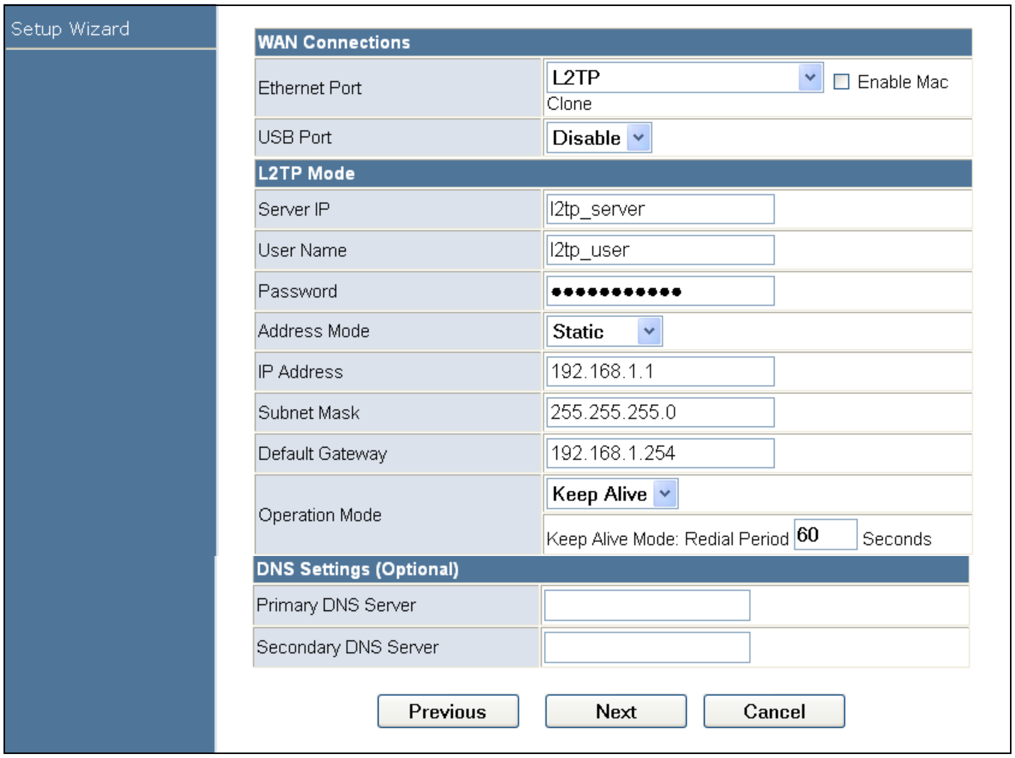
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

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

STEP 3 - WAN SETTINGS - L2TP

Enables the Layer 2 Tunneling Protocol (L2TP) for implementing virtual private networks. The service is provided in many European countries.

Figure 20: Wizard Step 3 - WAN Settings - L2TP



WAN Connections	
Ethernet Port	L2TP ☐ Enable Mac Clone
USB Port	Disable
L2TP Mode	
Server IP	l2tp_server
User Name	l2tp_user
Password	●●●●●●●●●●●●
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 Seconds
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

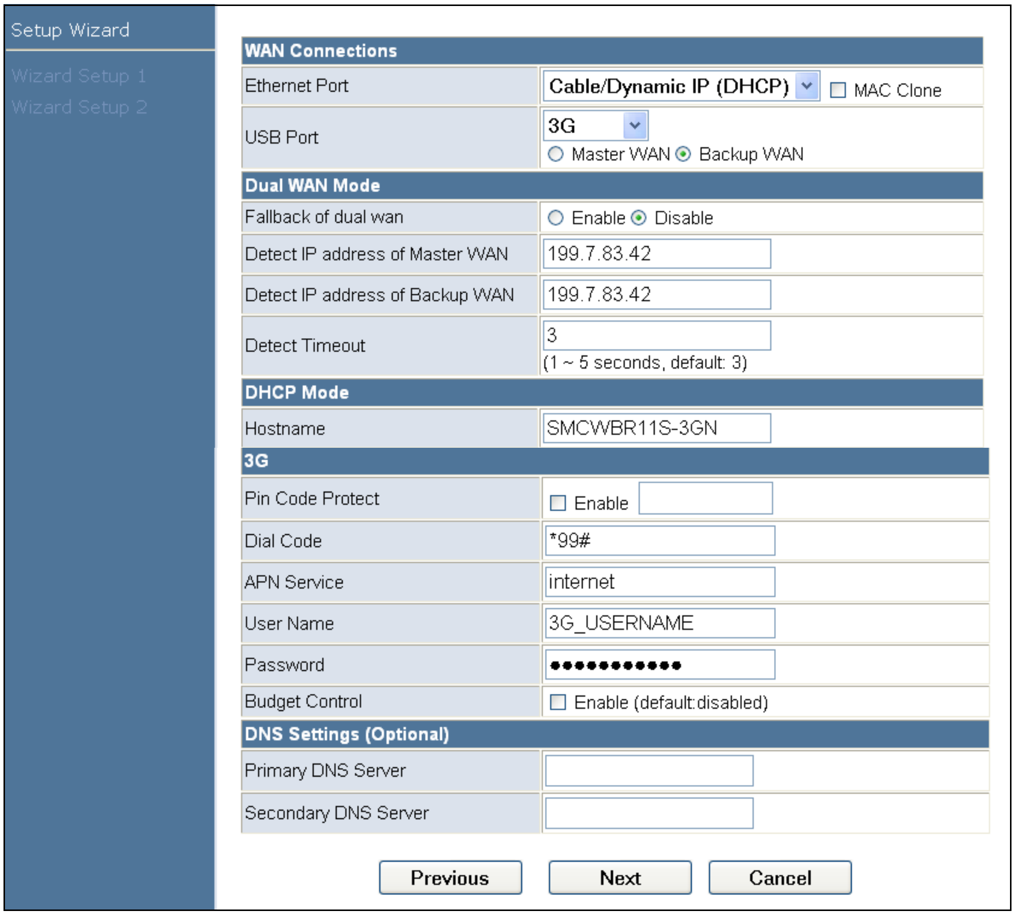
- **Ethernet Port** — Select “L2TP” for the WAN port connection from the drop-down list.
  - **Enable MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Gateway’s WAN interface to match the PC's MAC address 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 Gateway, then click the “Clone your PC’s MAC Address.” (Default: Disable)
- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see “Step 3 - WAN Settings - 3G” on page 42. (Default: Disabled)
- **Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)
- **User Name** — Sets the L2TP user name for the WAN port. (Default: l2tp_user; Range: 1~32 characters)
- **Password** — Sets a L2TP password for the WAN port. (Default: l2tp_password; Range: 1~32 characters)

- **Verify Password** — Prompts you to re-enter your chosen password.
- **Address Mode** — Sets a L2TP network mode. (Default: Static)
- **IP Address** — Sets the static IP address. (Default: 0.0.0.0, available when L2TP Network Mode is set to static IP.)
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0, available when L2TP 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.
- **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.

STEP 3 - WAN SETTINGS - 3G

Enables support for a USB 3G modem as a WAN connection, either as a primary (Master) link, or as a backup to the WAN port link.

Figure 21: Wizard Step 3 - WAN Settings - 3G



WAN Connections	
Ethernet Port	Cable/Dynamic IP (DHCP) □ MAC Clone
USB Port	3G ○ Master WAN ● Backup WAN
Dual WAN Mode	
Fallback of dual wan	○ Enable ● Disable
Detect IP address of Master WAN	199.7.83.42
Detect IP address of Backup WAN	199.7.83.42
Detect Timeout	3 (1 ~ 5 seconds, default: 3)
DHCP Mode	
Hostname	SMCWBR11S-3GN
3G	
Pin Code Protect	□ Enable
Dial Code	*99#
APN Service	internet
User Name	3G_USERNAME
Password	●●●●●●●●●●●
Budget Control	□ Enable (default:disabled)
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **Ethernet Port** — Select the WAN port connection type from the drop-down list. Alternatively, you can disable the Ethernet WAN port connection and just use the USB 3G modem connection.
  - **Enable MAC Clone** — Some ISPs limit Internet connections to a specified MAC address. This setting allows you to manually change the MAC address of the Gateway'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 Gateway, then click the "Clone your PC's MAC Address." (Default: Disable)

- **USB Port** — Enables support for a WAN connection using a USB 3G modem. When enabled, you can select if the 3G modem connection operates as the Master or Backup WAN link. (Default: Disabled)

  - **Master WAN** — Enables the USB 3G modem WAN connection to operate as the primary WAN link. The Ethernet WAN port then operates as the backup link. (Default: Disabled)

  - **Backup WAN** — Enables the USB 3G modem WAN connection to operate as the backup to the Ethernet WAN port link. (Default: Enabled)

- **Dual WAN Mode** — When both the WAN port and 3G modem connections are enabled, you can configure the following parameters:

  - **Fallback of Dual WAN** — The operation of the fallback between dual WAN connections is as follows: (Default: Disabled)

    - **Enable** — The Master WAN connection is used first. Whenever this connection is lost, the device automatically switches to the Backup WAN. During the operation of the Backup WAN, the Master WAN link is monitored for recovery of the lost connection. If the Master WAN link is re-established, the WAN connection automatically switches back to the Master from the Backup WAN connection.

    - **Disable** — The Master WAN connection is used first. Whenever this connection is lost, the device automatically switches to the Backup WAN. The device will only switch back to the Master WAN if the Backup connection is lost.

  - **Detect IP Address of Master WAN** — An IP address to which a ping packet is sent to detect if the Master WAN connection is valid.

  - **Detect IP Address of Backup WAN** — An IP address to which a ping packet is sent to detect if the Backup WAN connection is valid.

  - **Detect Timeout** — Sets the ping time out. (Range: 1~5 seconds; Default: 3 seconds)

- **Pin Code Protect** — Enables the use of a PIN code (personal identification number) to encrypt access to the 3G modem connection. Some service providers do not require PIN code authentication. If a PIN code is not required for your 3G or 3.5G modem, disable this function. (Default: Disabled)

- **Dial Code** — A dialled access code that connects the USB device to the service provider.

- **APN Service** — The access point name (APN) that uniquely identifies the 3G or 3.5G service provider.

- **User Name** — The user name of the account registered with the 3G or 3.5G service provider.

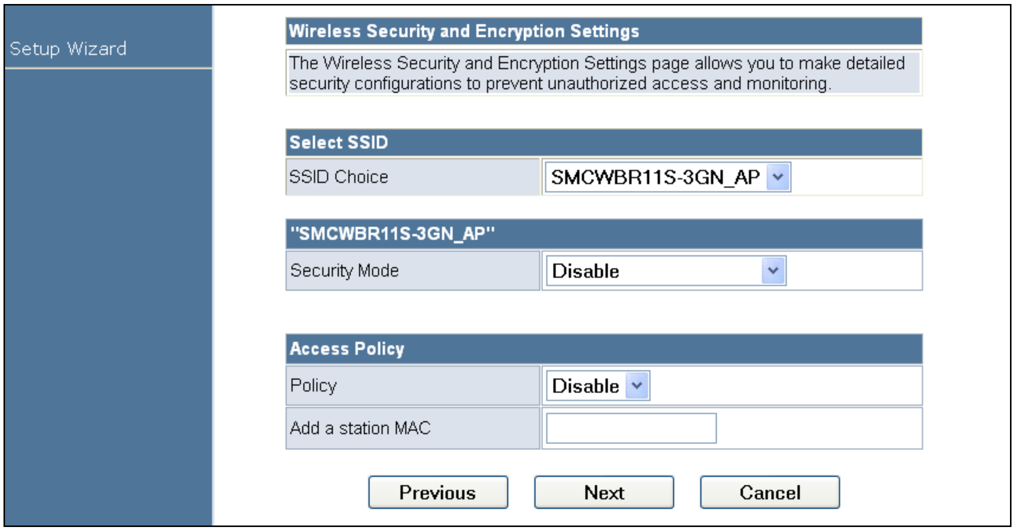
- **Password** — The password of the account registered with the 3G or 3.5G service provider.

- **Budget Control** — Enables a monthly limit on time or total data. For more information, see "3G" on page 59. (Default: Disabled)

STEP 4 - WIRELESS SECURITY

The Step 4 page of the Wizard configures the wireless network name and security options.

Figure 22: Wizard Step 4 - Wireless Security



Wireless Security and Encryption Settings

The Wireless Security and Encryption Settings page allows you to make detailed security configurations to prevent unauthorized access and monitoring.

Select SSID

SSID Choice: SMCWBR11S-3GN_AP

"SMCWBR11S-3GN_AP"

Security Mode: Disable

Access Policy

Policy: Disable

Add a station MAC:

The following items are displayed on this page:

- **SSID Choice** — The name of the wireless network service provided by the Gateway. Clients that want to connect to the network must set their SSID to the same as that of the Gateway. (Default: "SMCWBR11S-3GN_AP")

- **Security Mode** — Specifies the security mode for the SSID. Select the security method and then configure the required parameters. For more information, see "WLAN Security" on page 79. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK, WPA, WPA2, WPA1_WPA2, 802.1X; Default: Disabled)

NOTE: To keep your wireless network protected and secure, you should implement the highest security possible. For small networks, it is recommended to select WPA2-PSK using AES encryption as the most secure option. However, if you have older wireless devices in the network that do not support AES encryption, select TKIP as the encryption algorithm.

- **Access Policy** — The Gateway provides a MAC address filtering facility. The access policy can be set to allow or reject specific station MAC addresses. This feature can be used to connect known wireless devices that may not be able to support the configured security mode.

- **Add a station MAC —** Enter the MAC address of the station that you want to filter. MAC addresses must be entered 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 Gateway using the web browser interface.

This section includes these chapters:

5 Operation Mode

The Gateway 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

It is recommended to make initial configuration changes by connecting a PC directly to the Gateway's LAN port. The Gateway 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 Gateway (that is, the PC and Gateway addresses must both start 192.168.2.x).

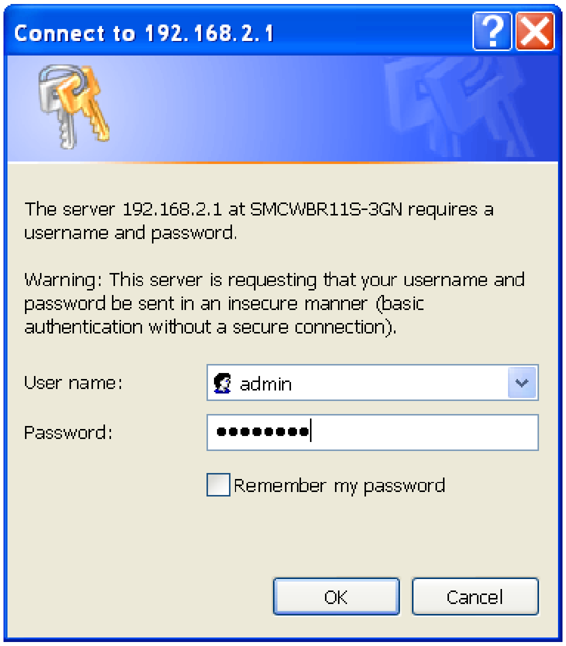
To access the configuration menu, follow these steps:

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 Gateway management interface by entering the default user name "admin" and password "smcadmin," then click OK.

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 101.

Figure 23: Logging On



Connect to 192.168.2.1

The server 192.168.2.1 at SMCWBR11S-3GN requires a username and password.

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

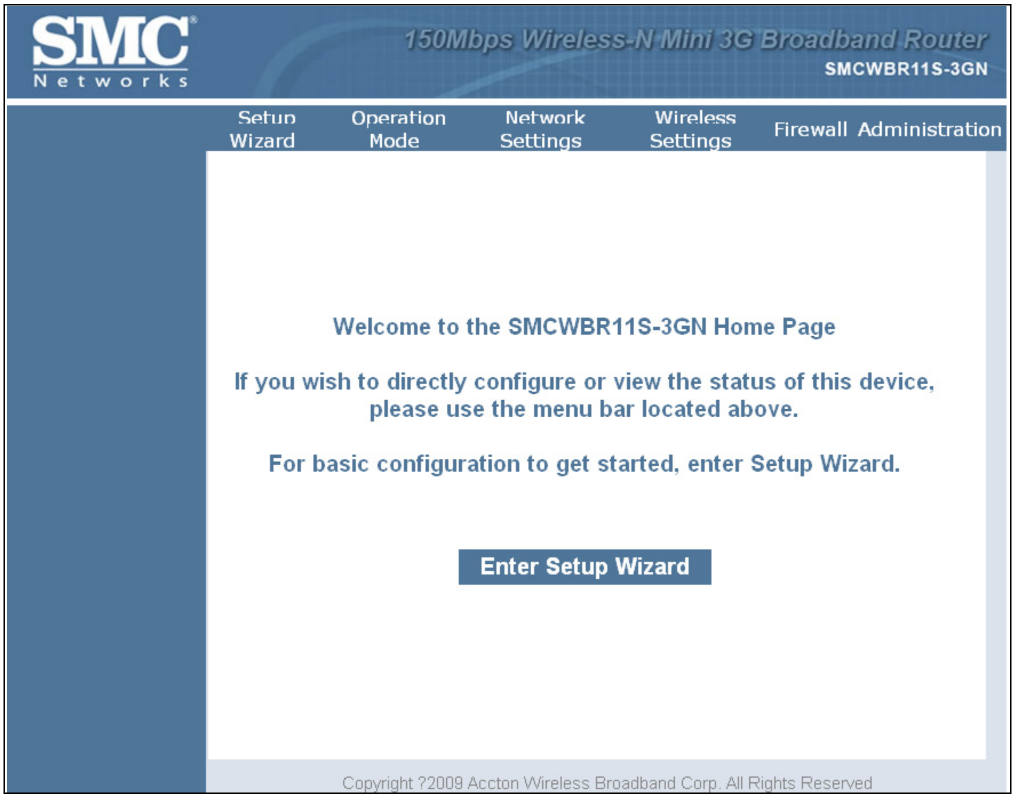
User name: admin

Password: •••••••••

□ Remember my password

The home page displays the main menu items at the top of the screen and the Setup Wizard. See "Setup Wizard" on page 33.

Figure 24: Home Page



Welcome to the SMCWBR11S-3GN Home Page

If you wish to directly configure or view the status of this device, please use the menu bar located above.

For basic configuration to get started, enter Setup Wizard.

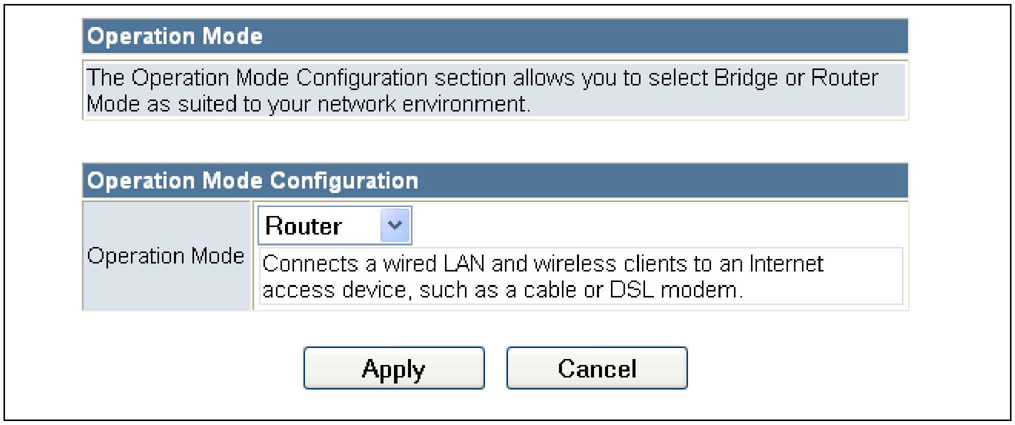
Copyright ?2009 Accton Wireless Broadband Corp. All Rights Reserved

NOTE: The displayed pages and settings may differ depending on whether the unit is in Router or Bridge Mode. See "Operation Mode" on page 50.

OPERATION MODE

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

Figure 25: Operation Mode



Operation Mode

The Operation Mode Configuration section allows you to select Bridge or Router Mode as suited to your network environment.

Operation Mode Configuration

Operation Mode: Router

Connects a wired LAN and wireless clients to an Internet access device, such as a cable or DSL modem.

The following items are displayed on this page:

- **Bridge Mode** — An access point mode that extends a wired LAN to wireless clients.
- **Router Mode** — The Internet 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 Network Settings

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

Note: In Bridge mode, the Gateway's Network 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 "Network Settings" followed by "WAN".

By default, the WAN port is configured with DHCP enabled. The options are Static IP, DHCP (cable modem), PPPoE (DSL modem), PPTP, and L2TP. You can also enable support for a USB 3G modem as a WAN connection, either as a primary (Master) link, or as a backup to the WAN port link. Each option selected changes the parameters that are displayed on the page.

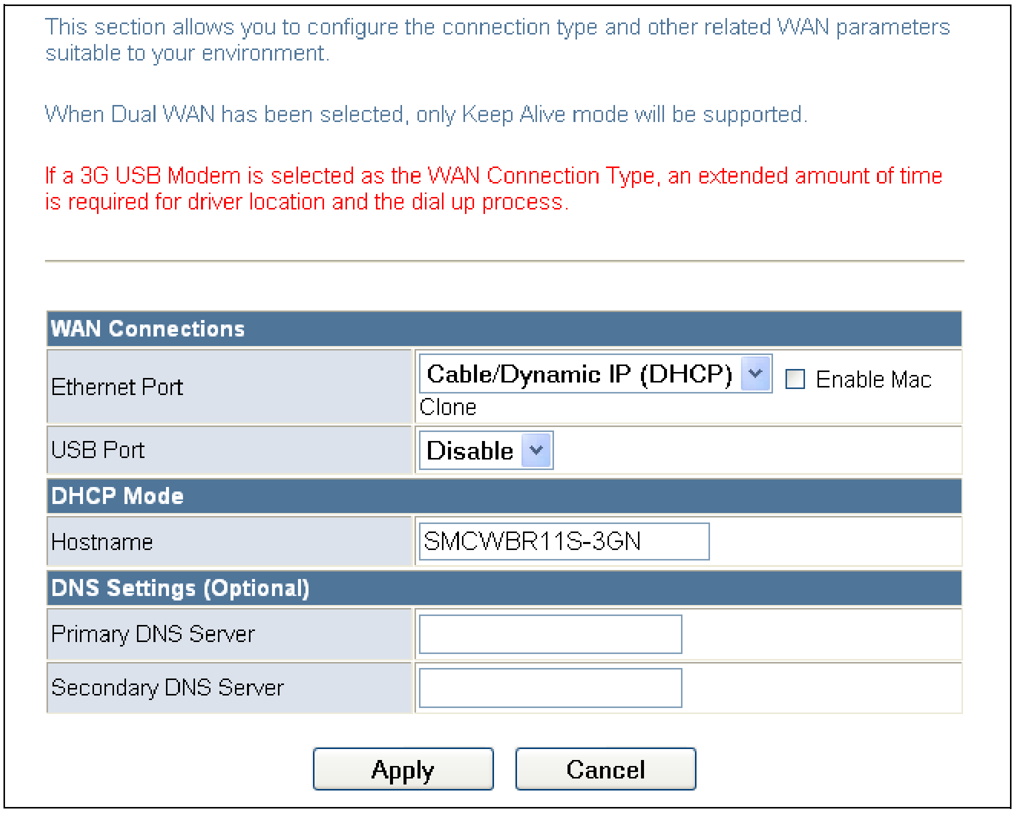
- **Ethernet Port** — Select the connection type for the WAN port from the drop-down list. (Default: DHCP).
  - **Cable/Dynamic IP (DHCP)** — See "DHCP" on page 53.
  - **Static (Fixed IP)** — See "Static IP" on page 54.
  - **PPPoE (ADSL)** — See "PPPoE" on page 55.
  - **PPTP** — See "PPTP" on page 56.
  - **L2TP** — See "L2TP" on page 58.
  - **Disable** — Disables a WAN connection on the WAN port. A single WAN connection can still be provided using the 3G USB port (see "3G" on page 59).
  - **Enable 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 Gateway's WAN port to match the PC MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the box provided. Otherwise, connect only the PC with the registered MAC address to the Gateway, 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 MAC address of the Gateway.

- **USB Port** — Enables support for a WAN connection using a USB 3G modem. For more information, see "3G" on page 59. (Default: Disabled)

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

Figure 26: DHCP Configuration



This section allows you to configure the connection type and other related WAN parameters suitable to your environment.

When Dual WAN has been selected, only Keep Alive mode will be supported.

If a 3G USB Modem is selected as the WAN Connection Type, an extended amount of time is required for driver location and the dial up process.

WAN Connections	
Ethernet Port	Cable/Dynamic IP (DHCP) □ Enable Mac Clone
USB Port	Disable
DHCP Mode	
Hostname	SMCWBR11S-3GN
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

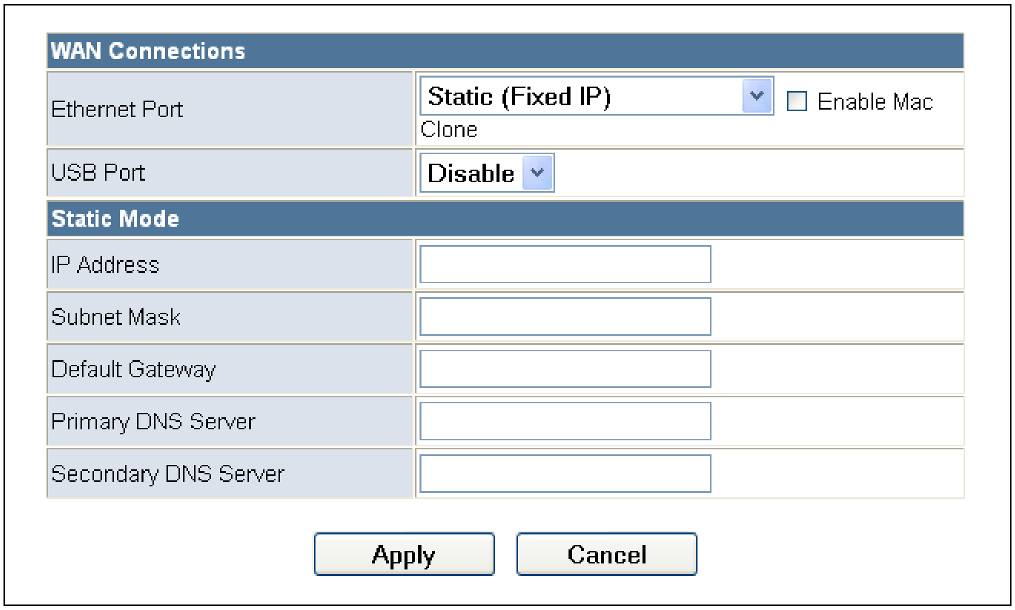
The following items are displayed on this page:

- **Hostname** (Optional) — The hostname of the DHCP client.
- **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.

STATIC IP

Configures a static IP for the WAN port.

Figure 27: Static IP Configuration



WAN Connections	
Ethernet Port	Static (Fixed IP) ☐ Enable Mac Clone
USB Port	Disable

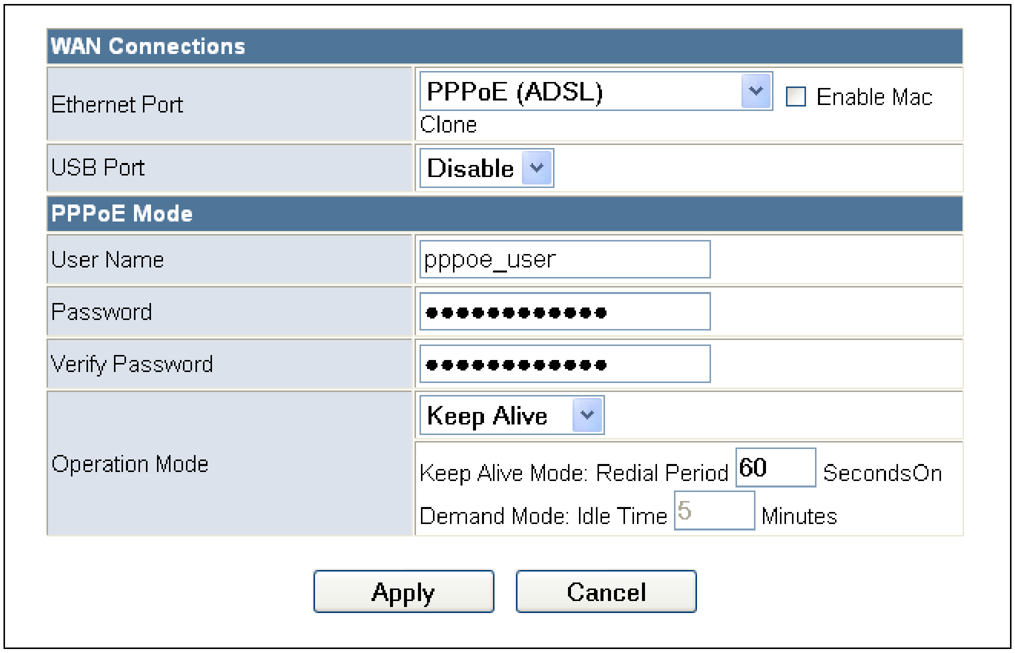
Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **IP Address** — The IP address of the Gateway. 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 Gateway, 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.

PPPoE Enables the Gateway IP address to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).

Figure 28: PPPoE Configuration



WAN Connections	
Ethernet Port	PPPoE (ADSL) ▾ □ Enable Mac Clone
USB Port	Disable ▾
PPPoE Mode	
User Name	pppoe_user
Password	••••••••••••
Verify Password	••••••••••••
Operation Mode	Keep Alive ▾ Keep Alive Mode: Redial Period 60 SecondsOn Demand Mode: Idle Time 5 Minutes

The following items are displayed on this page:

- **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.

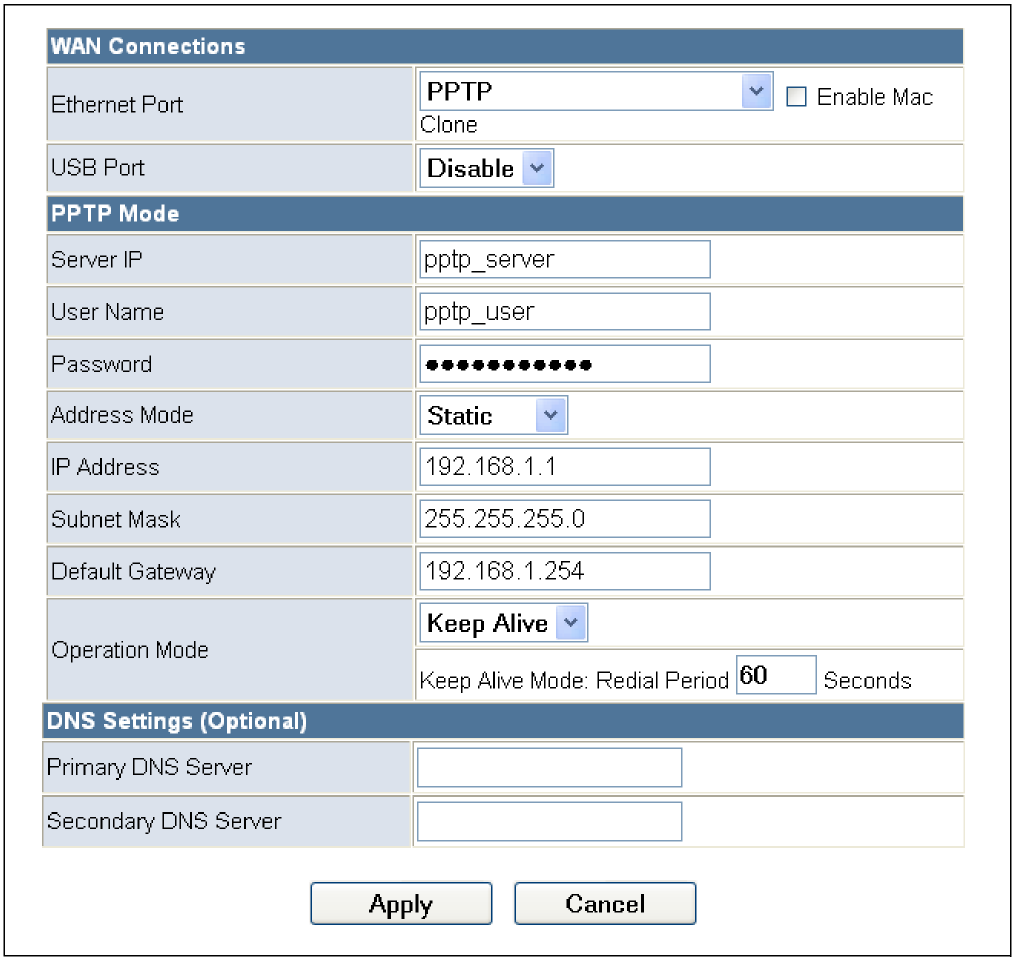
- **Operation Mode** — Selects the operation mode as Keep Alive, On Demand or Manual. (Default: Keep Alive)

  - **Keep Alive Mode**: The Gateway 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)

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

Figure 29: PPTP Configuration



WAN Connections	
Ethernet Port	PPTP ☐ Enable Mac Clone
USB Port	Disable
PPTP Mode	
Server IP	pptp_server
User Name	pptp_user
Password	●●●●●●●●●●●
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 Seconds
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **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 Gateway, 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 Gateway will periodically check your Internet connection and automatically re-establish your connection when disconnected. (Default: 60 seconds)

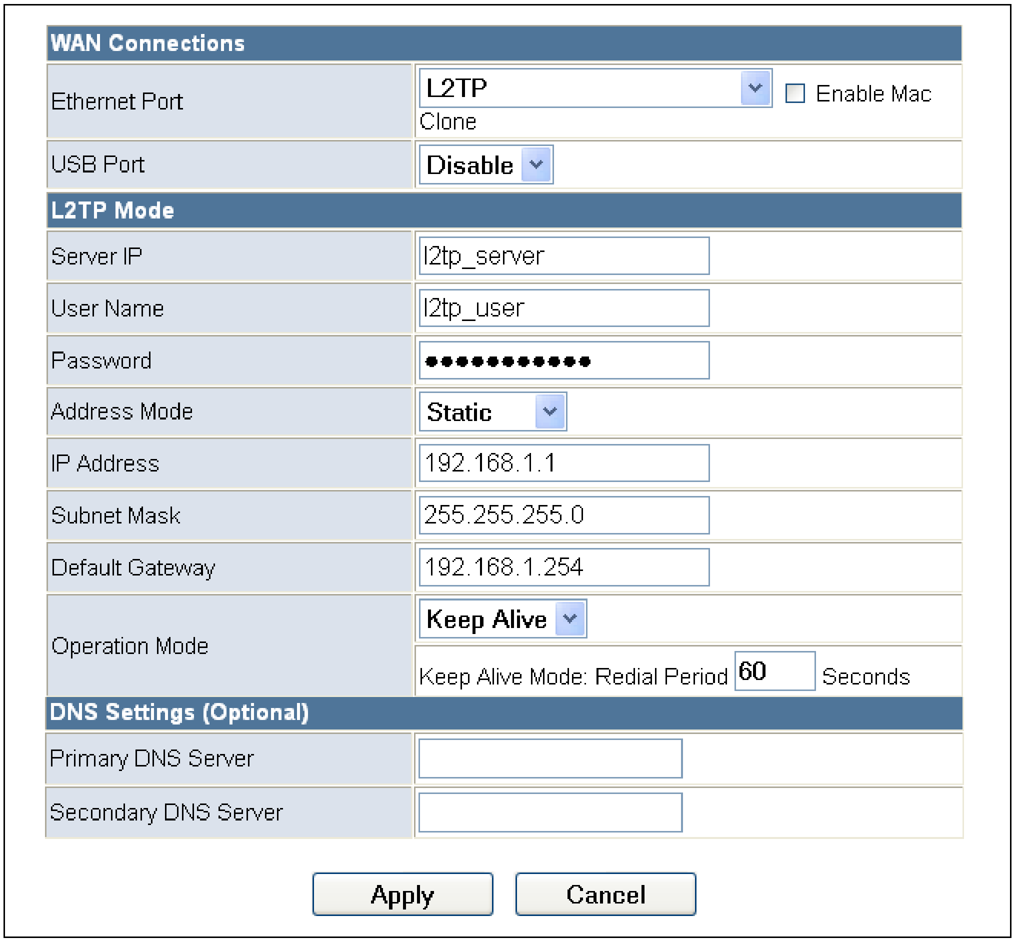
  - **Manual Mode**: The unit will remain connected to the Internet without disconnecting.

- **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.

L2TP Enables the Layer 2 Tunneling Protocol (L2TP) for implementing virtual private networks. The service is provided in many European countries.

Figure 30: L2TP Configuration



WAN Connections	
Ethernet Port	L2TP ☐ Enable Mac Clone
USB Port	Disable
L2TP Mode	
Server IP	l2tp_server
User Name	l2tp_user
Password	●●●●●●●●●●●
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 Seconds
DNS Settings (Optional)	
Primary DNS Server	
Secondary DNS Server	

The following items are displayed on this page:

- **Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)
- **User Name** — Sets the L2TP user name for the WAN port. (Default: l2tp_user; Range: 1~32 characters)
- **Password** — Sets a L2TP password for the WAN port. (Default: l2tp_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Address Mode** — Sets a L2TP network mode. (Default: Static)
- **IP Address** — Sets the static IP address. (Default: 0.0.0.0, available when L2TP Network Mode is set to static IP.)
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0, available when L2TP Network Mode is set to static IP.)

- **Default Gateway** — The IP address of the gateway router for the Gateway, 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 Gateway 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.

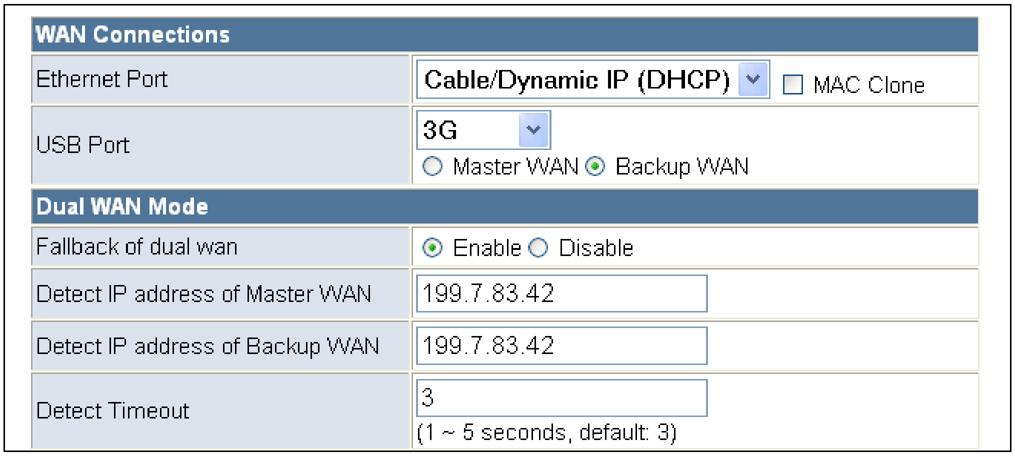
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.

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

3G

Enables support for a USB 3G modem as a WAN connection, either as a primary (Master) link, or as a backup to the WAN port link.

Figure 31: 3G Configuration - Dual WAN Mode



WAN Connections	
Ethernet Port	Cable/Dynamic IP (DHCP) □ MAC Clone
USB Port	3G ○ Master WAN ● Backup WAN
Dual WAN Mode	
Fallback of dual wan	● Enable ○ Disable
Detect IP address of Master WAN	199.7.83.42
Detect IP address of Backup WAN	199.7.83.42
Detect Timeout	3 (1 ~ 5 seconds, default: 3)

The following items are displayed in this section on this page:

- **USB Port** — Enables support for a WAN connection using a USB 3G modem. When enabled, you can select if the 3G modem connection operates as the Master or Backup WAN link. (Default: Disabled)

  - **Master WAN** — Enables the USB 3G modem WAN connection to operate as the primary WAN link. The Ethernet WAN port then operates as the backup link. (Default: Disabled)

  - **Backup WAN** — Enables the USB 3G modem WAN connection to operate as the backup to the Ethernet WAN port link. (Default: Enabled)

- **Dual WAN Mode** — When both the WAN port and 3G modem connections are enabled, you can configure the following parameters:

  - **Fallback of Dual WAN** — The operation of the fallback between dual WAN connections is as follows: (Default: Disabled)

    - **Enable** — The Master WAN connection is used first. Whenever this connection is lost, the device automatically switches to the Backup WAN. During the operation of the Backup WAN, the Master WAN link is monitored for recovery of the lost connection. If the Master WAN link is re-established, the WAN connection automatically switches back to the Master from the Backup WAN connection.

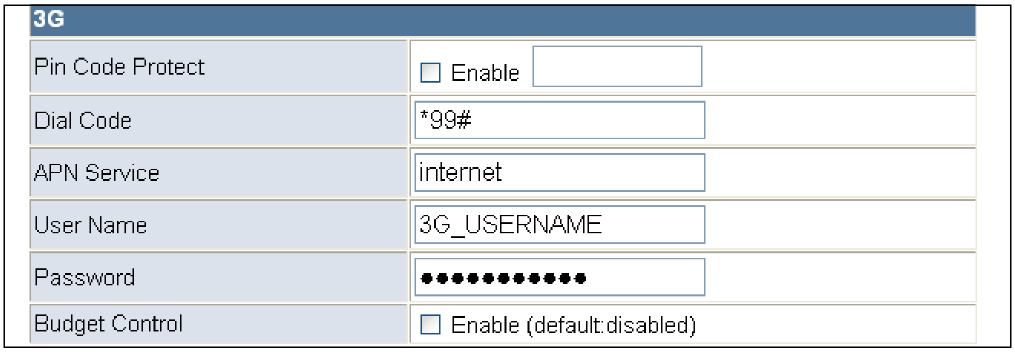
    - **Disable** — The Master WAN connection is used first. Whenever this connection is lost, the device automatically switches to the Backup WAN. The device will only switch back to the Master WAN if the Backup connection is lost.

  - **Detect IP Address of Master WAN** — An IP address to which a ping packet is sent to detect if the Master WAN connection is valid. (Default: 199.7.83.42)

  - **Detect IP Address of Backup WAN** — An IP address to which a ping packet is sent to detect if the Backup WAN connection is valid. (Default: 199.7.83.42)

  - **Detect Timeout** — Sets the ping time out. (Range: 1~5 seconds; Default: 3 seconds)

Figure 32: 3G Configuration - Account Setup



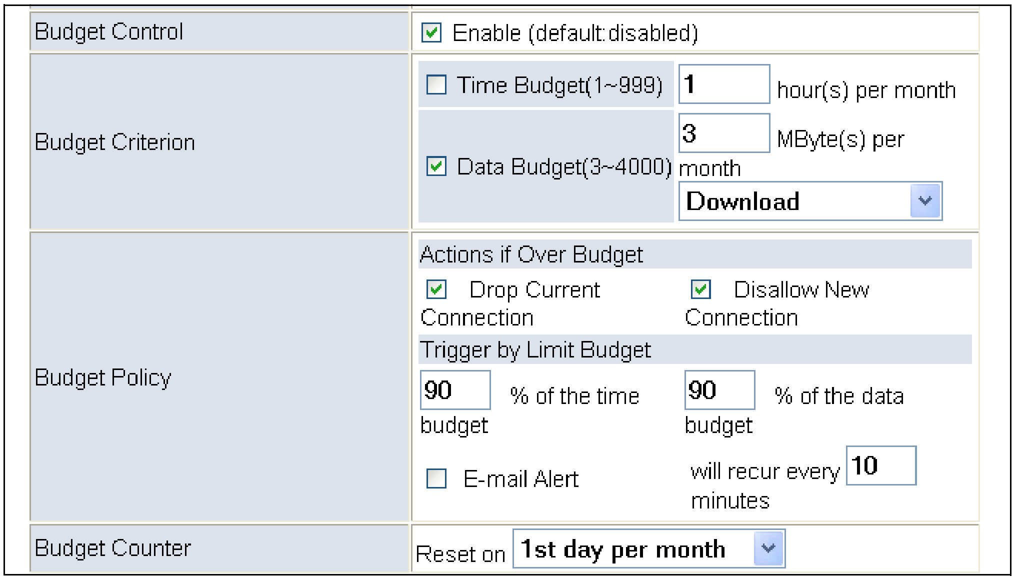
3G	
Pin Code Protect	□ Enable
Dial Code	*99#
APN Service	internet
User Name	3G_USERNAME
Password	●●●●●●●●●●●●
Budget Control	□ Enable (default:disabled)

The following items are displayed in this section on this page:

- **Pin Code Protect** — Enables the use of a PIN code (personal identification number) to encrypt access to the 3G modem connection. Some service providers do not require PIN code authentication. If a PIN code is not required for your 3G or 3.5G modem, disable this function. (Default: Disabled)

- **Dial Code** — A dialled access code that connects the USB device to the service provider.
- **APN Service** — The access point name (APN) that uniquely identifies the 3G or 3.5G service provider.
- **User Name** — The user name of the account registered with the 3G or 3.5G service provider.
- **Password** — The password of the account registered with the 3G or 3.5G service provider.

Figure 33: 3G Configuration - Budget Control



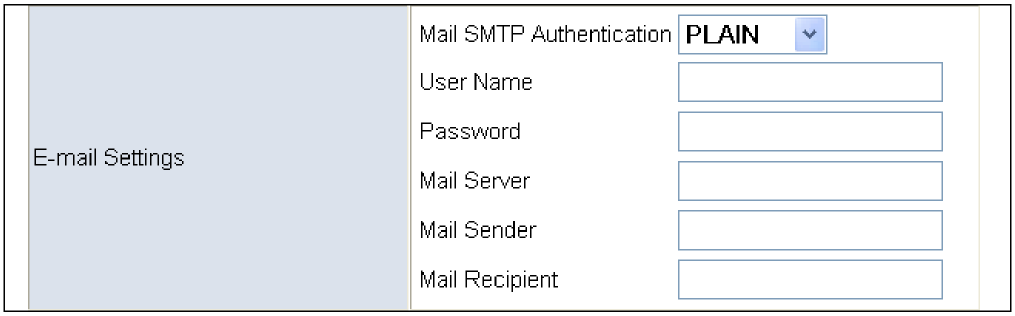
Budget Control	☑ Enable (default:disabled)
Budget Criterion	□ Time Budget(1~999) 1 hour(s) per month ☑ Data Budget(3~4000) 3 MByte(s) per month Download
Budget Policy	Actions if Over Budget ☑ Drop Current Connection ☑ Disallow New Connection Trigger by Limit Budget 90 % of the time budget 90 % of the data budget □ E-mail Alert will recur every 10 minutes
Budget Counter	Reset on 1st day per month

The following items are displayed in this section on this page:

- **Budget Control** — Enables a monthly limit on time or total data. (Default: Disabled)
- **Budget Criterion** — Specifies budget limits set by time or data.
  - **Time Budget** — Specify the amount of time (in hours) that can be used for the 3G connection per month. (Range: 1~999 hours; Default: 1 hour)
  - **Data Budget** — Specify how much Download/Upload data (in MBytes) is allowed per month for the 3G connection. The drop-down list specifies if the data budget is for download, upload, or download and upload. (Range: 3~4000 MBytes; Default: 3 MBytes)

- **Budget Policy** — Specifies the action to take when budget limits have been reached.
  - **Action if Over Budget** — Specifies the the action to take when a budget limit has been exceeded:
    - **Drop Current Connection** — Immediately drop the current connection. (Default: Enabled)
    - **Disallow New Connection** — Do not permit any new connections. (Default: Enabled)
  - **Trigger by Limit Budget** — Specifies the percentage of the time or data budget at which to start sending E-mail alerts at the indicated time interval. When E-mail alerts are enabled, be sure to configure the E-mail settings. (Default: 90% of budget, E-mail Alerts disabled, recurring every 10 minutes)
- **Budget Counter** — Select the day of the month on which to reset the time/data budget counters. (Default: 1st day per month)

Figure 34: 3G Configuration - E-mail Settings



E-mail Settings	Mail SMTP Authentication	PLAIN
	User Name	
	Password	
	Mail Server	
	Mail Sender	
	Mail Recipient	

The following items are displayed in this section on this page:

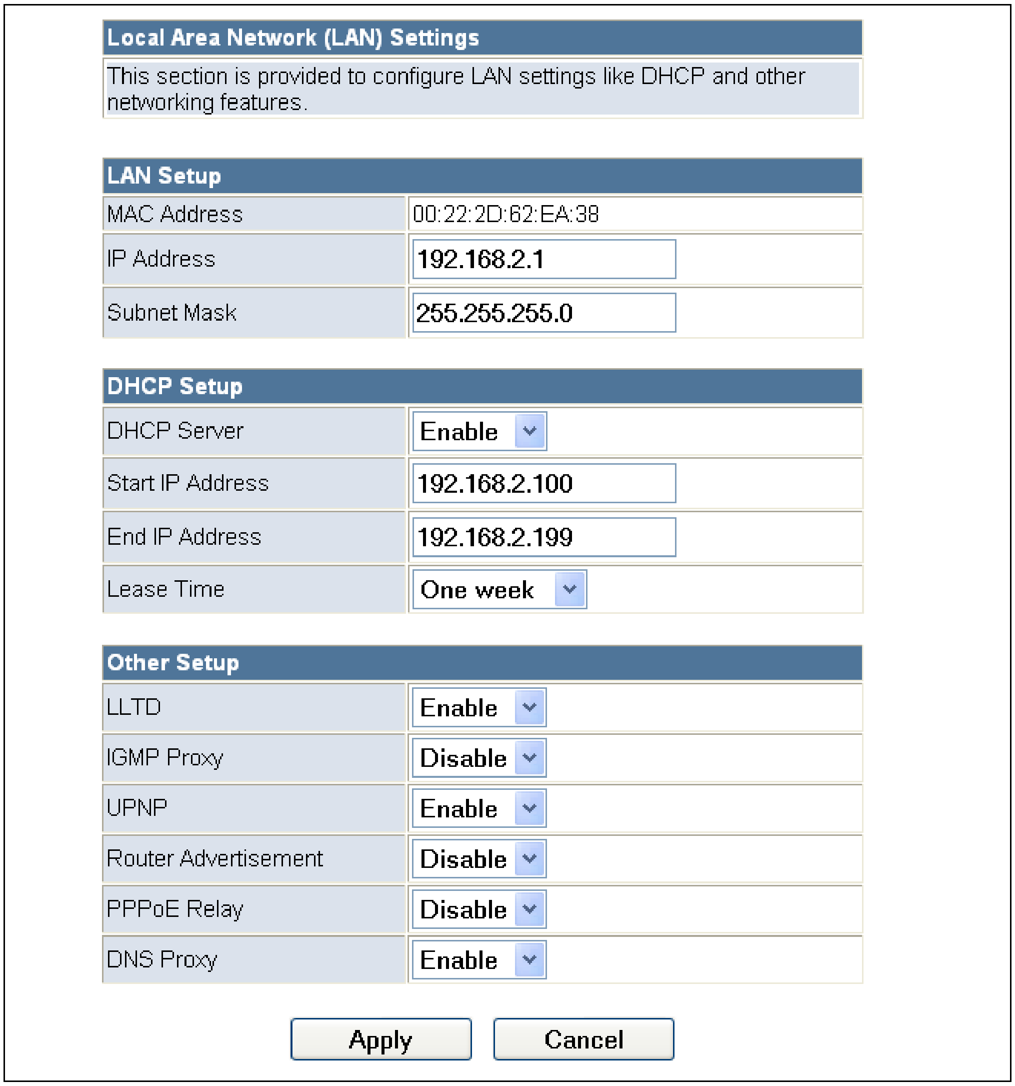
- **E-mail Settings** — The unit can use SMTP (Simple Mail Transfer Protocol) to send E-mail messages when triggered by the specified budget policy limits.
  - **Mail SMTP Authentication** — Specifies a user name and password for SMTP server authentication. (Options: PLAIN, LOGIN, or Disabled.)
  - **User Name** — Enter the user name for the SMTP server account.
  - **Password** — Enter the password for the SMTP server account.
  - **Mail Server** — Specifies the URL of the SMTP mail server that will send the alert messages.
  - **Mail Sender** — Specifies an E-mail address on the SMTP server that will send the alert messages.

- **Mail Recipient** — The E-mail address of the recipient of the alert messages.

LAN SETTING

The Gateway 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 "Network Settings" followed by "LAN."

Figure 35: LAN Configuration



Local Area Network (LAN) Settings

This section is provided to configure LAN settings like DHCP and other networking features.

LAN Setup	
MAC Address	00:22:2D:62:EA:38
IP Address	192.168.2.1
Subnet Mask	255.255.255.0

DHCP Setup	
DHCP Server	Enable
Start IP Address	192.168.2.100
End IP Address	192.168.2.199
Lease Time	One week

Other Setup	
LLTD	Enable
IGMP Proxy	Disable
UPNP	Enable
Router Advertisement	Disable
PPPoE Relay	Disable
DNS Proxy	Enable

The following items are displayed on this page:

- **MAC Address** — The physical layer address for the Gateway's LAN port.

- **IP Address** — Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)

- **Subnet Mask** — Indicate the local subnet mask. (Default: 255.255.255.0.)

- **DHCP Server** — Enable this feature to assign IP settings to wired and wireless clients connected to the Gateway. 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.

- **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: Forever, Two weeks, One week, Two days, One day, Half day, Two hours, One hour, Half hour; Default: One week)

- **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: Enable)

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

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

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

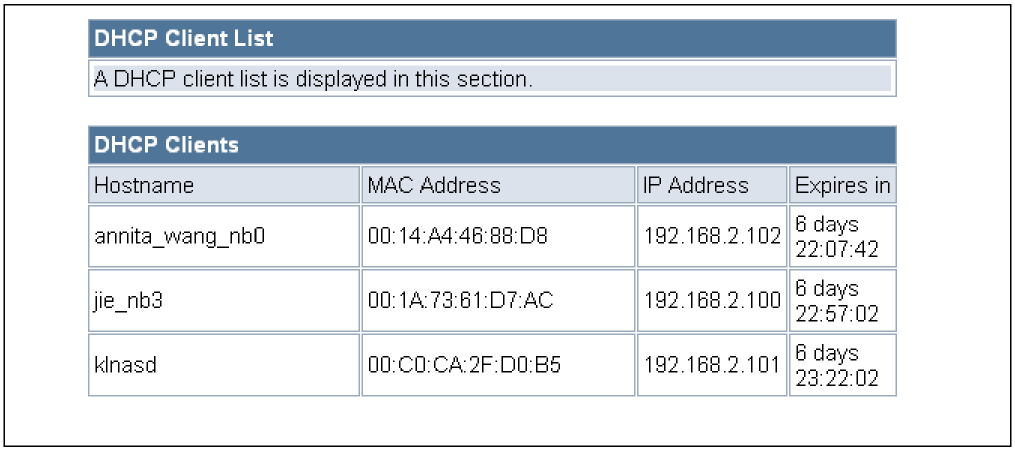
- **PPPoE Relay** — When enabled, the Gateway will forward PPPoE messages to clients. Clients are then able to connect to the PPPoE service through the WAN port. (Options: Disable/Enable, Default: Disable)

- **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)

DHCP CLIENTS

The DHCP Clients page displays information on connected client stations that have been assigned IP addresses from the DHCP address pool.

Figure 36: DHCP Clients



DHCP Client List

A DHCP client list is displayed in this section.

DHCP Clients

Hostname	MAC Address	IP Address	Expires in
annita_wang_nb0	00:14:A4:46:88:D8	192.168.2.102	6 days 22:07:42
jie_nb3	00:1A:73:61:D7:AC	192.168.2.100	6 days 22:57:02
klnasd	00:C0:CA:2F:D0:B5	192.168.2.101	6 days 23:22:02

The following items are displayed on this page:

Host name — The name of the connected client station.

MAC Address — The MAC address of the connected client station.

IP Address — The IP address assigned to the client from the IP pool.

Expires in — The time limit for the use of the IP address from the IP pool. When the time limit expires, the client has to request a new IP address.

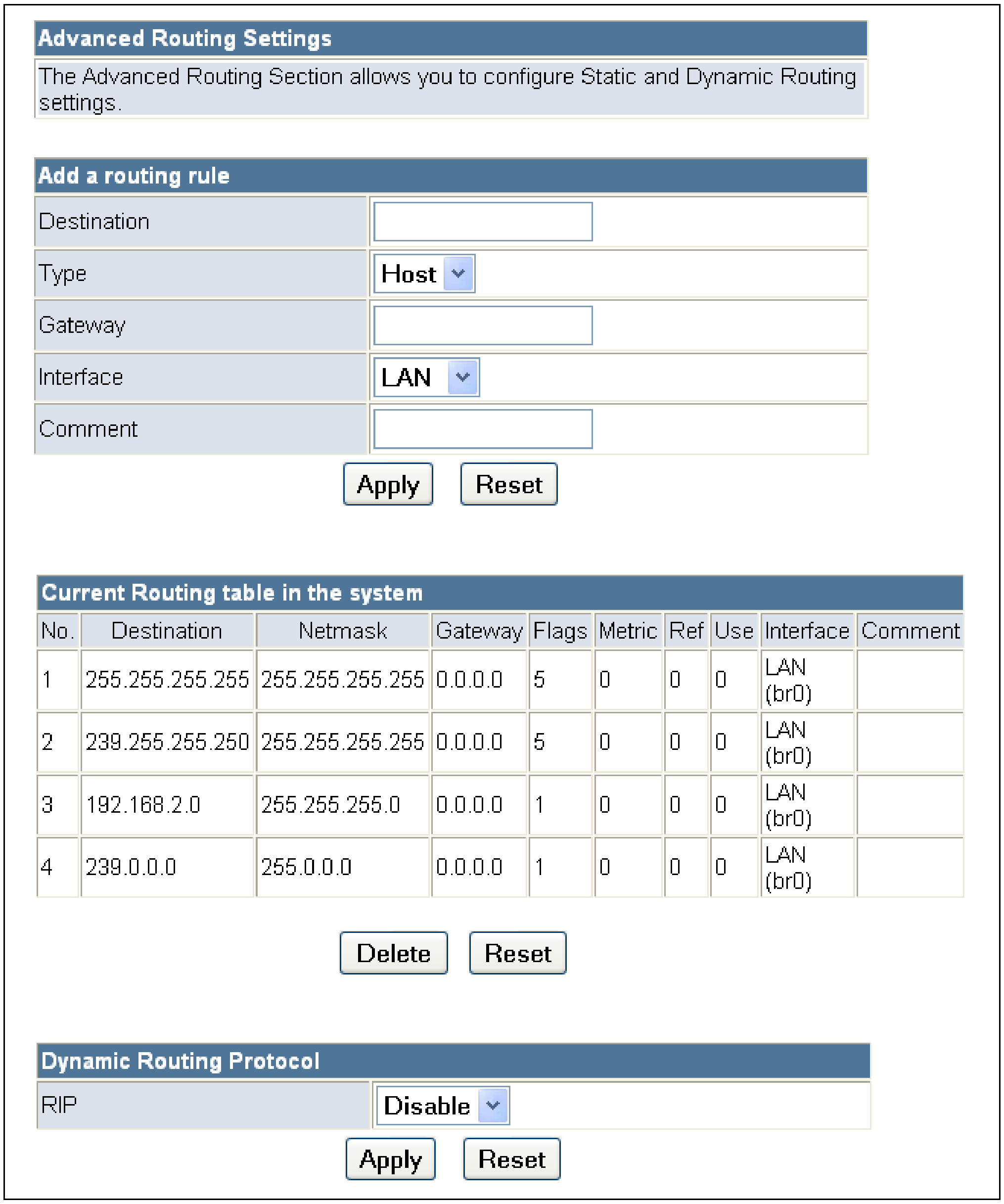
ADVANCED ROUTING

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 "Network Settings" followed by "Advanced Routing." (Maximum 32 entries are allowed.)

Figure 37: Advanced Routing (Router Mode)



Advanced Routing Settings

The Advanced Routing Section allows you to configure Static and Dynamic Routing settings.

Add a routing rule

Destination	
Type	Host
Gateway	
Interface	LAN
Comment	

Current Routing table in the system

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
3	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	
4	239.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	LAN (br0)	

Dynamic Routing Protocol

RIP	Disable

The following items are displayed on this page:

- **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 Gateway is set to Router 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

- **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 Gateway 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 Gateway. It includes the following sections:

- "Basic Settings" on page 69
- "Advanced Settings" on page 73
- "WLAN Security" on page 79
- "Wireless Distribution System (WDS)" on page 86
- "Wi-Fi Protected Setup (WPS)" on page 89
- "Station List" on page 92

BASIC SETTINGS

The IEEE 802.11n interface includes configuration options for radio signal characteristics and wireless security features.

The Gateway's radio can operate in six modes, mixed 802.11b/g/n, mixed 802.11b/g, mixed 802.11g/n, 802.11n only, 802.11b only, or 802.11g only. Note that 802.11g is backward compatible with 802.11b, and 802.11n is backward compatible with 802.11b/g at slower data transmit rates.

The Gateway supports two virtual access point (VAP) interfaces. One VAP is the primary (Network Name SSID), and the other one is referred to as "Multiple SSID1." Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces.

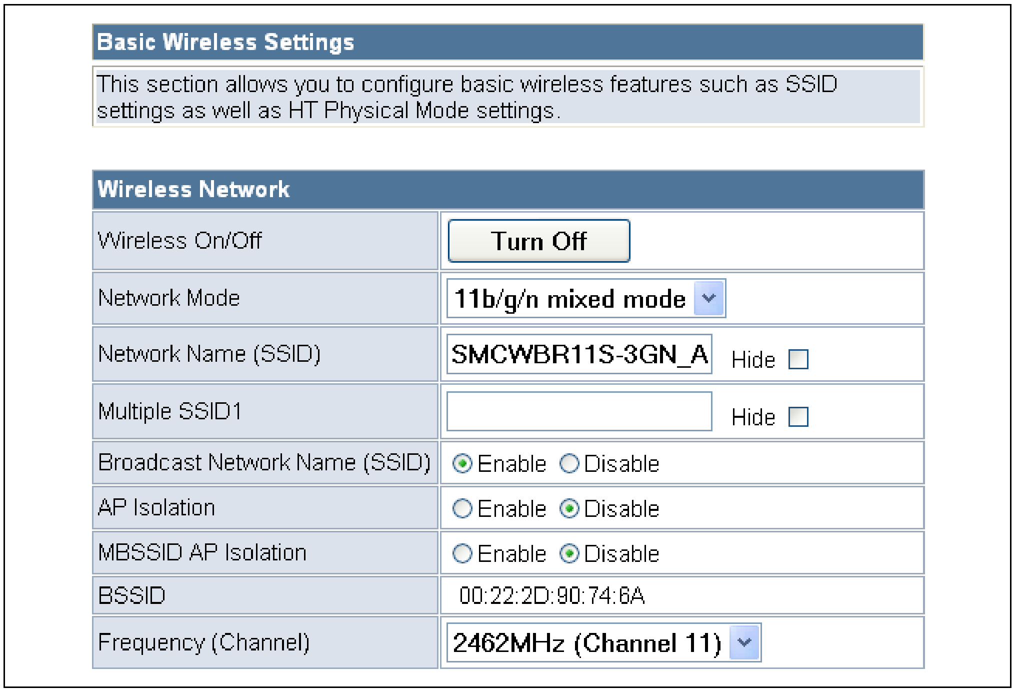
Traffic to specific VAPs can be segregated based on user groups or application traffic. All VAPs can have up to 64 wireless clients, whereby the clients associate with these VAPs the same as they would with a physical access point.

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

The Basic Settings page allows you to configure the wireless network name (Service Set Identifier or SSID) and set the wireless security method.

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

Figure 38: Basic Settings



Basic Wireless Settings

This section allows you to configure basic wireless features such as SSID settings as well as HT Physical Mode settings.

Wireless Network	
Wireless On/Off	Turn Off
Network Mode	11b/g/n mixed mode
Network Name (SSID)	SMCWBR11S-3GN_A Hide □
Multiple SSID1	Hide □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:22:2D:90:74:6A
Frequency (Channel)	2462MHz (Channel 11)

The following items are displayed on this page:

- **Wireless On/Off** — Enables or Disable the radio. (Default: Enable)
- **Network Mode** — Defines the radio operating mode. (Default: 11g/n Mixed)
  - **11b/g mixed**: Both 802.11b and 802.11g clients can communicate with the Gateway (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 Gateway, but they will be limited to 802.11g protocols and data transmission rates.
  - **11b only**: All 802.11b, 802.11g, and 802.11n clients will be able to communicate with the Gateway, but the 802.11g and 802.11n clients will be limited to 802.11b protocols and data transmission rates (up to 11 Mbps).
  - **11g only**: Both 802.11g and 802.11n clients will be able to communicate with the Gateway, 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 Gateway.
  - **11n only**: Only 802.11n clients will be able to communicate with the Gateway (up to 150 Mbps).

  - **11g/n mixed**: Both 802.11g and 802.11n clients can communicate with the Gateway (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11g clients.
  - **11b/g/n Mixed**: All 802.11b/g/n clients can communicate with the Gateway (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 Gateway. Clients that want to connect to the network must set their SSID to the same as that of the Gateway. (Default: "SMCWBR11S-3GN_AP"; Range: 1-32 characters)

- **Multiple SSID1** — One additional VAP interface supported on the device. (Default: no name configured; Range: 1-32 characters)

- **Broadcast Network Name (SSID)** — By default, the Gateway always broadcasts the SSID in its beacon signal. Disabling the SSID broadcast increases security of the network because wireless clients need to already know the SSID before attempting to connect. When set to disable, the Network Name SSID, and SSID1 are automatically set to "Hide." (Default: Enabled)

- **AP Isolation** — The Gateway will isolate communincation between all clients in order to protect them. Normally for users who are at hotspots. (Default: Disabled)

- **MBSSID AP Isolation** — The Gateway will isolate wireless clients from different SSID.

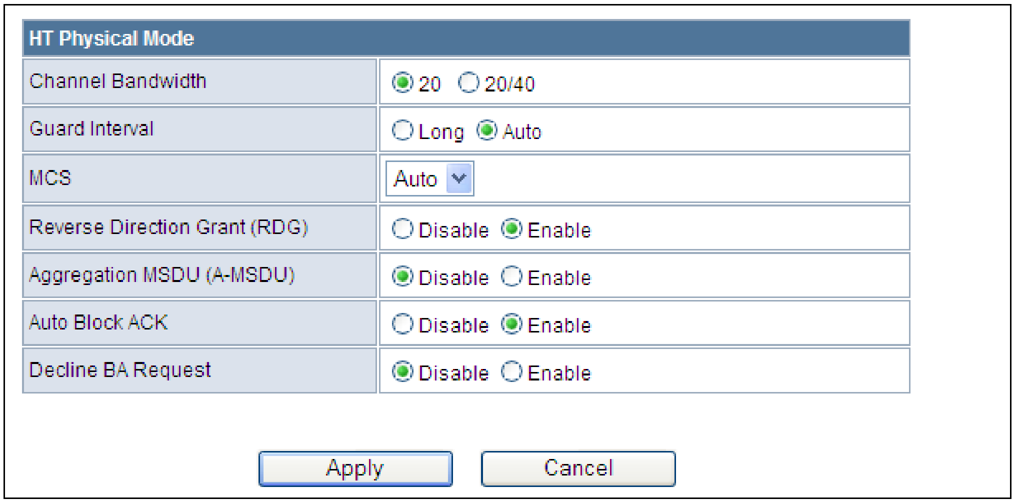
- **BSSID** — The identifier (MAC address) of the Gateway in the Basic Service Set (BSS) network.

- **Frequency (Channel)** — The radio channel that the Gateway 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 Gateway to which it is linked. Selecting Auto Select enables the Gateway to automatically select an unoccupied radio channel. (Default: AutoSelect)

HT Physical Mode Settings

The HT Physical Mode section on the Wireless Settings Advanced page includes additional parameters for 802.11n operation.

Figure 39: HT Physical Mode Settings



HT Physical Mode	
Channel Bandwidth	● 20 ○ 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant (RDG)	○ Disable ● Enable
Aggregation MSDU (A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable

The following items are displayed in this section on this page:

- **HT Channel Bandwidth** — The Gateway 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: 20MHz)

- **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 Reverse Direction Grant is enabled, the Gateway 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: AutoSelect.)

- **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.

ADVANCED SETTINGS

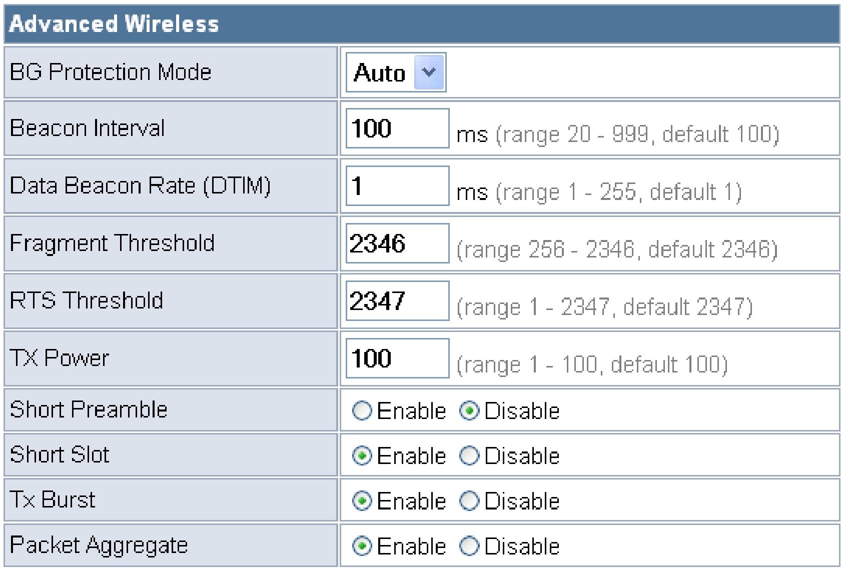
The Advanced Settings page includes additional parameters concerning the wireless network and Wi-Fi Multimedia settings.

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.

ADVANCED WIRELESS

The Advanced Wireless section on the Wireless Settings Advanced page includes additional radio parameters.

Figure 40: Advanced Wireless Settings



Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Packet Aggregate	● Enable ○ Disable

The following items are displayed in this section on this page:

- **BG Protection Mode** — Enables a backward compatible protection mechanism for 802.11b clients. There are three modes: (Default: Auto)

  - **Auto** — The unit enables its protection mechanism for 802.11b clients when they are detected in the network. When 802.11b clients are not detected, the protection mechanism is disabled.

  - **On** — Forces the unit to always use protection for 802.11b clients, whether they are detected in the network or not. Note that enabling b/g Protection can slow throughput for 802.11g/n clients by as much as 50%.

  - **Off** — Forces the unit to never use protection for 802.11b clients. This prevents 802.11b clients from connecting to the network.

- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-999 TUs; Default: 100 TUs)

- **Data Beacon Rate (DTIM)** — The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

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

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

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

  If the RTS threshold is set to 0, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this “Hidden Node Problem.” (Range: 1-2347 bytes: Default: 2347 bytes)

- **Short Preamble** — Sets the length of the signal preamble that is used at the start of a data transmission. Use a short preamble (96 microseconds) to increase data throughput when it is supported by all connected 802.11g clients. Use a long preamble (192 microseconds) to ensure all 802.11b clients can connect to the network. (Default: Disabled)

- **Short Slot** — Sets the basic unit of time the access point uses for calculating waiting times before data is transmitted. A short slot time (9 microseconds) can increase data throughput on the access point, but requires that all clients can support a short slot time (that is, 802.11g-compliant clients must support a short slot time). A long slot time (20 microseconds) is required if the access point has to support 802.11b clients. (Default: Enabled)

- **TX Burst** — A performance enhancement that transmits a number of data packets at the same time when the feature is supported by compatible clients. (Default: Enabled)

- **Packet Aggregate** — A performance enhancement that combines data packets together when the feature is supported by compatible clients. (Default: Enabled)

WI-FI MULTIMEDIA

The Gateway implements Quality of Service (QoS) using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard and it enables access points to interoperate with both WMM-enabled clients and other devices that may lack any WMM functionality.

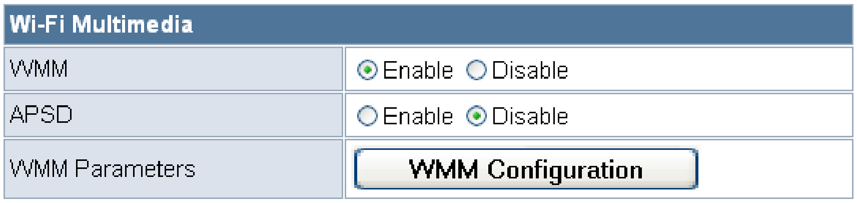
WMM defines four access categories (ACs): voice, video, best effort, and background. These categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags (see Table 3). The direct mapping of the four ACs to 802.1D priorities is specifically intended to facilitate interoperability with other wired network QoS policies. While the four ACs are specified for specific types of traffic, WMM allows the priority levels to be configured to match any network-wide QoS policy. WMM also specifies a protocol that access points can use to communicate the configured traffic priority levels to QoS-enabled wireless clients.

Table 3: WMM Access Categories

Access Category	WMM Designation	Description	802.1D Tags
AC_VO (AC3)	Voice	Highest priority, minimum delay. Time-sensitive data such as VoIP (Voice over IP) calls.	7, 6
AC_VI (AC2)	Video	High priority, minimum delay. Time-sensitive data such as streaming video.	5, 4
AC_BE (AC0)	Best Effort	Normal priority, medium delay and throughput. Data only affected by long delays. Data from applications or devices that lack QoS capabilities.	0, 3
AC_BK (AC1)	Background	Lowest priority. Data with no delay or throughput requirements, such as bulk data transfers.	2, 1

The Wi-Fi Multimedia section on the Wireless Settings Advanced page allows you to enable WMM and set detailed QoS parameters.

Figure 41: Wi-Fi Multimedia Settings



Wi-Fi Multimedia

WMM ● Enable ○ Disable

APSD ○ Enable ● Disable

WMM Parameters

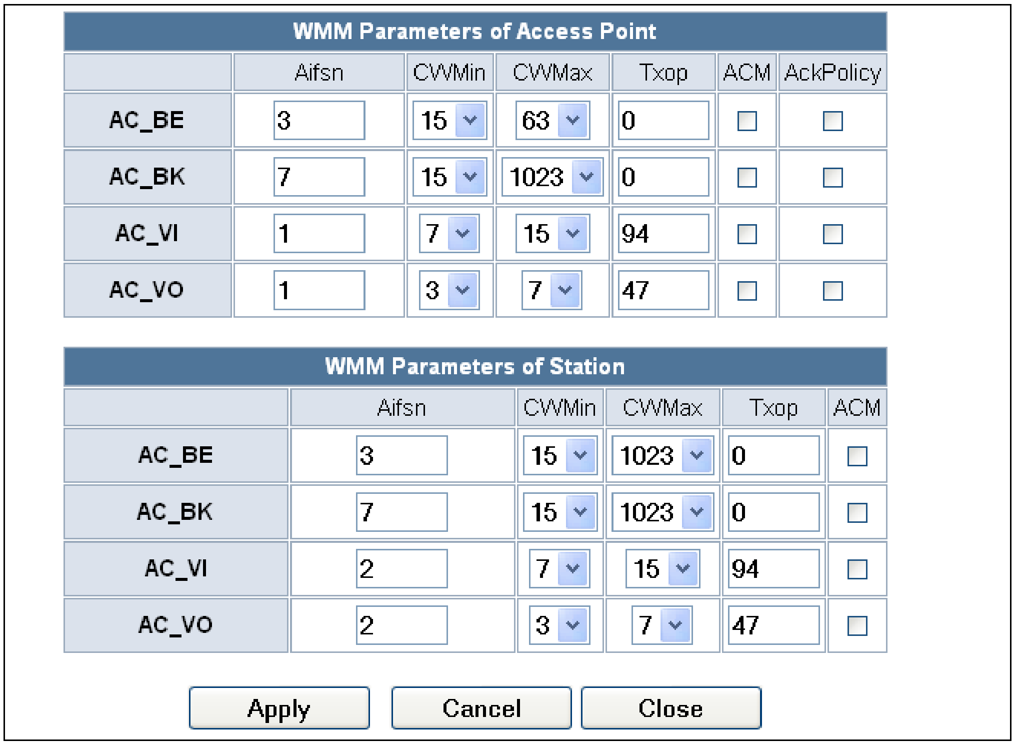
The following items are displayed in this section on this page:

- **WMM** — Sets the WMM operational mode on the access point. When enabled, the QoS capabilities are advertised to WMM-enabled clients in the network. WMM must be supported on any device trying to associated with the access point. Devices that do not support this feature will not be allowed to associate with the access point. (Default: Enabled)

- **APSD** — When WMM is enabled, Automatic Power Save Delivery (APSD) can also be enabled. APSD is an efficient power management method that enables client devices sending WMM packets to enter a low-power sleep state between receiving and transmitting data. (Default: Disabled)

- **WMM Parameters** — Click the WMM Configuration button to set detailed WMM parameters.

Figure 42: WMM Configuration



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

The following items are displayed in the WMM Configuration window:

- **AIFSN** (Arbitration Inter-Frame Space) — The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

- **CWMin** (Minimum Contention Window) — The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.

- **CWMax** (Maximum Contention Window) — The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.

- **Txop** (Transmit Opportunity Limit) — The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TxOpLimit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-65535 microseconds.

- **ACM** — The admission control mode for the access category. When enabled, clients are blocked from using the access category. (Default: Disabled)

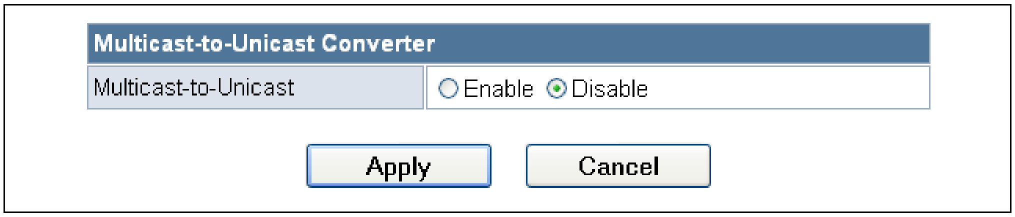
- **AckPolicy** — By default, all wireless data transmissions require the sender to wait for an acknowledgement from the receiver. WMM allows the acknowledgement wait time to be turned off for each Access Category (AC) 0-3. Although this increases data throughput, it can also result in a high number of errors when traffic levels are heavy. (Default: Acknowledge)

MULTICAST-TO-UNICAST CONVERTER

The Multicast-to-Unicast Converter section on the Wireless Settings Advanced page allows you to enable multicast traffic conversion.

Converting multicast traffic to unicast before sending to wireless clients allows a longer DTIM (Data Beacon Rate) interval to be set. A longer DTIM interval prevents clients in power-save mode having to activate their radios to receive the multicast data, which saves battery life.

Figure 43: Multicast-to-Unicast Converter



Multicast-to-Unicast Converter

Multicast-to-Unicast	○ Enable ● Disable

The following items are displayed in this section on this page:

- **Multicast-to-Unicast** — Enables multicast traffic streams to be converted to unicast traffic before delivery to wireless clients. (Default: Disabled)

WLAN SECURITY

The Gateway's wireless interface is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the wireless network.

To implement wireless network security, you have to employ one or both of the following functions:

- **Authentication** — It must be verified that clients attempting to connect to the network are authorized users.

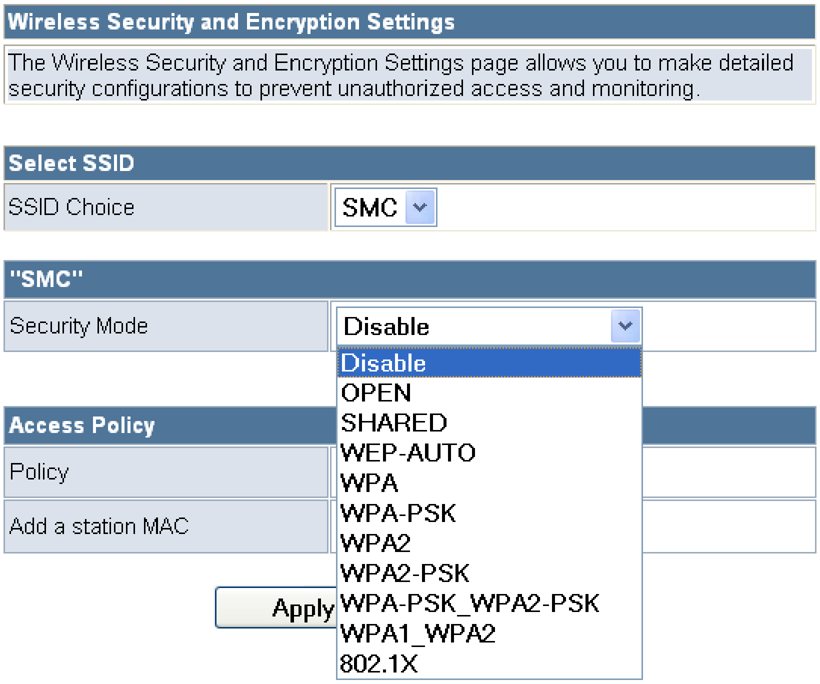
- **Traffic Encryption** — Data passing between the unit and clients must be protected from interception and eavesdropping.

The Gateway supports supports ten different security mechanisms that provide various levels of authentication and encryption depending on the requirements of the network.

The Gateway supports two SSID interfaces. Each SSID interface functions as a separate access point, and can be configured with its own security settings.

Click on "Wireless Settings," followed by "Basic".

Figure 44: Security Mode Options



Wireless Security and Encryption Settings

The Wireless Security and Encryption Settings page allows you to make detailed security configurations to prevent unauthorized access and monitoring.

Select SSID

SSID Choice: SMC

"SMC"

Security Mode: Disable

Access Policy

Policy

Add a station MAC

The supported security mechanisms and their configuration parameters are described in the following sections:

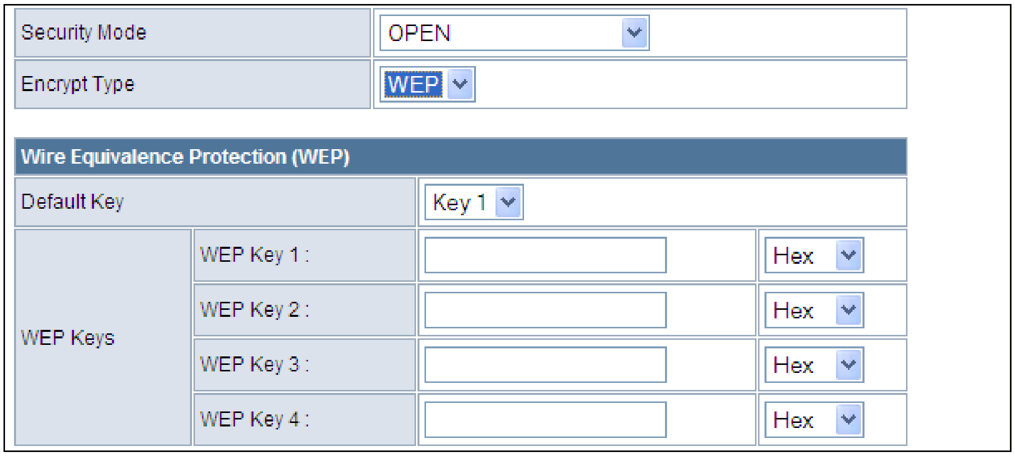
- **OPEN, SHARED, WEP-AUTO** — See "Wired Equivalent Privacy (WEP)" on page 80
- **WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK** — See "WPA Pre-Shared Key" on page 81
- **WPA, WPA2, WPA1_WPA2** — See "WPA Enterprise Mode" on page 82
- **802.1X** — See "IEEE 802.1X and RADIUS" on page 84

Wired Equivalent Privacy (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Figure 45: Security Mode - WEP



Security Mode	OPEN	
Encrypt Type	WEP	

Wire Equivalence Protection (WEP)

Default Key	Key 1		
WEP Keys	WEP Key 1 :		Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

The following items are displayed in this section on this page:

Security Mode — Configures the WEP security mode used by clients. When using WEP, be sure to define at least one static WEP key for the Gateway and all its clients. (Default: Disable)

- **OPEN** — Open-system authentication accepts any client attempting to connect the Gateway without verifying its identity. In this mode the default data encryption type is "WEP."
- **SHARED** — The shared-key security uses a WEP key to authenticate clients connecting to the network and for data encryption.

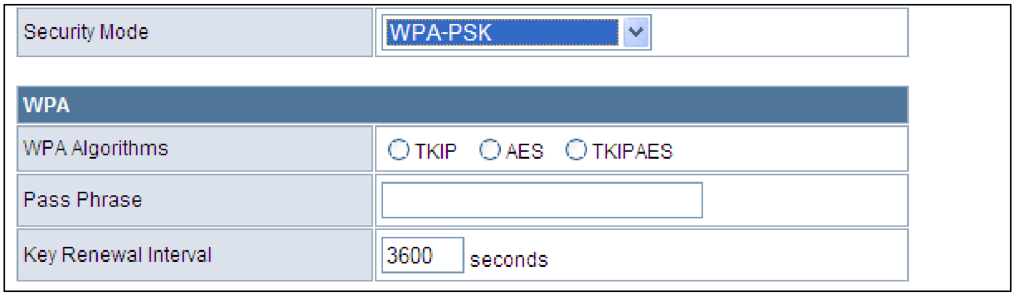
- **WEP-AUTO** — Allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).
- **Encrypt Type** — Selects WEP for data encryption (OPEN mode only).
- **Default Key** — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys. (Default: 1; Range: 1~4)
- **WEP Keys 1 ~ 4** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

WPA Pre-Shared Key

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an "enterprise" and "personal" mode of operation.

For small home or office networks, WPA and WPA2 provide a simple "personal" operating mode that uses just a pre-shared key for network access. The WPA Pre-Shared Key (WPA-PSK) mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.

Figure 46: Security Mode - WPA-PSK



Security Mode	WPA-PSK
WPA	
WPA Algorithms	○ TKIP ○ AES ○ TKIPAES
Pass Phrase	
Key Renewal Interval	3600 seconds

The following items are displayed in this section on this page:

Security Mode — Configures the WPA-PSK and WPA2-PSK security modes used by clients. When using WPA-PSK or WPA2-PSK, be sure to define the shared key for the Gateway and all its clients. (Default: Disable)

- **WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is TKIP.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is AES.

- **WPA-PSK_WPA2-PSK** — Clients using WPA or WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type is TKIP/AES.

- **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

  - **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

  - **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

- **Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

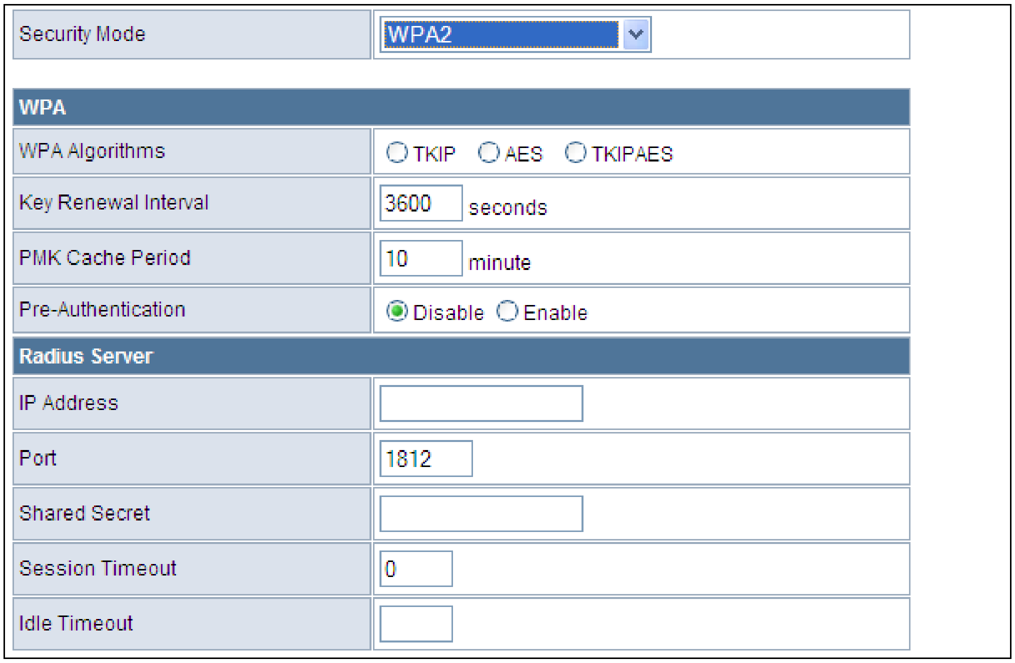
- **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

WPA ENTERPRISE MODE

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation.

For enterprise deployment, WPA and WPA2 use IEEE 802.1X for user authentication and require a RADIUS authentication server to be configured on the wired network. Data encryption keys are automatically generated and distributed to all clients connected to the network.

Figure 47: Security Mode - WPA



Security Mode	WPA2
WPA	
WPA Algorithms	○ TKIP ○ AES ○ TKIPAES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	● Disable ○ Enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The following items are displayed in this section on this page:

Security Mode — Configures the WPA and WPA2 security modes used by clients. When using WPA or WPA2, be sure there is a RADIUS server in the connected wired network, and that the RADIUS settings are configured. See "IEEE 802.1X and RADIUS" on page 84 for more information. (Default: Disable)

- **WPA** — Clients using WPA with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is TKIP.
- **WPA2** — Clients using WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is AES.
- **WPA1_WPA2** — Clients using WPA or WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type is TKIP/AES.
- **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)
  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for

message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

- **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

- **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

- **PMK Cache Period** — WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required. This parameter sets the time for deleting the cached WPA2 Pairwise Master Key (PMK) security information. (Default: 10 minutes)

- **Pre-Authentication** — When using WPA2, pre-authentication can be enabled that allows clients to roam to another access point and be quickly associated without performing full 802.1X authentication. (Default: Disabled)

IEEE 802.1X AND RADIUS

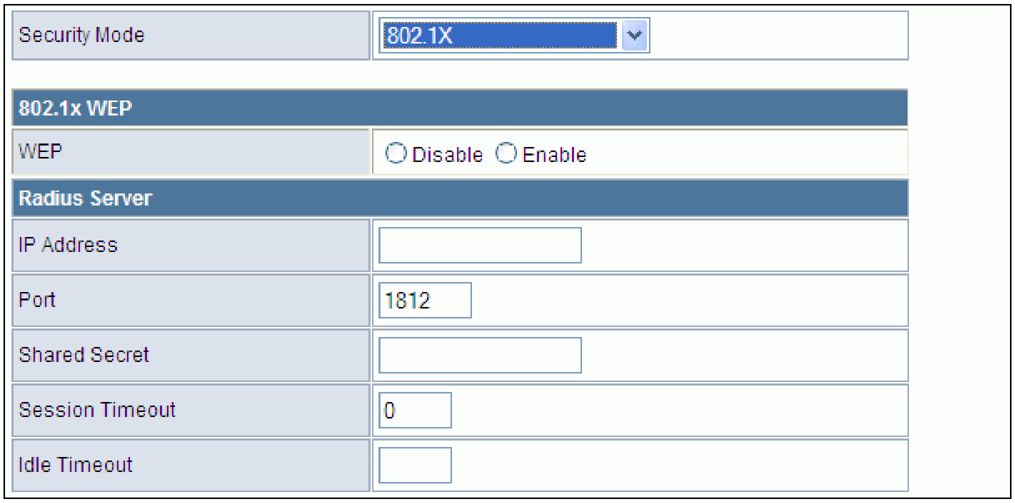
IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network.

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.

NOTE: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Figure 48: Security Mode - 802.1X



Security Mode	802.1X
802.1x WEP	
WEP	○ Disable ○ Enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The following items are displayed in this section on this page:

Security Mode — Configures the 802.1X security mode used by clients. When using 802.1X, either with WPA/WPA2 or on its own, be sure there is a configured RADIUS server in the connected wired network. (Default: Disable)

802.1X WEP: Selects WEP keys for data encryption. When enabled, WEP encryption keys are automatically generated by the RADIUS server and distributed to all connected clients. (Default: Disabled)

RADIUS Server — Configures RADIUS server settings.

- **IP Address** — Specifies the IP address of the RADIUS server.

- **Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

- **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

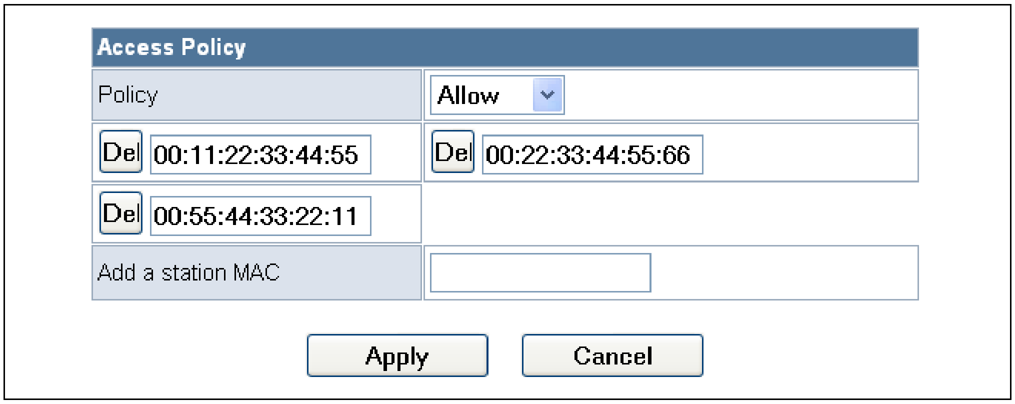
- **Session Timeout** — Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 0)

- **Idle Timeout** — Sets the maximum time (in seconds) of client inactivity before a session is terminated.

ACCESS POLICY

The Gateway provides a MAC address filtering facility. The access policy can be set to allow or reject specific station MAC addresses. This feature can be used to connect known wireless devices that may not be able to support the configured security mode.

Figure 49: Access Policy



Access Policy

Policy	Allow
00:11:22:33:44:55	00:22:33:44:55:66
00:55:44:33:22:11	
Add a station MAC	

The following items are displayed in this section on this page:

- **Access Policy** — The access policy can be set to allow or reject specific station MAC addresses.
- **Add a station MAC —** Enter the MAC address of the station that you want to filter. MAC addresses must be entered in the format xx:xx:xx:xx:xx:xx.

WIRELESS DISTRIBUTION SYSTEM (WDS)

The radio interface can be configured to operate in a mode that allows it to forward traffic directly to other Gateway units. This feature can be used to extend the range of the wireless network to reach remote clients, or to link disconnected network segments to an Internet connection.

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.

NOTE: All units in a WDS wireless network must be configured with the same SSID and use the same radio channel. Also each WDS link must be configured with the same encryption key on both units in the link.

Up to four WDS links can be specified for each unit in the WDS network. The following figures illustrate an example WDS network. Figure 50 shows the manual set up of MAC addresses for units in the WDS network. Figure 51 shows the basic configuration required on each unit in the WDS network.

Figure 50: Manual WDS MAC Address Configuration

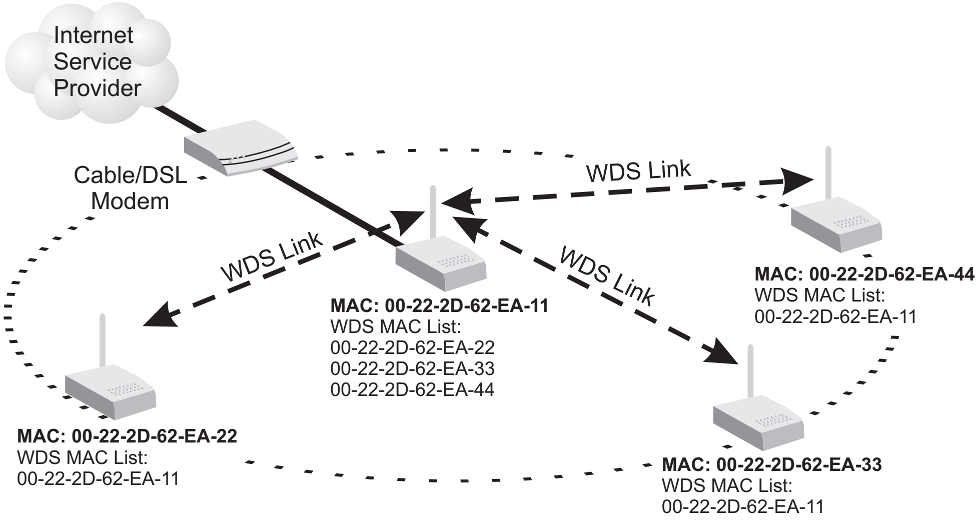
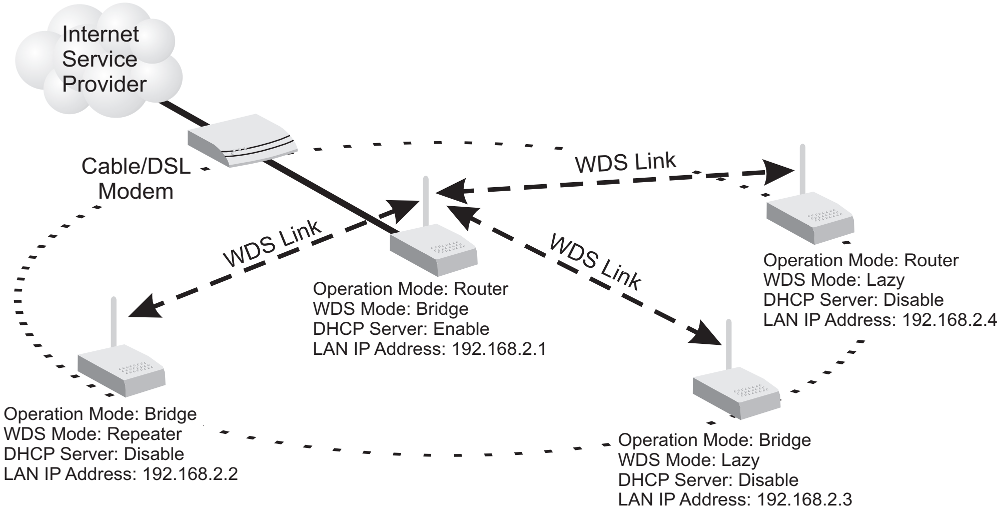


Figure 51: WDS Configuration Example



A WDS link between two units can be configured in any of the following Operation Mode combinations:

1. Both units in a link are configured as Router Mode.

2. One unit in a link is configured in Router Mode and the other in Bridge Mode.

3. Both units in a link are configured as Bridge Mode.

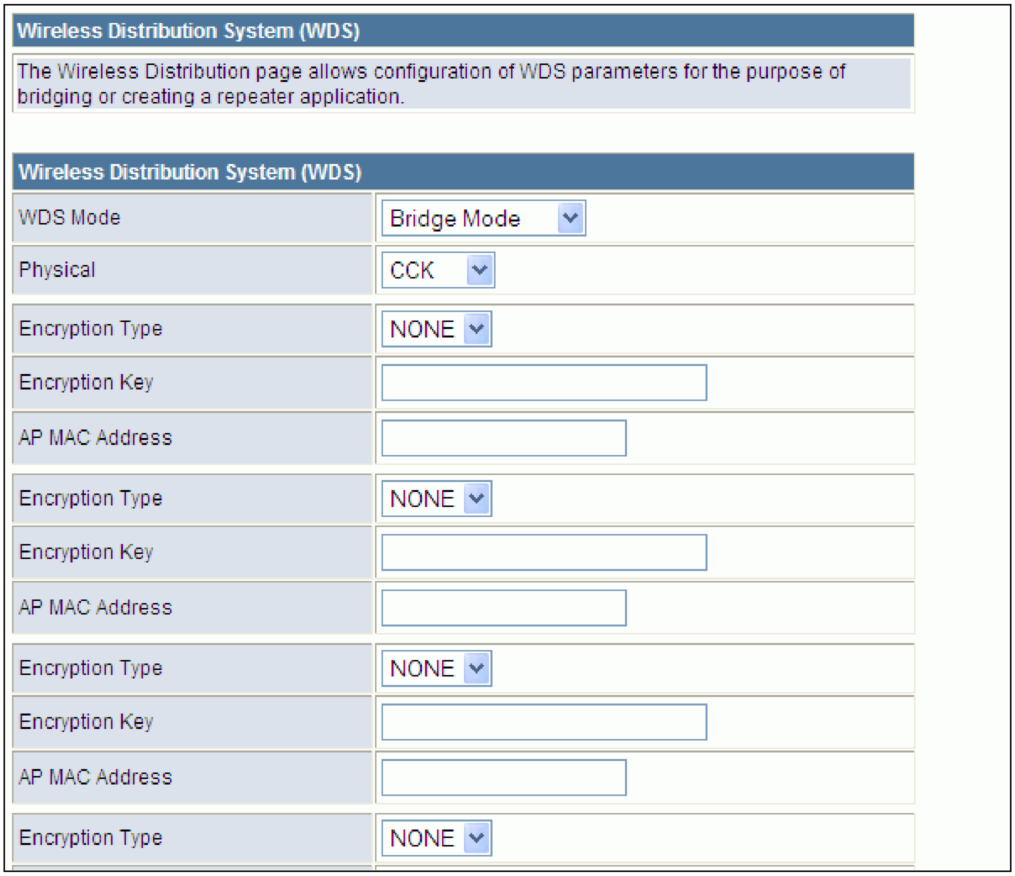
When two or more units in the WDS network are set to Router Mode, be sure to check these settings:

- Be sure each unit is configured with a different LAN IP address.

- Be sure that only one unit has an Internet access on its WAN port.
- Be sure the DHCP server is enabled only on one unit. When one unit is providing Internet access, enable the DHCP server on that unit.

NOTE: When using WDS Lazy mode in the network, at least one unit must be set to Bridge or Repeater mode.

Figure 52: WDS Configuration



Wireless Distribution System (WDS)

The Wireless Distribution page allows configuration of WDS parameters for the purpose of bridging or creating a repeater application.

Wireless Distribution System (WDS)

WDS Mode	Bridge Mode
Physical	CCK
Encryption Type	NONE
Encryption Key	
AP MAC Address	
Encryption Type	NONE
Encryption Key	
AP MAC Address	
Encryption Type	NONE
Encryption Key	
AP MAC Address	
Encryption Type	NONE

The WDS settings configure 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).

The following items are displayed on this page:

- **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 packets, without the need to

configure a WDS MAC list entry. This feature allows the Gateway to associate with other Gateways in the network and use their WDS MAC list. Lazy mode requires one other Gateway within the wireless network that is configured in Bridge or Repeater mode, and has a configured MAC address list.

- **Bridge**: Operates as a standard bridge that forwards traffic between WDS links (links that connect to other units in Repeater or Lazy mode). The MAC addresses of WDS peers must be configured on the Gateway.

- **Repeater**: Operates as a wireless repeater, extending the range for remote wireless clients and connecting them to an AP connected to the wired network. The MAC addresses of WDS peers must be configured on the Gateway.

- **Physical** — The radio media coding used on all WDS links. CCK corresponds to 11b, OFDM corresponds to 11g, and HTMIX corresponds to 11n.

- **Encryption Type** — The data encryption used on the WDS link. Be sure that both ends of a WDS link are configured with the same encryption type and key. (Options: None, WEP, TKIP, AES. Default: None)

- **Encryption Key** — The encryption key for the WDS link. The key type and length varies depending on the encryption type selected. For WEP, enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. For TKIP or AES, enter a password key phrase of between 8 to 63 ASCII characters, which can include spaces, or specify exactly 64 hexadecimal digits.

- **AP MAC Address** — The MAC address of the other Gateway in the WDS link.

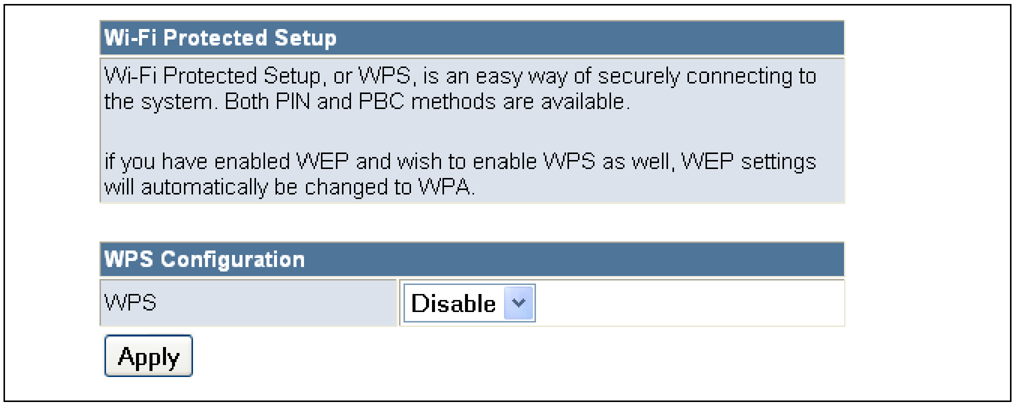
WI-FI PROTECTED SETUP (WPS)

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 Gateway 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 53: Enabling WPS



Wi-Fi Protected Setup

Wi-Fi Protected Setup, or WPS, is an easy way of securely connecting to the system. Both PIN and PBC methods are available.

if you have enabled WEP and wish to enable WPS as well, WEP settings will automatically be changed to WPA.

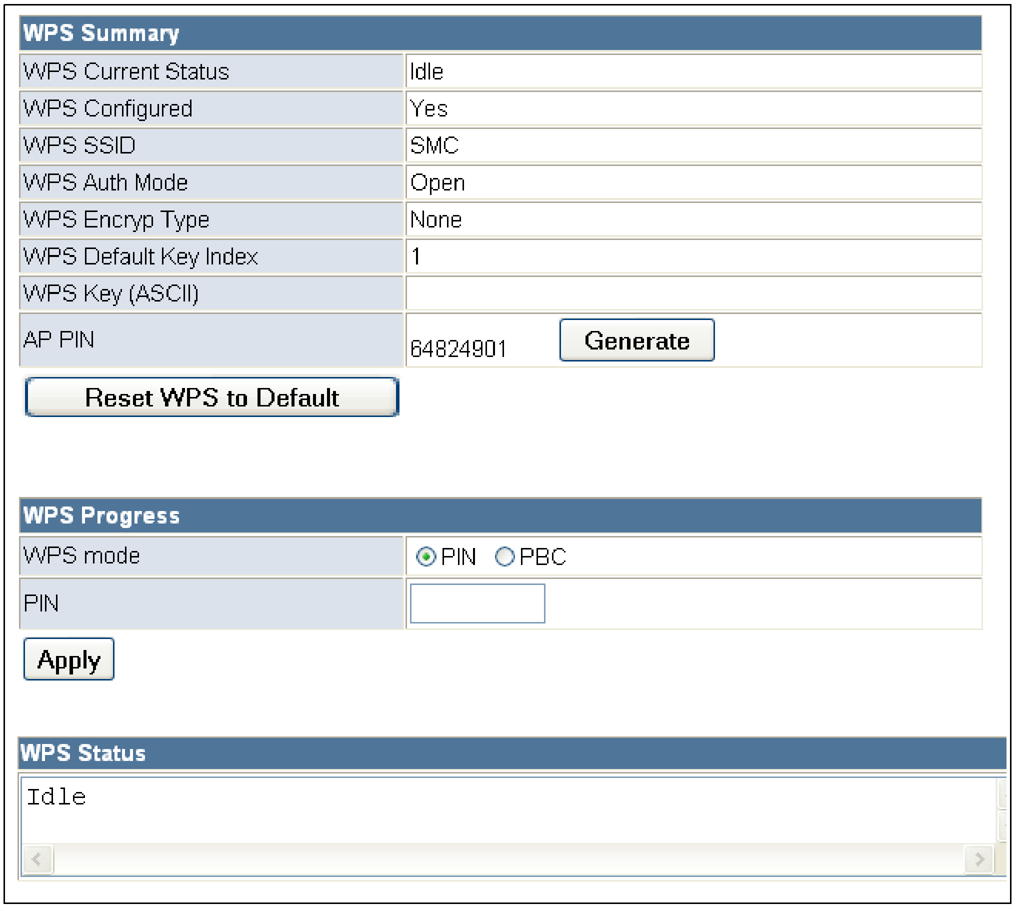
WPS Configuration

WPS	Disable

The following items are displayed on this page:

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

Figure 54: WPS Configuration



WPS Summary

WPS Current Status	Idle
WPS Configured	Yes
WPS SSID	SMC
WPS Auth Mode	Open
WPS Encryp Type	None
WPS Default Key Index	1
WPS Key (ASCII)	
AP PIN	64824901

WPS Progress

WPS mode	● PIN ○ PBC
PIN	

WPS Status

```
Idle
```

The following items are displayed on this page:

WPS Summary — Provides detailed WPS statistical information.

- **WPS Current Status** — Displays if there is currently any WPS traffic connecting to the Gateway. (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 Gateway. The default is exclusive for each unit. (Default: 64824901)
- **Reset WPS to Default** — Resets the WPS settings to factory default values.

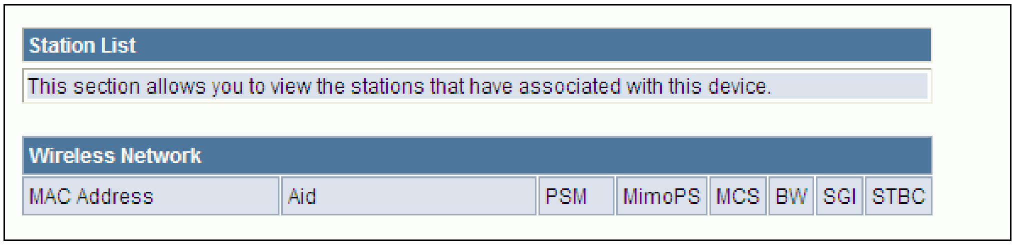
WPS Config — Configures WPS settings for the Gateway.

- **WPS Mode** — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:
  - **PIN**: The Gateway, 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 Gateway, 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 Gateway. 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 Gateway.

Figure 55: Station List



Station List

This section allows you to view the stations that have associated with this device.

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

8 Firewall Configuration

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

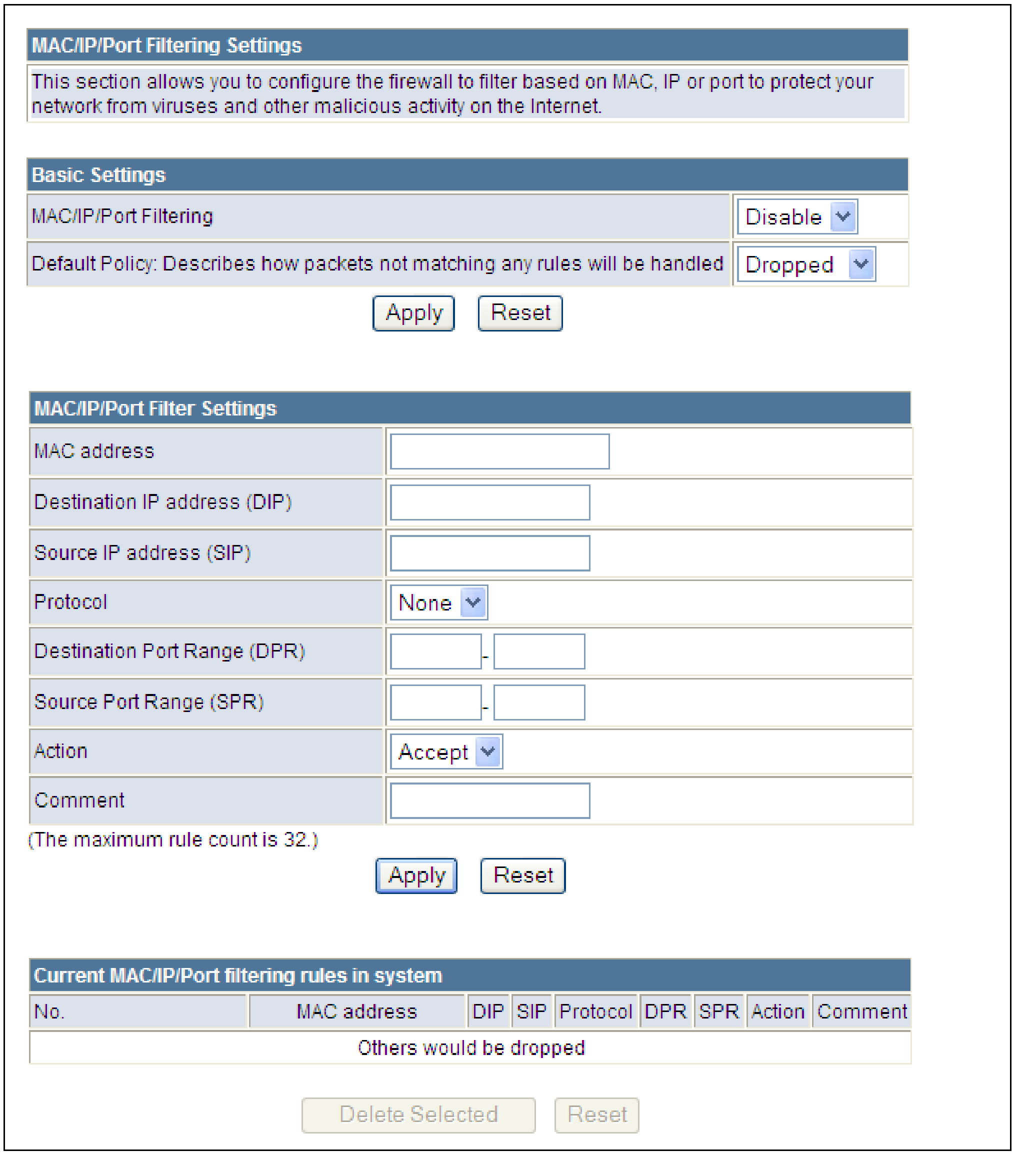
Firewall Configuration contains the following sections:

MAC/IP/Port Filtering

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 Gateway 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 56: MAC/IP/Port Filtering



MAC/IP/Port Filtering Settings

This section allows you to configure the firewall to filter based on MAC, IP or port to protect your network from viruses and other malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering	Disable
Default Policy: Describes how packets not matching any rules will be handled	Dropped

MAC/IP/Port Filter Settings

MAC address	
Destination IP address (DIP)	
Source IP address (SIP)	
Protocol	None
Destination Port Range (DPR)	-
Source Port Range (SPR)	-
Action	Accept
Comment	

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system

No.	MAC address	DIP	SIP	Protocol	DPR	SPR	Action	Comment
Others would be dropped								

The following items are displayed on this page:

- **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

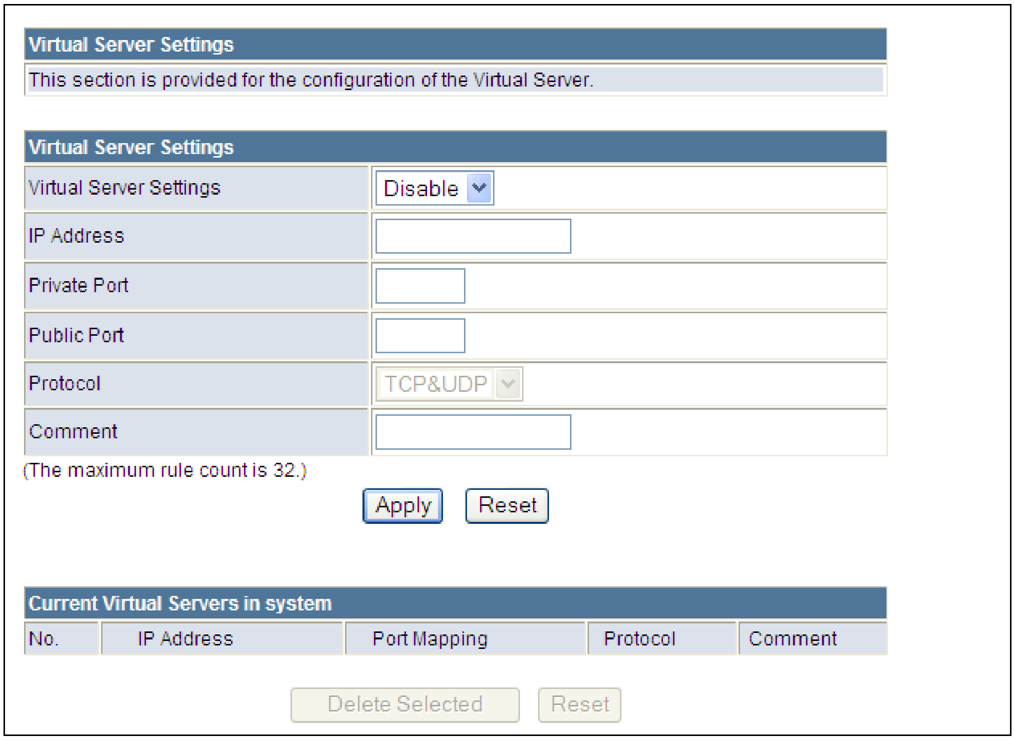
The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from the Gateway.

- **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 57: Virtual Server



Virtual Server Settings

This section is provided for the configuration of the Virtual Server.

Virtual Server Settings	
Virtual Server Settings	Disable
IP Address	
Private Port	
Public Port	
Protocol	TCP&UDP
Comment	

(The maximum rule count is 32.)

Current Virtual Servers in system

No.	IP Address	Port Mapping	Protocol	Comment

The following items are displayed on this page:

- **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

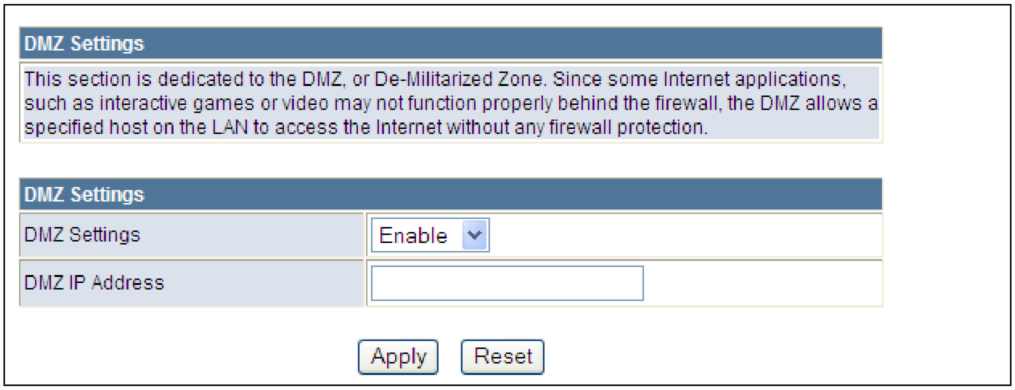
The Current Port Forwarding Table displays the entries that are allowed to forward packets through the Gateway’s firewall.

- **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 Gateway'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 58: DMZ



DMZ Settings

This section is dedicated to the DMZ, or De-Militarized Zone. Since some Internet applications, such as interactive games or video may not function properly behind the firewall, the DMZ allows a specified host on the LAN to access the Internet without any firewall protection.

DMZ Settings

DMZ Settings	Enable
DMZ IP Address	

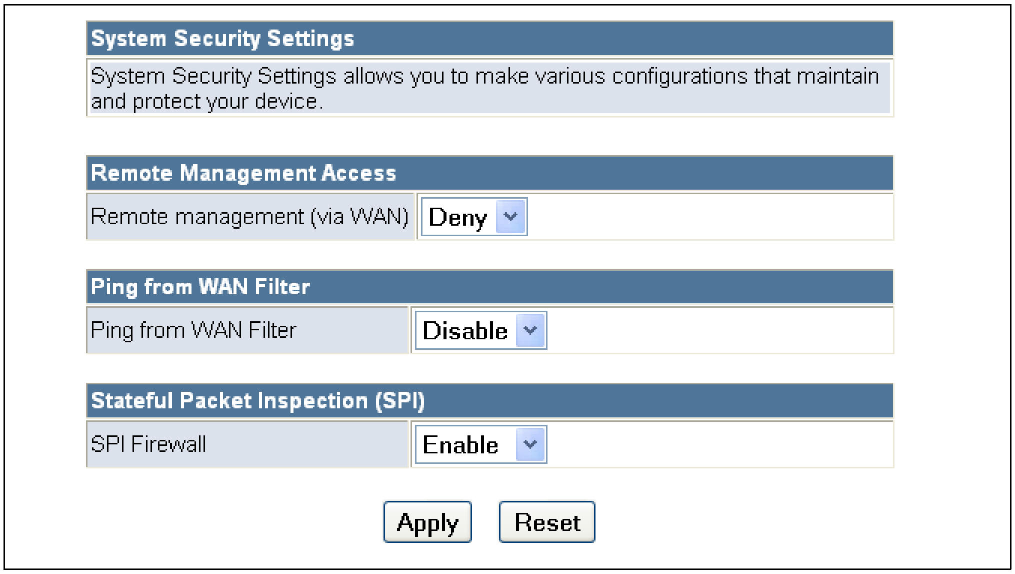
The following items are displayed on this page:

- **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 Gateway includes the facility to manage it from a remote location. The unit can also be sent a ping message from a remote location.

Figure 59: System Security



System Security Settings

System Security Settings allows you to make various configurations that maintain and protect your device.

Remote Management Access

Remote management (via WAN): Deny

Ping from WAN Filter

Ping from WAN Filter: Disable

Stateful Packet Inspection (SPI)

SPI Firewall: Enable

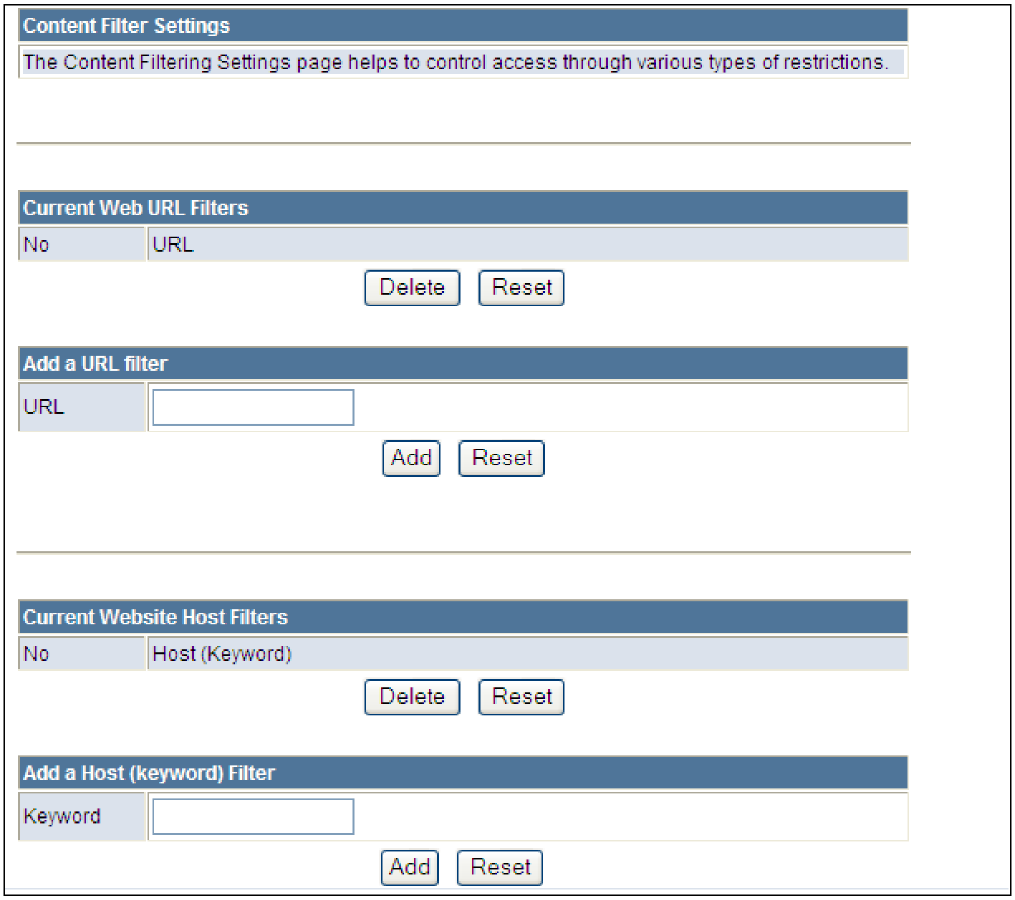
The following items are displayed on this page:

- **Remote Management** — Denies or allows management access to the Gateway through the WAN interface. (Default: Deny)
- **Ping from WAN Filter** — When enabled, the Gateway 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: Enable)

CONTENT FILTERING

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

Figure 60: Content Filtering



Content Filter Settings

The Content Filtering Settings page helps to control access through various types of restrictions.

Current Web URL Filters

No	URL

Add a URL filter

URL	

Current Website Host Filters

No	Host (Keyword)

Add a Host (keyword) Filter

Keyword	

The following items are displayed on this page:

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 Gateway 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 Gateway's Administration Settings menu provides the same configuration options in both Router 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.

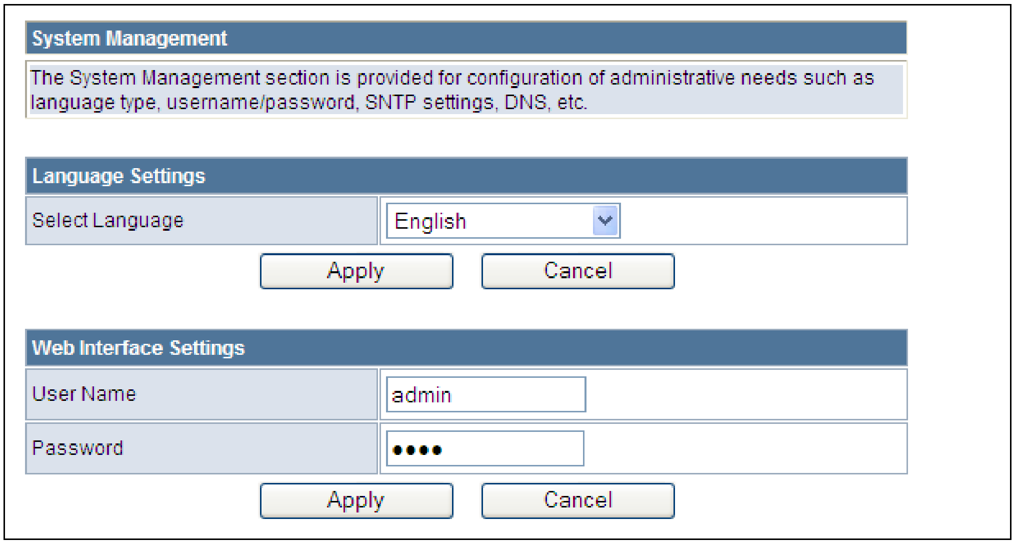
Administration Settings contains the following sections:

- "System Management" on page 102
- "Time Zone Settings" on page 102
- "DDNS Settings" on page 104
- "Firmware Upgrade" on page 105
- "Configuration Settings" on page 106
- "System Status" on page 107
- "Statistics" on page 109
- "System Log" on page 110
- "3G Budget Status" on page 111

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 61: System Management



System Management

The System Management section is provided for configuration of administrative needs such as language type, username/password, SNTP settings, DNS, etc.

Language Settings

Select Language	English

Web Interface Settings

User Name	admin
Password	••••

The following items are displayed in the first two sections on this page:

- **Language Settings** — You can change the language displayed in web interface. Select the language of your choice from the drop-down list, then click "Apply." (Options: English or 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 Gateway may be able to compromise the unit's security by entering the default values.

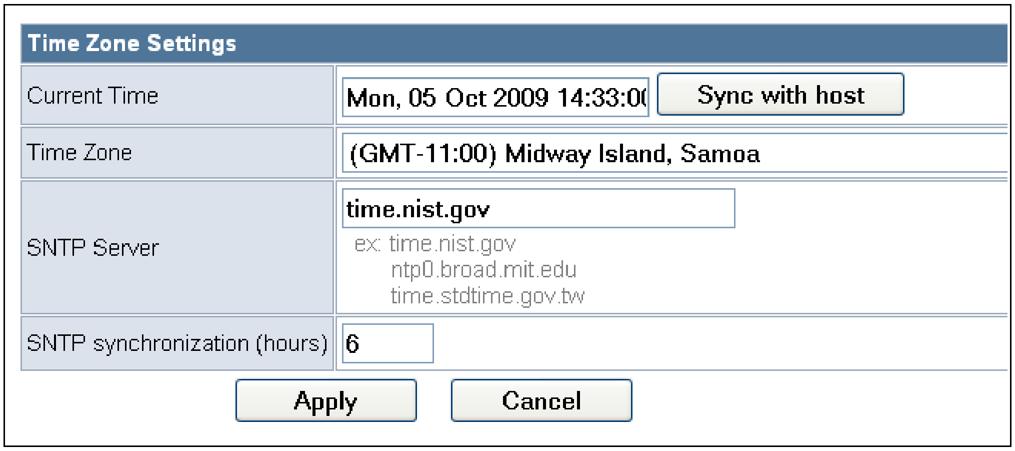
  - **User Name** — The name of the user. The default name for access to the unit is "admin." (Length: 3-16 characters, case sensitive)

  - **Password** — The password for management access. The default password preset for access to the unit is "smcadmin" (Length: 3-16 characters, case sensitive)

TIME ZONE 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 62: Time Zone Settings



Time Zone Settings

Current Time	Mon, 05 Oct 2009 14:33:0(Sync with host
Time Zone	(GMT-11:00) Midway Island, Samoa
SNTP Server	time.nist.gov ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
SNTP synchronization (hours)	6

The following items are displayed in this section on this page:

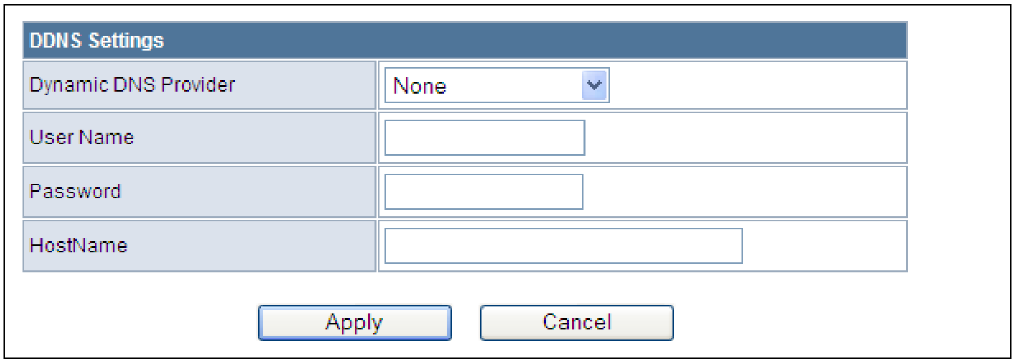
- **Current Time** — Displays the current system time on the unit.
- **Sync with host —** Updates the unit's time from the web management PC's system time.
- **Time Zone** — Specifies the time zone in relation to Greenwich Mean Time (GMT).
- **SNTP Server** — The IP address or URL of the NTP server to 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 Gateway 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 63: DDNS Settings (Router Mode)



DDNS Settings

Dynamic DNS Provider	None
User Name	
Password	
HostName	

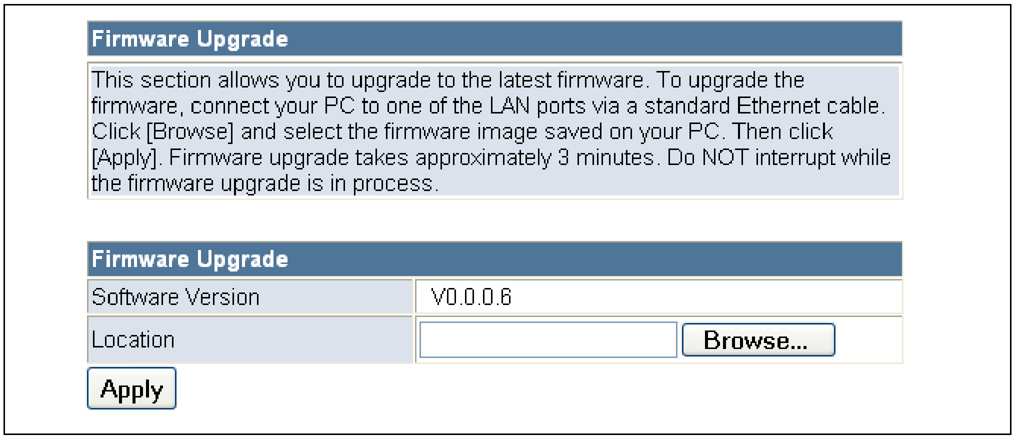
The following items are displayed in this section on this page:

- **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.

FIRMWARE UPGRADE

You can update the Gateway firmware by using the Firmware Update facility.

Figure 64: Firmware Upgrade



Firmware Upgrade

This section allows you to upgrade to the latest firmware. To upgrade the firmware, connect your PC to one of the LAN ports via a standard Ethernet cable. Click [Browse] and select the firmware image saved on your PC. Then click [Apply]. Firmware upgrade takes approximately 3 minutes. Do NOT interrupt while the firmware upgrade is in process.

Firmware Upgrade

Software Version	V0.0.0.6
Location	Browse...

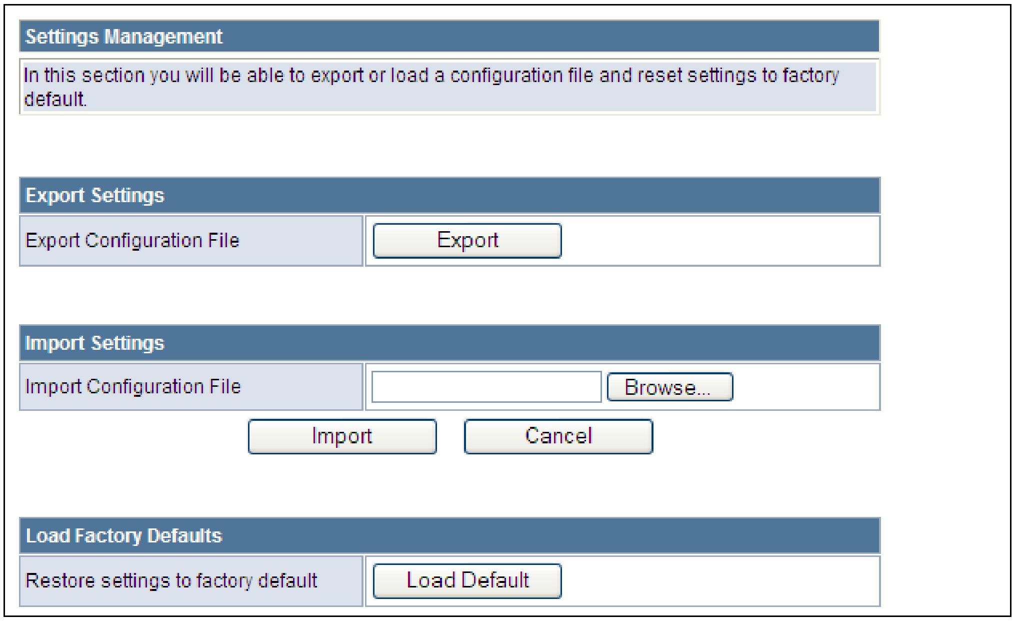
The following items are displayed on this page:

- **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.
  - **Software Version** — The current version number of the firmware.
  - **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 Gateway’s current configuration or restore a previously saved configuration back to the device.

Figure 65: Configuration Settings



Settings Management

In this section you will be able to export or load a configuration file and reset settings to factory default.

Export Settings

Export Configuration File	Export

Import Settings

Import Configuration File	Browse...

Load Factory Defaults

Restore settings to factory default	Load Default

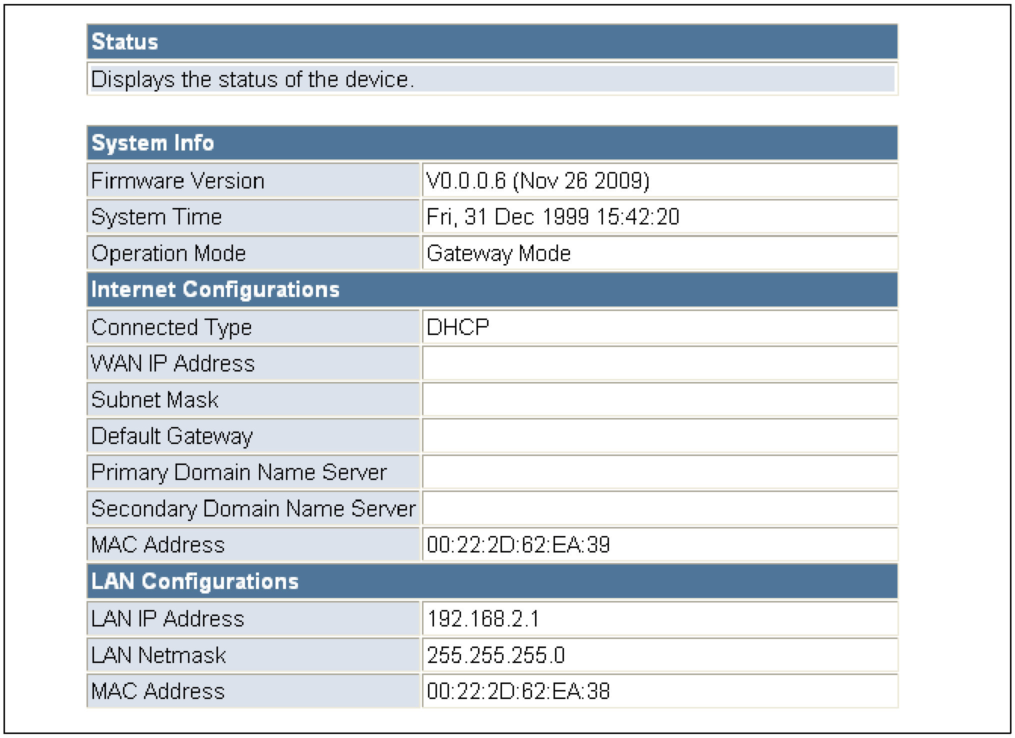
The following items are displayed on this page:

- **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 66: System Status (Router Mode)



Status

Displays the status of the device.

System Info	
Firmware Version	V0.0.0.6 (Nov 26 2009)
System Time	Fri, 31 Dec 1999 15:42:20
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

The following items are displayed on this page:

- **System Info** — Displays the basic system information in both Bridge and Router Modes.
  - **Firmware Version** — The version number of the current Gateway 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.
  - **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.

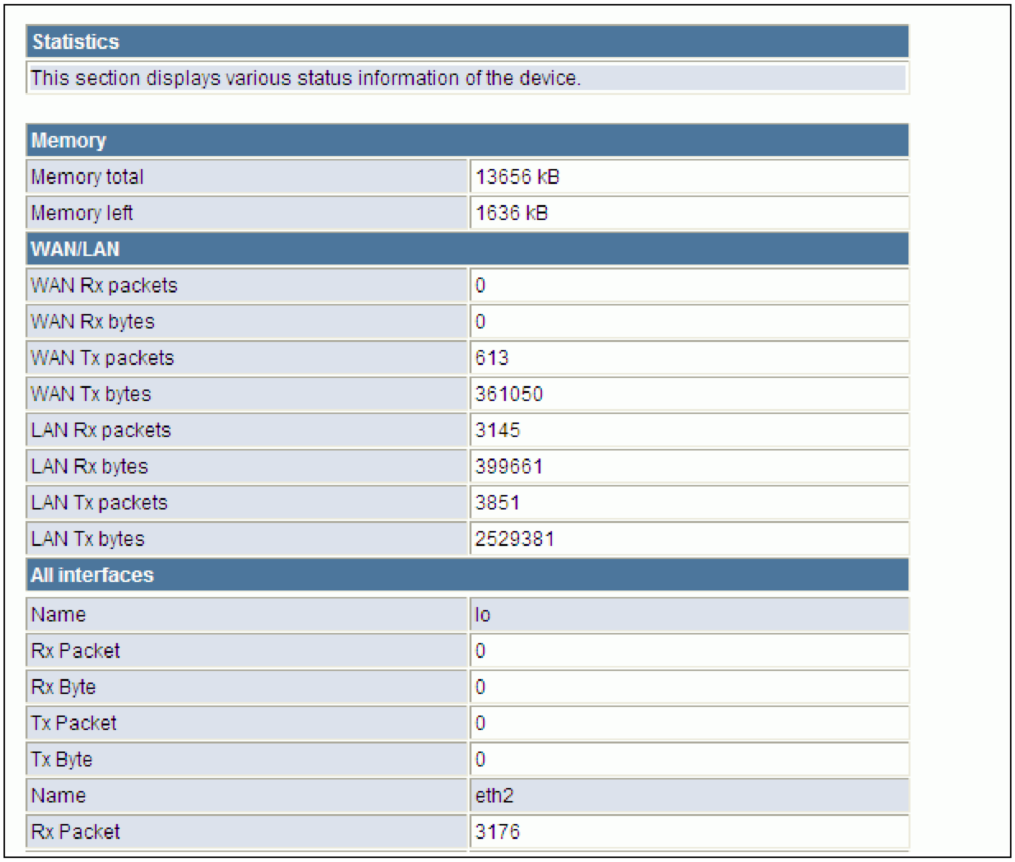
  - **Default Gateway** — The default gateway is the IP address of the router for the Gateway, which is used if the requested destination address is not on the local subnet.
  - **Primary DNS Server / Secondary DNS Server** — The IP address of Domain Name Servers. A DNS maps numerical IP addresses to domain 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 Gateway’s LAN ports.

- **Local Network** — Displays the basic LAN information.
  - **LAN IP Address** — The IP address configured on the Gateway.
  - **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 Gateway’s LAN ports.

STATISTICS

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

Figure 67: 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:

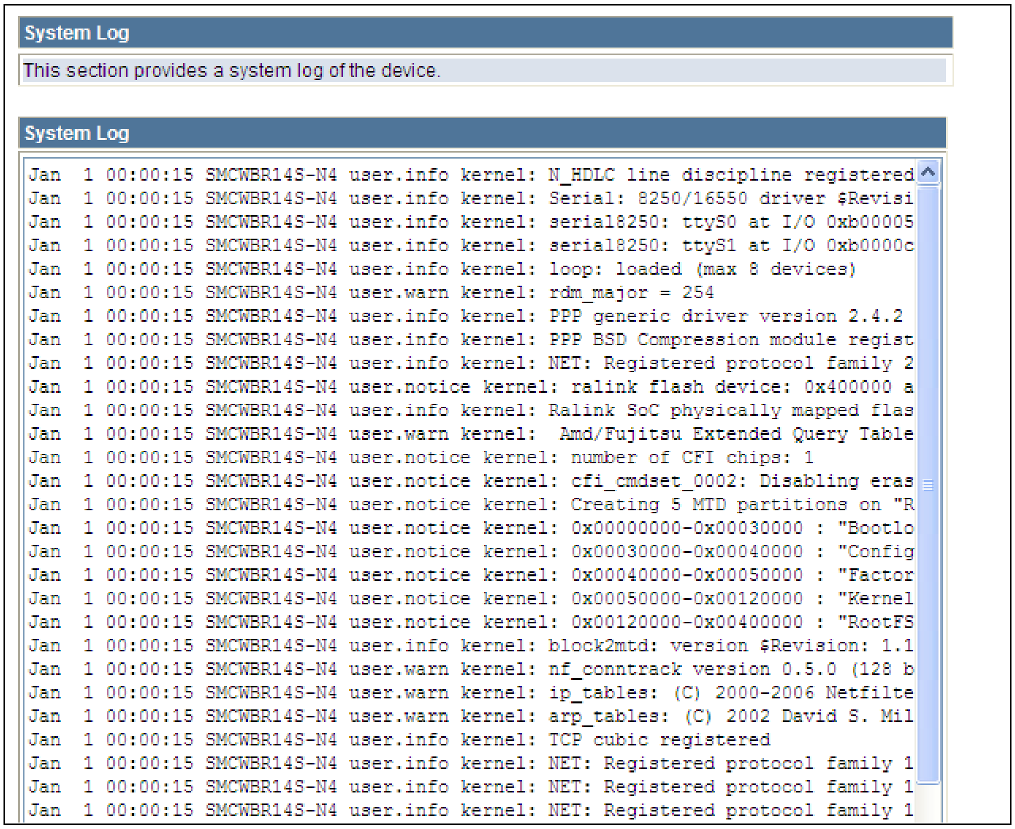
- **Memory total** — The total memory of this Gateway.
- **Memory left** — The available memory of this Gateway.
- **WAN/LAN/All Interfaces** — Displays the interface on which traffic is being monitored.
- **Rx packets** — Displays the total number of packets received by the specified interface.
- **Rx 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 Gateway 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 Gateway 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 Gateway's memory are erased when the device is rebooted.

Figure 68: System Log



System Log

This section provides a system log of the device.

System Log

```
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: N_HDLC line discipline registered
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: Serial: 8250/16550 driver $Revisi
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: serial8250: ttyS0 at I/O 0xb00005
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: serial8250: ttyS1 at I/O 0xb0000c
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: loop: loaded (max 8 devices)
Jan  1 00:00:15 SMCWBR14S-N4 user.warn kernel: rdm_major = 254
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: PPP generic driver version 2.4.2
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: PPP BSD Compression module regist
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: NET: Registered protocol family 2
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: ralink flash device: 0x400000 a
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: Ralink SoC physically mapped flas
Jan  1 00:00:15 SMCWBR14S-N4 user.warn kernel:  Amd/Fujitsu Extended Query Table
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: number of CFI chips: 1
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: cfi_cmdset_0002: Disabling eras
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: Creating 5 MTD partitions on "R
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: 0x00000000-0x00030000 : "Bootlo
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: 0x00030000-0x00040000 : "Config
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: 0x00040000-0x00050000 : "Factor
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: 0x00050000-0x00120000 : "Kernel
Jan  1 00:00:15 SMCWBR14S-N4 user.notice kernel: 0x00120000-0x00400000 : "RootFS
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: block2mtd: version $Revision: 1.1
Jan  1 00:00:15 SMCWBR14S-N4 user.warn kernel: nf_conntrack version 0.5.0 (128 b
Jan  1 00:00:15 SMCWBR14S-N4 user.warn kernel: ip_tables: (C) 2000-2006 Netfilte
Jan  1 00:00:15 SMCWBR14S-N4 user.warn kernel: arp_tables: (C) 2002 David S. Mil
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: TCP cubic registered
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: NET: Registered protocol family 1
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: NET: Registered protocol family 1
Jan  1 00:00:15 SMCWBR14S-N4 user.info kernel: NET: Registered protocol family 1
```

The following items are displayed on this page:

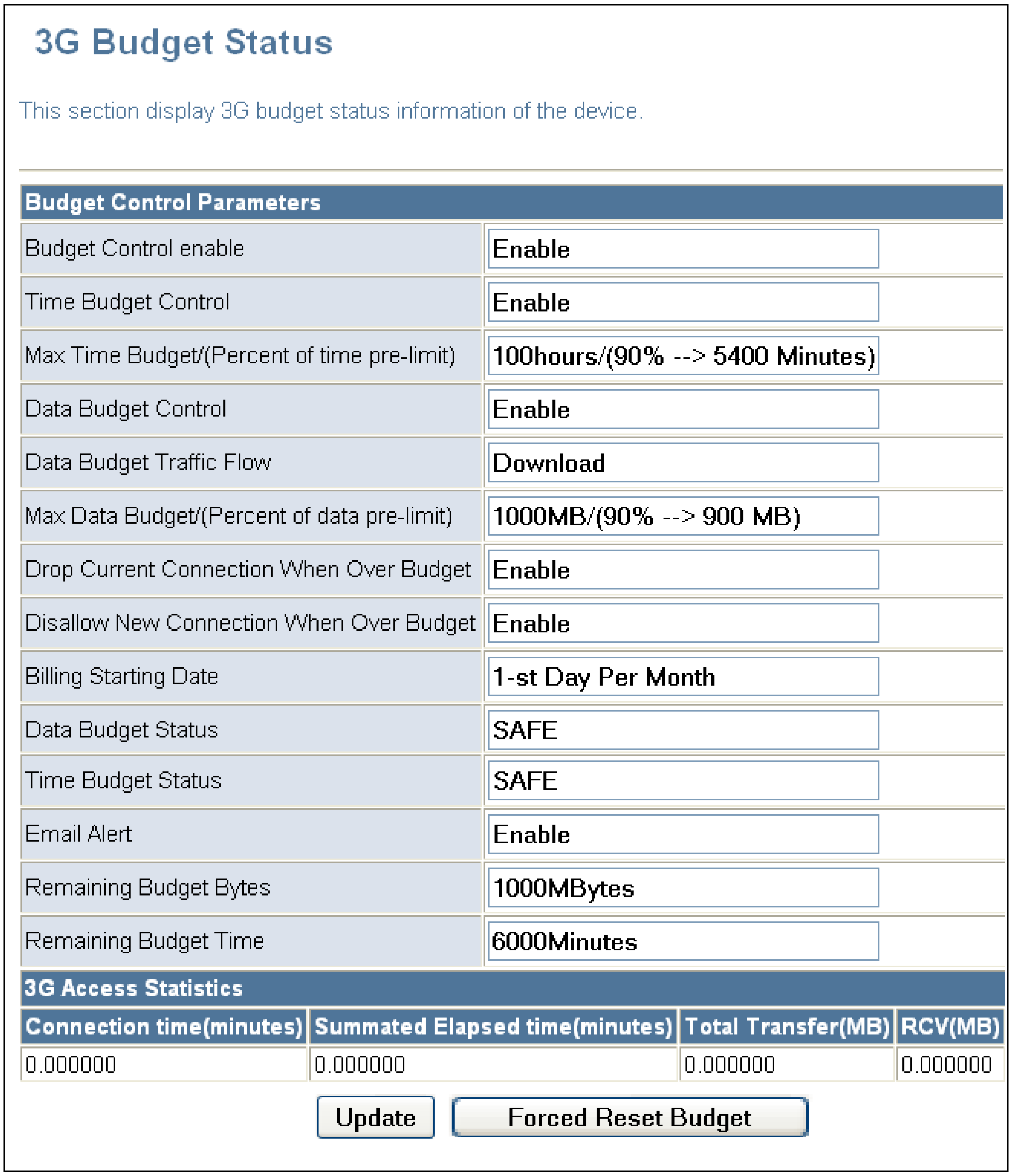
- **System Log** — Displays the latest log messages in chronological order, from the newest to the oldest.
- **Refresh** — Sends a request to add the latest entries to the System Log Table.
- **Clear** — Removes the current system log messages from the System Log Table.

3G BUDGET STATUS

The 3G Budget Status page displays the current 3G budget status information. The displayed settings are for information only and are not configurable on this page.

Parameters on this page are only visible when budget control has been set for the 3G WAN connection.

Figure 69: 3G Budget Status



3G Budget Status

This section display 3G budget status information of the device.

Budget Control Parameters	
Budget Control enable	Enable
Time Budget Control	Enable
Max Time Budget/(Percent of time pre-limit)	100hours/(90% --> 5400 Minutes)
Data Budget Control	Enable
Data Budget Traffic Flow	Download
Max Data Budget/(Percent of data pre-limit)	1000MB/(90% --> 900 MB)
Drop Current Connection When Over Budget	Enable
Disallow New Connection When Over Budget	Enable
Billing Starting Date	1-st Day Per Month
Data Budget Status	SAFE
Time Budget Status	SAFE
Email Alert	Enable
Remaining Budget Bytes	1000MBytes
Remaining Budget Time	6000Minutes

3G Access Statistics

Connection time(minutes)	Summated Elapsed time(minutes)	Total Transfer(MB)	RCV(MB)
0.000000	0.000000	0.000000	0.000000

The following items are displayed on this page:

- **Budget Control** — Displays the current budget control status.

- **Tme Budget Control** — Displays the currect time budget control status.
- **Max Time Budget/(Percent of Time Pre-limit)** — Displays the configured monthly time budget (in hours), and the percentage of the budget (in minutes) at which E-mail alerts are triggered (if enabled).
- **Data Budget Control** — Displays the currect data budget control status.
- **Data Budget Traffic Flow** — Displays if the data budget is set for download, upload, or download and upload traffic.
- **Max Data Budget/(Percent of Data Pre-limit)** — Displays the configured monthly data budget (in MBytes), and the percentage of the budget at which E-mail alerts are triggered (if enabled).
- **Drop Current Connection When Over Budget** — Displays the status of this over-budget action.
- **Disallow New Connection When Over Budget** — Displays the status of this over-budget action.
- **Billing Starting Date** — Displays the day of the month on which the time/data budget counters are reset.
- **Data Budget Status** — The current data budget status. (SAFE, REACH Pre-Limit, Over)
- **Time Budget Status** — The current time budget status. (SAFE, REACH Pre-Limit, Over)
- **Email Alert** — Displays the status of E-mail Alert.
- **Remaining Budget Bytes** — The remaining amount of the configured data budget.
- **Remaining Budget Time** — The remaining amount of the configured time budget.
- **3G Access Statistics** — Displays the access statistics of the 3G link.
    - **Connection time (min)** — The current connection time.
    - **Summated Elapsed time (min)** — The total summated elapsed time counts from the billing date.
    - **Total Transfer (MB)** — The total amount of the transferred data (includes download and upload).
    - **RCV (MB)** — The total current download data.
    - **TX (MB)** — The total current upload data.

SECTION III

APPENDICES

This section provides additional information and includes these items:

- "Troubleshooting" on page 115
- "Hardware Specifications" on page 117
- "Cables and Pinouts" on page 119

A TROUBLESHOOTING

DIAGNOSING LED INDICATORS

Table 4: LED Indicators

Symptom	Action
Power and LAN LEDs are off	◆ The AC power adapter may be disconnected. Check connections between the Gateway, the power adapter, and the wall outlet.
WLAN LED is off	◆ The Gateway radio has been disabled through it’s web management interface. Access the management interface using a web browser to enable the radio.
LAN LED is off (when port connected)	◆ Verify that the Gateway is powered on. ◆ Be sure cables are plugged into both the Gateway 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 the following items:

- 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 cannot be configured using a web browser:

   - Be sure to have configured the Gateway with a valid IP address, subnet mask and default gateway.

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

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

2. If you forgot or lost the password:

   - Set the Gateway 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 is still not functioning properly, take any of these steps:

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

B

Hardware Specifications

Port Interfaces	WAN: 10/100BASE-TX port, RJ-45 connector, auto MDI/X (100-ohm, UTP cable; Category 5 or better) LAN: 10/100BASE-TX port, RJ-45 connector, auto MDI/X (100-ohm, UTP cable; Category 5 or better)
AC Power Adapter	Asian Power Devices Inc. / APD: WA-12112FG, WA-12112R Sunny Electronics Corp.: SYS1381-1212-W2E, SYS1381-1212-W3U, SYS1381-1212-W2 Input: 100~240 VAC, 50/60 Hz Output: 12 VDC, 1 A
LED Indicators	Power, WLAN (Wireless Local Area Network), WAN (Wide Area Network), LAN (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)
Physical Size	93 x 70 x 26 mm
Weight	78 g (2.75 oz)
Frequency range	FCC/IC/NCC: 2412MHz ~ 2462MHz CE, AS/NZS: 2412 MHz ~ 2472MHz
Modulation Type	CCK, DQPSK, DBPSK for DSSS 64QAM, 16QAM, QPSK, BPSK for OFDM

DATA RATE	802.11b: 11 / 5.5 / 2 / 1Mbps 802.11g: 54/48/36/24/18/12/9/6 Mbps Draft 802.11n (20MHz, 800ns GI): 65/58.5/52/39/26/19.5/13/6.5 Mbps Draft 802.11n (40MHz, 800ns GI): 135/121.5/108/81/54/40.5/27/13.5 Mbps Draft 802.11n (20MHz, 400ns GI): 72.2/65/57.8/43.3/28.9/21.7/14.4/7.2 Mbps Draft 802.11n (40MHz, 400ns GI): 150/135/120/90/60/45/30/15 Mbps
RF OUTPUT POWER	22.5 +/- 2dBm
RADIO	FCC Part 15C (Section 15.247) EN 301 489-1 V1.8.1 (2008-04) EN 301 489-17 V1.3.2 (2008-04) LP0002 RSS-210 AS/NZS 4268
EMC	FCC Part 15B ICES-003 EN 55022:2006 + A1:2007 EN 55024:1998 + A1:2001 + A2:2003
SAR	FCC IEEE C95.1 EN 50385 (2002)
SAFETY	EN 60950-1 (2006) NRTL -TUV(cUL)
ENVIRONMENTAL	ETSI EN 300 019-2-1 Class 1.2 (Storage) ETSI EN 300 019-2-2 Class 2.3 (Packaged) ETSI EN 300 019-2-3 Class 3.2 (Operating)

C

Cables and Pinouts

Twisted-Pair Cable Assignments

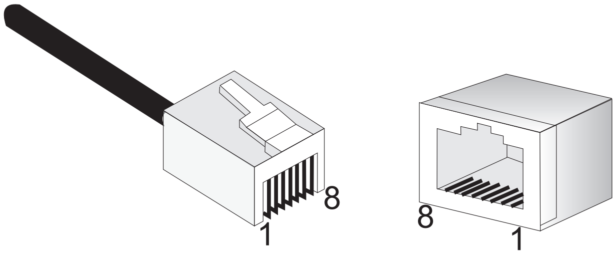
For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. For 1000BASE-T connections the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, 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 70: 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 ports on the Gateway support automatic MDI/MDI-X operation, so you can use straight-through or crossover cables for all network connections to PCs, switches, or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable.

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

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

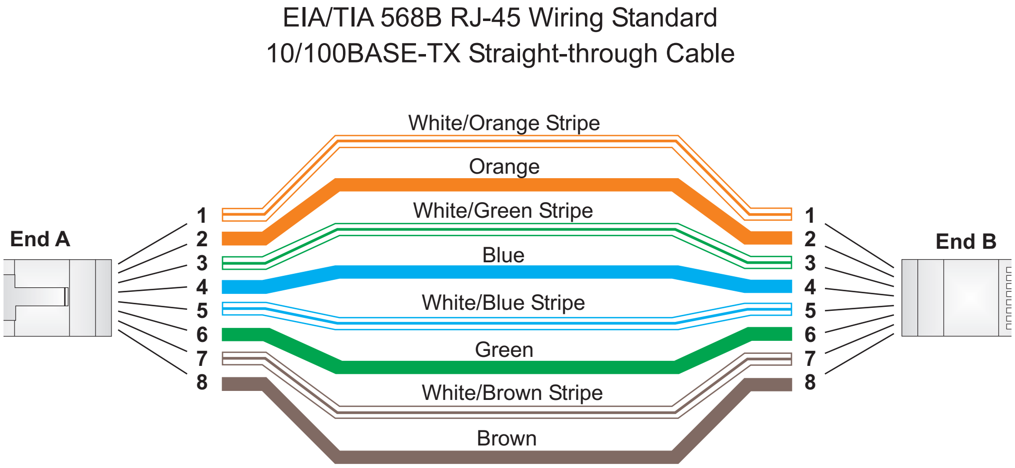
[a] The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

STRAIGHT-THROUGH WIRING

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on this 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 71: Straight-through Wiring

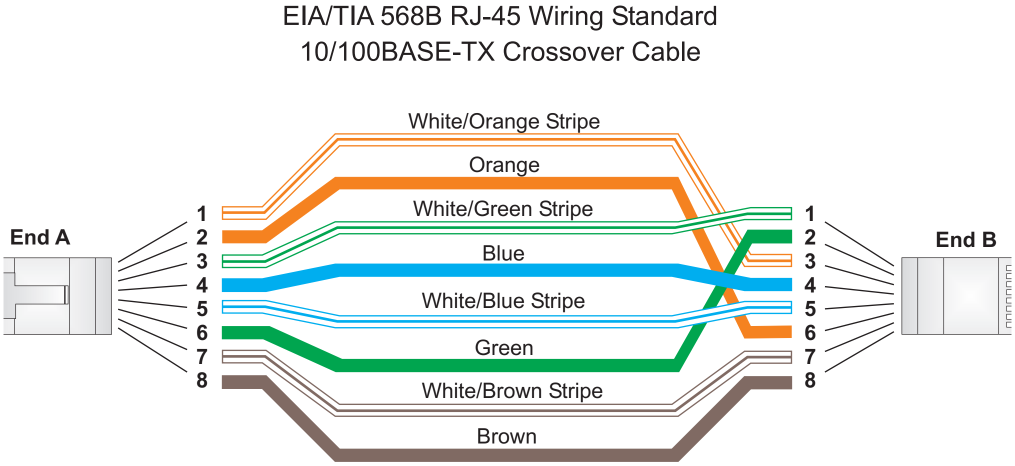


CROSSOVER WIRING

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 72: 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

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