SMC®
Networks

EliteConnect™

2.4GHz 802.11g Wireless Hotspot Gateway

User Guide

SMCWHSG44-G

Copyright

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

Trademarks

SMC is a registered trademark; and EliteConnect is a trademark of SMC Networks. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product. The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:
http://www.smc.com/index.cfm?action=customer_service_warranty.
All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product. Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968.

Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD. LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

Warranty in EMEA and Asia Pacific:
For details regarding warranty in EMEA and Asia Pacific, please contact your country sales representative. All contact information can be found at www.smc.com

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 radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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 & your body.

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.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of Industry Canada.

Cet appareil numerique respecte les limites de bruits radioelectriques applicables aux appareils umeriques de Classe B prescrites dans la norme sur le material brouilleur: “Appareils Numeriques,” NMB-003 edictee par l'Industrie.

EC Conformance Declaration
SMC contact for these products in Europe is:
SMC Networks Spain S.L.,
Edificio Conata II,
Calle Fructuós Gelabert 6-8, 2o, 4a,
08970 - Sant Joan Despí,
Barcelona, Spain.

Signed and dated Copy of the Declaration of Conformity can be found in the product section of www.smc-europe.com

This RF product complies with R&TTE Directive 99/5/EC. For the evaluation of the compliance with this Directive, the following standards were applied:

- Electromagnetic compatibility and radio spectrum matters (ERM)
  EN300 328-1 (2001-12)
  EN300 328-2 (2001-12)
- Electromagnetic Compatibility (EMC) Standard for radio equipment and services
  EN301 489-1 V1.4.1 : 2002
  EN301 489-17 V1.2.1 : 2002
- Safety Test
  EN60950-1 : 2001

The conformity assesment procedure referred to in Article 10 and detailed in Annex IV of the Directive 1999/5/EC has been followed related to Articles 3.2 with the involvement of the following Notified Body:

BTS-ETZ Certification GmBH, Storkkower Strasser 38c, D-15562, Reichenwalde B, Berlin, Germany

Identification Mark

CE0681(!)

Countries of Operation & Conditions of Use in the European Community
This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below:
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 requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device.
- 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 system. 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.

- This device may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below.
- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7

Notified Countries for intended use:

Austria, Belgium, Denmark, Finland, France, Germany, Italy, Luxembourg, Netherlands, Norway, Spain, Sweden Switzerland, United Kingdom, Portugal, Greece, Ireland, Iceland

Safety Compliance

Power Cord Safety

Please read the following safety information carefully before installing the switch:
WARNING: Installation and removal of the unit must be carried out by qualified personnel only.

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.
- Do not connect the unit to an A.C. outlet (power supply) without an earth (ground) connection.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

France and Peru only
This unit cannot be powered from IT supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to earth (ground).
† Impédance à la terre

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified.
	The minimum specifications for the flexible cord are: - No. 18 AWG - not longer than 2 meters, or 16 AWG. - Type SV or SJ - 3-conductor
	The cord set must have a rated current capacity of at least 10 A
	The attachment plug must be an earth-grounding type with NEMA 5-15P (15 A, 125 V) or NEMA 6-15P (15 A, 250 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362.
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
Europe	The supply plug must comply with CEE7/7 ("SCHUKO").
	The mains cord must be <HAR> or <BASEC> marked and be of type HO3VVF3GO.75 (minimum).
	IEC-320 receptacle.

Veuillez lire à fond l'information de la sécurité suivante avant d'installer le Switch:

AVERTISSEMENT: L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.

- Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).
- Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes internationales de sécurité.
- Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN 60320/IEC 320.

- La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.
- L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.

France et Pérou uniquement:
Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

Cordon électrique- Il doit être agréé dans le pays d'utilisation	
Etats-Unis et Canada:	Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA.
	Les spe'cifications minimales pour un cable flexible sont AWG No. 18, ouAWG No. 16 pour un cable de longueur infe'rieure a` 2 me'tres. - type SV ou SJ - 3 conducteurs
	Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A.
	La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V).
Danemark:	La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.

Cordon électrique- Il doit être agréé dans le pays d'utilisation	
Suisse:	La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 (“SCHUKO”)
	LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum).

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüs-sigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlu βsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daβ diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluβ an das Stromnetz die Anschluβwerte.
9. Verlegen Sie die Netzanschluβleitung so, daβ niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sind beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, daβ die Stromversorgung dieses Gerätes nach der EN 60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8V, 50-60Hz nicht über oder unterschreiten sowie den minimalen Strom von 1A nicht unterschreiten.

Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

<table>
<tr><th colspan="2">Stromkabel. <b>Dies muss von dem Land, in dem es be-nutzt wird geprüft werden:</b></th></tr>
<tr><td>U.S.A und Canada</td><td>Der Cord muß das UL gepruft und war das CSA beglaubigt.</td></tr>
<tr><td></td><td>Das Minimum spezifikation fur der Cord sind:</td></tr>
<tr><td></td><td>- Nu. 18 AWG - nicht mehr als 2 meter, oder 16 AWG.</td></tr>
<tr><td></td><td>- Der typ SV oder SJ</td></tr>
<tr><td></td><td>- 3-Leiter</td></tr>
<tr><td></td><td>Der Cord muß haben eine strombelast-barkeit aus</td></tr>
<tr><td></td><td>wenigstens 10 A</td></tr>
<tr><td></td><td>Dieser Stromstecker muß hat einer erdschluss mit der typ NEMA 5-15P (15A, 125V) oder NEMA 6-15P (15A, 250V) konfiguration.</td></tr>
<tr><td>Danemark</td><td>Dieser Stromstecker muß die ebene 107-2-D1, der standard DK2-1a oder DK2-5a Bestimmungen einhalten.</td></tr>
<tr><td>Schweiz</td><td>Dieser Stromstecker muß die SEV/ASE 1011Bestimmungen einhalten.</td></tr>
<tr><td>Europe</td><td>Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen.</td></tr>
<tr><td></td><td>Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO").</td></tr>
</table>

Table of Contents

1. Introduction

The EliteConnect 2.4GHz 802.11g Wireless Hotspot Gateway (**SMCWHSG44-G**) enables VARs, WISPs and System Integrators to install secure, easy to manage Hotspots as a one-box solution. The features of the SMCWHSG44-G support applications that are well suited for Hotspot environments such as coffee shops and hotel lobbies as well as small to midsized transportation hubs such as harbors, regional airports, train stations or bus stations where Internet Access can be an added value for guest-services.

The **SMCWHSG44-G** Wireless Hotspot Gateway provides up to 4 DSL/CATV connections, so it can support out-bound load-balancing and bandwidth aggregation. The multiple WAN connections provide fail-over and connection back-up capability to guarantee 'always-on-line' connections.

AP/WDS: The **SMCWHSG44-G** comes with a built-in 2.4GHz 802.11g 54Mbps Access Point. WDS (Wireless Distribution System) provides a standard static bridging function to extend wireless coverage within a LAN or to join LAN segments that are physically separated(e.g., two or more buildings). Up to 6 WDS bridge links work with AP function simultaneously.

Radius and Local Authentication: For wireless service, **SMCWHSG44-G** provides 2 kinds of user authentication methods: 802.1x/RADIUS and Local Authentication Database. Authentication, Authorization and Accounting (AAA) services are supported via 802.1x/RADIUS client and server devices, while the Local Authentication Database provides more flexible authentication procedure that allows non-802.1x wireless users to be authenticated. **SMCWHSG44-G** also provides the capability to allow operators or venue owners to display their Web or advertisement contents during the user login period. For some unauthorized wireless users who want to access the Internet, the venue owners can also limit such users to access certain levels of Internet resources.

Ticket Printing: The **SMCWHSG44-G** Hotspot Gateway supports an external ticket printer/keypad, so a Hotspot Venue can print a ticket that shows the clients available access time, price and a username and password to log-on to the Internet. SMC provides the Mini-POS Ticket Printer (SMCWHS-POS - sold separately outside the US and Canada) for ticket printing and device control.

POE: For environments where power outlets are difficult to access due to location or distance, the SMCWHSG44-G supports 802.11af compliant Power over Ethernet. With the application of the SMCPWR-INJ3 Power Injector, (sold separately) the Wireless Hotspot Gateway can be powered via CAT 5 Ethernet cable.

Detachable Antenna: The flexible R-SMA detachable antennas can be replaced with high-gain directional/omni-directional antennas to increase wireless signal range and coverage.

1.1. Overview

1.2. Features

- **User Authentication, Authorization, and Accounting (AAA)**
  - **Web redirection** - When an unauthenticated wireless user is trying to access a Web page, he/she is redirected to a logon page for entering the user name and password. Then, the user credential information is sent to a back-end RADIUS server for authentication or via the Local Authentication Database.
    - **Local pages or external pages** - The SMCWHSG44-G can be configured to use log-on, log-off, authentication success, and authentication failure pages, which are stored internally or stored in an external Web server maintained by the WISP. The contents of the local authentication pages can be customized.
    - **Advertisement links** - The log-off authentication page can be configured to show a sequence of advertisement banners.
    - **Unrestricted clients** - Client computers with specific IP addresses or MAC ad-dresses can bypass the Web redirection-based access control.
    - Walled garden. Some specific URLs can be accessed without authentication. These URLs can be exploited by WISPs or Hotspot Venues for advertisement purposes.
  - **IEEE 802.1x** - If a wireless client computer supports IEEE 802.1x Port-Based Network Access Control, the user of the computer can be authenticated by the Wireless Hotspot Gateway and wireless data can be encrypted by 802.1x EAP authentication method combined with WEP encryption.
  - **RADIUS client** - The SMCWHSG44-G communicates with a back-end RADIUS server for wireless user authentication, authorization, and accounting. Authentication methods, including EAP-MD5, EAP-TLS/EAP-TTLS, PAP, and CHAP are supported.
  - **Internal Database** - The Wireless Hotspot Gateway also supports an Internal Database of users so that you do not have to add an additional Radius Server. The Internal Database supports up to 2,000 user accounts.
    - **Robustness** - To enhance AAA integrity, the Wireless Hotspot Gateway can be configured to notify the RADIUS server after it reboots.
    - **Authenticated users** - Shows the status and statistics of every authenticated user. And an authenticated user can be terminated at any time for management purposes.
    - **Authentication session control** - Several mechanisms are provided for the network administrator to control user authentication session lifetimes.
- **IEEE 802.11b/g Compliant**
  - **Wireless Operation**
    - **Access Point** - The AP enables IEEE 802.11 Stations (STAs) to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two APs.

- **64-bit and 128-bit WEP (Wired Equivalent Privacy)** - For authentication and data encryption.
- **Enable/Disable SSID broadcast** - The user can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcast functionality is disabled, a client computer cannot associate with the wireless AP with an "any" network name (SSID, Service Set ID); the correct SSID has to be specified on client computers.
- **MAC-address-based control** - Blocks unauthorized wireless client computers based on MAC (Media Access Control) addresses.
- **Repeater** - A wireless AP can communicate with other wireless APs via WDS (Wireless Distribution System). Therefore, the wireless AP can wirelessly forward packets from wireless clients to another wireless AP, and then the later wireless AP forwards the packets to the Ethernet network.
- **Wireless client isolation** - Wireless-to-wireless traffic can be blocked so that the wireless clients cannot see each other. This capability can be used in Hotspot applications to prevent wireless hackers from attacking other wireless user´s computers.
- **Transmit power control** - Transmit power of the wireless AP's RF module can be adjusted to change RF coverage of the wireless AP.
- **Associated wireless clients** - Shows the status of every wireless client that is associated with the built in wireless AP.
- **Replaceable antenna** - The factory-mounted antenna can be replaced with high-gain antennas for extending range or increasing wireless coverage to a particular area.

- **Internet Connection Sharing**
  - **DNS proxy** - The SMCWHSG44-G can forward DNS (Domain Name System) requests from client computers to DNS servers on the Internet. And DNS responses from the DNS servers can be forwarded back to the client computers.
    - **Static DNS mappings** - The network administrator can specify static FQDN (Fully Qualified Domain Name) to IP address mappings. Therefore, a host on the internal network can access a server also on the intranet by a registered FQDN.
  - **DHCP server** - The SMCWHSG44-G can automatically assign IP addresses to client computers by DHCP (Dynamic Host Configuration Protocol).
    - **Static DHCP mapping capability** - The network administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.
    - **Current DHCP mappings** - Shows which IP address is assigned to which host identified by a MAC address.
  - **NAT Features** - Client computers share a public IP address provided by an ISP (Internet Service Provider) by NAT (Network Address Translation). Our NAT server functionality supports the following:

  - **Virtual server** - Exposing servers on the intranet to the Internet.
  - **PPTP, IPSec, and L2TP pass-through** - Passing VPN (Virtual Private Network) packets through the intranet-Internet boundary. PPTP means Point-to-Point Tunneling Protocol, IPSec means IP Security, and L2TP means Layer 2 Tunneling Protocol.
  - **DMZ (DeMilitarized Zone)** - All unrecognized IP packets from the Internet can be forwarded to a specific computer on the intranet.
  - **MSN Messenger support** - Supporting Microsoft MSN Messenger for chat, file transfer, and real-time communication applications.
  - Session monitoring. Latest 50 incoming sessions and 50 outgoing sessions are shown for monitoring user traffic.
- **DSL/Cable Modem Support** - Supporting dynamic IP address assignment by PPPoE (Point-to-Point Protocol over Ethernet) or DHCP and static IP address assignment.
  - **Multiple DSL/Cable connections support** - Supporting up to 4 DSL/cable-based In-ternet connections. All outgoing traffic load from the internal network is shared among the multiple Internet connections, so that total outgoing throughput is increased.
  - **Load Balancing** - The SMCWHSG44-G provides multiple WAN port Load Balancing mechanism for balancing the incoming data traffic between every enabled WAN port. The balancing mechanism can also be defined by Port or IP range policy.
- **Zero Client Reconfiguration** - The SMCWHSG44-G provides 'Zero Client Reconfiguration' function to allow wireless clients that associate to the SMCWHSG44-G the ability to not have to change any network setting.
- **Network Security**
  - **Packet address and port filtering** - Filtering outgoing packets based on IP address and port number. (Incoming packet filtering is performed by NAT.)
  - **URL filtering** - Preventing client users from accessing defined Web sites. The HTTP (Hyper Text Transfer Protocol) traffic to the specified Web sites identified by URLs (Universal Resource Locators) is blocked.
  - **WAN ICMP request blocking** - Some DoS (Denial of Service) attacks are based on ICMP requests with large payloads. Such kind of attacks can be blocked.
  - **Stateful Packet Inspection (SPI)** - Analyzing incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile.
  - **Wireless-to-Ethernet-LAN traffic blocking capability** - Traffic between the wireless interface and the Ethernet LAN interface can be blocked.
- **Configurable MAC Address of the Ethernet WAN Interface** - Some ADSL modems work only with Ethernet cards provided by the ISP. If SMCWHSG44-G is used in such an environment, the MAC address of the WAN interface of the Router has to be changed to the MAC address of the ISP-provided Ethernet network card.

- **SNTP** - Support for system time by SNTP (Simple Network Time Protocol).
- **Dynamic DNS** - Support for dynamic DNS services provided by dyndns.org and no-ip.com, so that the SMCWHSG44-G can be associated with a domain name even if it obtains an IP address dynamically by PPP, PPPoE or DHCP.
- **LAN Device Management** - The Wireless Hotspot Gateway can pass management requests from the Internet through its built-in NAT server to devices on the private network. As a result, network devices (such as access points) behind the NAT server can be managed from the Internet. In this way, the Wireless Hotspot Gateway acts as a management proxy for the LAN devices.
- **Firmware Tools**
  - **Firmware upgrade** - The firmware can be upgraded, so that more features can be added in the future.
    - **TFTP-based** - Upgrading firmware by TFTP (Trivial File Transfer Protocol).
    - **HTTP-based** - Upgrading firmware by HTTP (Hyper Text Transfer Protocol).
  - **Configuration backup.** The configuration settings of the SMCWHSG44-G can be backed up to a file via TFTP or HTTP for restoring later.
- **Management**
  - **Web-based Network Manager for configuring and monitoring the SMCWHSG44-G** - The management protocol is HTTP (Hyper Text Transfer Protocol)-based. The SMCWHSG44-G can be configured to be managed:
    - **Only from the LAN side**
    - **Both from the LAN side and WAN side**
    - **Only from the WAN side**

In addition, it can also be configured to accept management commands only from specific hosts.

  - UPnP - The SMCWHSG44-G responds to UPnP discovery messages so that a Windows XP user can locate the Wireless Hotspot Gateway in My Network Places and use a Web browser to configure it.
  - **SNMP** - SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x, Private Enterprise MIB are supported.
  - **System log** - For system operational status monitoring.
    - **Local log** - System events are logged to the on-board RAM of the Gateway and can be viewed using a Web browser.
    - **Remote log by SNMP trap** - Systems events are sent in the form of SNMP traps to a remote SNMP management server.
- **LAN/WAN Configurable Ethernet Switch Ports** - The SMCWHSG44-G provides a 4-port Ethernet switch so that a stand-alone Ethernet hub/switch is not necessary for connecting Ethernet client computers to the Router. These Ethernet ports can be configured as WAN ports for multiple DSL/cable-based Internet connections support.
- **Hardware Watchdog Timer** - If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the gateway. Accordingly, the SMCWHSG44-G can provide continuous services.

- **Configuration Reset -** Reset the configuration settings to factory-set values.

1.2.1 Package Checklist

* Check that you have the following contents in the box:

- SMCWHSG44-G Wireless Hotspot Gateway
- User Guide
- Utility & Documentation CD
- Wallmount Kit
- Power Adapter
- 2 dBi Dipole Antenna

1.3. LED Definition

- **PWR** : Power
- **ALIVE** : Blinks when the SMCWHSG44-G is working normally.
- **RF** : IEEE 802.11b/g interface activity
- **WAN/LAN**: Ethernet WAN/LAN interface activity

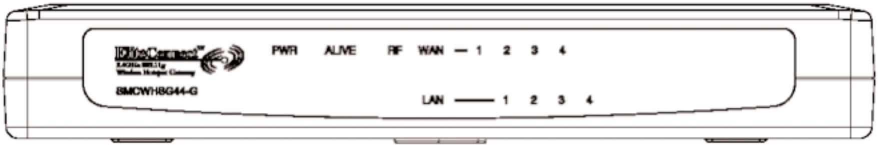


Fig. 1. LED Indicator

1.4. Rear Panel

- **+12V DC** : AC/DC power jack (12VDC input)
- **WAN/LAN**: Ethernet WAN/LAN interface indication
- **POE** : POE-enabled LAN port interface
- **COM** : RS232 serial port for Printer/keypad
- **RESET** : Hardware reset button

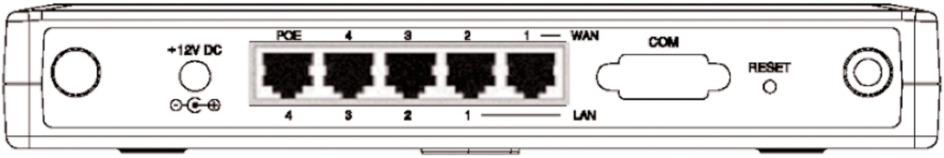


Fig. 2. Rear Panel

1.5. Selecting a Power Supply Method

The **SMCWHSG44-G** can be powered by either the supplied AC power adapter or the optional SMCPWR-INJ3 EliteConnect™ Power Injector. The **SMCWHSG44-G** automatically selects the suitable power depending on your decision.

To power the SMCWHSG44-G by the supplied power adapter:

1. Plug the power adapter to an AC socket.
2. Plug the connector of the power adapter to the power jack of the **SMCWHSG44-G**.

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked "Class 2" or "LPS" and output rated "12V DC, 1.25 A minimum" or equivalent statement.

To power the **SMCWHSG44-G** by **SMCPWR-INJ3** Power Injector (SMCPWR-INJ3 sold separately):

1. Connect the power cord cable from power outlet to the **SMCPWR-INJ3** power connector.

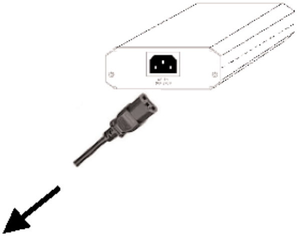


Fig. 3. Connecting the power cord cable to SMCPWR-INJ3.

2. Check the "POWER" LED: if system is normal, the LED will be on (Green light); otherwise, the "POWER" LED will be off.
3. Connect the Ethernet cable (RJ-45 Category 5) from Ethernet Hub/Switch to the "DATA IN" port of **SMCPWR-INJ3** Power Injector.
4. Connect another Ethernet cable (RJ-45 Category 5) from "POWER & DATA OUT" port of the **SMCPWR-INJ3** Power Injector to the **SMCWHSG44-G**. Please note the indication on the panel of POE-enabled RJ45 port of **SMCWHSG44-G** (LAN interface #4).

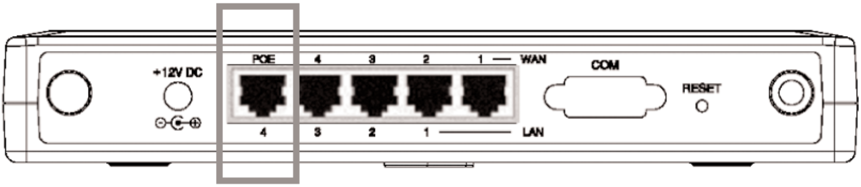


Fig. 4. POE enabled LAN Port Position.

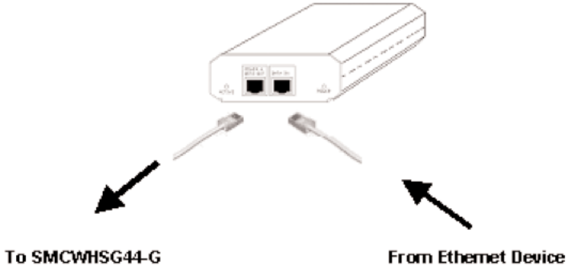


Fig. 5. Connecting Ethernet cables to SMCPWR-INJ3.

5. Check the "ACTIVE" LED: if power is successfully fed into the SMCWHSG44-G, the "ACTIVE" LED will be on (Red light); otherwise, the "ACTIVE" LED will be off.
6. If the electricity current is over the normal condition (Io°✥1.0 A), the "ACTIVE" LED will flash (Red light).

NOTE: SMCPWR-INJ3 is specially designed for **SMC2582W-B, SMC2586W-G,** and **SMCWHSG44-G**. The use of **SMCPWR-INJ3** with other Ethernet-ready devices that are not compliant to IEEE 802.3af may cause damage to the devices.

1.6. Mounting the SMCWHSG44-G on a Wall

The **SMCWHSG44-G** is wall-mountable.

1. Stick the supplied sticker for wall-mounting.
2. Use a ←6.5mm driller to drill a 25mm-deep hole at each of the cross marks.
3. Plug in a supplied plastic conical anchor in each hole.
4. Screw a supplied screw in each plastic conical anchor for a proper depth so that the **SMCWHSG44-G** can be hung on the screws.
5. Hang the **SMCWHSG44-G** on the screws.

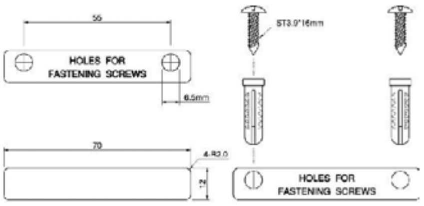


Fig. 6. Mounting the SMCWHSG44-G on a wall.

1.7. Preparing for Configuration

To configure the Wireless Hotspot Gateway, a managing computer with a Web browser is needed. For first-time configuration of a **SMCWHSG44-G**, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance/configuration of a deployed **SMCWHSG44-G**, either a wireless computer or a wired computer can be employed as the managing computer.

NOTE: If you are using the browser, Opera, to configure an **SMCWHSG44-G**, click the menu item File, click Preferences... click File types, and edit the MIME type, text/html, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the **SMCWHSG44-G**.

Since the configuration/management protocol is HTTP-based, you have to make sure that the IP address of the managing computer and the IP address of the managed **SMCWHSG44-G** are in the same IP subnet (the default IP address of the **SMCWHSG44-G** is **192.168.2.1** and the default subnet mask is **255.255.255.0**.) For ease of configuration you can set your computer to "Obtain IP Address automatically" since the Wireless Hotspot Gateway has a built in DHCP server.

1.7.1. Connecting the Managing Computer and the SMCWHSG44-G

To connect the managing computer and the SMCWHSG44-G for first-time configuration, you have two choices as illustrated in Fig. 7.

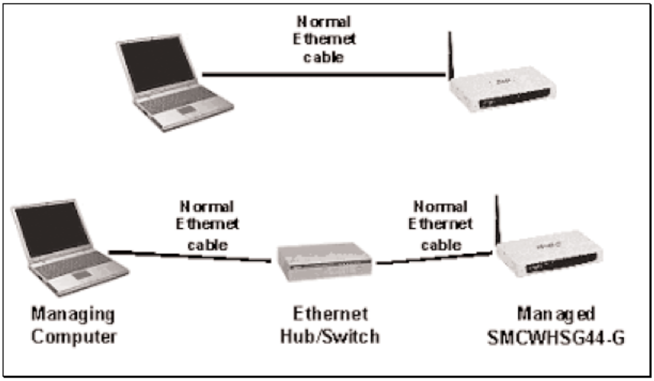


Fig. 7. Connecting a managing computer and SMCWHSG44-G via Ethernet.

You can use either an Ethernet cable (included in the package) or a switch/hub with 2 straight-through Ethernet cables.

1.7.2. Changing the TCP/IP Settings of the Managing Computer

Use the Windows Network Control Panel Applet to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the **SMCWHSG44-G** are in the same IP subnet. Set the IP address of the computer to **192.168.2.xxx** (the default IP address of the **SMCWHSG44-G** is **192.168.2.1**) and the subnet mask to 255.255.255.0.) It is preferred to set the computer to "obtain an IP address automatically" so the router will give your computer the correct settings automatically.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

1.8. Configuring the SMCWHSG44-G

The **SMCWHSG44-G** is DHCP server enabled by default. After the IP addressing is configured, launch a Web browser on the managing computer. Then, go to "http://192.168.2.1" to log on to the Wireless Hotspot Gateway for Web-based management.

1.8.1. Entering the Password

To log onto the Web based management interface, you will be prompted to enter the password. For first-time configuration, default password is "smcadmin". And then, click the LOGIN button.

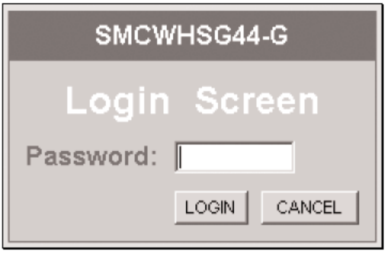
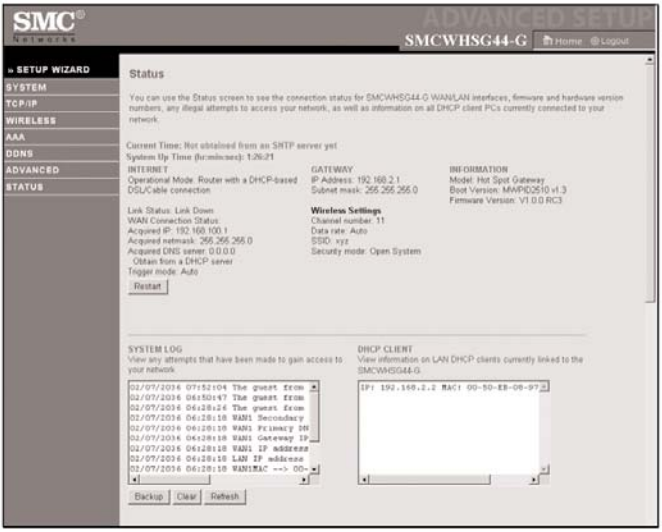


Fig. 9. Entering the Password.

NOTE: It is strongly recommended that the password be changed to another value for security reasons. On the start page, go to the SYSTEM\Password Settings page to change the value of the password (see Section 2.3.2 for more information).



Status

You can use the Status screen to see the connection status for SMCWHSG44-G WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: Not obtained from an SNTP server yet
System Up Time (hr:min:sec): 1:26:21

INTERNET
Operational Mode: Router with a DHCP-based DSL/Cable connection

Link Status: Link Down
WAN Connection Status:
Acquired IP: 192.168.100.1
Acquired netmask: 255.255.255.0
Acquired DNS server: 0.0.0.0
Obtain from a DHCP server
Trigger mode: Auto

Restart

GATEWAY
IP Address: 192.168.2.1
Subnet mask: 255.255.255.0

Wireless Settings
Channel number: 11
Data rate: Auto
SSID: xyz
Security mode: Open System

INFORMATION
Model: Hot Spot Gateway
Boot Version: MWPID2510 v1.3
Firmware Version: V1.0.0 RC3

SYSTEM LOG
View any attempts that have been made to gain access to your network.

```
02/07/2036 07:52:04 The guest from
02/07/2036 06:50:47 The guest from
02/07/2036 06:28:24 The guest from
02/07/2036 06:28:18 WAN1 Secondary
02/07/2036 06:28:18 WAN1 Primary DN
02/07/2036 06:28:18 WAN1 Gateway IP
02/07/2036 06:28:18 WAN1 IP address
02/07/2036 06:28:18 LAN IP address
02/07/2036 06:28:18 WAN1MAC --> 00-
```

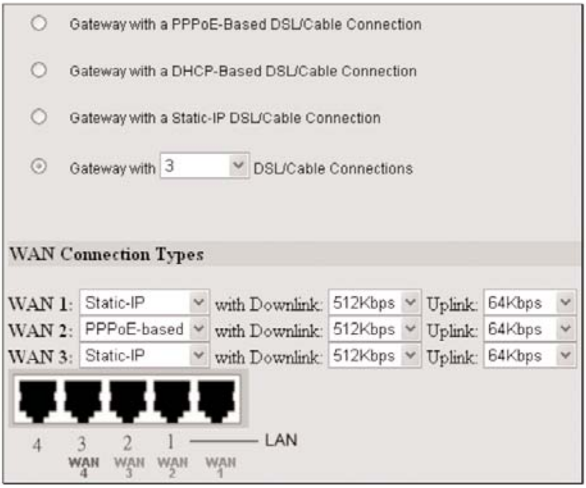
Backup Clear Refresh

DHCP CLIENT
View information on LAN DHCP clients currently linked to the SMCWHSG44-G

```
IP: 192.168.2.2 MAC: 00-50-EB-08-97
```

Fig. 10. Home Page.

1.8.2. SETUP WIZARD Step 1: Selecting an Operational Mode



○ Gateway with a PPPoE-Based DSL/Cable Connection

○ Gateway with a DHCP-Based DSL/Cable Connection

○ Gateway with a Static-IP DSL/Cable Connection

◉ Gateway with 3 DSL/Cable Connections

WAN Connection Types

WAN 1: Static-IP with Downlink: 512Kbps Uplink: 64Kbps
WAN 2: PPPoE-based with Downlink: 512Kbps Uplink: 64Kbps
WAN 3: Static-IP with Downlink: 512Kbps Uplink: 64Kbps

Fig. 11. Operational Modes.

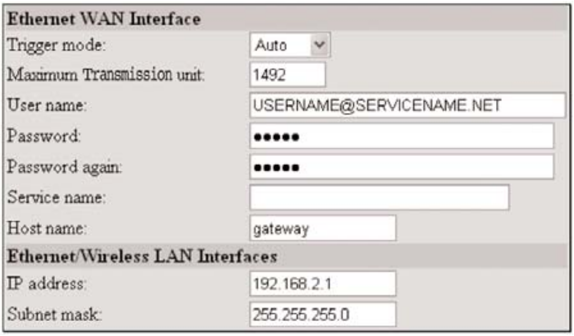
- If the Router is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by PPPoE, select Router with a PPPoE-Based DSL/Cable Connection.
- If the Router is to be used with a DSL or cable modem and the IP address assignment for the Ethernet WAN interface is achieved by DHCP, select Router with a DHCP-Based DSL/Cable Connection.
- If the Router is to be used with a DSL or cable modem and the IP address

of the Ethernet WAN interface has to be manually set, select Router with a Static-IP DSL/Cable Connection.

- If you have multiple ADSL/cable connections, select Router with n DSL/Cable Connections. Select the number of connections using the drop-down list, and then specify the type, downlink date rate and uplink data rate of each ADSL/cable connection. The specified data rates affect the load-balancing engine of the SMCWHSG44-G.

1.8.3. SETUP WIZARD Step 2: Configuring TCP/IP Settings

1.8.3.1. Router with a PPPoE-Based DSL/Cable Connection



Ethernet WAN Interface	
Trigger mode:	Auto
Maximum Transmission unit:	1492
User name:	USERNAME@SERVICENAME.NET
Password:	•••••
Password again:	•••••
Service name:	
Host name:	gateway
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.2.1
Subnet mask:	255.255.255.0

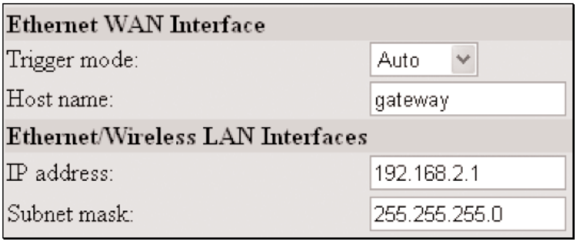
Fig. 12. TCP/IP Settings for Router with a PPPoE-Based DSL/Cable Connection mode.

If the **SMCWHSG44-G** is set to be in Router with a PPPoE-Based DSL/Cable Connection mode, two IP addresses are needed-one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say **192.168.2.xxx**. The default LAN IP address is **192.168.2.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct User name, Password, and Service name settings.

The Trigger mode setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and disconnected manually (Manual) by clicking the Connect and Disconnect buttons on the Start page, respectively. Or you can choose to let the device automatically (Auto) establish a PPPoE connection at boot-up time. In Auto mode, if the connection is disrupted, the device will omtry to reestablish the broken connection automatically.

1.8.3.2. Router with a DHCP-Based DSL/Cable Connection

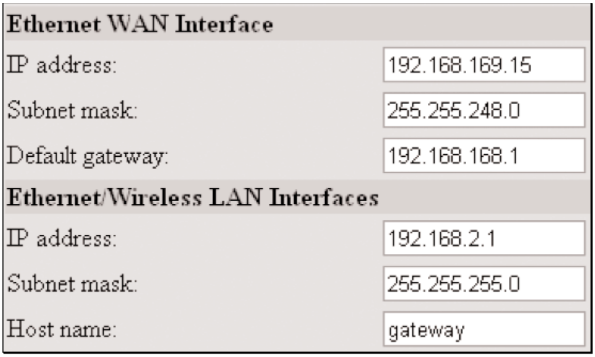


Ethernet WAN Interface	
Trigger mode:	Auto
Host name:	gateway
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.2.1
Subnet mask:	255.255.255.0

Fig. 13. TCP/IP settings for Router with a DHCP-Based DSL/Cable Connection mode.

If the **SMCWHSG44-G** is set to be in 'Router with a DHCP-Based DSL/Cable Connection 'mode, two IP addresses are needed-one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say **192.168.2.xxx**. The default LAN IP address is **192.168.2.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.
As for the WAN IP address, it is obtained by DHCP from the ISP. The Trigger mode setting affects the behavior of the DHCP client of the Router. In Auto mode, you don't have to worry about the DHCP process; the device takes care of everything. In Manual mode, there are two buttons on the Start page for you to manually release an obtained IP address (Release) and re-obtain a new one from a DHCP server (Renew).

1.8.3.3. Router with a Static-IP DSL/Cable Connection



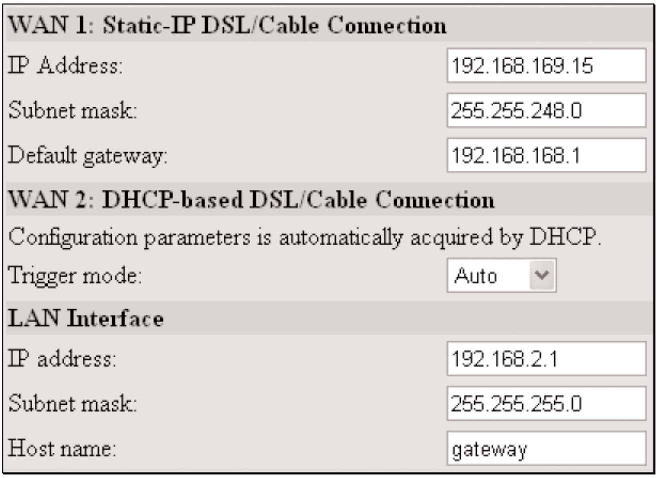
Ethernet WAN Interface	
IP address:	192.168.169.15
Subnet mask:	255.255.248.0
Default gateway:	192.168.168.1
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.2.1
Subnet mask:	255.255.255.0
Host name:	gateway

Fig. 14. TCP/IP settings for Router with a Static-IP DSL/Cable Connection mode.

If the **SMCWHSG44-G** is set to be in 'Router with a Static-IP DSL/Cable Connection' mode, two IP addresses are needed-one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say **192.168.2.xxx**. The default LAN IP address is **192.168.2.1** and the default subnet mask is **255.255.255.0**. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct IP address, Default gateway, Subnet mask, Primary DNS server, and Secondary DNS server settings.

1.8.3.4. Router with Multiple DSL/Cable Connections



WAN 1: Static-IP DSL/Cable Connection

IP Address: 192.168.169.15

Subnet mask: 255.255.248.0

Default gateway: 192.168.168.1

WAN 2: DHCP-based DSL/Cable Connection

Configuration parameters is automatically acquired by DHCP.

Trigger mode: Auto

LAN Interface

IP address: 192.168.2.1

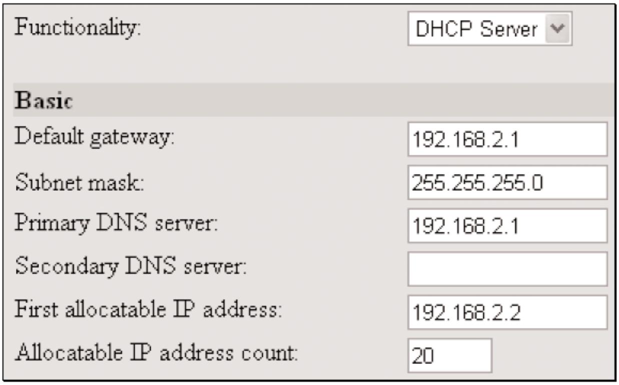
Subnet mask: 255.255.255.0

Host name: gateway

Fig. 15. TCP/IP settings for Router with Multiple DSL/Cable Connections mode.

Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of 'Router with a PPPoE-Based DSL/Cable Connection', 'DHCP-Based DSL/Cable Connection', or 'Router with a Static-IP DSL/Cable Connection', respectively. As a result, refer to Sections 1.8.3.1, 1.8.3.2, and 1.8.3.3 for more information.

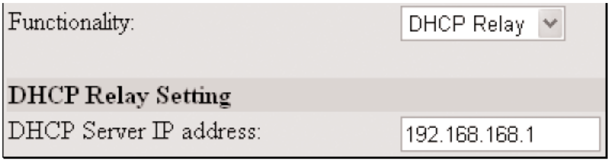
1.8.4. SETUP WIZARD Step 3: Configuring DHCP Server Settings



Functionality:	DHCP Server
Basic	
Default gateway:	192.168.2.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.2.1
Secondary DNS server:	
First allocatable IP address:	192.168.2.2
Allocatable IP address count:	20

Fig. 16. DHCP Server Settings.

The **SMCWHSG44-G** can automatically assign IP addresses to client computers by DHCP. DHCP server settings include Default gateway, Subnet mask, Primary DNS server, and Secondary DNS server. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocatable IP addresses. In most cases, Default Gateway and Primary DNS server should be set to the IP address of the Router's LAN interface (e.g., the default LAN IP address is **192.168.2.1**), and Subnet mask is set to **255.255.255.0**.



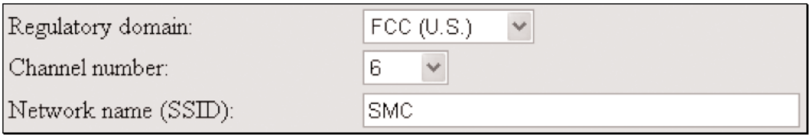
Functionality:	DHCP Relay
DHCP Relay Setting	
DHCP Server IP address:	192.168.168.1

Fig. 17. DHCP Relay Settings.

When the functionality is chosen to “DHCP Relay”, the SMCWHSG44-G will not assign any IP address to the clients. It forwards the received DHCP requests from the clients to the designate DHCP server. The only setting for DHCP relay is DHCP server IP address.

1.8.5. SETUP WIZARD Step 4: Configuring IEEE 802.11 Settings

IEEE 802.11-related communication settings include Regulatory domain, Channel number, and Network name (SSID).



Regulatory domain:	FCC (U.S.)
Channel number:	6
Network name (SSID):	SMC

Fig. 18. IEEE 802.11b Communication Settings.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the wireless Hotspot gateway must be identical for them to communicate with each other.

Note: SMCWHSG44-Gs sold in North America and EMEA are already configured to FCC and ETSI domain respectively, and the domain settings are not able to be changed.

1.8.6. Configuring User Authentication Settings

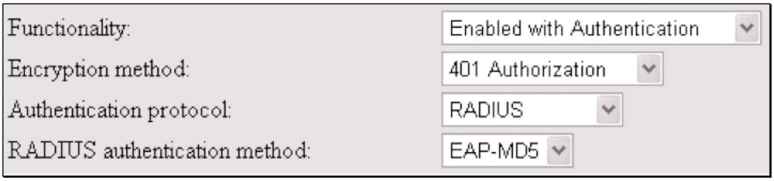
The **SMCWHSG44-G** supports both Web redirection-based and non-802.1x-based user and IEEE 802.1x-based user authentication.

NOTE: If both web redirection and IEEE 802.1x are enabled, the authentication process is 2-phase. In the first phase, IEEE 802.1x is tried and in the second phase, Web redirection is tried. A user, who fails in the first phase or uses a computer that does not support IEEE 802.1x, is given a second chance. In this way, the **SMCWHSG44-G** can serve both IEEE 802.1x-enabled and IEEE 802.1x-disabled wireless users.

1.8.6.1. Web Redirection

If you want to do Web redirection-based user authentication, go to the AAA\Web Redirection section for configuration. There are three combinations for Web Redirection and Authentication method:

1. **Enabled with Authentication** - Enable both Web-Redirection and user Authentication mechanism.



Functionality: Enabled with Authentication

Encryption method: 401 Authorization

Authentication protocol: RADIUS

RADIUS authentication method: EAP-MD5

Fig. 19. Web Redirection Settings - Enable with Authentication

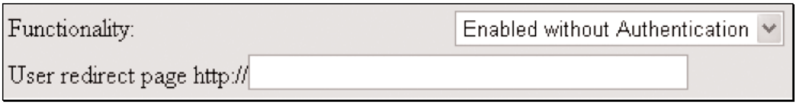
Encryption Method:

401 Authorization : Logon page on Pop-up window.
CGI with Plain Code: Logon page on web browser, username/password without encryption (plain text).
CGI with Base64: Logon page on web browser, username/password with Base64 encryption.
CGI with SSL: Logon page on web browser, username/password with SSL encryption.

Authentication protocol:

RADIUS: Authentication by external RADIUS server.
Local Accounts: Authentication by local database, associated with ticket printing or manually configured users.
RADIUS authentication method:
EAP-MD5
PAP
CHAP

2. **Enabled without Authentication** - Enables only the Web-Redirection, but disables the user Authentication mechanism. Users will automatically redirect to the destination web page of the URL indicated.



Functionality: Enabled without Authentication
User redirect page http://

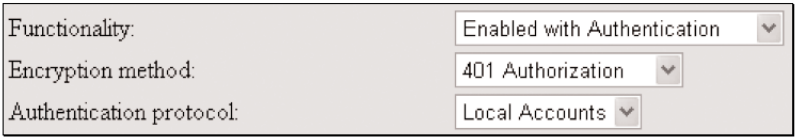
Fig. 20. Web Redirection Settings - Enable without Authentication

3. Disable - Disable all Web-Redirection mechanisms.

1.8.6.2. Local Authentication Sever

The SMCWHSG44-G supports local Authentication Sever capabilities for Hotspot venues where standard RADIUS or a Billing server(s) are difficult to implement. The local Authentication Server contains a built-in database for 2,000 user entries.
To setup the Local Authentication method:

1. Go to the section AAA\Web-redirection, in 'Functionality' of 'Basic' column, select 'Enable with Authentication'.
2. In 'Authentication protocol', select 'Local Accounts'.



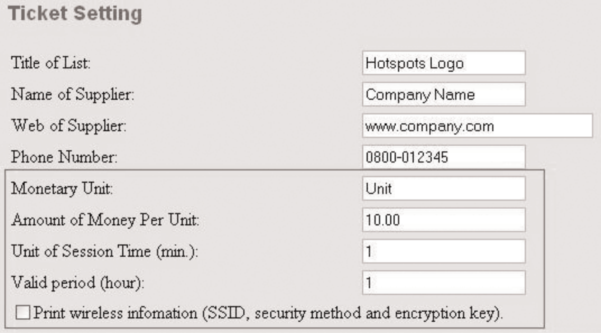
Functionality: Enabled with Authentication
Encryption method: 401 Authorization
Authentication protocol: Local Accounts

Fig. 21. Local Authentication Server Settings

3. Go to the AAA\Ticket Settings to setup the billing information. In the Ticket Setting page, the fields related to the billing information are the 'Monetary Unit' and the 'Amount of Money Per Unit'. The fields that relate to the user permitted access time (or session time) are 'Unit of Session Time (min)' and 'Valid period (hour)'. You can specify the appropriate content which reflects the information of Hotspot venues to be shown on the ticket content. More detail for the Ticket Setting configuration is described as below:

- **Monetary Unit:** to define the unit of currency, eg., input 'USD' for US Dollars or 'EURO' for Euro Dollars. The currency unit will show on the billing ticket.

- **Amount of Money Per Unit**: defines the money to be charged per unit.
- **Unit of Session time (min):** defines the time frame (by min) for the user to access the Internet. Default is '1' min. For example: x number of minutes = 1 Unit of Session Time
- **Valid period (hour):** to define the valid period (by hour) while the user account is generated. If the user account is generated but not activated during the valid period, the gateway will automatically disable the user after the valid period expired. Default is '1' hour.
- **Print wireless information (SSID, security method and encryption key):** by checking the box, the SSID, security method and encryption key information will appear on the printed ticket. This information can be configured in the Wireless/Security section within the Web manager interface. (See section 2.5.2.1)



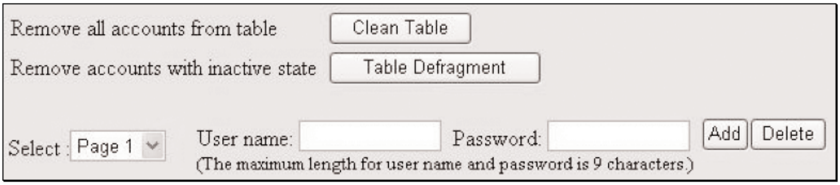
Ticket Setting

Title of List:	Hotspots Logo
Name of Supplier:	Company Name
Web of Supplier:	www.company.com
Phone Number:	0800-012345
Monetary Unit:	Unit
Amount of Money Per Unit:	10.00
Unit of Session Time (min.):	1
Valid period (hour):	1

□ Print wireless infomation (SSID, security method and encryption key).

Fig. 22. Ticket Settings (Default settings)

4. Go to the section STATUS\Account Table, to manually generate users. These users are permanent and do not have a predefined amount of time.



Remove all accounts from table

Remove accounts with inactive state

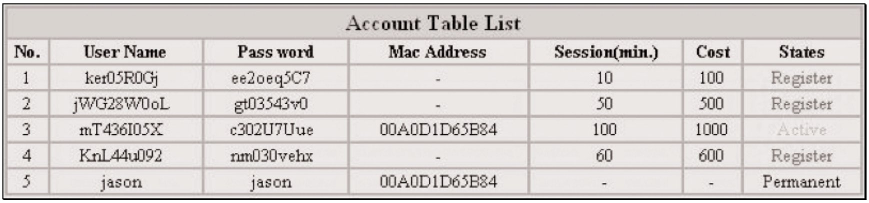
Select : Page 1 User name: Password:

(The maximum length for user name and password is 9 characters.)

Fig. 23. Local User Generator

5. The status of generated local users will be shown in the 'Account Table List'. The 'User Name' and 'Password' are randomly generated by the key-pad/printer combo. Users must use the generated username and password for the logon process. There are 3 types of status of each user account:

- **Register**: shows the generated user who has not yet logged on and been activated.
- **Active**: the generated user who has successfully logged on and accessed the Internet. The MAC address and Login Time of the activated user will be also shown while user has been activated.
- **Inactive:** shows the user account that access time frame has expired, or 'Valid Period' expired.



Account Table List

No.	User Name	Pass word	Mac Address	Session(min.)	Cost	States
1	ker05R0Gj	ee2oeq5C7	-	10	100	Register
2	jWG28W0oL	gt03543v0	-	50	500	Register
3	mT436I05X	c302U7Uue	00A0D1D65B84	100	1000	Active
4	KnL44u092	nm030vehx	-	60	600	Register
5	jason	jason	00A0D1D65B84	-	-	Permanent

Fig. 24. Account Table List

1.8.6.3. How to Setup the Mini-POS Ticket Printer

The **SMCWHSG44-G** supports a built-in user database for local authentication. This function also associates with the external Mini-POS Ticket Printer (SMCWHS-POS) for billing and printing purposes. The benefit of the built-in user database is to provide a local user authentication database as some Hotspot venues do not have the capability to setup a complete RADIUS environment for user authentication. Additionally, the external control keypad offers a way to control ticket printing without the addition of a PC, hence reduces the cost of Hotspot venue deployment.
To setup the Mini-POS Ticket Printer:

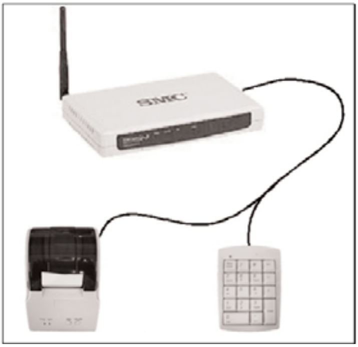
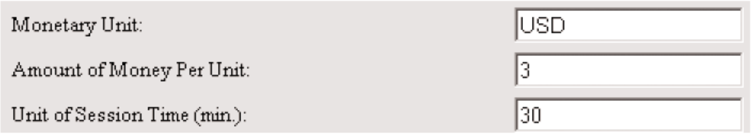


Fig. 25. Mini-POS Ticket Printer & Control Keypad Deployment

1. Connect the Mini-POS Ticket Printer (SMCWHS-POS) and the control keypad with the Y cable (both the control keypad and the Y cable can be found in the package of the SMCWHS-POS printer.)
2. Connect the Y cable to the COM port of the SMCWHSG44-G.
3. Open the web browser of the SMCWHSG44-G (see section 1.7).
4. Go to the section AAA\Web Redirection, in 'Functionality' of 'Basic' column, select 'Enable with Authentication'. (see section 1.8.5.2)
5. In 'Authentication protocol', select 'Local Accounts'.
6. Go to the AAA\Ticket Settings to setup the billing information.
7. Save and Restart the gateway to make the changed setting effective.
8. Power ON the printer, note that both LED light for 'POWER' and 'MODE' should be ON.
9. In step 6 above you have assigned a value to the "Amount of Money Per

Unit" and a value for the number of minutes for "Units of Session time". In order to produce a ticket from the Mini-POS Ticket Printer, you will need to key in selected numbers, and press ENTER. The numbers you select on the keypad will always correspond to the Units of Session Time.

- For Example: You have assigned "3" as the value for the Amount of Money Per Unit. You have assigned "30" as the number of minutes equal to 1 Unit of Session Time.



Monetary Unit:	USD
Amount of Money Per Unit:	3
Unit of Session Time (min.):	30

Ticket Settings for Ticket printing

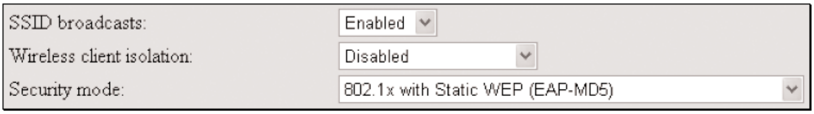
Based on this Ticket Setting, if the client requests 1 hour of access time then you must press the following three keys on the Control Keypad: 0_2_ENTER
In other words, 02 Units of Session Time x (30 minutes per Unit) = 1 hour. In this case, the ticket will show that the amount owed by the customer is 6 USD.

NOTE: You will always need to key in at least 2 digits on they keypad before pressing ENTER (For example: 02 = 2 "Units of Session Time").

10. After pressing the 'Enter' button on the control keypad, the new local account will be automatically generated, and the billing ticket will be printed simultaneously.

To make sure the Mini-POS Ticket Printer is in good condition, you can print out the paper by holding the 'FEED' button. Make sure the Mode light is off to do this. Also check the status of the lights. The power light should be blue and the mode light should be red.

1.8.6.4. IEEE 802.1x



SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	802.1x with Static WEP (EAP-MD5)

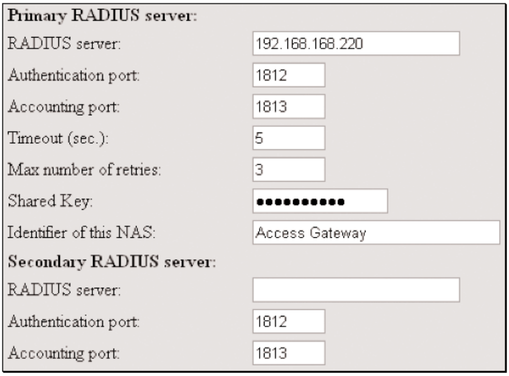
Fig. 26. Changing security mode to an IEEE 802.1x option.

If you want to do IEEE 802.1x-based user authentication, go to the Wireless\ Security section, and then change the Security mode setting to an IEEE 802.1x-related option according to your needs. The SMCWHSG44-G supports IEEE 802.1x EAP-MD5 and EAP-TLS authentication methods. Click Save when finished.

1.8.6.5 Configuring RADIUS Settings

The RADIUS client on the SMCWHSG44-G works in conjunction with the Web redirection component and IEEE 802.1x component for wireless user authentication. The Web redirection and IEEE 802.1x components are responsible for acquiring user credential information, and the RADIUS client communicates with a back-end RADIUS server using the user credential information.

Go to the AAA\RADIUS section (see section 2.6.2), and then configure the RADIUS settings. You have to configure at least Authentication method, Primary RADIUS server, Shared key, and Identifier of the NAS settings. Leave other settings to their default values. Click Save & Restart when finished.



Primary RADIUS server:	
RADIUS server:	192.168.168.220
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	●●●●●●●●●●●
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 27. RADIUS Settings.

NOTE: When configured for EAP authentication, the RADIUS server supports either EAP-TLS or EAP-MD5, but not both at the same time. As a result, not all combinations of EAP-MD5, EAP-TLS, PAP and CHAP authentication methods are available if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes on the Wireless Advanced edition of Wireless Hotspot Gateway.

Table 1. Allowable Authentication Modes.

	IEEE 802.1x disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
Web redirection disabled	■	■	■
Web redirection EAP-MD5	■	■	
Web redirection PAP	■	■	■
Web redirection CHAP	■	■	■

1.9. Deploying the SMCWHSG44-G

After the settings have been configured, deploy the Wireless Hotspot Gateway to the field application environment. The system configuration in Fig. 28 illustrates how to deploy the **SMCWHSG44-G**.

In this configuration, one DSL/cable modem is connected to the WAN port (as WAN 1) of the **SMCWHSG44-G** and another modem is connected to the LAN 1 port (as WAN 2) of the **SMCWHSG44-G**. Two APs are connected to the LAN 2 port and LAN 3 port, respectively. Finally, a RADIUS server is connected to the LAN 4 port of the **SMCWHSG44-G**. The **SMCWHSG44-G** works together with the RADIUS server to decide whether a wireless client (the notebook computer or the PDA) is allowed to access the Internet through the broadband modems. The Radius Server is optional since the built in Local Authentication Database can handle all wireless users.

NOTE: Although the RADIUS server in this sample configuration is on the "LAN" side, in a real application, it can also be on the "WAN" side, accessible via the Internet.

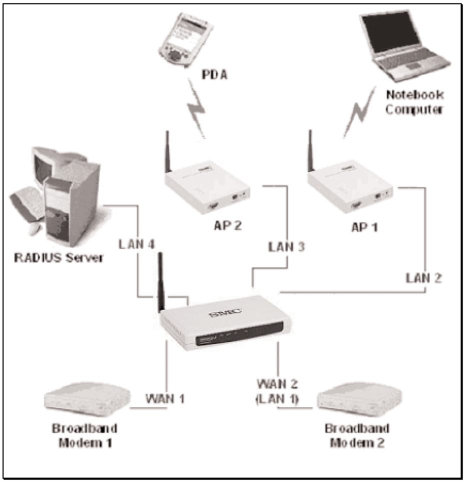


Fig. 28. Example SMCWHSG44-G Deployment.

Since **SMCWHSG44-G** also provides the WDS static wireless bridge function, it can connect the other wireless AP's with the WDS method (See section 2.5.1.2 Wireless Distribution System for more detail information).

1.10. Setting up Client Computers

Before a wireless user can access the Internet through the **SMCWHSG44-G**, the wireless and TCP/IP settings of his/her computer or PDA must be configured adequately to match the environment of **SMCWHSG44-G**. In addition, if Web redirection or IEEE 802.1x EAP-MD5 authentication methods are used, user name and password information must be set up on the RADIUS server or Locally on the Wireless Hotspot Gateway. On the other hand, if IEEE 802.1x EAP-TLS authentication method is used, a digital certificate must be installed on the computer or PDA and on the back end RADIUS server.

1.10.1. Configuring IEEE 802.11-Related Settings

Before the TCP/IP networking system of a wireless client computer can communicate with other hosts, the underlying wireless link must be established between this wireless computer and a deployed AP or the SMCWHSG44-G's built-in AP.

To establish a wireless link to an AP:

1. Launch the configuration/monitoring utility provided by the vendor of the installed WLAN NIC.
2. Use the utility to make appropriate operating mode, SSID and Security settings.

NOTE: A wireless client computer must be in infrastructure mode, so that it can associate with a wireless access point.

NOTE: The SSID of the wireless client computer and the SSID of the deployed APs must be identical. Or, in case the SSID broadcasts capability of the deployed APs is enabled (by default), the SSID of the wireless client computer could be set to “any”.

NOTE: Both the wireless client computer and the deployed APs must have the same Security settings for them to communicate with each other. Hotspot

Configuring TCP/IP-Related Settings

If a wireless user is using a Windows-based computer, he/she can use Windows Network Control Panel Applet to change the TCP/IP settings of his/her computers, so that the IP addresses of the client computers and the IP address of the Router are in the same IP subnet. If the SMCWHSG44-G is to be used in a Hotspot, the client computers must be set to obtain IP addresses automatically by DHCP.

NOTE: Set the client computers to obtain IP addresses automatically by DHCP.

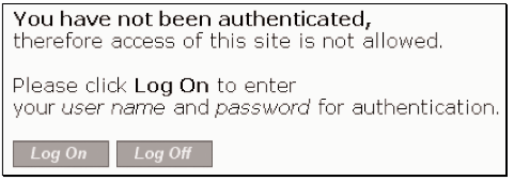
NOTE: Configure the client computers so that Web browsing is not through any Web Proxy servers; otherwise the Web redirection-based authentication will not work properly.

If a client computer is already set to obtain an IP address automatically, you can use the Windows-provided tool, WinIPCfg.exe (on Windows 9x/ME) or IPConfig.exe (on Windows 2000/XP), to obtain an IP address from the Router. WinIPCfg.exe is a GUI program, and has command buttons for releasing the current IP address and reobtaining an IP address. IPConfig.exe is a command-line program, and the /release option releases the current IP address and the /renew option triggers the Windows DHCP client subsystem to re-obtain an IP address.

1.11. Confirming the Settings of the SMCWHSG44-G and Client Computers

To make sure you have correctly set up the **SMCWHSG44-G** for Web redirection-based authentication or not, follow the procedure below:

1. Establish a wireless link from the wireless client computer or PDA to an AP that is controlled by the **SMCWHSG44-G** or to the **SMCWHSG44-G** itself.
2. On the wireless client computer or PDA, run a Web browser, and then go to a Web site on the Internet, e.g., **http://www.smc.com**.
3. Instead of showing the requested page, a log-on page is shown. Click Log On for authentication.



You have not been authenticated,
therefore access of this site is not allowed.

Please click **Log On** to enter
your *user name* and *password* for authentication.

Fig. 29. Log-On Page.

4. Type a correct user name and password that has been registered either manually configured on the Wireless Hotspot Gateway or printed out from the Printer.

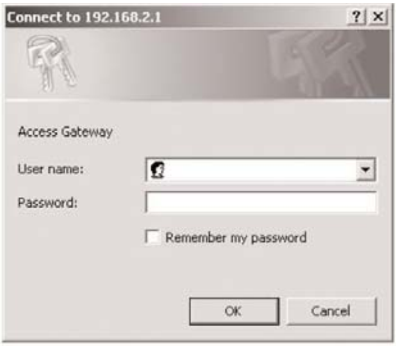
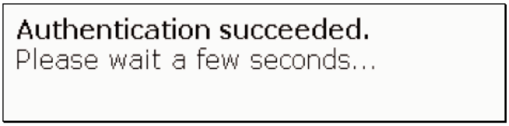


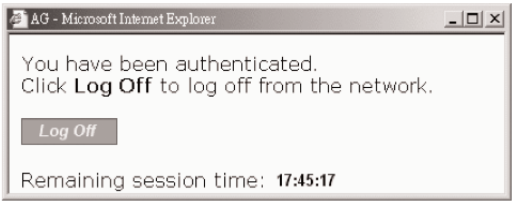
Fig. 30. User Name and Password for Authentication.

5. If the user name and password are correct, you will be brought to the original page you have requested after waiting for a few seconds. Meanwhile, a window for log-off and session status appears.



Authentication succeeded.
Please wait a few seconds...

Fig. 31. Authentication Success.



You have been authenticated.
Click **Log Off** to log off from the network.

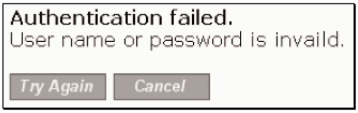
Remaining session time: **17:45:17**

Fig. 32. Log-Off Window.

6. Click Log Off within the log-off window to end the session.

NOTE: On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the Log-on page, and then click Log Off to end the session.

7. If the user name or password is invalid, you will be prompted to try again or cancel the authentication process.



Authentication failed.
User name or password is invaild.

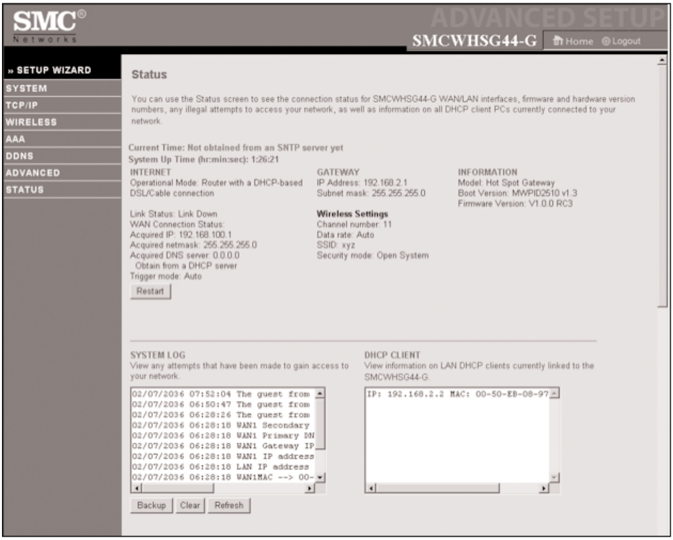
Fig. 33. Authentication Failure.

NOTE: If IEEE 802.1x capability of the SMCWHSG44-G is enabled, the user of an IEEE 802.1x-compliant wireless client computer is authenticated by IEEE 802.1x rather than by Web redirection.

2. Using Web-Based Network Manager

In this section, we will explain each Web management page of the Web-based Network Manager in detail.

2.1. Overview



Status

You can use the Status screen to see the connection status for SMCWHSG44-G WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: Not obtained from an SNTP server yet
System Up Time (hr:min:sec): 1:26:21

INTERNET
Operational Mode: Router with a DHCP-based DSL/Cable connection

Link Status: Link Down
WAN Connection Status:
Acquired IP: 192.168.100.1
Acquired netmask: 255.255.255.0
Acquired DNS server: 0.0.0.0
Obtain from a DHCP server
Trigger mode: Auto

GATEWAY
IP Address: 192.168.2.1
Subnet mask: 255.255.255.0

Wireless Settings
Channel number: 11
Data rate: Auto
SSID: xyz
Security mode: Open System

INFORMATION
Model: Hot Spot Gateway
Boot Version: MWPID2510 v1.3
Firmware Version: V1.0.0 RC3

SYSTEM LOG
View any attempts that have been made to gain access to your network.

```
02/07/2036 07:52:04 The guest from
02/07/2036 06:50:47 The guest from
02/07/2036 06:28:26 The guest from
02/07/2036 06:28:18 WAN1 Secondary
02/07/2036 06:28:18 WAN1 Primary DN
02/07/2036 06:28:18 WAN1 Gateway IP
02/07/2036 06:28:18 WAN1 IP address
02/07/2036 06:28:18 LAN IP address
02/07/2036 06:28:18 WAN1MAC --> 00-
```

DHCP CLIENT
View information on LAN DHCP clients currently linked to the SMCWHSG44-G.

```
IP: 192.168.2.2 MAC: 00-50-EB-08-97
```

Fig. 34. Home Page.

2.1.1. Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

- **Home**. For going back to the start page.
  - Current Time.
  - System Up Time.
  - Internet Information.
  - Gateway Information.
  - System Information.
  - DHCP Client. Current IP-MAC address mappings.
  - System Log. Logging console of the Router. Displays all informational messages.
- **Logout**.
- **SETUP WIZARD**. Basic Steps for you to quickly set up the Wireless Hotspot Gateway.
- **SYSTEM**. Global operations.
  - Operational Mode. Operational mode of the SMCWHSG44-G based on the type of the Internet connection provided by the ISP.
  - Password Settings. For gaining rights to change or view the settings and status of the Router.

  - Firmware Tools. For upgrading the firmware of the Router and backing up and restoring configuration settings.
  - Time Zone. Time zone and SNTP (Simple Network Time Protocol) server settings.
- **TCP/IP**. TCP/IP-related settings.
  - Address. IP addressing settings for the Router to work with your ISP, user name and password provided by the ISP and LAN settings
  - DNS. DNS (Domain Name System) proxy settings.
  - NAT. Virtual Server, DMZ and session control settings.
  - DHCP Server. Settings for the DHCP (Dynamic Host Configuration Protocol) server on the Router.
  - Load Balancing. Settings for the WAN ports load-balancing policy by Port or IP address range.
  - Zero Client Reconfiguration. Settings for wireless clients to associate to SMCWHSG44-G without any network setting modifications.
- **Wireless**. IEEE 802.11-related settings.
  - Communication. Settings for the IEEE 802.11b/g interface of the SMCWHSG44-G to work properly with wireless clients.
  - Security. Settings for authenticating wireless users by IEEE 802.1x and encrypting wireless data.
- **AAA**. Wireless user authentication settings.
  - Web Redirection. Web redirection settings for how a wireless user's HTTP request is “redirected” for authentication.
  - RADIUS. RADIUS settings for communication with the primary and secondary RADIUS servers.
  - Session Control. Settings for controlling the lifetime of a users authentication session.
  - Auth Page Customization. Settings for customizing the contents of log-on, log-off, authentication success, and authentication failure authentication pages.
  - Ticket Settings. Settings for the billing ticket format.
- **DDNS**. Settings for Dynamic DNS.
- **Advanced**. Advanced settings of the Router.
  - Filters & Firewall. Packet filtering and firewall settings for user access control and protection from hacker attacks from the Internet.
  - Management. Web-based management types, UPnP, Syslog, and SNMP settings.
  - Access Rules. Settings for the time frame policy to Permit/Deny administrator access to the SMCWHSG44-G.
  - LAN Device Management. Settings for the Router to know what LAN devices it has to manage.
- **Status**. System monitoring information.
  - Associated Wireless Clients. Display the status of all wireless clients who associated to the Wireless Hotspot Gateway.
  - Authenticated Users. Display the status of the users who have been

authenticated by SMCWHSG44-G. Authenticated users can also be terminated in this table.

- Account Table. Manually generates new users, or is automatically populated with accounts after entering amount of time required via the keypad.
- Session list. Display the status of session traffic
- Managed LAN Devices. Display the status of local LAN devices connected to the Wireless Hotspot Gateway.

2.1.2. Save, Save & Restart, and Cancel Commands

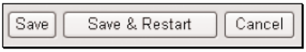


Fig. 35. Save, Save & Restart, and Cancel.

At the bottom of each page, there are up to three buttons-Save, Save & Restart, and Cancel. Clicking **Save** stores the settings changes to the memory of the Router and brings you back to the start page. Once all the changes are complete you will need to click the Restart button on the home page to reboot the router. Clicking **Save & Restart** stores the setting changes to the memory of the Router and restarts the Router immediately for the setting changes to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

2.1.3. Home and Refresh Commands

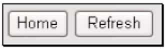
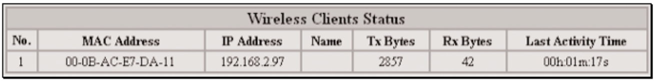


Fig. 36. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons-**Home** and **Refresh**. Clicking Home brings you back to the start page. Clicking Refresh updates the shown status information.

2.2. Status

2.2.1. Associated Wireless Clients



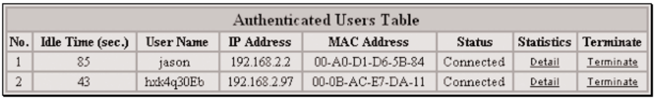
Wireless Clients Status

No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-0B-AC-E7-DA-11	192.168.2.97		2857	42	00h:01m:17s

Fig. 37. Status of Associated Wireless Clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name (if the client has been IEEE 802.1x authenticated), number of bytes it has sent, number of bytes it has received, and the time of its last activity, is shown.

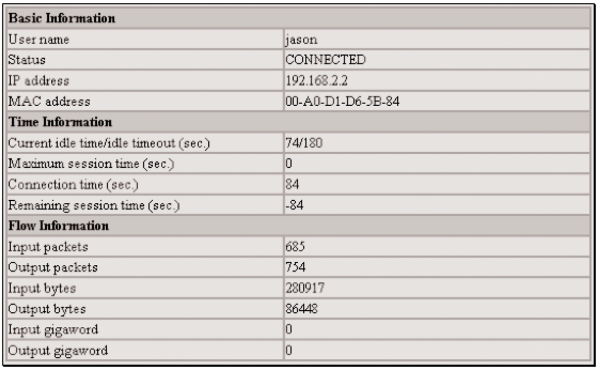
2.2.2. Authenticated Users



Authenticated Users Table							
No.	Idle Time (sec.)	User Name	IP Address	MAC Address	Status	Statistics	Terminate
1	85	jason	192.168.2.2	00-A0-D1-D6-5B-84	Connected	Detail	Terminate
2	43	hxk4q30Eb	192.168.2.97	00-0B-AC-E7-DA-11	Connected	Detail	Terminate

Fig. 38. Authenticated Users.

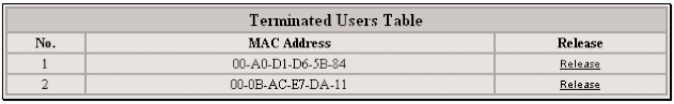
On this page, the status information of each authenticated user, including its current idle time, user name, IP address, MAC address, and status, is shown. In addition, you can click the **Detail** link in the Statistics column to see more detailed statistics information, such as Input packets, Output packets, Input bytes, and Output bytes.



Basic Information	
User name	jason
Status	CONNECTED
IP address	192.168.2.2
MAC address	00-A0-D1-D6-5B-84
Time Information	
Current idle time/idle timeout (sec.)	74/180
Maximum session time (sec.)	0
Connection time (sec.)	84
Remaining session time (sec.)	-84
Flow Information	
Input packets	685
Output packets	754
Input bytes	280917
Output bytes	86448
Input gigaword	0
Output gigaword	0

Fig. 39. Authenticated RADIUS User Detailed Information.

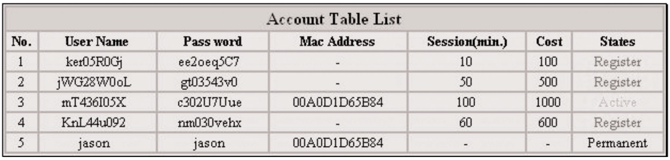
Any authenticated user can be terminated by clicking the corresponding Terminate link so that this user is blocked from using networking services provided by the Router. A terminated user is moved to the Terminated Users Table. Clicking the corresponding **Release** link puts a terminated user back into authenticated state.



Terminated Users Table		
No.	MAC Address	Release
1	00-A0-D1-D6-5B-84	Release
2	00-0B-AC-E7-DA-11	Release

Fig. 40. Terminated Users.

2.2.3. Account Table

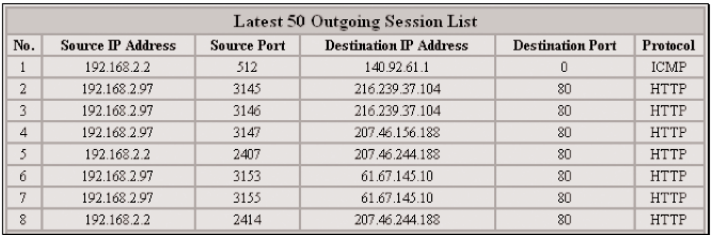


Account Table List						
No.	User Name	Pass word	Mac Address	Session(min.)	Cost	States
1	ker05R0Gj	ee2oeq5C7	-	10	100	Register
2	jWG28W0oL	gt03543v0	-	50	500	Register
3	mT436I05X	c302U7Uue	00A0D1D65B84	100	1000	Active
4	KnL44u092	nm030vehx	-	60	600	Register
5	jason	jason	00A0D1D65B84	-	-	Permanent

Fig. 41. Account Table List

On this page, all the registered users in local user database are shown. An activated user is identified by its MAC address, login time and the 'Active' display under the 'Status' column.

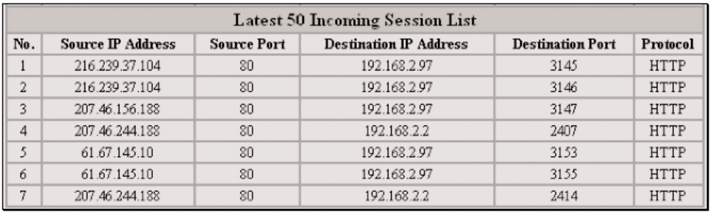
2.2.4. Session List



Latest 50 Outgoing Session List

No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	192.168.2.2	512	140.92.61.1	0	ICMP
2	192.168.2.97	3145	216.239.37.104	80	HTTP
3	192.168.2.97	3146	216.239.37.104	80	HTTP
4	192.168.2.97	3147	207.46.156.188	80	HTTP
5	192.168.2.2	2407	207.46.244.188	80	HTTP
6	192.168.2.97	3153	61.67.145.10	80	HTTP
7	192.168.2.97	3155	61.67.145.10	80	HTTP
8	192.168.2.2	2414	207.46.244.188	80	HTTP

Fig. 42. Latest Outgoing User Traffic Sessions.



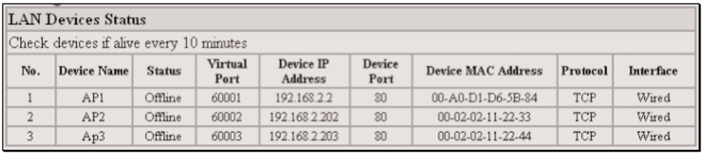
Latest 50 Incoming Session List

No.	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol
1	216.239.37.104	80	192.168.2.97	3145	HTTP
2	216.239.37.104	80	192.168.2.97	3146	HTTP
3	207.46.156.188	80	192.168.2.97	3147	HTTP
4	207.46.244.188	80	192.168.2.2	2407	HTTP
5	61.67.145.10	80	192.168.2.97	3153	HTTP
6	61.67.145.10	80	192.168.2.97	3155	HTTP
7	207.46.244.188	80	192.168.2.2	2414	HTTP

Fig. 43. Latest Incoming User Traffic Sessions.

On this page, latest 50 outgoing and 50 incoming user traffic sessions are shown for monitoring net-work activity.

2.2.5. Managed LAN Devices



LAN Devices Status

Check devices if alive every 10 minutes

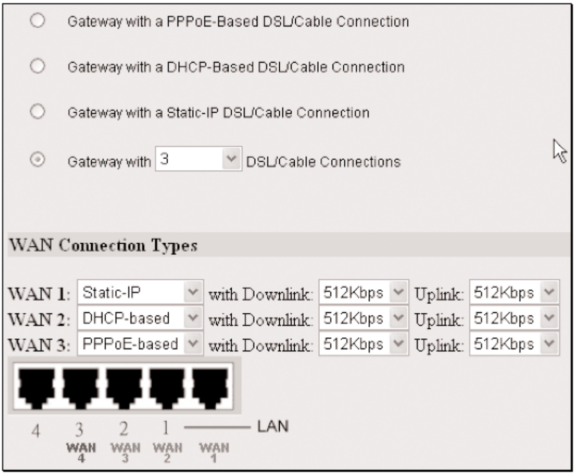
No.	Device Name	Status	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface
1	AP1	Offline	60001	192.168.2.2	80	00-A0-D1-D6-5B-84	TCP	Wired
2	AP2	Offline	60002	192.168.2.202	80	00-02-02-11-22-33	TCP	Wired
3	Ap3	Offline	60003	192.168.2.203	80	00-02-02-11-22-44	TCP	Wired

Fig. 44. Managed LAN devices.

On this page, the status of every managed LAN device is shown. The Offline status indicates a non-working device while the Online status indicates a working device. The **Add Device** button serves as a shortcut to the Advanced, LAN Device Management configuration page, on which you can specify which devices to manage. See Section 2.8.4 for more information.

2.3. SYSTEM

2.3.1. Specifying Operational Mode



○ Gateway with a PPPoE-Based DSL/Cable Connection

○ Gateway with a DHCP-Based DSL/Cable Connection

○ Gateway with a Static-IP DSL/Cable Connection

● Gateway with 3 DSL/Cable Connections

WAN Connection Types

WAN 1:	Static-IP	with Downlink:	512Kbps	Uplink:	512Kbps
WAN 2:	DHCP-based	with Downlink:	512Kbps	Uplink:	512Kbps
WAN 3:	PPPoE-based	with Downlink:	512Kbps	Uplink:	512Kbps

Fig. 44. Operational Modes.

On this page, you can specify the operational mode for the Router. Currently, 5 modes are available:

- Router with a PPPoE-based DSL/Cable Connection. In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by PPPoE from the ISP.
- Router with a DHCP-based DSL/Cable Connection. In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cablebased Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface is obtained automatically by DHCP from the ISP.
- Router with a Static-IP DSL/Cable Connection. In this mode, the Router assumes that a DSL or cable modem is connected to its Ethernet WAN interface. The client computers can therefore share this DSL/cable-based Internet connection by the NAT server functionality. The IP address of the Ethernet WAN interface must be manually set.
- Router with n DSL/Cable Connections. In this mode, the Router can support up to 4 (n = 2 to 4) DSL/cable-based Internet connections. The client computers can share the bandwidth of these Internet connections by the NAT server functionality. Since there are multiple Internet connections, total throughput is increased. The specified downlink and uplink data rates affect the load-balancing engine of the Router.

NOTE: When the Router is in Router with Multiple DSL/Cable Connections mode, connect your first DSL/Cable connection to WAN, the second to LAN 1, the third to LAN 2, and the fourth to LAN 3. Then, WAN becomes WAN 1, LAN 1 becomes WAN 2, LAN 2 becomes WAN 3, and LAN 3 becomes WAN 4 when referred to on the Web management pages.

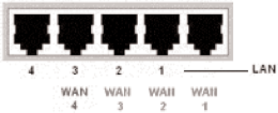
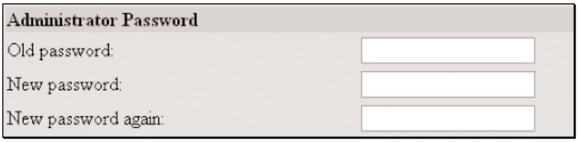


Fig. 45. WAN Port IDs.

TIP: After you have selected the operational mode of the Router, go to the TCP/IP, Addressing section of the management UI (see Section 2.4.1) to configure the addressing settings of the WAN and LAN interfaces.

NOTE: Since the WAN load-balancing algorithm is based on the "TCP session" rather than on the "packet," a TCP session is allocated to a WAN connection at session initialization time. As a result, if there is only one client, no throughput improvement will be perceived even if there are several WAN connections. WAN load balancing is for multiple clients to share multiple WAN connections. All the TCP sessions from the clients are intelligently distributed to the WAN connections by the built-in NAT server.

2.3.2. Changing Password



Administrator Password

Old password:

New password:

New password again:

Fig. 46. Password.

On this page, you can change the user name and password of the administrator. The administrator can view and modify the configuration of the SMCWHSG44-G. The new password must be typed twice for confirmation.

2.3.3. Managing Firmware

Firmware management protocol: HTTP

Fig. 47. Firmware Management Protocol Setting.

Firmware management operations for the Wireless Hotspot Gateway include firmware upgrade, configuration backup, configuration restore, and configuration reset. Firmware upgrade, configuration backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it's more user friendly. However, due to different behavior of different Web browser versions, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based way.

2.3.3.1. Upgrading Firmware by HTTP

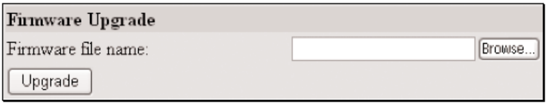


Fig. 48. Firmware Upgrade by HTTP.

To upgrade firmware of the SMCWHSG44-G by HTTP:

1. Click Browse and then select a correct firmware .bin file. The firmware file path will be shown in the Firmware file name text box.
2. Click Upgrade to begin the upgrade process.

2.3.3.2. Backing up and Restoring Configuration Settings by HTTP

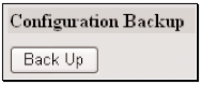


Fig. 49. Firmware Backup by HTTP.

To back up configuration of the SMCWHSG44-G by HTTP:

1. Click Back Up.
2. You'll be prompted to open or save the configuration file. Click Save.
3. The configuration file is named by the SMCWHSG44-G _backup.hex. Don't change the con-figuration file name in the Save As dialog box. Select a folder in which the configuration file is to be stored. And then, click Save.

NOTE: The procedure may be a little different with different Web browsers.

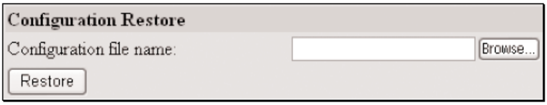
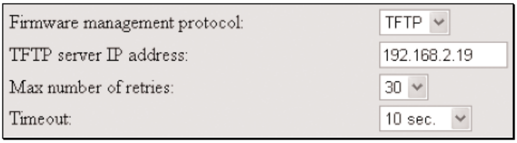


Fig. 50. Configuration Restore by HTTP.

To restore configuration of the SMCWHSG44-G by HTTP:

1. Click Browse and then select a correct configuration .hex file. You have to make sure the file name is the correct name “SMCWHSG44-G_Backup”. The configuration file path will be shown in the Configuration file name text box.
2. Click Restore to upload the configuration file to the wireless Hotspot gateway.

2.3.3.3. Upgrading Firmware by TFTP



Firmware management protocol:	TFTP
TFTP server IP address:	192.168.2.19
Max number of retries:	30
Timeout:	10 sec.

Fig. 51. TFTP Server Settings.

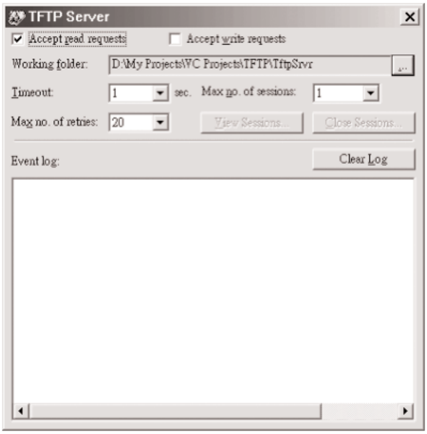
When using TFTP as the firmware management protocol, you can configure settings for the SMCWHSG44-G's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the Timeout setting, it will resend the previous request. The Max number of retries setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server. Within the folder "TFTP Server" on the companion CD-ROM disk, we offered a TFTP server program (TftpSrvr.exe) for firmware upgrade. Run this program on the computer that is to serve as a TFTP server.

Firmware Upgrade

Fig. 52. Firmware Upgrade by TFTP.

To upgrade firmware of the SMCWHSG44-G by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.
2. Connect the computer and one of the LAN Ethernet switch ports with a normal Ethernet cable.
3. Configure the IP address of the computer so that the Router and the computer are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.
5. On the computer, run a Web browser and click the System, Firmware Tools hyperlink.
6. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type ipconfig, then press the Enter key.
7. Trigger the firmware upgrade process by clicking Upgrade.


TFTP Server

☑ Accept read requests □ Accept write requests

Working folder: D:\My Projects\VC Projects\TFTP\TftpSrvr

Timeout: 1 sec. Max no. of sessions: 1

Max no. of retries: 20

Event log:

Fig. 53. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the Accept read requests check box of TFTP Server is selected.

NOTE: The LAN IP address of the SMCWHSG44-G and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: Due to the unreliable nature of wireless media, it's highly recommended that the TFTP server and the to-be-upgraded wireless gateway be connected by Ethernet, and on the same LAN, so that the upgrade process will be smooth.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the SMCWHSG44-G unstartable. When this occurs, reset the gateway to defaults by holding down the reset button on the back of the unit for about 10 seconds. If this does not work call for technical support.

2.3.3.4. Backing up and Restoring Configuration Settings by TFTP

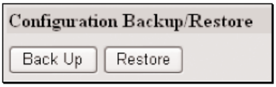


Fig. 54. Configuration Backup/Restore.

To back up configuration of the SMCWHSG44-G by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.

2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the SMCWHSG44-G are in the same IP subnet.
4. On the computer, run the TFTP Server utility. Select the Accept write requests check box, and specify the folder to which the configuration settings of the Router will be saved.
5. On the computer, run a Web browser and click the SYSTEM\Firmware Tools hyperlink.
6. Within the Configuration Backup/Restore section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type ipconfig, then press the Enter key.
7. Trigger the backup process by clicking Back Up. The Router's configuration settings will be saved as "SMCWHSG44-G_Backup.hex" by the TFTP server,

NOTE: Remember to select the Accept write requests check box of TFTP Server.

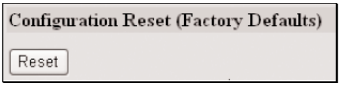
To restore configuration of the SMCWHSG44-G by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the SMCWHSG44-G are in the same IP subnet. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named SMCWHSG44-G_Backup. On the computer, run a Web browser and click the System, Firmware Tools.
4. Within the Configuration Backup/Restore section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type ipconfig, then press the Enter key.
5. Trigger the restore process by clicking Restore. The Router will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the Wireless Hotspot Gateway.

TIP: The configuration of a deployed SMCWHSG44-G can also be backed up or restored remotely from the Internet. In this case, you must have configured the Router to be remotely manageable (see Section 2.8.2) and adjust the Timeout and Max no. of retries settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

2.3.3.5. Resetting Configuration to Factory Defaults

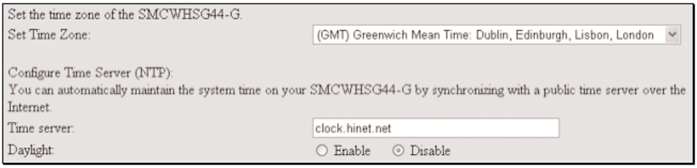


Configuration Reset (Factory Defaults)

Fig. 55. Configuration Reset.

Clicking the Reset button resets the device configuration to factory defaults. WARNING: Once you click Reset you will lose all your current configuration settings.

2.3.4. Time Zone



Set the time zone of the SMCWHSG44-G.

Set Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Configure Time Server (NTP):
You can automatically maintain the system time on your SMCWHSG44-G by synchronizing with a public time server over the Internet.

Time server: clock.hinet.net

Daylight: ○ Enable ● Disable

Fig. 56. Time Zone and Time Server Settings.

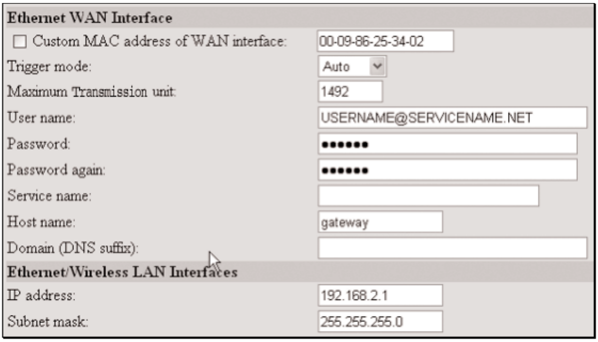
The SMCWHSG44-G supports system time by querying the SNTP (Simple Network Time Protocol) time server specified by the Time server setting. And you should specify the Time zone according to where you are.

2.4. Configuring TCP/IP Related Settings

2.4.1. Address

The addressing settings depend on the operational mode of the SMCWHSG44-G. Each operational mode requires different addressing settings.

2.4.1.1. Router with a PPPoE-Based DSL/Cable Connection



Ethernet WAN Interface	
□ Custom MAC address of WAN interface:	00-09-86-25-34-02
Trigger mode:	Auto
Maximum Transmission unit:	1492
User name:	USERNAME@SERVICENAME.NET
Password:	••••••
Password again:	••••••
Service name:	
Host name:	gateway
Domain (DNS suffix):	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.2.1
Subnet mask:	255.255.255.0

Fig. 57. TCP/IP Settings for Router with a PPPoE-Based DSL/Cable Connection Mode.

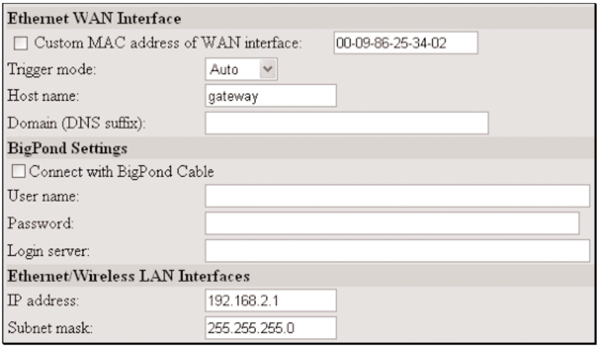
If the SMCWHSG44-G was set to be in Router with a PPPoE-Based DSL/Cable Connection mode, two IP addresses are needed: one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say 192.168.0.xxx. The default LAN IP address is 192.168.2.1 and the default subnet mask is 255.255.255.0. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained automatically by PPPoE from the ISP. Consult your ISP for the correct User name, Password, and Service name settings.

The Trigger mode setting specifies the way a PPPoE connection is established. Your PPPoE connection can be established and disconnected manually (Manual) by clicking the Connect and Disconnect buttons on the Start page, respectively. Or you can choose to let the device automatically (Auto) establish a PPPoE connection at boot-up time. In Auto mode, if the connection is disrupted, the device will try to re-establish the broken connection automatically.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.4.1.2. Router with a DHCP-Based DSL/Cable Connection



Ethernet WAN Interface

☐ Custom MAC address of WAN interface: 00-09-86-25-34-02

Trigger mode: Auto

Host name: gateway

Domain (DNS suffix):

BigPond Settings

☐ Connect with BigPond Cable

User name:

Password:

Login server:

Ethernet/Wireless LAN Interfaces

IP address: 192.168.2.1

Subnet mask: 255.255.255.0

Fig. 58. TCP/IP Settings for Router with a DHCP-Based DSL/Cable Connection Mode.

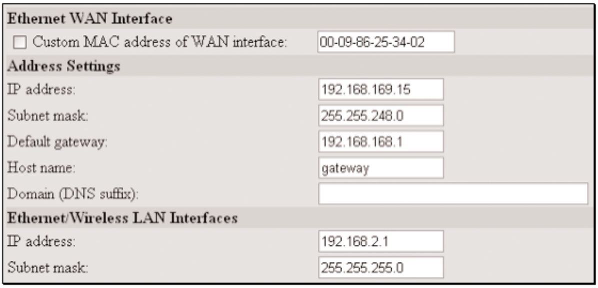
If the SMCWHSG44-G was set to be in Router with a DHCP-Based DSL/Cable Connection mode, two IP addresses are needed-one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say 192.168.0.xxx. The default LAN IP address is 192.168.2.1 and the default subnet mask is 255.255.255.0. In most cases, these default settings need no change.

As for the WAN IP address, it is obtained by DHCP from the ISP. The Trigger mode setting affects the behavior of the DHCP client of the Router. In Auto mode, you don't have to worry about the DHCP process; the device takes care of everything. In Manual mode, there are two buttons on the Start page for you to manually release an obtained IP address (Release) and reobtain a new one from a DHCP server (Renew).

“Big Pond Settings” is the settings for service of Telstra, Australia. Please consult the Telstra ISP for detail information.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.4.1.3. Router with a Static-IP DSL/Cable Connection



Ethernet WAN Interface

□ Custom MAC address of WAN interface: 00-09-86-25-34-02

Address Settings

IP address: 192.168.169.15

Subnet mask: 255.255.248.0

Default gateway: 192.168.168.1

Host name: gateway

Domain (DNS suffix):

Ethernet/Wireless LAN Interfaces

IP address: 192.168.2.1

Subnet mask: 255.255.255.0

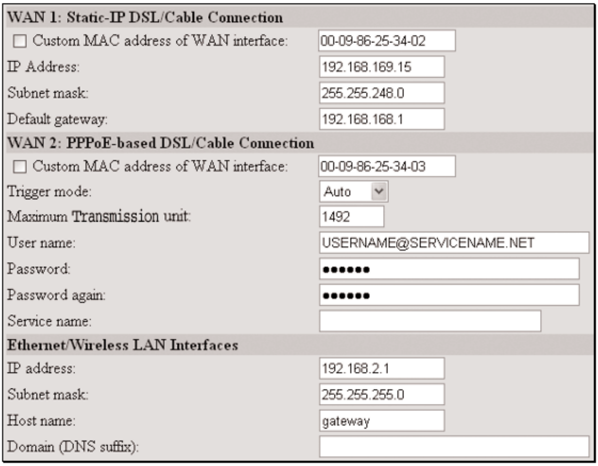
Fig. 59. TCP/IP Settings for Router with a Static-IP DSL/Cable Connection Mode.

If the Router was set to be in Router with a Static-IP DSL/Cable Connection mode, two IP addresses are needed-one for the Ethernet LAN interface and the other for the WAN interface. The LAN IP address must be set manually to a private IP address, say 192.168.2.xxx. The default LAN IP address is 192.168.2.1 and the default subnet mask is 255.255.255.0. In most cases, these default settings need no change.

As for the WAN IP address, it must be manually set. Consult your ISP for the correct IP address, Default gateway, Subnet mask, Primary DNS server, and Secondary DNS server settings.

Custom MAC Address of WAN Interface enables you to change the MAC address of the Ethernet WAN interface. Therefore, if the ISP-provided DSL or cable modem works only with the ISP-provided Ethernet card for a computer, the WAN interface of the Router can mimic the ISP-provided Ethernet card by changing its MAC address to the Ethernet card's MAC address.

2.4.1.4. Router with Multiple DSL/Cable Connections



WAN 1: Static-IP DSL/Cable Connection	
□ Custom MAC address of WAN interface:	00-09-86-25-34-02
IP Address:	192.168.169.15
Subnet mask:	255.255.248.0
Default gateway:	192.168.168.1
WAN 2: PPPoE-based DSL/Cable Connection	
□ Custom MAC address of WAN interface:	00-09-86-25-34-03
Trigger mode:	Auto
Maximum Transmission unit:	1492
User name:	USERNAME@SERVICENAME.NET
Password:	••••••
Password again:	••••••
Service name:	
Ethernet/Wireless LAN Interfaces	
IP address:	192.168.2.1
Subnet mask:	255.255.255.0
Host name:	gateway
Domain (DNS suffix):	

Fig. 60. TCP/IP Settings for Router with Multiple DSL/Cable Connections Mode.

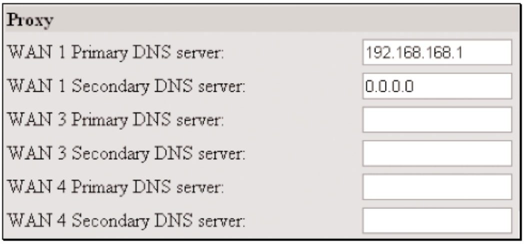
Since the Internet connection can be PPPoE-based, DHCP-based, or Static-IP-based, the addressing settings of each WAN interface are the same as those of Router with a PPPoE-Based DSL/Cable Connection, DHCP-Based DSL/Cable Connection, or Router with a Static-IP DSL/Cable Connection, respectively. As a result, refer to previous sections for more information.

2.4.2. DNS

2.4.2.1. DNS Proxy

SMCWHSG44-G provides the DNS Proxy function to enhance the network flexibility. Once the DNS Proxy function is enabled, SMCWHSG44-G will forward the DNS request from the client to a remote DNS server, the destination IP address response will also be forwarded by the DNS Proxy. The benefit is to allow the wireless clients to point the DNS to the IP address of the SMCWHSG44-G, no remote DNS IP address is required to be set on the wireless clients.

The setting of DNS Proxy corresponds with the 'Router with a Static-IP DSL/Cable Connection' of the WAN interface. If multiple WAN ports are enabled, all the DNS Proxy settings of the bound WAN ports under 'Router with a Static-IP DSL/Cable Connection' settings will be shown. For example, if WAN1 to WAN4 are all enabled and WAN1, WAN3, and WAN4 are using 'Router with a Static-IP DSL/Cable Connection' mode, the DNS Proxy settings will be shown as below:

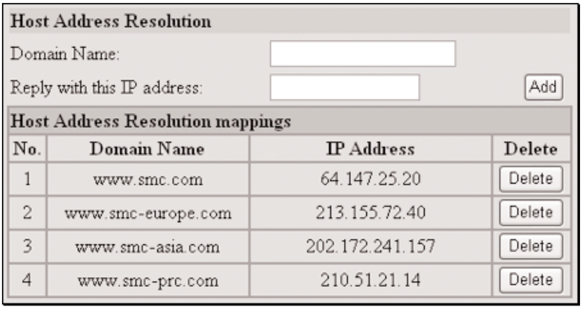


Proxy

WAN 1 Primary DNS server:	192.168.168.1
WAN 1 Secondary DNS server:	0.0.0.0
WAN 3 Primary DNS server:	
WAN 3 Secondary DNS server:	
WAN 4 Primary DNS server:	
WAN 4 Secondary DNS server:	

Fig. 61. DNS Proxy under Multi-WAN Mode.

2.4.2.2. Host Address Resolution



Host Address Resolution

Domain Name:

Reply with this IP address:

Host Address Resolution mappings

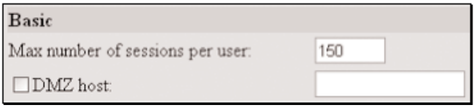
No.	Domain Name	IP Address	Delete
1	www.smc.com	64.147.25.20	Delete
2	www.smc-europe.com	213.155.72.40	Delete
3	www.smc-asia.com	202.172.241.157	Delete
4	www.smc-prc.com	210.51.21.14	Delete

Fig. 62. Host Address Resolution Mappings.

The SMCWHSG44-G provides the Host Address Resolution to provide the local DNS server capability. The Host Address Resolution (local DNS server) function of SMCWHSG44-G will respond to the DNS request of wireless clients and reply the requested destination IP address. The benefits for local DNS server is that there is no Internet traffic (request going out through WAN port) required for local queries, hence it lowers the Internet traffic.

2.4.3. NAT

2.4.3.1. Basic



Basic

Max number of sessions per user:	150
□ DMZ host:	

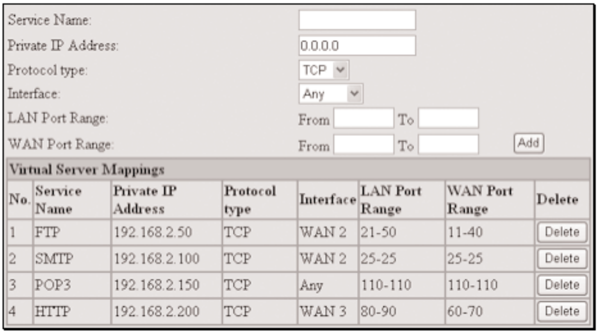
Fig. 63. Basic NAT Server Settings.

When the SMCWHSG44-G is in Router with a Static-IP DSL/Cable Connection mode, the NAT server functionality can be enabled or disabled.
You can restrict the maximum number of user traffic sessions by specifying the Max number of sessions per user setting. In this way, you can prevent a single user from consuming too many network resources by initiating a large number of network sessions.

A DMZ (DeMilitarized Zone) host receives all unrecognized TCP/IP packets from the NAT server on the Router; therefore TCP/IP networking applications running on the DMZ host would have better compatibility with NAT.
To specify the DMZ host:

- Enter the private IP address of the computer to be used as a DMZ host, and select the corresponding check box.

2.4.3.2. Virtual Server Mappings



Service Name:	
Private IP Address:	0.0.0.0
Protocol type:	TCP
Interface:	Any
LAN Port Range:	From To
WAN Port Range:	From To Add

Virtual Server Mappings

No.	Service Name	Private IP Address	Protocol type	Interface	LAN Port Range	WAN Port Range	Delete
1	FTP	192.168.2.50	TCP	WAN 2	21-50	11-40	Delete
2	SMTP	192.168.2.100	TCP	WAN 2	25-25	25-25	Delete
3	POP3	192.168.2.150	TCP	Any	110-110	110-110	Delete
4	HTTP	192.168.2.200	TCP	WAN 3	80-90	60-70	Delete

Fig. 64. Virtual Server Mappings.

The SMCWHSG44-G enables you to expose internal servers on the intranet through NAT to the Internet for public use. The exposed internal servers are called virtual servers because from the perspective of hosts on the Internet, these servers are invisible in terms of TCP/IP.

To expose "preset" internal servers:

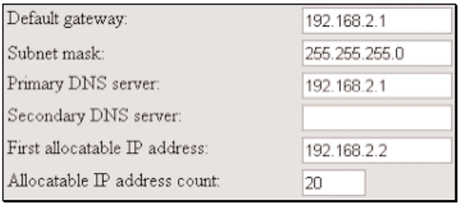
1. Input the service name (FTP, IMAP4, SMTP, POP3, TELNET, and HTTP) for the kinds of servers you want to expose.
2. Specify the private IP addresses of the internal servers.
3. Select the protocol type (TCP or UDP) of this service
4. Select the WAN port interface for particular service port.
5. Input the LAN and WAN port range which will be associated to this service. Note that the port range of LAN and WAN must be the same length.

2.4.4. DHCP Server

There are three modes of the DHCP Server to be defined in 'Functionality': Disable, DHCP Server, and DHCP Relay.

2.4.4.1. DHCP Server

i. Basic



Default gateway:	192.168.2.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.2.1
Secondary DNS server:	
First allocatable IP address:	192.168.2.2
Allocatable IP address count:	20

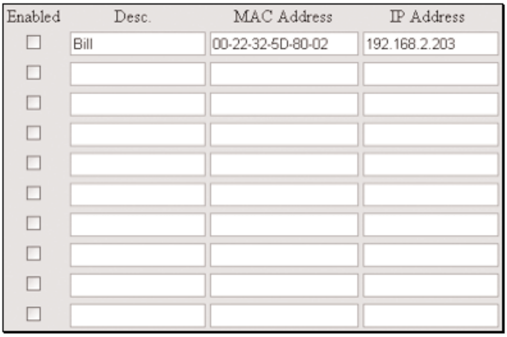
Fig. 65. Basic DHCP server settings.

The SMCWHSG44-G can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the Default gateway, Subnet mask, Primary DNS server, and Secondary DNS server settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocatable IP addresses.

In most cases, Default Gateway and Primary DNS server should be set to the IP address of the Router's LAN interface (e.g., the default LAN IP address is 192.168.2.1), and Subnet mask is set to 255.255.255.0.

NOTE: There should be only one DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the Router.

ii. Static DHCP Mappings



Enabled	Desc.	MAC Address	IP Address
□	Bill	00-22-32-5D-80-02	192.168.2.203
□			
□			
□			
□			
□			
□			
□			
□			
□			

Fig. 66. Static DHCP Mappings.

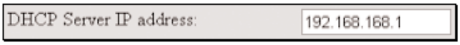
IP addresses of servers are often static so that clients can always locate the servers by the static IP ad-dresses. By Static DHCP Mappings, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is always assigned the same IP address.

To always assign an IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description for this mapping.
2. Select the corresponding Enabled check box.

2.4.4.2. DHCP Relay

When the DHCP server functionality is set to "DHCP Relay", the SMCWHSG44 won't assign the IP address to the clients. It will forward the received DHCP requests from the clients to the designate DHCP server. The only setting for DHCP relay is DHCP server IP address.



DHCP Server IP address: 192.168.168.1

Fig. 67. DHCP Relay Settings.

2.4.5. Load Balancing

The SMCWHSG44-G provides a WAN port Load Balancing mechanism. Without any policy specified in default settings, the outgoing traffic (from LAN to WAN, also known as 'Out-bound Load-balancing') will be automatically balanced between every enabled WAN port, hence the traffic will be equally balanced under the same throughput level of every WAN interface.

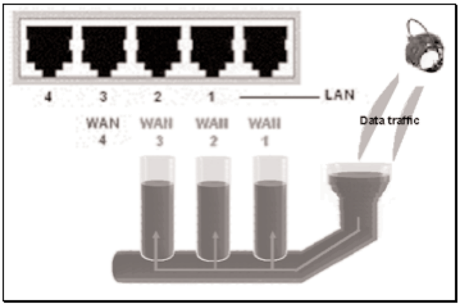
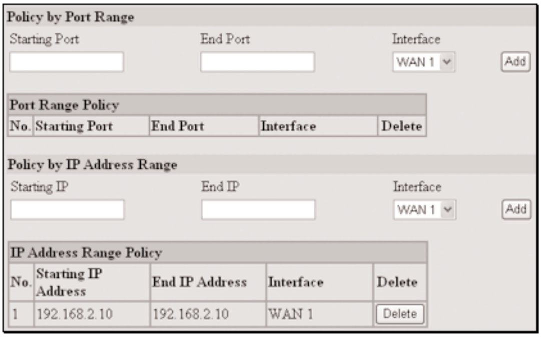


Fig. 68. Load Balancing Mechanism.

In addition, the SMCWHSG44-G can also set the load balancing policy by Port or IP range, so that the traffic of specified Port or IP range will be assigned the appointed WAN interface.



Policy by Port Range

Starting Port	End Port	Interface	
		WAN 1	Add

Port Range Policy

No.	Starting Port	End Port	Interface	Delete

Policy by IP Address Range

Starting IP	End IP	Interface	
		WAN 1	Add

IP Address Range Policy

No.	Starting IP Address	End IP Address	Interface	Delete
1	192.168.2.10	192.168.2.10	WAN 1	Delete

Fig. 69. Load Balancing Policy Settings.

2.4.6. Zero Client Reconfiguration

☐ Client IP/ARP handling

Fig. 70. Zero Client Reconfiguration Settings.

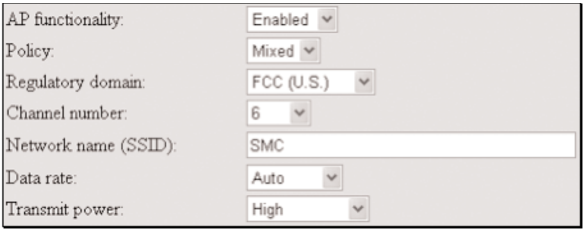
The SMCWHSG44-G provides the 'Zero Client Reconfiguration' function to allow the wireless clients that associate to the SMCWHSG44-G the ability to not make any network setting modifications. This feature is useful in case users already have static IP information or IP addressing set for another network. With this feature any user can connect to the Gateway without changing any network settings. The 'Zero Client Reconfiguration' function is enabled by checking the box of 'Client IP/ARP handling'.

2.5. Configuring IEEE 802.11-Related Settings

2.5.1. Wireless

2.5.1.1. Basic

Basic IEEE 802.11b/g-related communication settings include AP functionality, Regulatory domain, Channel number, Network name (SSID), Data rate, and Transmit power.



AP functionality:	Enabled
Policy:	Mixed
Regulatory domain:	FCC (U.S.)
Channel number:	6
Network name (SSID):	SMC
Data rate:	Auto
Transmit power:	High

Fig. 71. Basic IEEE 802.11b/g Communication Settings.

For specific needs such as configuring the SMCWHSG44-G as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the SMCWHSG44-G.

The Policy setting allows you to run in mode, B only or G only. In mixed mode both 802.11b and 802.11g clients are able to connect. In B only mode only 802.11b clients can connect, and in G only mode only 802.11g clients will be able to connect wirelessly to the gateway.
The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations.

An SSID is the name in which wireless clients will use to associate to your wireless LAN. The SSID of a wireless client computer and the SSID of the SMCWHSG44-G must be identical for them to communicate with each other Since the IEEE 802.11g-based SMCWHSG44-G is also IEEE 802.11b compatible, you can configure the Data rate setting to meet your backwards compatibility needs. If there is RF interference, you may want to reduce the Data rate for more reliable wireless transmission. In most cases, leave the setting to Auto.

NOTE: The Regulatory domain setting of the SMCWHSG44-G sold in the U.S. and Canada is not configurable. It's set to FCC by default. As a result, only channels from 1 to 11 are available.

The transmit power of the RF module of the SMCWHSG44-G can be adjusted so that the RF cover-age of the SMCWHSG44-G can be changed. This is helpful when you only need to cover a certain area and do not want your signal to go beyond that point of coverage.

2.5.1.2. Wireless Distribution System

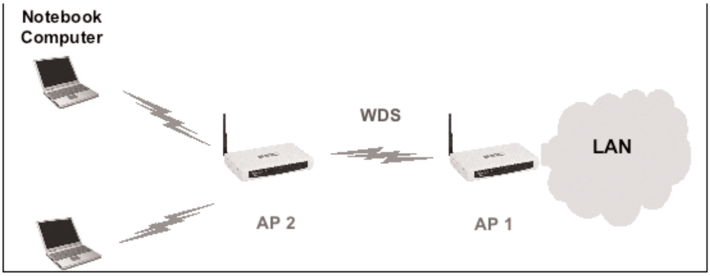
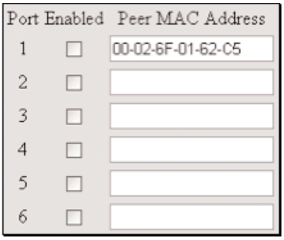


Fig. 72. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 72, the SMCWHSG44-G acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to the AP/bridge through WDS. Then, the SMCWHSG44-G forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the SMCWHSG44-G to the notebook computers. In this way, the SMCWHSG44-G plays a role of "AP repeater."

NOTE: The SMCWHSG44-G can have up to 6 WDS links to other wireless AP/bridge.



Port	Enabled	Peer MAC Address
1	□	00-02-6F-01-62-C5
2	□	
3	□	
4	□	
5	□	
6	□	

Fig. 73. Wireless Distribution System Settings.

To enable a WDS link:

1. Specify the MAC address of the AP or wireless bridge at the other end of the WDS link.
2. Select the corresponding Enabled check box.

For example, assume you want the SMCWHSG44-G and an AP (with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 respectively) to establish a WDS link between them. On the SMCWHSG44-G (00-02-65-01-62-C5), set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on AP (00-02-65-01-62-C6), set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how the SMCWHSG44-G is connected to other peer APs or wireless bridges by WDS.

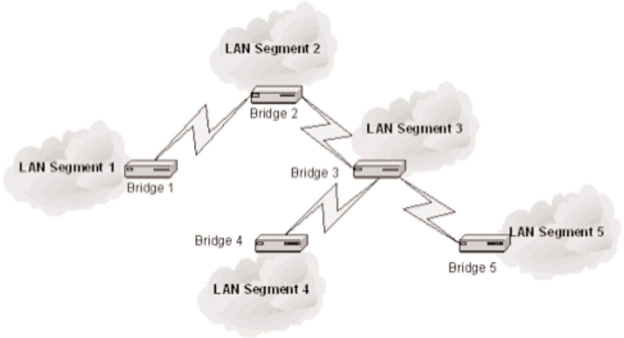


Fig. 74. Sample Wireless Bridge Network Topology.

WARNING: Do not let your network topology consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links that form a loop. If there are any loops that exist, packets will circle around the loops and network performance will be seriously degraded.

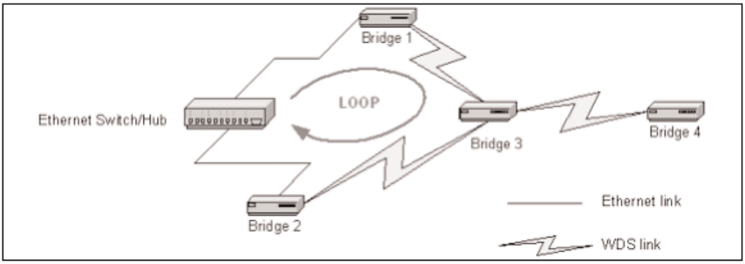
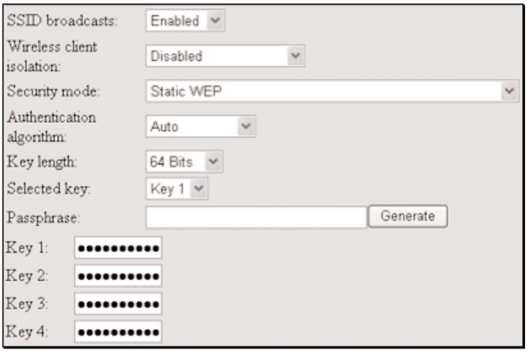


Fig. 75. Network Topology Containing a Loop.

2.5.2. Security

IEEE 802.11b/g security settings include SSID broadcasts, Client Isolation, IEEE 802.11 Authentication algorithm, WEP, WPA, and MAC-Address-Based Access Control.

2.5.2.1. Basic



SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	Static WEP
Authentication algorithm:	Auto
Key length:	64 Bits
Selected key:	Key 1
Passphrase:	Generate
Key 1:	●●●●●●●●●●●
Key 2:	●●●●●●●●●●●
Key 3:	●●●●●●●●●●●
Key 4:	●●●●●●●●●●●

Fig. 76. Basic IEEE 802.11g Security Settings.

For security reasons, it's highly recommended that the security mode be set to options other than Open System. When the security mode is set to Open System, no authentication and data encryption will be performed.

You can disable the SSID broadcasts functionality so that a wireless client (STA or AP) with an "ANY" SSID cannot associate with the SMCWHSG44-G. With this feature enabled any wireless user can see your wireless LAN and connect to it with an SSID of "ANY".

Wireless Client Isolation is a feature for the SMCWHSG44-G to block wireless-to-wireless traffic between STAs so that the STAs cannot see each other. This feature is useful for WLANs deployed in public places. This way, hackers have no chance to attack other wireless users in a Hotspot.

When the Wireless client isolation setting is set to This AP Only, wireless clients (STAs) associated to this SMCWHSG44-G, which acts as an AP, cannot see each other, and wireless-to-wireless traffic between the STAs is blocked.

When the setting is set to "All APs in This Subnet", traffic among wireless users of different SMCWHSG44-Gs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

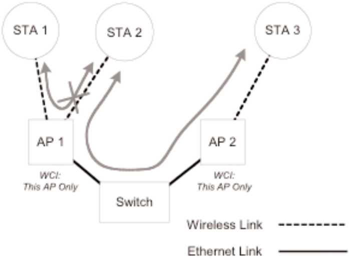


Fig. 77. Behavior of the “This AP Only” Wireless Client Isolation Option.

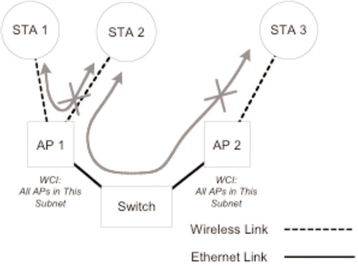


Fig. 78. Behavior of the “All APs on This Subnet”
Wireless Client Isolation Option.

As illustrated in Fig. 77 when AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the “All APs in This Subnet” option is used as shown in Fig. 78, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 7 security modes: supported by the SMCWHSG44-G (based on WEP, WPA or Authentication Algorithm)

- Open System. No authentication, no data encryption.
- Static WEP. WEP (Wired Equivalent Privacy) keys must be manually configured.
- Static TKIP (WPA-PSK). Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the Pre-shared key, which will be used by the TKIP engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

NOTE: The number of characters of the Pre-shared key setting must be at least 8 and can be up to 63.

- IEEE 802.1x EAP without Encryption (EAP-MD5). The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- IEEE 802.1x EAP with Static WEP (EAP-MD5). The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP). The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- IEEE 802.1x EAP with Dynamic TKIP (WPA). This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The SMCWHSG44-G is highly secure in this mode.

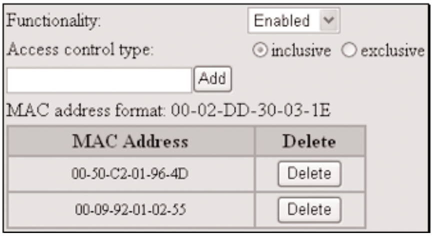
In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, Shared Key authentication is used if WEP data encryption is enabled. In rare cases, Open System authentication may be used when WEP data encryption is enabled. The Authentication algorithm setting is provided for better compatibility with wireless client computers with various WLAN network adapters. There are three options available, including Open System, Shared Key, and Auto.

When WEP is enabled by a security mode, the Key length can be specified to be 64 Bits or 128 Bits. The Selected key setting specifies the key to be used as a send-key for encrypting traffic from the local device side to the remote device side. All 4 WEP keys are used as receive-keys to decrypt traffic from the remote device side to the local device side.

NOTE: Each field of a WEP key setting is a hex-decimal number from 0-9, A-F. For example, when the security mode is Static WEP and the key length is 64 Bits, you could set Key 1 to “00012E3ADF”.

2.5.2.2. MAC-Address-Based Access Control



Functionality: Enabled

Access control type: ● inclusive ○ exclusive

MAC address format: 00-02-DD-30-03-1E

MAC Address	Delete
00-50-C2-01-96-4D	Delete
00-09-92-01-02-55	Delete

Fig. 79. MAC-Address-Based Access Control Settings.

With MAC-Address-Based Access Control, you can specify the wireless clients (STAs or Bridge Slaves) that are permitted or not permitted to associate with the SMCWHSG44-G. When the table type is set to inclusive, entries in the table are permitted to associate and all other users are blocked. When the table type is set to exclusive, entries in the table are not permitted to associate with the SMCWHSG44-G while other users are allowed access.

To deny wireless clients' access to the wireless network:

1. Select Enabled from the Functionality drop-down list.
2. Set the Access control type to exclusive.
3. Specify the MAC address of a wireless client to be denied access, and then click Add.
4. Repeat Step 3 for each other wireless client.

To grant wireless clients' access to the wireless network:

1. Select Enabled from the Functionality drop-down list.
2. Set the Access control type to inclusive.
3. Specify the MAC address of a wireless client to allow access, and then click Add.
4. Repeat Step 3 for each other wireless client.

To delete an entry in the access control table:

- Click Delete next to the entry.

NOTE: The size of the access control table is 64.

2.5.3. IEEE 802.1x/RADIUS

IEEE 802.1x Port-Based Network Access Control is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x, a RADIUS (Remote Authentication Dial-In User Service) server, and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granting access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her user name and password or digital certificate to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the access point is controlled by the security mode (see Section 2.5.2.1). So far, the wireless access point supports two authentication mechanisms-EAP-MD5 (Message Digest version 5), EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her user name and password for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's digital certificate that is stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

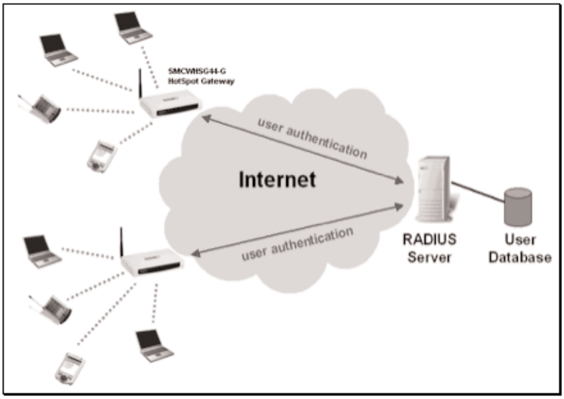
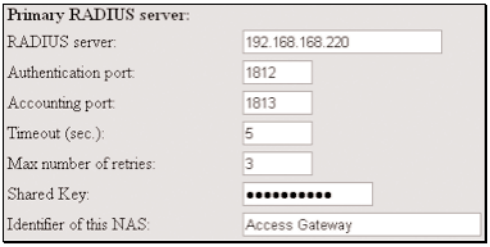


Fig. 80. IEEE 802.1x and RADIUS.

The SMCWHSG44-G supports IEEE 802.1x and can be configured to communicate with two RA-DIUS servers. When the primary RADIUS server fails to respond, the SMCWHSG44-G will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the secondary RADIUS server after failing to commu-nicate with the primary RADIUS server.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1x-capable wireless access point must have a unique NAS identifier.



Primary RADIUS server:

RADIUS server:	192.168.168.220
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	●●●●●●●●●●●
Identifier of this NAS:	Access Gateway

Fig. 81. IEEE 802.1x/RADIUS Settings.

2.6. Configuring Authentication Settings

The SMCWHSG44-G supports both IEEE 802.1x-based and Web redirection-based user authentication.

Here is a brief description of how Web redirection works: When an unauthenticated wireless user is trying to access a Web page, a logon page is shown instead of the requested page, so that the user can type his/her user name and password for authentication. Then, the user credential information is sent to a back-end RADIUS (Remote Authentication User Dial-In Service) server or checked against the built In Local Authentication database in the Wireless Hotspot Gateway to see if the wireless user is allowed to access the Internet. The authentication mechanism employed for RADIUS is EAP-MD5, PAP, or CHAP.

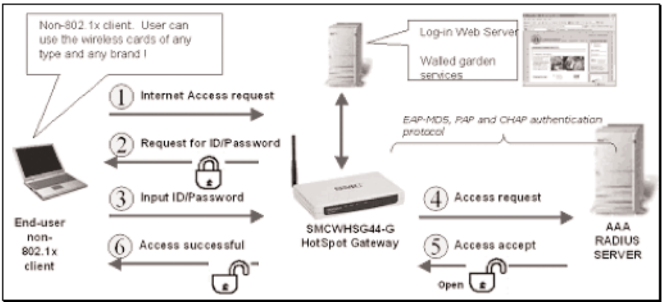
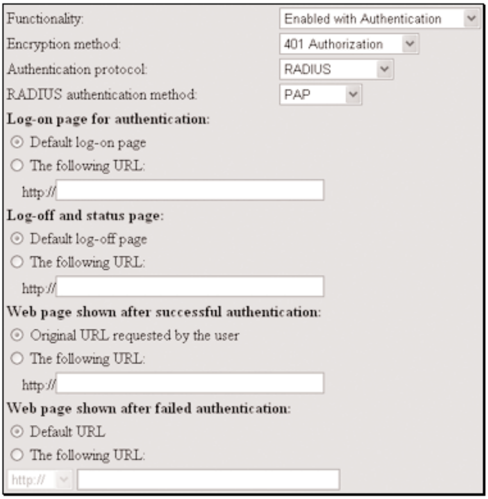

Non-802.1x client. User can use the wireless cards of any type and any brand !
Log-in Web Server
Walled garden services
1 Internet Access request
2 Request for ID/Password
3 Input ID/Password
6 Access successful
EAP-MD5, PAP and CHAP authentication protocol
4 Access request
5 Access accept
Open
End-user non-802.1x client
SMCWHSG44-G HotSpot Gateway
AAA RADIUS SERVER

Fig. 82. Web-Redirection Mechanism.

TIP: For IEEE 802.1x-based user authentication, see Section 2.5.3

2.6.1. AAA

2.6.1.1. Basic



Functionality: Enabled with Authentication

Encryption method: 401 Authorization

Authentication protocol: RADIUS

RADIUS authentication method: PAP

Log-on page for authentication:

● Default log-on page

○ The following URL:

http://

Log-off and status page:

● Default log-off page

○ The following URL:

http://

Web page shown after successful authentication:

● Original URL requested by the user

○ The following URL:

http://

Web page shown after failed authentication:

● Default URL

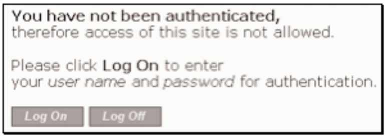
○ The following URL:

http://

Fig. 83. Web-Redirection Enabled with Authentication.

There are three modes for Web redirection-Enabled with Authentication, Enabled without Authentication, and Disabled.
In Enabled with Authentication mode, you have two options. Radius Authenticaion or Local Authentication built into the SMCWHS44-G. Currently for Radius Authentication EAP-MD5, PAP, and CHAP are supported.

When a wireless user tries to access the Internet, he/she is redirected to a Default log-on page or a page stored on an external Web server (The following URL), depending on the network administrator's choice.



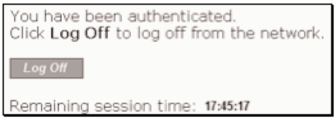
You have not been authenticated,
therefore access of this site is not allowed.

Please click **Log On** to enter
your *user name* and *password* for authentication.

Fig. 84. Default log-On Page.

After the wireless user passes authentication, the user can be brought to the original page requested (Original URL requested by the user) or to a default page for advertisement purposes (The following URL). For example, if “http://www.smc.com” is set for The following URL, the user will be brought to the website of SMC.

In addition, the Log-Off window is also shown after the wireless user passes authentication. The Log-Off window can be configured to contain the Default log-off page or a page stored on an external Web server (The following URL).



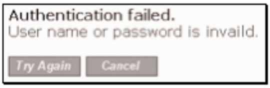
You have been authenticated.
Click **Log Off** to log off from the network.

Remaining session time: 17:45:17

Fig. 85. Default Log-Off Page.

NOTE: On a PDA such as Pocket PC, the log-off would not be shown. To log off from the network, go back to the log-on page, and then click Log Off to end the session.

If the user fails the authentication, the user can be brought to a default warning page (Default page) or a page for the user to subscribe a wireless Internet access service (The following URL).

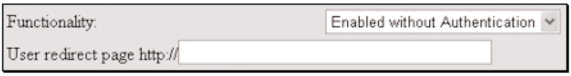


Authentication failed.
User name or password is invaild.

Fig. 86. Default Authentication Failure Warning Page.

NOTE: If you choose The following URL for Log-on page for authentication, Log-off and status page, or Web page shown after failed authentication, the pages stored on an external server have to contain specific HTML/ JavaScript code so that Web redirection can work without error. Use the source of the default pages as templates for design your own authentication pages.

NOTE: Because your customized versions of authentication pages have to contain references to the SMCWHSG44-G's LAN IP address (192.168.2.1 by default). If the LAN IP address of the Wireless Hotspot Gateway is changed, you must remember to change the IP address references in your customized pages.



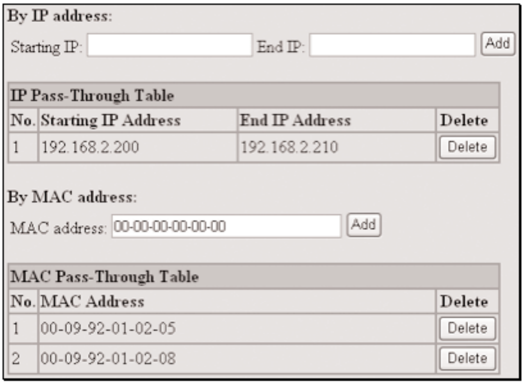
Functionality: Enabled without Authentication

User redirect page http://

Fig. 87. Web-Redirection Enabled without Authentication.

In Enabled without Authentication mode, a user can access the Internet through the SMCWHSG44-G without being authenticated first. However, instead of accessing his/her requested page, he/she is first redirected to a URL for advertisement purposes (User redirect page).

2.6.1.2. Unrestricted Clients



By IP address:

Starting IP: End IP: Add

IP Pass-Through Table			
No.	Starting IP Address	End IP Address	Delete
1	192.168.2.200	192.168.2.210	Delete

By MAC address:

MAC address: 00-00-00-00-00-00 Add

MAC Pass-Through Table		
No.	MAC Address	Delete
1	00-09-92-01-02-05	Delete
2	00-09-92-01-02-08	Delete

Fig. 88. Unrestricted Clients Settings.

There are occasions on which you want some computers to be able to freely access the Internet without being authenticated first. For example, you may want your wired desktop computers connected with the SMCWHSG44-G to be uncontrolled while providing wireless Internet access service for your customers with wireless laptop computers. The Unrestricted Clients feature is for this purpose.

You can specify the computers to be uncontrolled by IP address or MAC address.

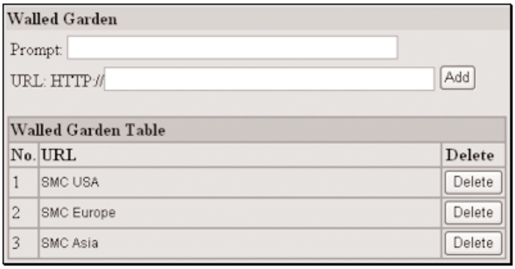
To specify uncontrolled computers within an IP address range:

1. Specify the Stating IP and End IP addresses of the IP address range.
2. Click Add. Then you'll see the newly entered IP address range appear in the IP Pass-Though Table.

To specify an uncontrolled computer by MAC address:

1. Specify its MAC address.
2. Click Add. Then you'll see the newly entered MAC address appear in the MAC Pass-Through Table.

2.6.1.3. Walled Garden



Walled Garden

Prompt:

URL: HTTP://

Walled Garden Table

No.	URL	Delete
1	SMC USA	Delete
2	SMC Europe	Delete
3	SMC Asia	Delete

Fig. 89. Walled Garden Settings.

IP addresses or URLs in the walled garden can be accessed without authentication. This feature is useful for WISPs to do advertisement. For example, a WISP can set up a Web server to contain advertisement information for users who have not subscribed to its wireless Internet service. The walled garden links are shown on the log-on authentication page.

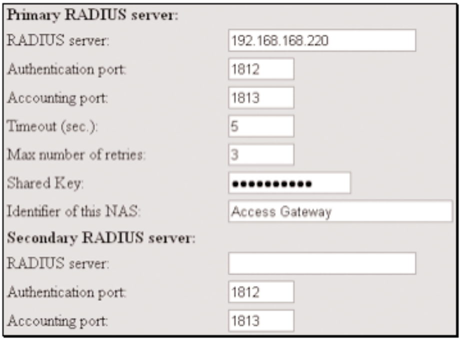
To add a link to the walled garden:

1. Describe this link in the Prompt text box.
2. Specify the URL of this link in the URL text box.
3. Click Add. Then you'll see the newly entered hyperlink appear in the Walled Garden Table.

NOTE: You cannot specify a Web site that supports Web redirection, which redirects HTTP requests to another URL, as a walled garden site. If such a Web-redirection-enabled site is specified in the walled garden, an HTTP access request to this site is redirected to another site that is "out of" the walled garden. And the user is therefore needs to be authenticated to access this out-of-walled-garden site. Always specify a Web site that actually hosts Web content as a walled garden site.

2.6.2. RADIUS

2.6.2.1. Basic



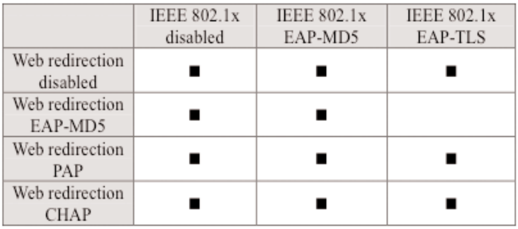
Primary RADIUS server:	
RADIUS server:	192.168.168.220
Authentication port:	1812
Accounting port:	1813
Timeout (sec.):	5
Max number of retries:	3
Shared Key:	●●●●●●●●●●●
Identifier of this NAS:	Access Gateway
Secondary RADIUS server:	
RADIUS server:	
Authentication port:	1812
Accounting port:	1813

Fig. 90. RADIUS Basic Settings.

For the SMCWHSG44-G, the RADIUS client component of the Router is shared by the IEEE 802.1x and Web redirection components. The RADIUS settings are for the RADIUS client to communicate with backend RADIUS servers.

NOTE: When configured for EAP authentication, the RADIUS server supports either EAP-TLS or EAP-MD5, but not both at the same time. As a result, not all combinations of EAP-MD5, EAP-TLS, PAP and CHAP authentication methods are available if both IEEE 802.1x and Web redirection are enabled. The following table shows the allowable IEEE 802.1x and Web redirection authentication modes on the Wireless Advanced edition of access Router.

Table 2. Allowable Authentication Modes.

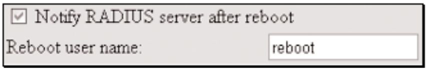


	IEEE 802.1x disabled	IEEE 802.1x EAP-MD5	IEEE 802.1x EAP-TLS
Web redirection disabled	■	■	■
Web redirection EAP-MD5	■	■	
Web redirection PAP	■	■	■
Web redirection CHAP	■	■	■

The SMCWHSG44-G can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the SMCWHSG44-G will try to communicate with the secondary RADIUS server. You can specify the length of timeout and the number of retries before communicating with the secondary RADIUS server after failing to communicate with the primary RA-DIUS server.

The SMCWHSG44-G and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, the SMCWHSG44-G can identify itself by an NAS (Network Access Server) identifier. Each SMCWHSG44-G must have a unique NAS identifier.

2.6.2.2. Robustness



☑ Notify RADIUS server after reboot

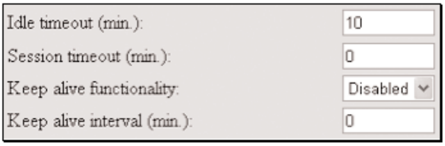
Reboot user name: reboot

Fig. 91. RADIUS Robustness Settings.

The Router can be configured to notify the RADIUS server after it reboots. The RADIUS server can make use of the notification to clean up user authentication session records in the event that the Router reboots unexpectedly due to abnormal operation.

Select the Notify RADIUS server after reboot check box to enable this capability, and then specify the name of the pseudo user (default to "reboot") for this operation in the Reboot user name text box.

2.6.3. Authentication Session Control



Idle timeout (min.):	10
Session timeout (min.):	0
Keep alive functionality:	Disabled
Keep alive interval (min.):	0

Fig. 92. Authentication Session Control Settings.

Authentication session control settings are for controlling the lifetimes of user authentication sessions. The Idle timeout setting specifies how long a user can be idle without generating any traffic before being terminated. The Session timeout setting specifies the maximum session lifetime.

In addition, the Router provides a mechanism for detecting whether a user has left unexpectedly by handshaking between JavaScript code in the log-off authentication page and the Router. The log-off page notifies the Router periodically to announce user existence. When this mechanism for user existence detection is enabled (Keep alive functionality), the Router will terminate a user if no notification is received from the log-off page on the user's computer within the number of minutes specified by the Keep alive interval setting.

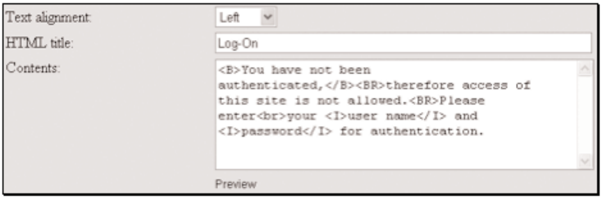
NOTE: A zero value in the Idle timeout, Session timeout, or Keep alive interval setting disables the corresponding functionality effectively.

NOTE: The Log-Off window cannot not be shown on a Windows CE-based Pocket PC due to different JavaScript behavior of Pocket Explorer. To support Windows CE-based clients, you have to disable the keep-alive mechanism; otherwise the clients will be terminated unexpectedly.

2.6.4. Authentication Page Customization

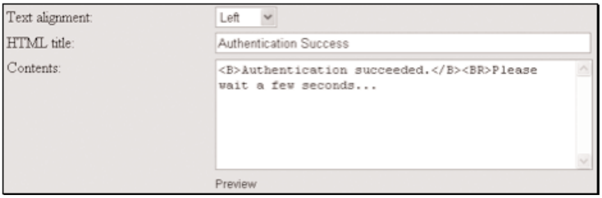
2.6.4.1. Log-On, Authentication Success, and Authentication Failure Pages

Log-on, authentication success, and authentication failure authentication pages can be customized in a similar way. You can specify the Text alignment style, page title (HTML title) and the Contents. The Contents setting accepts HTML tagging. Clicking the Preview link shows a test page for you to see the results.



Text alignment:	Left
HTML title:	Log-On
Contents:	<B>You have not been authenticated,</B><BR>therefore access of this site is not allowed.<BR>Please enter your <I>user name</I> and <I>password</I> for authentication.

Fig. 93. Log-On Page Customization Settings.



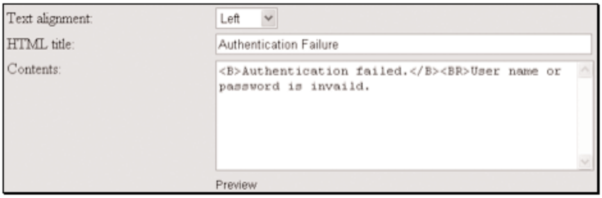
Text alignment: Left

HTML title: Authentication Success

Contents:

```
<B>Authentication succeeded.</B><BR>Please
wait a few seconds...
```

Fig. 94. Authentication Success Page Customization Settings.



Text alignment: Left

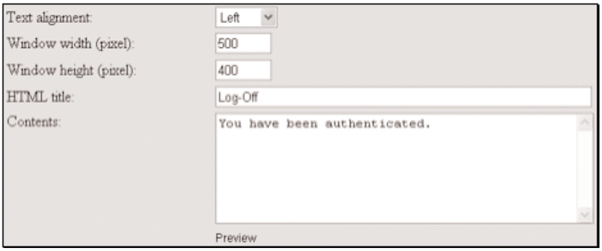
HTML title: Authentication Failure

Contents:

```
<B>Authentication failed.</B><BR>User name or
password is invaild.
```

Fig. 95. Authentication Failure Page Customization Settings.

In addition to the Text alignment, HTML title, and Contents setting, two more settings are provided for specifying the size of the Log-Off window (Windows width and Window height).



Text alignment: Left

Window width (pixel): 500

Window height (pixel): 400

HTML title: Log-Off

Contents:

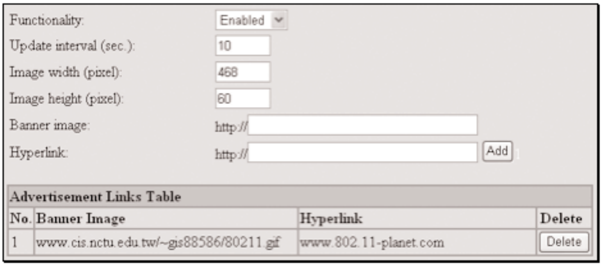
```
You have been authenticated.
```

Fig. 96. Log-Off Page Customization Settings.

Furthermore, Banner images and Hyperlinks can be added to the Log-Off window for advertisement purposes. The banner images are shown in sequence at an interval specified by the Update interval setting. You can also specify the size of the banner image (Image width and Image height).

To specify an advertisement link:

1. Type the Banner image URL.
2. Type the Hyperlink URL.
3. Click the Add button, and then this advertisement link appears in the Advertisement Links Table.

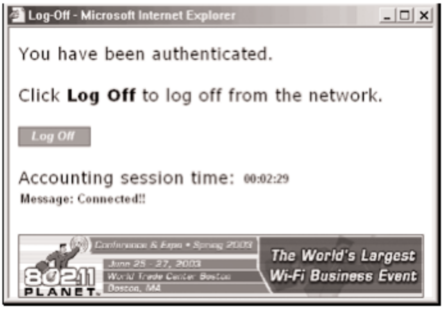


Functionality:	Enabled
Update interval (sec.):	10
Image width (pixel):	468
Image height (pixel):	60
Banner image:	http://
Hyperlink:	http://

Advertisement Links Table

No.	Banner Image	Hyperlink	Delete
1	www.cis.nctu.edu.tw/~gis88586/80211.gif	www.802.11-planet.com	Delete

Fig. 97. Advertisement Links Settings.



Log-Off - Microsoft Internet Explorer

You have been authenticated.

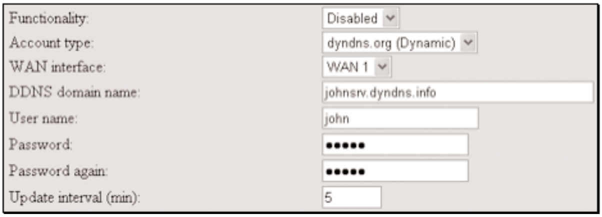
Click **Log Off** to log off from the network.

Accounting session time: 00:02:29

Message: Connected!!

Fig. 98. Advertisement Links in Action.

2.7. DDNS



Functionality:	Disabled
Account type:	dyndns.org (Dynamic)
WAN interface:	WAN 1
DDNS domain name:	johnsrv.dyndns.info
User name:	john
Password:	●●●●●
Password again:	●●●●●
Update interval (min):	5

Fig. 99. Dynamic DNS Settings.

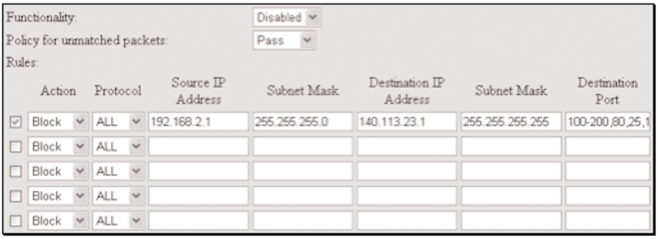
With the help of dynamic DNS (DDNS) services provided by dyndns.org or no-ip.com, you can make your device automatically register the IP address it obtains dynamically by PPPoE or DHCP with the DDNS servers. DDNS is useful if you want to set up a Web server whose IP address is dynamically obtained rather than statically configured.

Choose your DDNS service provider from the Account type drop-down list, choose the WAN inter-face on which the DDNS client operates, and specify the DDNS domain name, User name, and Password you have registered with your service provider. The DDNS client of the Router periodically communicates with its DDNS server at an interval specified by the Update interval setting.

2.8. Configuring Advanced Settings

2.8.1. Filters and Firewall

2.8.1.1. Packet Filters



Functionality: Disabled

Policy for unmatched packets: Pass

Rules:

	Action	Protocol	Source IP Address	Subnet Mask	Destination IP Address	Subnet Mask	Destination Port
☑	Block	ALL	192.168.2.1	255.255.255.0	140.113.23.1	255.255.255.255	100-200,80,25,1
□	Block	ALL					
□	Block	ALL					
□	Block	ALL					
□	Block	ALL					

Fig. 100. Packet Filters Settings.

You can specify rules for the firewall component of the Router to check outgoing packets. Packets that meet the rules can be permitted or denied. The protocol field, source IP address field, destination IP address field, and destination port field of a packet's IP header are inspected to see if it meets a rule. A packet that meets a rule can be dropped (Block) or accepted (Accept) as specified in the Action setting of the rule. Packets that do not meet any rules can be dropped (Discard) or accepted (Pass) as specified in the Policy setting.

A rule is composed of 5 parts:

- What to do if a packet meets this rule (Action)
- Protocol type
  - All
  - ICMP
  - TCP
  - UDP
- Source IP address range (Source IP Address AND Source Subnet Mask)
- Destination IP address range (Destination IP Address AND Destination Subnet Mask)
- Port ranges

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

Up to 5 port ranges can be specified in a rule, and these ranges must be separated by commas. For example, “21,80,85-89,140,200-230” in the destination port field signifies 5 port ranges.

To set a rule for packet filtering:

1. Specify the protocol type, source IP address, source IP mask, destination IP address, destination IP mask, and destination port for the rule. Then specify in the Action setting how to deal with a packet that meets the rule.
2. Select the corresponding Enabled check box.

NOTE: Set the rules with great care since incorrect rules would make the Router inaccessible. The last resort to restore the Router to service may be resetting its configuration to factory-set values by pressing the reset button on the back of the Router.

2.8.1.2. VLAN

□ Block wireless-to-Ethernet-LAN traffic

Fig. 101. VALN Settings.

VLAN (Virtual Local Area Network) settings are for traffic isolation. When the Block wireless-to-Ethernet-LAN traffic check box is selected, the Router does not forward packets between the wireless network interface and the Ethernet LAN interface-traffic is allowed only between the Ethernet WAN interface and the wireless network interface.

2.8.1.3. Firewall

□ Enable SPI (Stateful Packet Inspection)

□ Block ICMP PING from Internet

Fig. 102. Packet Filters and Firewall Settings.

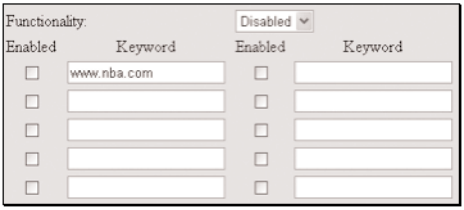
SPI analyzes incoming and outgoing packets based on a set of criteria for abnormal content. Therefore, SPI can detect hacker attacks, and can summarily reject an attack if the packet fits a suspicious profile. To enable SPI, select the Enable Stateful Packet Inspection (SPI) check box.

Some DoS (Denial of Service) attacks are based on sending invalid ICMP request packets to hosts. The Router can be set to not accept any ICMP requests on the Ethernet WAN interface to defend against attacks of this kind. Enable this capability by selecting the Block ICMP PING from Internet check box.

NOTE: SPI can detect hacker attacks, including IP-Spoofing, Zero IP Length, Land, Smurf, Fraggle, Teardrop, Ping of Death, Syn-Flood, and X-Tree.

NOTE: Because some of the Router's CPU resources are spent in checking packets for these security features, you may notice network performance degradation if the security functions are enabled.

2.8.1.4. URL Filters


Functionality: Disabled

Enabled	Keyword	Enabled	Keyword
□	www.nba.com	□	
□		□	
□		□	
□		□	
□		□	

Fig. 103. URL Filters Settings.

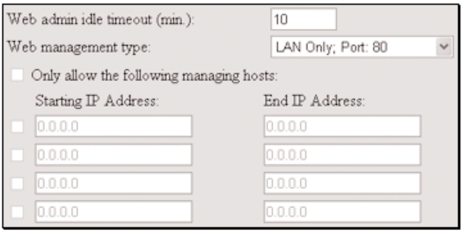
The SMCWHSG44-G is capable of blocking HTTP traffic from the intranet to specified unwelcome Web sites.

To block HTTP traffic to an unwelcome Web site:

1. Specify the URL (ex. www.xxx.com) of the unwelcome Web site.
2. Select the corresponding Enabled check box.

2.8.2. Management

2.8.2.1. Basic


Web admin idle timeout (min.): 10

Web management type: LAN Only; Port: 80

□ Only allow the following managing hosts:

	Starting IP Address:	End IP Address:
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0
□	0.0.0.0	0.0.0.0

Fig. 104. Web-Based Management Setting.

Web admin idle timeout (min) means the idle timeout period for an administrator while logged into the Router

The SMCWHSG44-G can be managed locally from the LAN side, remotely from the WAN side, or from both LAN and WAN. If the management type is WAN Only or WAN and LAN, be sure to specify the port 8080 when typing a URL for managing a Router within a Web browser. For example, if the WAN interface of a Router is configured to be 61.16.33.113, the URL for managing this Router is “http://61.16.33.113:8080”.

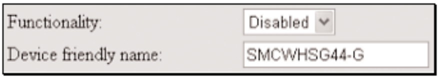
In addition, if the management type is set to WAN Only, the Router can be configured to be manageable only from specific hosts. In this way, security of remote management is enhanced.

To make the Router remotely manageable from specific hosts within an IP address range:

1. Select the Only allow the following managing hosts check box.

2. Type the Starting IP address and the End IP Address of the host IP address range.
3. Select the corresponding check box next to the IP address range.

2.8.2.2. UPnP



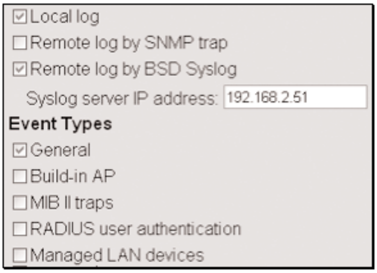
Functionality: Disabled

Device friendly name: SMCWHSG44-G

Fig. 105. UPnP Settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the Router in My Network Places of Windows XP. The Router can be given a name that will be shown in My Network Places. Double-clicking the icon in My Network Places will launch the default Web browser for you to configure the Router.

2.8.2.3. System Log



☑ Local log
☐ Remote log by SNMP trap
☑ Remote log by BSD Syslog
Syslog server IP address: 192.168.2.51

Event Types
☑ General
☐ Build-in AP
☐ MIB II traps
☐ RADIUS user authentication
☐ Managed LAN devices

Fig. 106. System Log Settings.

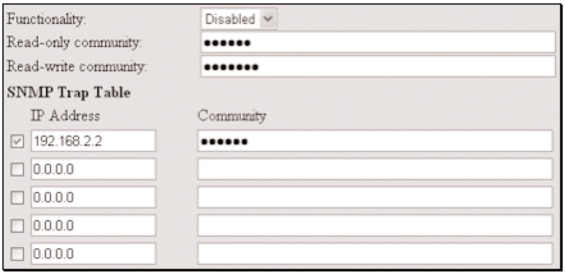
System events can be logged to the on-board RAM of the SMCWHSG44-G (Local log) or sent in the form of SNMP trap (Remote log by SNMP trap) or BSD Syslog (Remote log by BSD Syslog) to a remote SNMP trap monitoring server or remote Syslog server, respectively. See the next subsection for more information about SNMP trap settings. Set the IP address of the Syslog server in the Syslog server IP address text box.

The system events are divided into the following categories:

- General: system and network connectivity status changes.
- Built-in AP: wireless client association and WEP authentication status changes.
- MIB II traps: Cold Start, Warm Start, Link Up, Link Down and SNMP Authentication Failure.

NOTE: The SNMP Authentication Failure trap is issued when using an incorrect community string to manage the Router via SNMP and the SNMP MIB II OID, snmpEnableAuthenTraps, is enabled (disabled by default).

2.8.2.4. SNMP



Functionality: Disabled

Read-only community: ••••••

Read-write community: •••••••

SNMP Trap Table

	IP Address	Community
☑	192.168.2.2	••••••
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	
□	0.0.0.0	

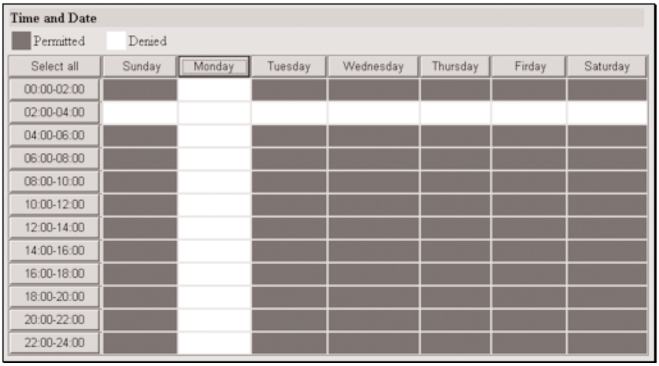
Fig. 107. SNMP Settings.

The SMCWHSG44-G can be managed by SNMP (Simple Network Management Protocol). You can specify the name (used as a password) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the SNMP Trap table.

To specify a trap target:

1. Type the IP address of the target host.
2. Type the Community for the host.
3. Select the corresponding check box next to the IP address text box.

2.8.3. Access Rules



Time and Date

▨ Permitted □ Denied

Select all	Sunday	Monday	Tuesday	Wednesday	Thursday	Firday	Saturday
00:00-02:00	▨	□	▨	▨	▨	▨	▨
02:00-04:00	□	□	□	□	□	□	□
04:00-06:00	▨	□	▨	▨	▨	▨	▨
06:00-08:00	▨	□	▨	▨	▨	▨	▨
08:00-10:00	▨	□	▨	▨	▨	▨	▨
10:00-12:00	▨	□	▨	▨	▨	▨	▨
12:00-14:00	▨	□	▨	▨	▨	▨	▨
14:00-16:00	▨	□	▨	▨	▨	▨	▨
16:00-18:00	▨	□	▨	▨	▨	▨	▨
18:00-20:00	▨	□	▨	▨	▨	▨	▨
20:00-22:00	▨	□	▨	▨	▨	▨	▨
22:00-24:00	▨	□	▨	▨	▨	▨	▨

Fig. 109. Access Rules Settings.

The SMCWHSG44-G provides the 'Access Rules' to permit/deny the wireless users access in specified date/time frame.

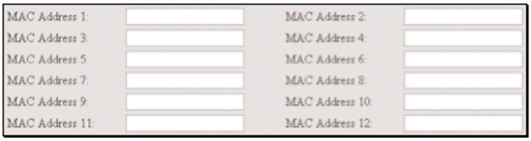
To specify the SMCWHSG44-G access rule with the date/time frame:

1. Select the Column of the Date / Time Access Rule Table (default all columns are 'Permitted'), the specified column will be 'Denied' and turn to white.
2. Continue step 1 until all preferred Date/Time column specified to be 'Denied'.

3. The 'Denied' columns can be also specified by selecting the head of lines (time) or columns (date).

Wireless users cannot access the internet resources in the specified date/time columns. For example, see Fig. 105, the specified columns mean 'Wireless users are not allowed to access the Internet every Monday and 02:00 ~ 04:00 Sunday through Saturday.

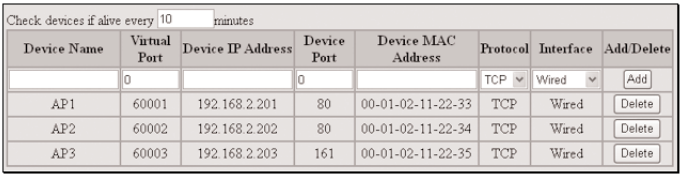
With Unrestricted Host, you can specify the MAC address of wireless clients that are permitted to access the Internet within the Access Rule defined period. There are 12 MAC address entries to allow multiple unrestricted hosts.



MAC Address 1:		MAC Address 2:	
MAC Address 3:		MAC Address 4:	
MAC Address 5:		MAC Address 6:	
MAC Address 7:		MAC Address 8:	
MAC Address 9:		MAC Address 10:	
MAC Address 11:		MAC Address 12:	

Fig. 110. Unrestricted Host MAC Address Settings.

2.8.4. LAN Device Management



Check devices if alive every 10 minutes

Device Name	Virtual Port	Device IP Address	Device Port	Device MAC Address	Protocol	Interface	Add/Delete
	0		0		TCP	Wired	Add
AP1	60001	192.168.2.201	80	00-01-02-11-22-33	TCP	Wired	Delete
AP2	60002	192.168.2.202	80	00-01-02-11-22-34	TCP	Wired	Delete
AP3	60003	192.168.2.203	161	00-01-02-11-22-35	TCP	Wired	Delete

Fig. 110. LAN Device Management Settings.

LAN device management is for the SMCWHSG44-G to pass management requests from the Internet through its built-in NAT server to devices on the private network. As a result, network devices (such as access points) behind the NAT server can be managed from the Internet. In this way, the Wireless Hotspot Gateway acts as a management proxy for the LAN devices. In addition, the SMCWHSG44-G can periodically check whether the managed devices are working by Pinging them (Check devices if alive every n minutes). If it detects a device not working, it can send an SNMP trap (remote system logging) to a back-end server to report such a situation. The LAN device management functionality is especially useful for a WISP to remotely manage deployed APs that are usually invisible from the Internet due to the employment of NAT for IP address space conservation.

A management server from the Internet sees a managed LAN device as a combination of the Wireless Hotspot Gateway's WAN IP address and a Virtual Port reserved for this device. When a TCP or UDP-based management request (specified by the Protocol field) is received by the Wireless Hotspot Gateway from the Internet, the SMCWHSG44-G translates the destination IP address and destination port of the request to the corresponding Device IP Address and Device Port. In other words, this request is passed through the built-in NAT server of the Router and routed to the corresponding man-aged LAN device.

For example, Fig. 111 illustrates a LAN device management scenario based on the settings values in Fig. 110. AP1 can be managed from the management server by using a Web browser and a URL “http://61.16.31.110:60001”. AP2 can be managed by using a Web browser and a URL “http://61.16.31.110:60002”. AP3 can be managed from the management server by using an SNMP manager program via IP address 61.16.31.110 and port 60003. Destination IP addresses and destination ports of management packets for AP1, AP2, and AP3 are translated to 192.168.168.201:80, 192.168.168.202:80, and 192.168.168.203:161, respectively. (161 is a well known port for SNMP management.)

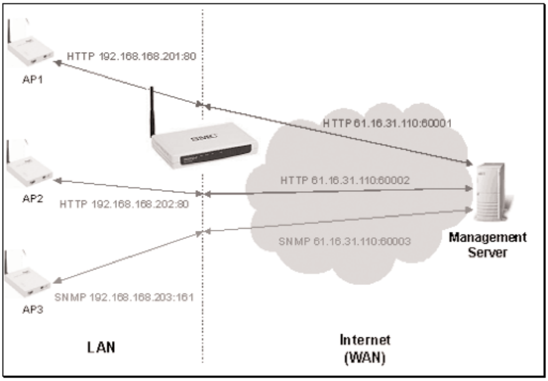


Fig. 111. Example for LAN Device Management.

To specify a LAN device to manage:

1. Give a name for this device in the Device Name text box.
2. Type the Virtual Port, Device IP Address, Device Port, and Device MAC Address for this device.
3. Choose the type of the management protocol (TCP or UDP) from the Protocol drop-down list.
4. Choose whether the Router communicates with the device wirelessly by WDS (Wireless) or by Ethernet (Wired) from the Interface drop-down list.
5. Select the corresponding check box next to the Device Name text box.

NOTE: A valid input for the Virtual Port field must be between 60001 and 60100 inclusive.

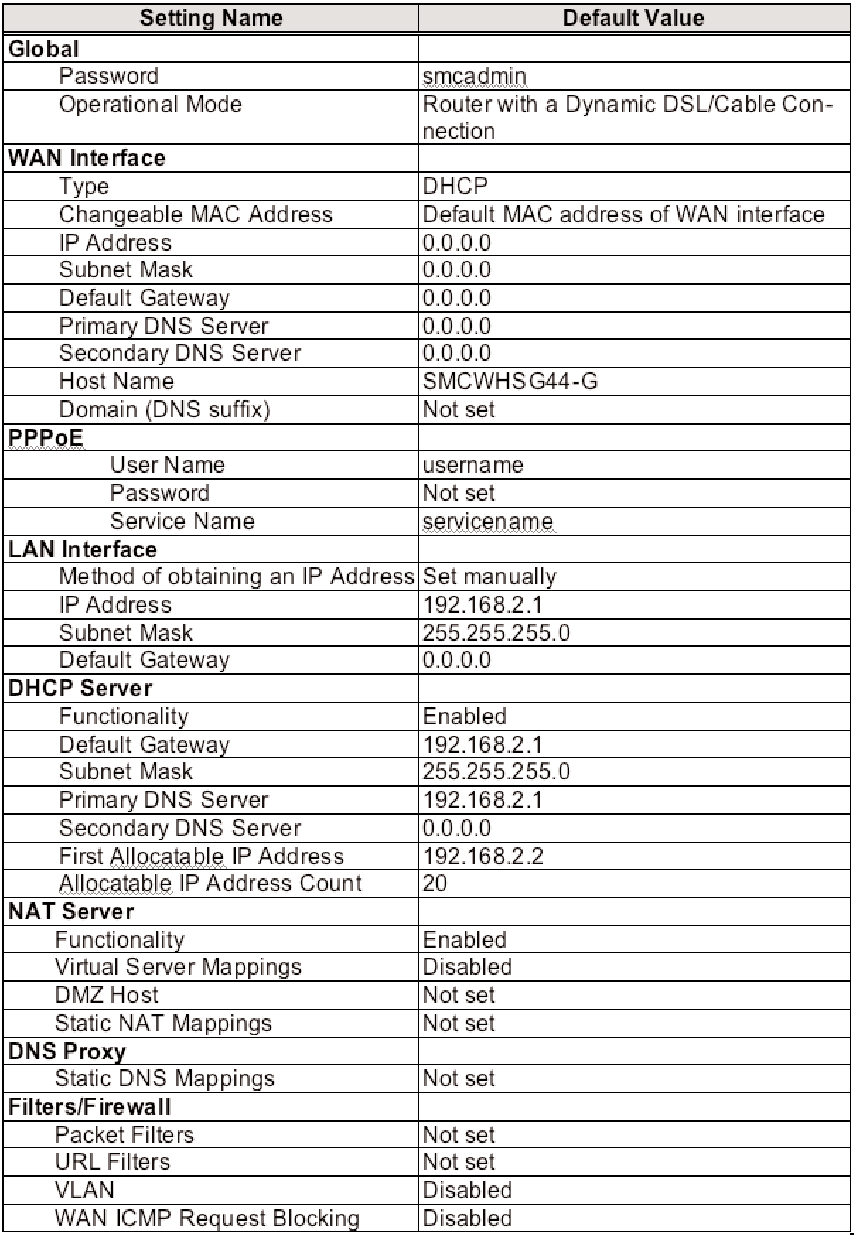
NOTE: The IP address in a Device IP Address text box and the Router's LAN IP address must be in the same IP subnet.

NOTE: The Device Name, Device MAC Address, and the Interface fields are informational. They do not affect the inner workings of LAN device management.

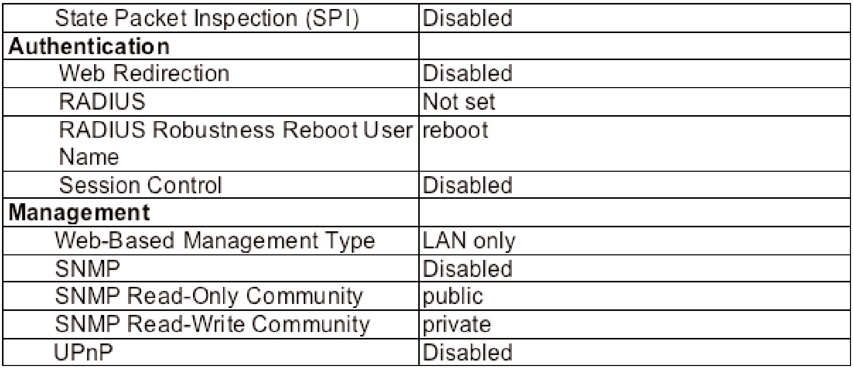
Appendix A

A-1: Default Settings

TIP: Press the reset button of a powered-on Router to reset the configuration settings to factory-set values.



Setting Name	Default Value
Global	
Password	smcadmin
Operational Mode	Router with a Dynamic DSL/Cable Connection
WAN Interface	
Type	DHCP
Changeable MAC Address	Default MAC address of WAN interface
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Host Name	SMCWHSG44-G
Domain (DNS suffix)	Not set
PPPoE	
User Name	username
Password	Not set
Service Name	servicename
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	
Functionality	Enabled
Default Gateway	192.168.2.1
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.2.1
Secondary DNS Server	0.0.0.0
First Allocatable IP Address	192.168.2.2
Allocatable IP Address Count	20
NAT Server	
Functionality	Enabled
Virtual Server Mappings	Disabled
DMZ Host	Not set
Static NAT Mappings	Not set
DNS Proxy	
Static DNS Mappings	Not set
Filters/Firewall	
Packet Filters	Not set
URL Filters	Not set
VLAN	Disabled
WAN ICMP Request Blocking	Disabled

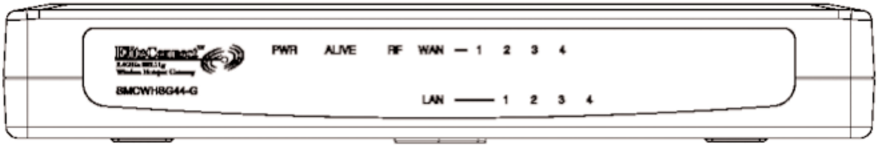


State Packet Inspection (SPI)	Disabled
Authentication	
Web Redirection	Disabled
RADIUS	Not set
RADIUS Robustness Reboot User Name	reboot
Session Control	Disabled
Management	
Web-Based Management Type	LAN only
SNMP	Disabled
SNMP Read-Only Community	public
SNMP Read-Write Community	private
UPnP	Disabled

A-2: LED Definitions

There are several LED indicators on the housing of a Router. They are defined as follows:

- **PWR** : Power
- **ALV** : Alive. Blinks when the SMCWHSG44-G is working normally.
- **RF** : IEEE 802.11b/g interface activity
- **WAN/LAN** : Ethernet WAN/LAN interface activity



Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the Router is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the Router.
- Make sure that the LED ALV of the Router is blinking to indicate the Router is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types-normal and crossover.
- Make sure that the DSL or cable modem connected to the Router is powered on.

B-1: TCP/IP Setting Problems

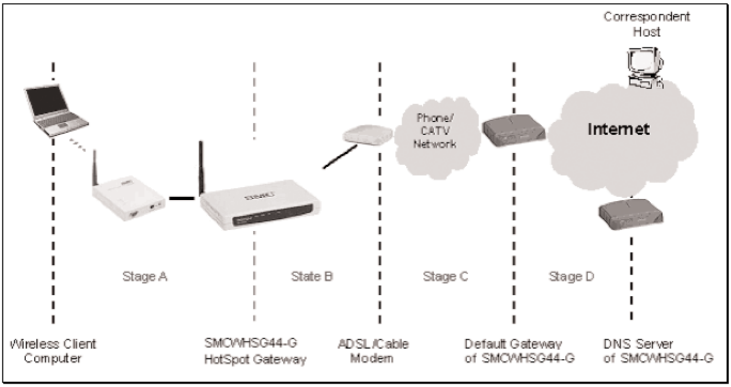


Fig. 113. Communication Stages for A Client to Reach its Correspondent Host.

For a client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. http://www.smc.com), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the SMCWHSG44-G, then the SMCWHSG44-G relays this request to the default gateway of the SMCWHSG44-G through a modem. Finally, this request is forwarded by the default gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP ad-dress.

As illustrated in Fig. 113, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, ping.exe, can be employed to find out TCP/IP-related communication problems.

NOTE: If two or more NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, route.exe, to add or delete entries from the routing table. Or, use Windows-provided Device Manager to disable unnecessary NICs.

Solve the following problems in order:

- The wireless client cannot pass Web redirection-based authentication.
  - Verify whether the user name and password are correct?
    - Check the user credential information stored on the RADIUS server or locally on the SMCWHS44-G.
- Is the RADIUS server correctly set up?
  - Check whether the password for the wireless client is stored using reversible encryption on the RADIUS server.

  - Check if the RADIUS server is set to use EAP-MD5, PAP, and CHAP authentication.
- The SMCWHSG44-G does not respond to ping from the client computer.
  - Are two or more NICs (wireless or wired) installed on the client computer?
    - Use Windows-provided Device Manager to disable unnecessary NICs.
  - Is the underlying communication link established?
    - Make sure the wireless link is OK.
    - Make sure the Ethernet link between the AP and the SMCWHSG44-G is OK.
    - Make sure the settings of the client computer and of the SMCWHSG44-G match.
  - Are the IP address of the client computer and the IP address of the SMCWHSG44-G in the same IP subnet?
    - Use WinIPCfg.exe or IPConfig.exe to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the SMCWHSG44-G are in the same IP subnet.
- The default gateway of the SMCWHSG44-G does not respond to ping from the client computer.
  - Solve the preceding problem first.
  - Is the modem working?
  - You may find out the answer by directly connecting the modem to a computer. Refer-ring to the manual of the modem if necessary.
  - Is the NAT server functionality of the SMCWHSG44-G enabled?
    - Find out the answer on the start page of the Web-Based Network Manager.
  - If you cannot find any incorrect settings of the SMCWHSG44-G, the default gateway of the SMCWHSG44-G may be really down or there are other communication problems on the network backbone.
- The DNS server(s) of the SMCWHSG44-G do not respond to ping from the client computer.
  - Solve the preceding problems first.
  - If you cannot find any incorrect settings of the SMCWHSG44-G, the default gateway of the SMCWHSG44-G may be really down or there are other communication problems on the network backbone.
- Cannot access the Internet.
  - Solve the preceding problems first.
  - Make sure there are no incorrect packet filter settings that would block the traffic from the local computer to the Internet. In case you are not sure, the last resort may be resetting the configuration settings of the SMCWHSG44-G to default values by pressing the Reset button.

B-2: Wireless Settings Problems

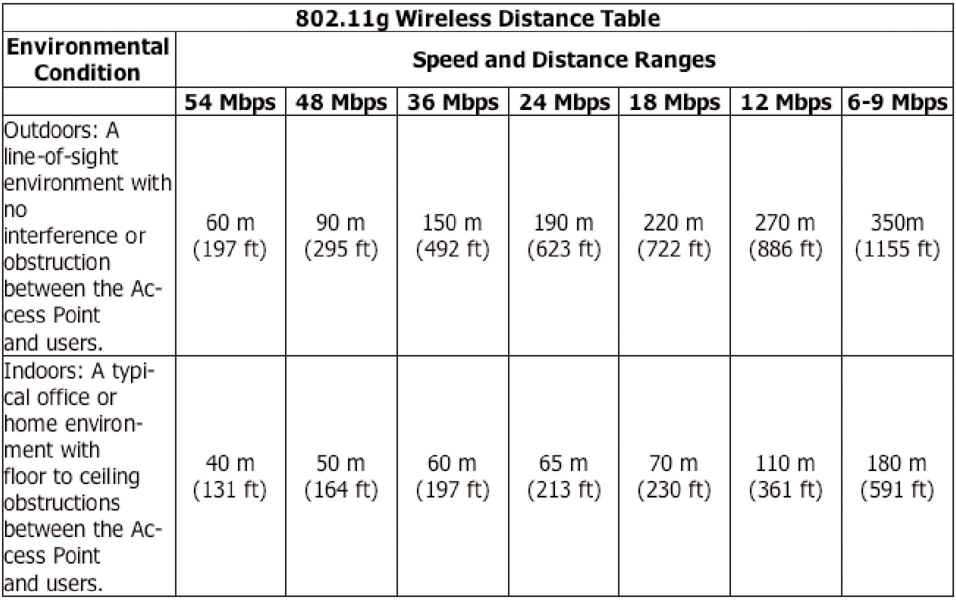
- The wireless client computer cannot associate with an SMCWHSG44-G.
  - Is the wireless client set in infrastructure mode?
    - Check the operating mode of the WLAN NIC.
  - Is the SSID of the WLAN NIC identical to that of the prospective SMCWHSG44-G?
    - Check the SSID setting of the WLAN NIC and of the SMCWHSG44-G.
  - Is the Security functionality of the prospective SMCWHSG44-G enabled?
    - Make appropriate Security settings of the client computer to match those of the SMCWHSG44-G.
  - Is the prospective SMCWHSG44-G within range of wireless communication?
    - Check the signal strength and link quality sensed by the WLAN NIC.

B-3: Other Problems

- My SMCWHSG44-G stops working and does not respond to Web management requests.
  - The firmware of the SMCWHSG44-G may be stuck in an incorrect state.
    - Unplug the power connector from the power jack, and then re-plug the connector to restart the SMCWHSG44-G.
    - Contact our technical support representatives to report this problem, If this happens after a failed firmware upgrade process, the firmware of the SMCWHSG44-G may have been corrupted.
  - If the SMCWHSG44-G still does not work after restarting, there may be hardware component failures in the SMCWHSG44-G.
    - Contact our technical support representatives for repair.

Appendix C: Distances and Data Rates

Important Notice: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below. If you have any questions or comments regarding the features or performance of this product, or if you'd like information regarding our full line of wireless products, you can visit us on the web at www.smc.com or you can call us toll-free at 800.SMC.4YOU. SMC Networks stands behind this and every product we sell with a 30 day satisfaction guarantee and with a limited-lifetime warranty.



802.11g Wireless Distance Table							
Environmental Condition	**Speed and Distance Ranges**						
	54 Mbps	**48 Mbps**	**36 Mbps**	**24 Mbps**	**18 Mbps**	**12 Mbps**	**6-9 Mbps**
Outdoors: A line-of-sight environment with no interference or obstruction between the Access Point and users.	60 m (197 ft)	90 m (295 ft)	150 m (492 ft)	190 m (623 ft)	220 m (722 ft)	270 m (886 ft)	350m (1155 ft)
Indoors: A typical office or home environment with floor to ceiling obstructions between the Access Point and users.	40 m (131 ft)	50 m (164 ft)	60 m (197 ft)	65 m (213 ft)	70 m (230 ft)	110 m (361 ft)	180 m (591 ft)

Appendix D: Technical Specifications

D-1: SMCWHSG44-G

Standards

- 802.11b
- 802.11g
- 802.3
- 802.3u
- 802.3af

Data Rate

- 802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps per channel
- 802.11b: 1, 2, 5.5, 11 Mbps per channel

Modulation Type

- 802.11g: CCK, BPSK, QPSK, OFDM
- 802.11b: CCK, BPSK, QPSK

Network Configuration

- Infrastructure

Radio Technology

- OFDM
- DSSS

Operating Range

- Up to 1,155 feet / 350 m

Channels

- USA: 1-11 (FCC),
- Canada: 1-11 (IC),
- Europe: 1-13 (ETSI),
- France: 10-13
- Japan: 1-13 (Japan)

Frequency range

- 2.402 ~ 2.472 GHz (North America)
- 2.402 ~ 2.4970 GHz (Japan)
- 2.402 ~ 2.4835 GHz (Europe ETSI)
- 2.4465 ~ 2.4835 GHz (France)

Transmission output Power

- 18 dBm max

Receiving Sensitivity

- < -80 dBm, Typical

Antenna

- Removable Antenna with R-SMA connector

Operational Modes

- Wireless
  - Access Point / WDS Static Wireless Bridge

Gateway

- Router with PPPoE-based DSL/Cable connection.
- Router with DHCP-based DSL/Cable connection.
- Router with Static-IP DSL/Cable connection.
- Router with n WAN DSL/Cable connection (n = 2, 3, 4)

Interface

- 10/100 Mbps RJ-45 Connector
- RS-232c Serial Connector
- 802.11b/g WLAN

Security

- 64/128-bit WEP
- 802.1x
- WPA
- MAC address filtering
- Disable SSID broadcast
- Wireless client isolation

Configuration and Management

- Web-browser
- TFTP
- SNMP
- Syslog
- Event Logging

LEDs

- Power
- LAN/WAN
- WLAN
- Alive

Environmental

- Temperature: Operating (0~55C), storage (-20~70C)
- Humidity: 5% to 95% non-condensing in storage

Electromagnetic Compatibility

- FCC Class B
- Industry Canada
- CE
- ETS 300.328; ETS 300 826

Power Supply

- Input: 100VAC 60Hz
- Output: 12VDC, 1A

Dimensions (without antenna)

- 8. x 5.5 x 1.25 in
- 21.6 x 14 x 3.2 cm

Weight

- 0.96 lbs / 436 grams

MTBF

- 80000 hours

D-2: SMCWHS-POS

Print Method

- Direct thermal

Paper Width

- 57.5 mm ✥ 0.5 mm

Effective Print Width

- 48 mm

Print Speed

- Approx. 52 mm/sec or 14 lines/sec

Print Head

- Print density: 384 dots/line or 8 dots/mm
- Print dot space: 0.125 mm
- Print life: 50 km
- Overheat suspension protection

Interface (Serial)

- Dsub 25-pin female connecter
- 9600 bps, none, 8 bits, 1 stop bit
- RTS/CTS and Xon/Xoff protocol

Power Supply

- Input: 100-240V AC 60Hz
- Output: 7.5V DC 2.0A

Net Weight

- 740 g (without cable and paper roll)

Dimensions

- 185 x 114 x 90 mm

Operating Environment

- Temperature: 0 - 50_
- Humidity: 10 - 80 RH

Net Weight

- 740 g (without cable and paper roll)

D-3: Keypad

Key Switches

- Rubber Conduct

Pull Out Forces

- Larger than 1.5 kgf

Operating Forces

- 55 gf

Key Layout

- 18 key

Switch Life

- 1 Million Cycles

Interface

- PS/2

Dimensions

- 128 x 96 x 28 mm

Operating Environment

- Temperature: 5 - 50_
- Humidity: 10 - 80 RH

Glossary

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

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

Access Point
A networking 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.

Ad Hoc
A group of computers connected as an independent wireless network, without an access point.

Advanced Encryption Standard (AES)
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.

Basic Service Set (BSS)
A set of 802.11-compliant stations and an access point that operate as a fully-connected wireless network.

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 802.1x 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.

CSMA/CA
Carrier Sense Multiple Access with Collision Avoidance.

Dynamic Host Configuration Protocol (DHCP)
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 eavesdropping.

Extended Service Set (ESS)
More than one wireless cell can be configured with the same Service Set Identifier to allow mobile users can roam between different cells with the Extended Service Set.

Extensible Authentication Protocol (EAP)
An authentication protocol used to authenticate network clients. EAP is combined with IEEE 802.1x port authentication and a RADIUS authentication server to provide "mutual authentication" between a client, the access point, and the a RADIUS server

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

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

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

Internet Control Message Protocol (ICMP)
A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

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, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.1x
Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

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

Inter Access Point Protocol (IAPP)
A protocol that specifies the wireless signaling required to ensure the successful handover of wireless clients roaming between different 802.11f-compliant access points.

Local Area Network (LAN)
A group of interconnected computer and support devices.

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

Network Time Protocol (NTP)
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.

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

Power over Ethernet (PoE)
A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in the locating of access point's and network devices, and significantly decreased installation costs.

RADIUS
A logon authentication protocol that uses software running on a central server to control access to the network.

Roaming
A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

RTS Threshold
Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem.” If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

Service Set Identifier (SSID)
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.

Simple Network Management Protocol (SNMP)
The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)
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.

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

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

Virtual LAN (VLAN)
A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Wireless Distribution System (WDS)
A Wireless Access Point mode that enables wireless bridging in which WDS APs communicate only with each other only (without allowing for wireless clients or stations to access them), and/or wireless repeating in which APs communicate both with each other and with wireless stations (at the expense of half the throughput).

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.

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

WPA Pre-shared Key (PSK)
PSK can be used for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access.

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481
From Europe : Contact details can be found on
www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com

Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

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

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 1932 866553	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com or www.smc-europe.com.

SMC®
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMCWHSG44-G