SMC Networks

SMC2585W-G
EliteConnect 2.4GHz
Dual-Radio 802.11 g Bridge

USER GUIDE

SMC2585W-G EliteConnect™ 2.4GHz dual-radio 802.11g Wireless Bridge

User's Guide

Version: 1.0 Draft 2

Last Updated: 10/03/2005

Copyright

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

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.

LIMITED WARRANTY

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

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 CE 0560 (!)

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

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
EN301 489-17
• Safety Test
EN60950

Safety Compliance
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 Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlu ßsteckdose 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, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß 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, daß 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 of Contents

1. Introduction

1.1. Overview

The SMC2585W-G is a versatile device that can be configured to be in one of the 3 operational modes—Bridge Repeater, AP Repeater, Dual AP—for various wireless bridging applications. With the convenient Web-based user interface, a network administrator can easily and clearly manage the SMC2585W-G.

1.2. Features

- **IEEE 802.11b/g Compliant**

  - **Operational modes.**

    - **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges.

    - **Static AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface.

    - **Dynamic AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as an AP client-based dynamic bridge Interface.

    - **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP.

  - **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For wireless data encryption.

  - **IEEE 802.1x/RADIUS.** When the SMC2585W-G is in Access Point mode, it can be configured to authenticate wireless users and distribute encryption keys dynamically by IEEE 802.1x Port-Based Network Access Control and RADIUS (Remote Authentication Dial-In User Service).

  - **WPA (Wi-Fi Protected Access).** The SMC2585W-G supports the new WPA standard.   Both WPA-PSK (Pre-Shared Key) mode and full WPA mode are supported. WPA is composed of TKIP (Temporal Key Integrity Protocol) and IEEE 802.1x and serves as a successor to WEP for better WLAN security.

  - **Enabling/disabling SSID broadcasts.** When the SMC2585W-G is in AP mode, the administrator can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcasts functionality is disabled, an STA cannot associate with the AP with an ANY network name (SSID, Service Set ID); the correct SSID has to be specified on the STA.

  - **MAC-address-based access control.** When the SMC2585W-G is in AP mode, it can be configured to block unauthorized STAs based on MAC (Media Access Control) addresses. The ACL (Access Control List) can also be downloaded from a

TFTP server.

- ■ **Transmit power control.** Transmit power of the SMC2585W-G can be adjusted to control the area of coverage.

- ■ **Wireless client isolation.** When the SMC2585W-G is in AP mode, wireless-to-wireless traffic between STAs can be blocked so that the STAs cannot see each other. This capability can be used in hotspots applications to prevent wireless hackers from attacking other wireless users' computers.

- ■ **Link integrity.** When the SMC2585W-G is in AP mode and the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the SMC2585W-G and no wireless client can associate with it thereafter.

- ■ **Associated wireless clients status.** Showing the status of all wireless clients that are associated with the SMC2585W-G.

- ■ **Detachable antenna.** The SMC2585W-G antenna can be replaced with SMC high-gain antennas for long operating range.

- ● **DHCP client.** The SMC2585W-G can automatically obtain an IP address from a DHCP server.

- ● **DHCP server.** The SMC2585W-G can automatically assign IP addresses to computers or other devices by DHCP (Dynamic Host Configuration Protocol).

  - ■ **Static DHCP mappings.** The 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.** Showing which IP address is assigned to which host identified by a MAC address.

- ● **Packet Filtering.** The SMC2585W-G provides Layer 2, Layer 3, and Layer 4 filtering capabilities.

- ● **Firmware Tools**

  - ■ **Firmware upgrade.** The firmware of the SMC2585W-G can be upgraded via the following methods:

    - ◆ **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).

    - ◆ **HTTP-based.** Upgrading firmware by HTTP (HyperText Transfer Protocol).

  - ■ **Configuration backup.** The configuration settings of the SMC2585W-G can be backed up to a file via TFTP or HTTP.

  - ■ **Configuration reset.** Resetting the configuration settings to factory-default values.

- ● **Management**

  - ■ **Web-based management** for configuring and monitoring SMC2585W-G via a Web-Browser.

◆ **Single administrator logon.** Only one administrator can log on to the SMC2585W-G for management purposes at a time.

■ **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, and Private Enterprise MIB are supported.

■ **UPnP.** The SMC2585W-G responds to UPnP discovery messages so that a Windows XP user can locate the SMC2585W-G in My Network Places and use a Web browser to configure it.

■ **Telnet.** The SMC2585W-G can be managed by Telnet.

■ **System log.** For system operational status monitoring.

◆ **Local log.** System events are logged to the on-board RAM of the SMC2585W-G 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.

◆ **Remote log by BSD Syslog.** Systems events are sent in the form of BSD Syslog (RFC3164) to a remote Syslog server.

● **Power over Ethernet.** Supplying power to an SMC2585W-G over an Ethernet cable using optional SMCPWR-INJ3 Power Injector (IEEE 802.3af compliant). This feature facilitates large-scale wireless LAN deployment.

● **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the SMC2585W-G. This way, the SMC2585W-G can provide continuous services.

1.3. LED Definitions

There are several LED indicators on the SMC2585W-G. They are defined as follows:

- **ALV**: Alive. Blinks when the SMC2585W-G is working normally.
- **RF1**: IEEE 802.11b/g interface activity
- **RF2**: IEEE 802.11b/g interface activity
- **LAN**: Ethernet LAN interface activity
- **PWR**: Power

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

The SMC2585W-G can be powered by either the supplied power adapter or the optional SMCPWR-INJ3 EliteConnect™ Power Injector. The SMC2585W-G automatically selects the suitable power depending on your decision.

To power the SMC2585W-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 SMC2585W-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 SMC2585W-G by SMCPWR-INJ3 Power Injector:

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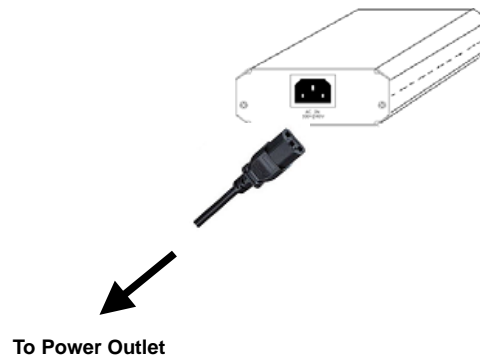

To Power Outlet

Fig. 1. 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 SMC2585W-G Wireless Bridge.
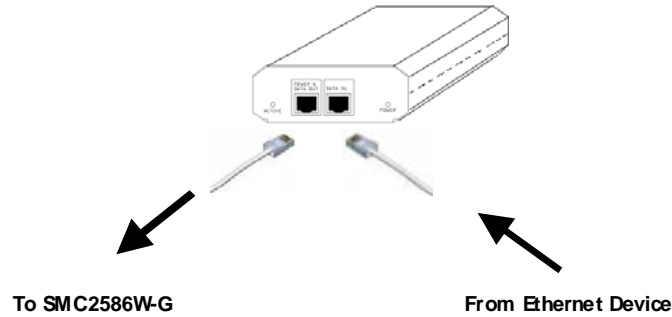
To SMC2586W-G   From Ethernet Device

Fig. 2. Connecting Ethernet cables to SMCPWR-INJ3.

5. Check the "ACTIVE" LED: if power is successfully fed into the SMC2585W-G, the "AC-TIVE" 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 "SMC2585W-G EliteConnect™ 2.4GHz 11Mbps Wireless Bridge. The use of SMCPWR-INJ3 with other Ethernet-ready devices that are not compliant to IEEE 802.3af may cause damage to the devices.

2.2. Mounting the SMC2585W-G on a Wall

The SMC2585W-G is wall-mountable.

1. Stick the supplied sticker for wall-mounting.

2. Use a ϕ7.0mm 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 SMC2585W-G can be hung on the screws.

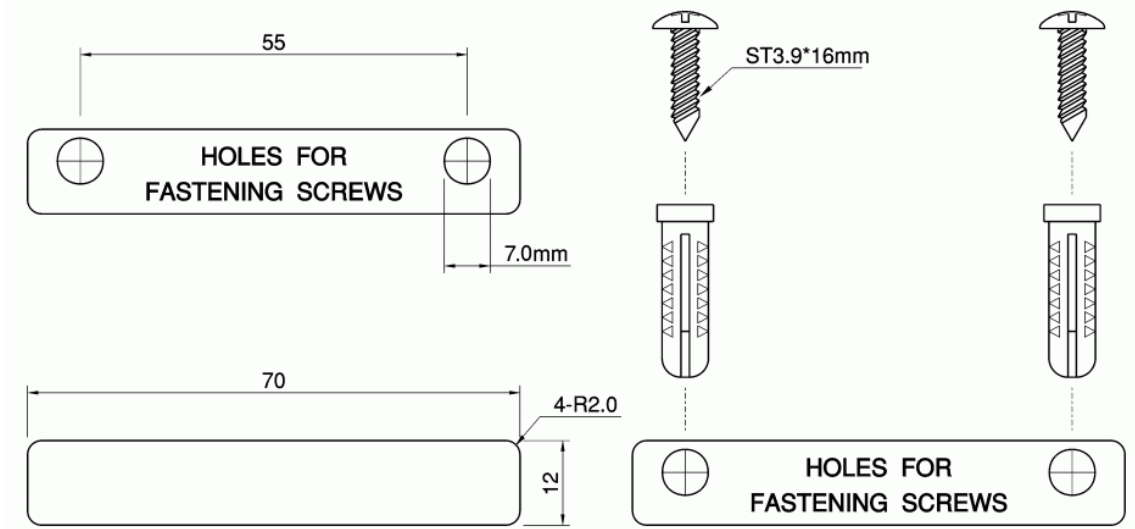5. Hang the SMC2585W-G on the screws.

Fig. 3. Mounting the SMC2585W-G on a wall.

2.3. Preparing for Configuration

To configure a SMC2585W-G, a managing computer with a Web browser is needed. For first-time configuration of a SMC2585W-G, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed SMC2585W-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 SMC2585W-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 SMC2585W-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 SMC2585W-G are in the same IP subnet** (Default IP address is set to DHCP client, it will default to 192.168.2.50 if there is no DHCP server present.)

2.3.1. Connecting the Managing Computer and the SMC2585W-G

To connect the managing computer and the SMC2585W-G for first-time configuration, you have two choices as illustrated in Fig. 4.
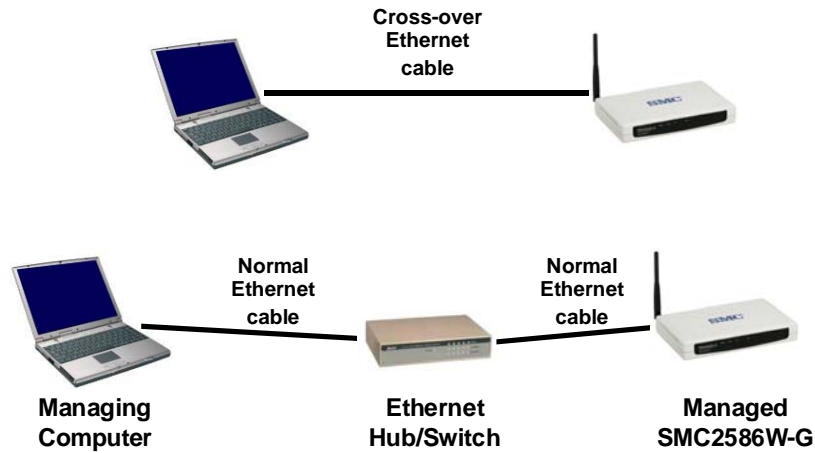
7

Fig. 4. Connecting a managing computer and an SMC2585W-G via Ethernet.

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

> **NOTE:** One connector of the Ethernet cable must be plugged into the **LAN** Ethernet port of the SMC2585W-G for configuration.

2.3.2. 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 SMC2585W-G are in the same IP subnet. Set the IP address of the computer to **192.168.2.xxx** (Default IP address is set to DHCP client, it will default to 192.168.2.50 if there is no DHCP server present.)

> **TIP:** You can use SMC2585W-G Scan Utility on the CD-ROM to scan for all the SMC2585W-Gs on the network. Double-click a scanned SMC2585W-G to launch the Web browser to manage the SMC2585W-G. Note that this utility does not discover the SMC2682W.
>
> **NOTE:** On Windows 2000/XP, SMC2585W-G Scan Utility can only be run by a user with administrator privilege.
>
> **NOTE:** For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

2.4. Configuring the SMC2585W-G

The SMC2585W-G is DHCP client enabled by default. After the IP addressing is configured, launch a Web browser on the managing computer. Then, go to "**http://192.168.2.50**" to log on to the SMC2585W-G for Web-based management.

TIP: For maintenance configuration of an SMC2585W-G, the SMC2585W-G can be reached by its host name using a Web browser. For example, if the SMC2585W-G is named "AP", you can use the URL "http://AP" to access the Web-based management interface of the SMC2585W-G.

2.4.1. Entering the User Name and Password

To log onto the Web based management interface, you will be prompted to enter the user name and password. For first-time configuration, use the default user name "**admin**" and default password "**smcadmin**", respectively. And then, click **Log On**.

Please type your user name and password.

User name: [   ]

Password: [   ]

Log On

Fig. 5. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.1 for more information).

TIP: Since the Status page shows the current settings and status of the SMC2585W-G, it can be saved or printed within the Web browser for future reference.

Fig. 6. The Status page.

9

2.4.2. Step 1: Selecting an Operational Mode

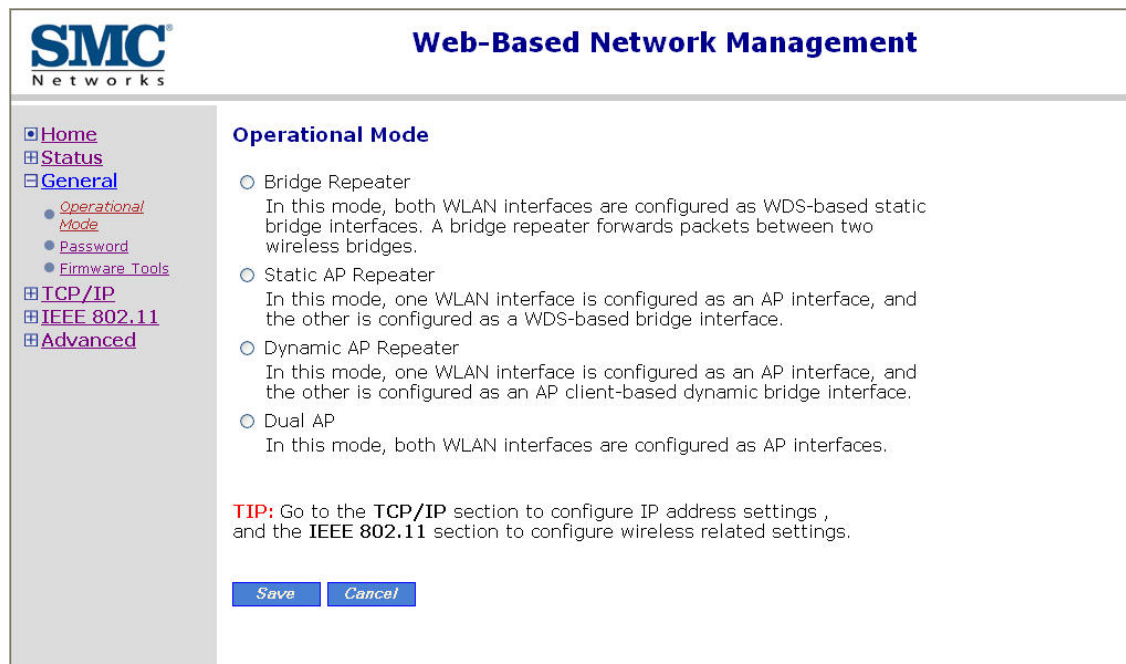Fig. 7. Operational modes settings.

The SMC2585W-G supports 3 operational modes for meeting various wireless connectivity requirements:

◆ **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges.

◆ **Static AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface.

◆ **Dynamic AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as an AP client-based dynamic bridge Interface.

◆ **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP.

In any mode, the SMC2585W-G forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There is 1 type of wireless link to bridge between other SMC2585W-G or SMC2586W-G, and SMC2582W-B bridges.

■ **WDS.** This type of wireless link is specified in the IEEE 802.11 standard for communication between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

10

2.4.3. Step 2: Configuring TCP/IP Settings

Fig. 8. TCP/IP settings.

Go to the **TCP/IP Addressing** section to configure IP address settings. The IP address can be manually set or automatically assigned by a DHCP server on the LAN (Default: DHCP client enabled). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the SMC2585W-G.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

Step 3: Configuring IEEE 802.11 Settings

Fig. 9. IEEE 802.11g communication settings.

Go to the **IEEE 802.11, Communication** section to configure IEEE 802.11g-related communication settings, including **Channel number** and **Network name (SSID)**.

The number of available RF channels depends on local regulations.

11

NOTE: The **Regulatory domain** setting of the SMC2585W-G sold in the U.S. and Canada in not configurable. It's set to FCC by default. As a result, only channels from 1 to 11 are available.

NOTE: For two SMC2585W-Gs or one wireless client computer and one SMC2585W-G to establish a wireless link, both devices must be configured with the same channel number and SSID.

Fig. 10. Wireless Distribution System settings.

To enable a WDS link:

1.   Specify the MAC address of the AP or bridge at the other end of the WDS link.

2.   Select the corresponding **Enabled** check box.

For example, assume you want two SMC2585W-Gs with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On SMC2585W-G 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on SMC2585W-G 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

3.   When you are finished, click **Save** at the bottom of this page. You will be brought back to the Status page.

TIP: Plan your wireless network and draw a diagram, so that you know how the SMC2585W-G is connected to other peer APs or wireless bridges by WDS.
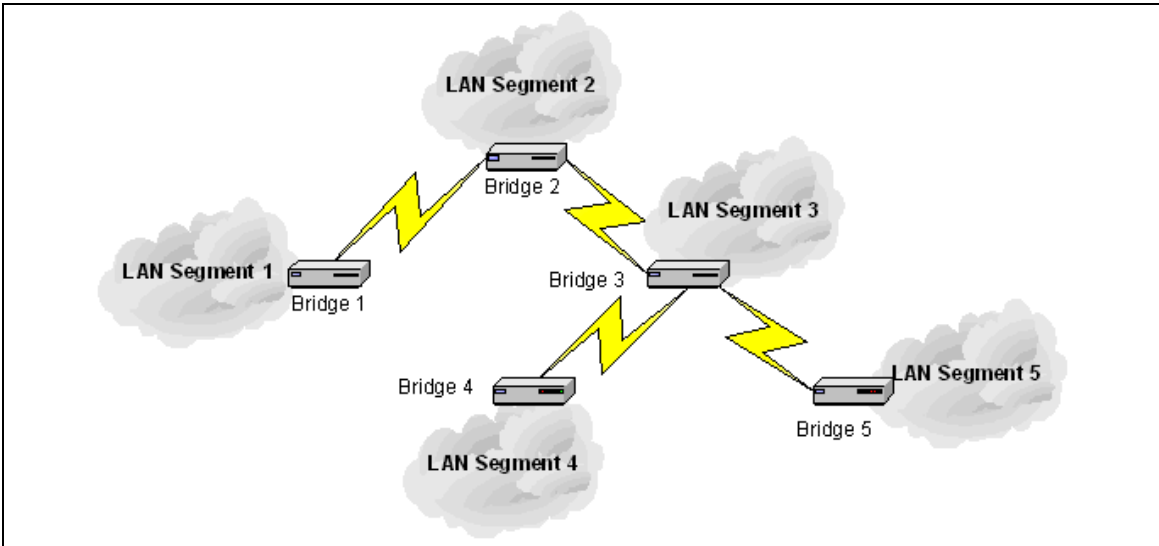
Fig. 11. Sample wireless bridge network topology.

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.
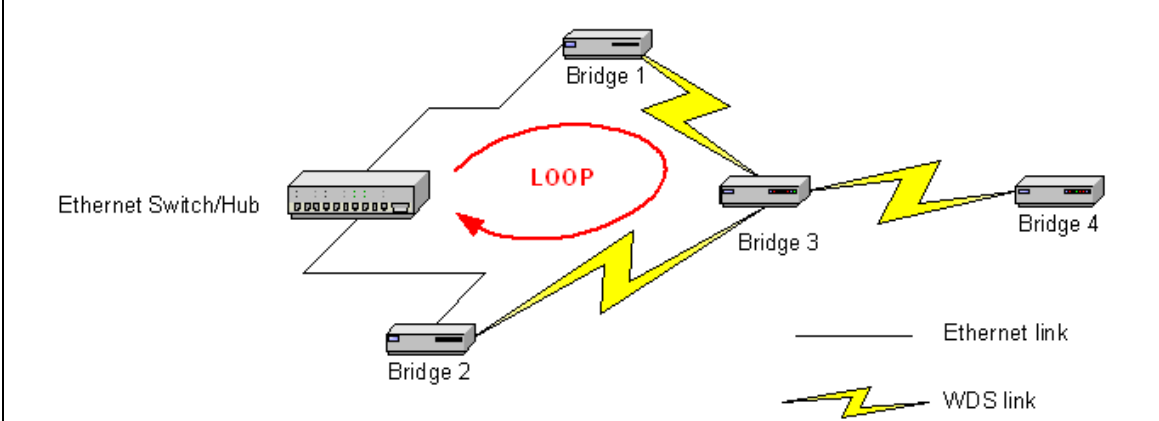

Fig. 12. Network topology containing a loop.

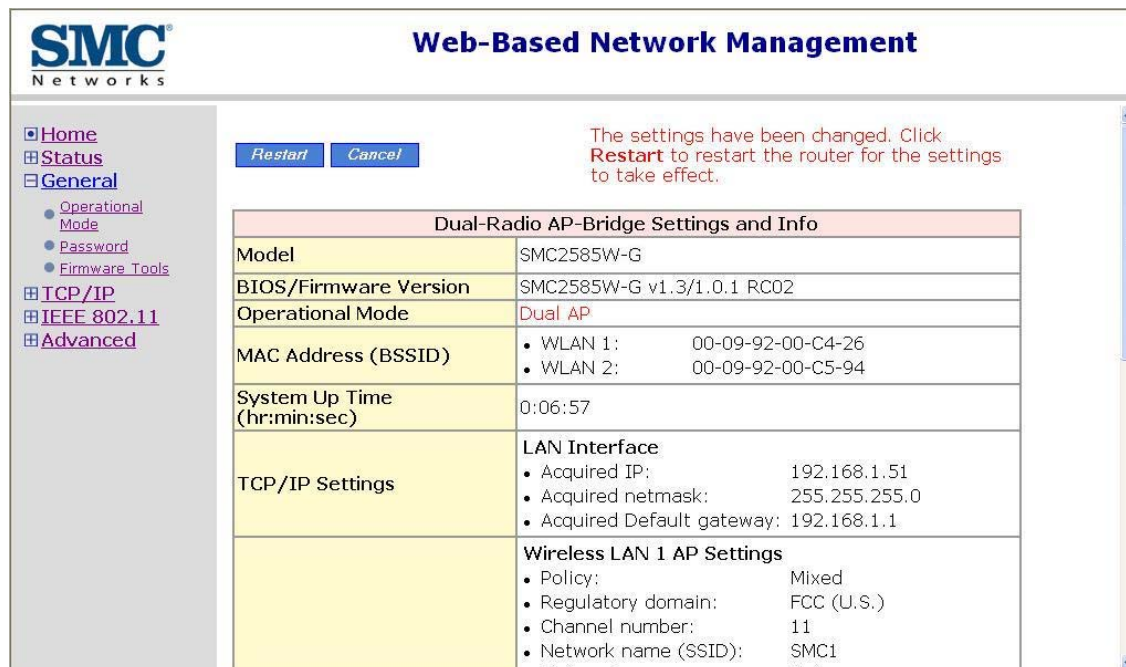## 2.4.4. Step 4: Reviewing and Applying Settings

Fig. 13. Settings changes are highlighted in red.

On the start page, you can review all the settings you have made. Changes are highlighted in red. If they are OK, click **Restart** for the new settings to take effect.

> **NOTE:** It takes about 7 seconds for the SMC2585W-G to complete its restart process.
>
> **NOTE:** If you decide not to change settings of the SMC2585W-G, be sure to log off by clicking the **Log Off** button on the left menu. This way another administrator can log on to the device to do configuration and management. If you do not click the **Log Off** button or have not interacted with the Web management interface for a period of time specified by the **Web admin idle timeout** setting (5 minutes by default), you'll be automatically logged off by the device.

2.5. Deploying the SMC2585W-G

After the settings have been configured, deploy the SMC2585W-G to the field application environment. Connect the SMC2585W-G to an Ethernet LAN through an Ethernet switch/hub.

If external high-gain directional antennas are needed, it may be difficult to align the antennas. Here are some suggestions for antenna alignment.

To adjust the alignments of a pair of SMC high-gain antennas:

1. Connect each SMC2585W-G to a computer via Ethernet.

2. Configure the date rate of each SMC2585W-G to the lowest value, 1Mbps.

3.   Fix the alignment of the antenna on one side.

4.   Adjust the alignment of the antenna on other side by using response time information obtained from PINGing (run PING.exe) the "fixed-side" computer.

5.   Fine-tune the alignment of the antenna until you get the best response time.

6.   Increase the data rate of each SMC2585W-G simultaneously until an optimal workable data rate is reached. You may not be able to use the highest data rate, 54Mbps, because of the distance and the gain of the antennas.
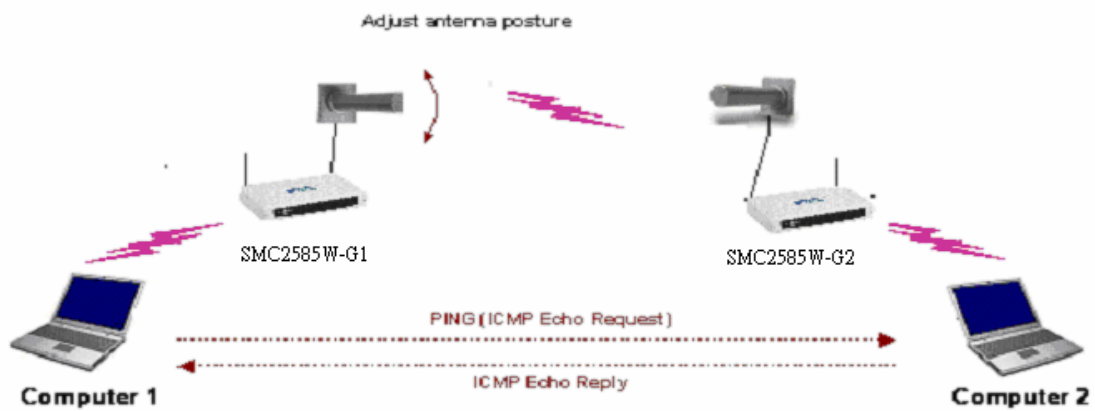
Fig. 14 illustrates the idea.
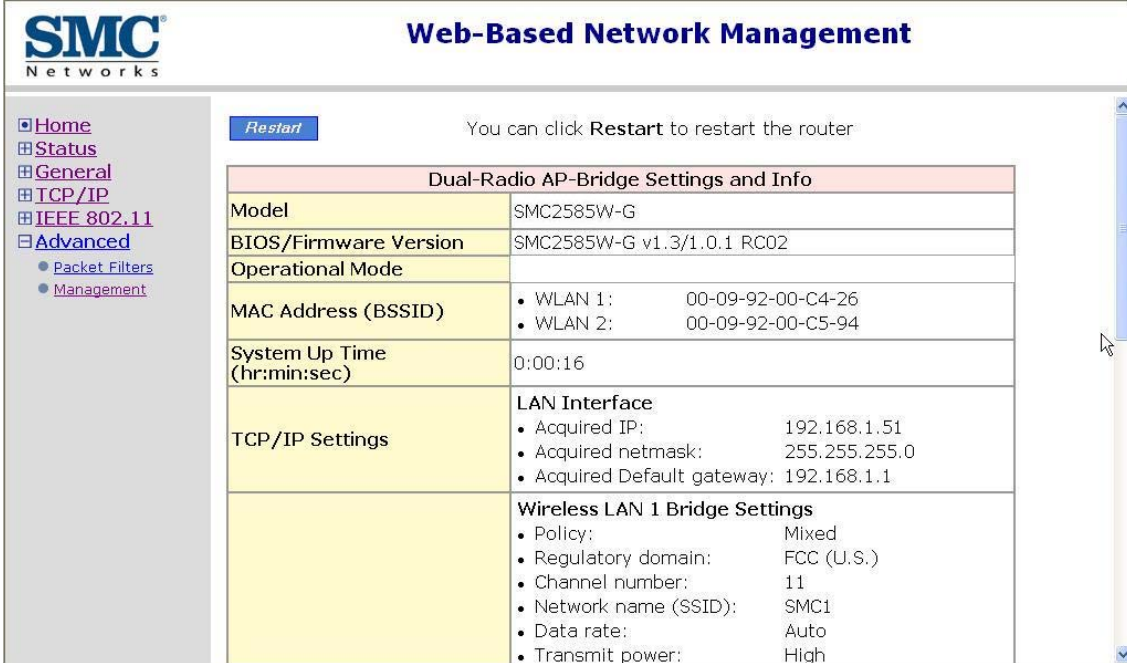
Fig. 14. Adjusting alignments of external directional antennas.

3. Using Web-Based Management

3.1. Overview

Fig. 15. The Start page.

3.1.1. 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.

● **Status.** Status information.

   ■ **Wireless Clients.** The status of the wireless clients currently associated with the SMC2585W-G.

   ■ **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.

   ■ **System Log.** System events log.

● **General.** Global operations.

   ■ **Operational Mode.** Operational mode settings.

   ■ **Password.** For gaining rights to change the settings of the SMC2585W-G.

   ■ **Firmware Tools.** For upgrading the firmware of the SMC2585W-G, backing up and restoring configuration, and configuration reset of the SMC2585W-G.

16

- **TCP/IP.** TCP/IP-related settings.

  - **Addressing.** IP address settings for the SMC2585W-G to work with TCP/IP.

  - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the SMC2585W-G.

- **IEEE 802.11.** IEEE 802.11g-related settings.

  - **Communication.** Basic settings for the IEEE 802.11g interface of the SMC2585W-G to work properly with wireless clients.

  - **Security.** Security settings for authenticating wireless users and encrypting wireless data.

- **Advanced.** Advanced settings of the SMC2585W-G.

  - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.

  - **Management.** UPnP, System Log, and SNMP settings.

3.1.2. Save, Save & Restart, and Cancel Commands

Fig. 16. Save, Save & Restart, and Cancel.

There are three buttons - **Save**, **Save & Restart**, and **Cancel** - at the bottom of each page Clicking **Save** stores the settings changes to the memory of the SMC2585W-G and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the SMC2585W-G and restarts the SMC2585W-G immediately for the settings to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the SMC2585W-G for the new settings to take effect.

Fig. 17. Settings have been changed.

3.1.3. Home and Refresh Commands

Fig. 18. Home and Refresh.

At the bottom of each status page 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.

3.2. Viewing Status

3.2.1. Associated Wireless Clients

Fig. 19. Status of associated wireless clients.

On this page, the status information of each associated client, including its MAC address, IP address, user name, number of bytes it has send, number of bytes it has received, and the time of its last activity, is shown.

18

3.2.2. Current DHCP Mappings

DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 20. Current DHCP mappings.

On this page, all the current static or dynamic DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the DHCP server. You can set static DHCP mappings in the **Static DHCP Mappings** section of the **DHCP Server** configuration page (see Section 3.4.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool from the **DHCP Server** configuration page.

3.2.3. System Log

System Log

Model:	SMC2585W-G
BIOS/Firmware version:	SMC2585W-G v1.3/1.0.1 RC03
Operational mode:	Dual AP
Current time:	Monday, October 03, 2005 3:04:44 PM

Monday, October 03, 2005 3:03:40 PM Set LAN IP address --> 10.1.172.102 by DHCP client.
Monday, October 03, 2005 3:03:42 PM Wireless client 00-0C-20-00-2D-EA is associated with.
Monday, October 03, 2005 3:03:42 PM SYSTEM START UP!
Monday, October 03, 2005 3:03:42 PM Wireless LAN interface 1 initializes success.
Monday, October 03, 2005 3:03:42 PM BSSID --> 00-90-4B-DE-68-FC
Monday, October 03, 2005 3:03:42 PM Wireless LAN interface 2 initializes success.
Monday, October 03, 2005 3:03:42 PM BSSID --> 00-90-4B-DE-6B-4D
Monday, October 03, 2005 3:03:42 PM LAN IP address will get by DHCP client.
Monday, October 03, 2005 3:03:42 PM Set Primary DNS IP address --> 10.1.172.1.
Monday, October 03, 2005 3:03:59 PM Wireless client 00-0C-20-00-2D-EA is disassociated with.

Home   Refresh

Fig. 21. System log.

System events are recorded in the memory of the SMC2585W-G. The logged information is useful for troubleshooting purposes. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.6.2.3 for more information.

3.3. General Operations

3.3.1. Selecting an Operational Mode
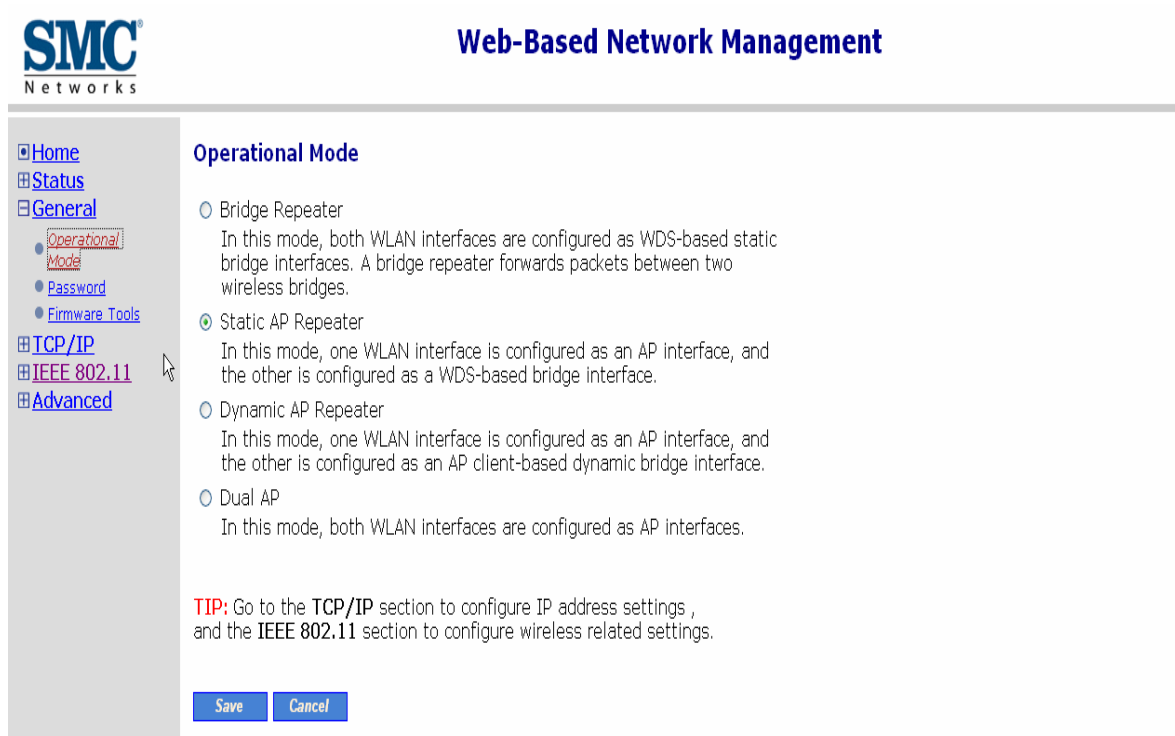
Fig. 22. Operational modes settings.

The SMC2585W-G supports 4 operational modes for meeting various wireless connectivity requirements:

- ◆ **Bridge Repeater**. In this mode, both WLAN interfaces are configured as LAN-to-LAN bridge interfaces. A bridge repeater forwards packets between two wireless LAN-to-LAN bridges.

- ◆ **Static AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as a LAN-to-LAN bridge interface.

- ◆ **Dynamic AP Repeater.** In this mode, one WLAN interface is configured as an AP interface, and the other is configured as an AP client-based dynamic bridge Interface.

- ◆ **Dual AP.** In this mode, both WLAN interfaces are configured as AP interfaces. The dual AP can handle *twice* the number of wireless clients than a normal AP.

In any mode, the SMC2585W-G forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links between two SMC2585W-Gs or between an

SMC2585W-G and another wireless device.

- **STA-AP.** This type of wireless link is specified in the IEEE 802.11 standard for communication between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC).

- **WDS.** This type of wireless link is specified in the IEEE 802.11 standard for communication between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.

The relationships among the operational modes and the wireless link types are shown in the following table:

3.3.2. Changing Password

Old password:	****
New user name:	admin
New password:	******
New password again:	******

Fig. 23. Password.

On this page, you can change the user name and password for the rights to modify the configuration of the SMC2585W-G. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware

Firmware management protocol:	HTTP ▼

Fig. 24. Firmware management protocol setting.

Firmware management operations for the SMC2585W-G 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 types and 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 method.

3.3.3.1. Upgrading Firmware by HTTP

Firmware Upgrade

Firmware file name:		Browse...
Upgrade		

Fig. 25. Firmware upgrade by HTTP.

21

To upgrade firmware of the SMC2585W-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.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP
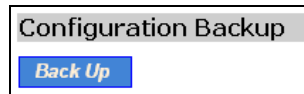
Fig. 26. Firmware backup by HTTP.

To back up configuration of the SMC2585W-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 SMC2585W-G_Backup.hex. Don't change the configuration 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.
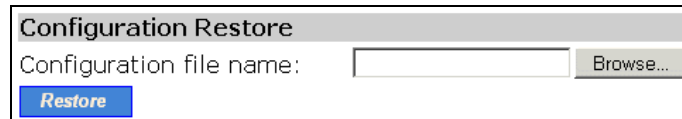
Fig. 27. Configuration restore by HTTP.

To restore configuration of the SMC2585W-G by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file name is the SMC2585W-G_Backup.hex. The file path will be shown in the **Configuration file name** text box.

2. Click **Restore** to upload the configuration file to the SMC2585W-G.

3.3.3.3. Upgrading Firmware by TFTP
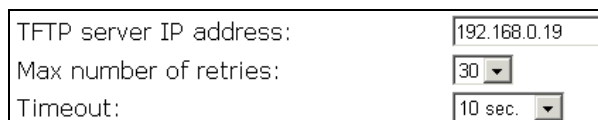
Fig. 28. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the SMC2585W-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.

The SMC2585W-G Installation CD includes a TFTP server program (**TftpSrvr.exe**) for firmware upgrade. Run this program on the computer which serves as a TFTP server.

Firmware Upgrade

Upgrade

Fig. 29. Firmware upgrade by TFTP.

To upgrade firmware of the SMC2585W-G by TFTP:

1. Use a computer that will serve 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 port with a standard Ethernet cable.

3. Configure the IP address of the computer so that the SMC2585W-G and the computer are in the same IP subnet.

4. Run the TFTP Server utility on the computer. Specify the folder in which the firmware files reside.

5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6. Choose **TFTP** as the **Firmware management protocol**.

7. 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.

8. Trigger the firmware upgrade process by clicking **Upgrade**.
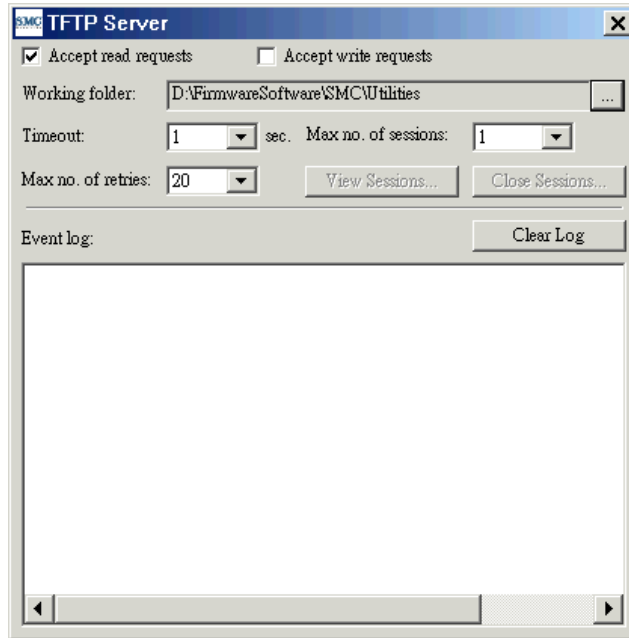
Fig. 30. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the folder 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 SMC2585W-G and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: It is highly recommended that the TFTP server and the to-be-upgraded SMC2585W-G be connected by Ethernet and on the same LAN.

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 cause the SMC2585W-G to not be restarted. When this occurs, call for technical support.

TIP: If you want to remotely upgrade the firmware of a deployed SMC2585W-G from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP

Fig. 31. Configuration backup/restore.

To back up configuration of the SMC2585W-G by TFTP:

1.   Use a computer that will serve 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 standard Ethernet cable.

3.   Configure the IP address of the computer so that the computer and the SMC2585W-G are in the same IP subnet.

4.   Run the TFTP Server utility on the computer. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the SMC2585W-G will be saved.

5.   On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6.   Choose **TFTP** as the **Firmware management protocol**.

7.   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.

8.   Trigger the backup process by clicking **Back Up**. The backup file is named SMC2585W-G_Backup

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

To restore configuration of the SMC2585W-G by TFTP:

1.   Use a computer that will serve 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 standard Ethernet cable.

3.   Configure the IP address of the computer so that the computer and the SMC2585W-G are in the same IP subnet.

4.   Run the TFTP Server utility on the computer. Specify the folder in which the configuration backup file resides. A configuration backup file is named SMC2585W-G_Backup.hex.

5.   On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.

6.   Choose **TFTP** as the **Firmware management protocol**.

7.   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.

8.   Trigger the restoring process by clicking **Restore**. The SMC2585W-G will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the SMC2585W-G.

TIP: If you want to remotely back up or restore configuration from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults
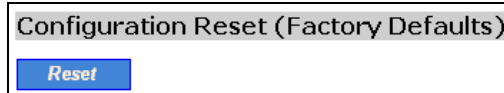
Fig. 32. Configuration reset.

Click on the **Reset** button to reset the device configuration to factory defaults.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing
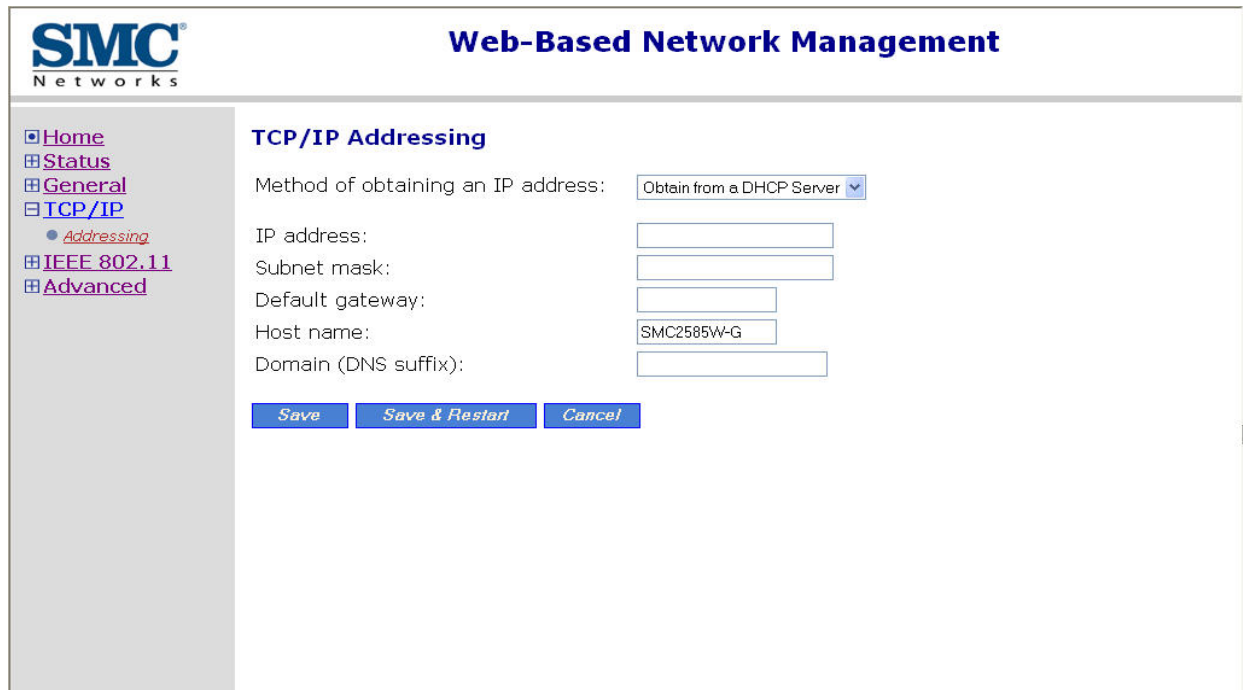
Fig. 33. TCP/IP settings.

The IP address of the SMC2585W-G can be manually set (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server – enabled by default**). If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the SMC2585W-G.

26

3.4.2. DHCP Server

3.4.2.1. Basic

Functionality:	Enabled
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. 34. Basic DHCP server settings.

The SMC2585W-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 allocateable IP addresses.

NOTE: There should be only one DHCP server on the LAN; otherwise, DHCP would not work properly. If there is a DHCP server on the LAN already, disable the DHCP server functionality of the SMC2585W-G.

NOTE: By default the DHCP server function is disabled.

3.4.2.2. Static DHCP Mappings

Enabled	Desc.	MAC Address	IP Address
☐	Bill	00-22-32-5D-80-02	192.168.0.203
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			
☐			

Fig. 35. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. 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 a static 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 of this mapping.

2. Select the corresponding **Enabled** check box.

3.5. Configuring IEEE 802.11b/g-Related Settings

3.5.1. Communication

3.5.1.1. 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. 36. Basic IEEE 802.11b/g communication settings.

For specific needs such as configuring the SMC2585W-G as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the SMC2585W-G.

Since the IEEE 802.11g-based SMC2585W-G is also IEEE 802.11b compatible, you can configure the **Policy** setting to meet your backwards compatibility needs. If the SMC2585W-G is used in an environment in which all wireless clients are IEEE 802.11b-based, set **Policy** to **b only**. If all the wireless clients are IEEE 802.11g-based, set **Policy** to **g only**. For maximal flexibility, set **Policy** to **Mixed**, in which mode, the SMC2585W-G supports both IEEE 802.11b- and IEEE 802.11g-based wireless clients.

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 SMC2585W-G must be identical for them to communicate with each other.

NOTE: The **Regulatory domain** setting of the SMC2585W-G sold in the U.S. and Canada in not configurable. It's set to FCC by default. As a result, only channels from 1 to 11 are available.

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**.

The transmit power of the RF module of the SMC2585W-G can be adjusted so that the RF coverage of the SMC2585W-G can be changed.

3.5.1.2. Link Integrity

Functionality:	Disabled ▾
Reference host:	0.0.0.0

Fig. 37. Link integrity settings.

When the SMC2585W-G is in AP mode and the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients are disassociated by the SMC2585W-G and no wireless client can associate with the SMC2585W-G. The detection mechanism is based on pinging the IP address specified in **Reference host**.

3.5.1.3. Wireless Distribution System
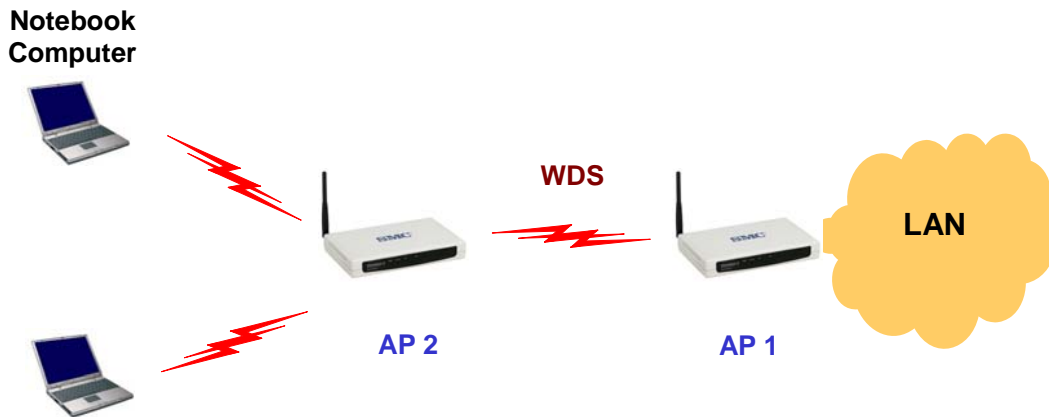
Fig. 38. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By IEEE 802.11 Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 38, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 plays a role of "AP repeater".
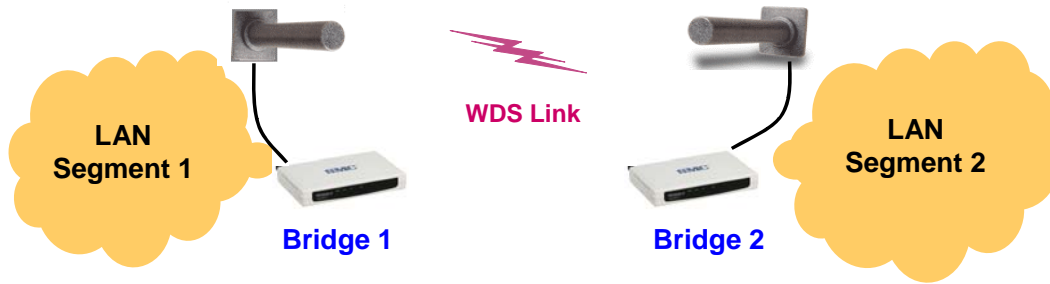
Fig. 39. LAN-to-LAN bridging.

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 39, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the SMC2585W-G is WDS-enabled, it can be used as a wireless bridge even when it is in AP mode.

> **NOTE:** An SMC2585W-G can have up to 6 WDS links to other APs or wireless bridges per radio.

Fig. 40. Wireless Distribution System settings.

To enable a WDS link:

3. Specify the MAC address of the AP or bridge at the other end of the WDS link.

4. Select the corresponding **Enabled** check box.

For example, assume you want two SMC2585W-Gs with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On SMC2585W-G 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on SMC2585W-G 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 an AP is connected to other peer APs or wireless bridges by WDS.
>
> **TIP:** Plan your wireless network and draw a diagram, so that you know how a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.
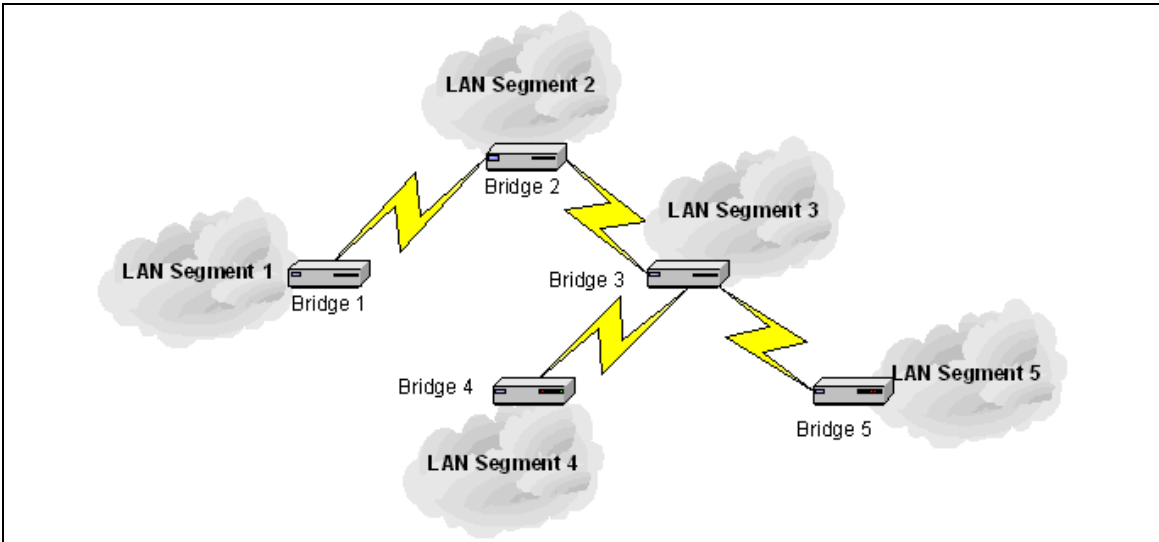
Fig. 41. Sample wireless bridge network topology.

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.
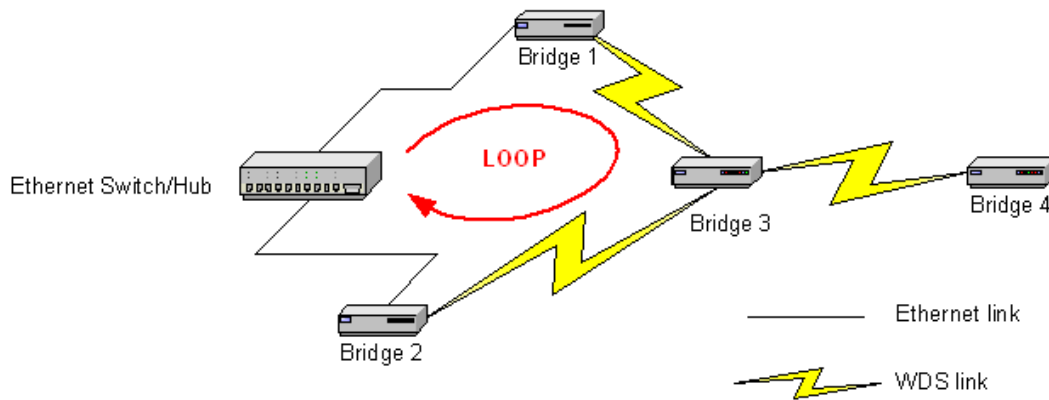
Fig. 42. Network topology containing a loop.

3.5.2. Security

IEEE 802.11b/g security settings include **SSID broadcasts**, **Security mode**, **IEEE 802.11 Authentication algorithm**, **WEP keys**, **MAC-Address-Based Access Control**.

3.5.2.1. Basic

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

Fig. 43. 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. Additionally, you can disable the SSID broadcasts functionality so that a wireless client with an "ANY" SSID cannot associate with the SMC2585W-G.

Wireless Client Isolation is a feature for the SMC2585W-G in AP mode 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 SMC2585W-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 SMC2585W-Gs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.
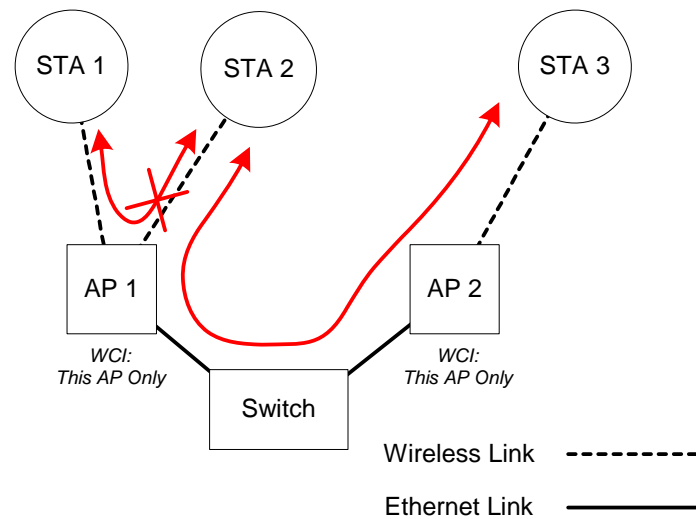

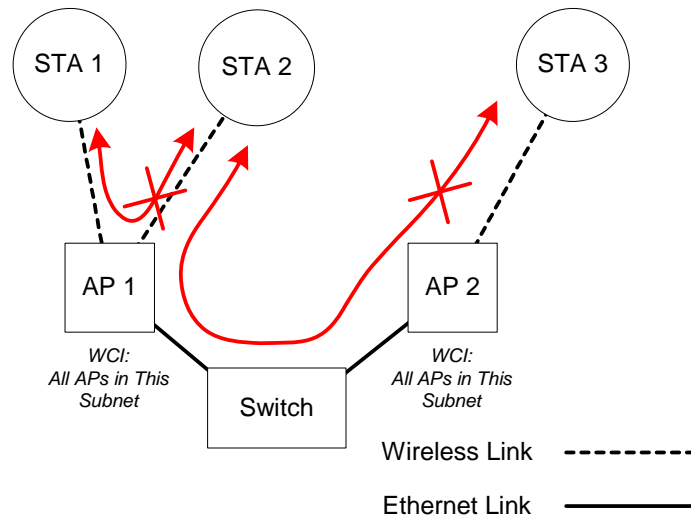Fig. 44. Behavior of the "This AP Only" wireless client isolation option.

Fig. 45. Behavior of the "All APs on This Subnet" wireless client isolation option.

As illustrated in Fig. 44 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. 45, 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:

● **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

33

the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The SMC2585W-G is highly secured 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".

3.5.2.2. MAC-Address-Based Access Control

Fig. 46. MAC-address-based access control settings.

With **MAC-Address-Based Access Control**, you can specify the wireless clients that are permitted or not permitted to associate with the SMC2585W-G. When the table type is set to inclusive, entries in the table are permitted to associate with the SMC2585W-G. When the table type is set to exclusive, entries in the table are not permitted to associate with the SMC2585W-G.

NOTE: MAC-address-based access control is only available when the SMC2585W-G is in AP mode.

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.

Fig. 47. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then download the MAC ACL (Access Control List) file from the TFTP server to the SMC2585W-G. Fig. 48 shows the contents of a sample ACL file.

Fig. 48. Sample MAC ACL file.

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.

2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.

3. Click **Download**.

3.5.3. 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 3.5.2.1). 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.
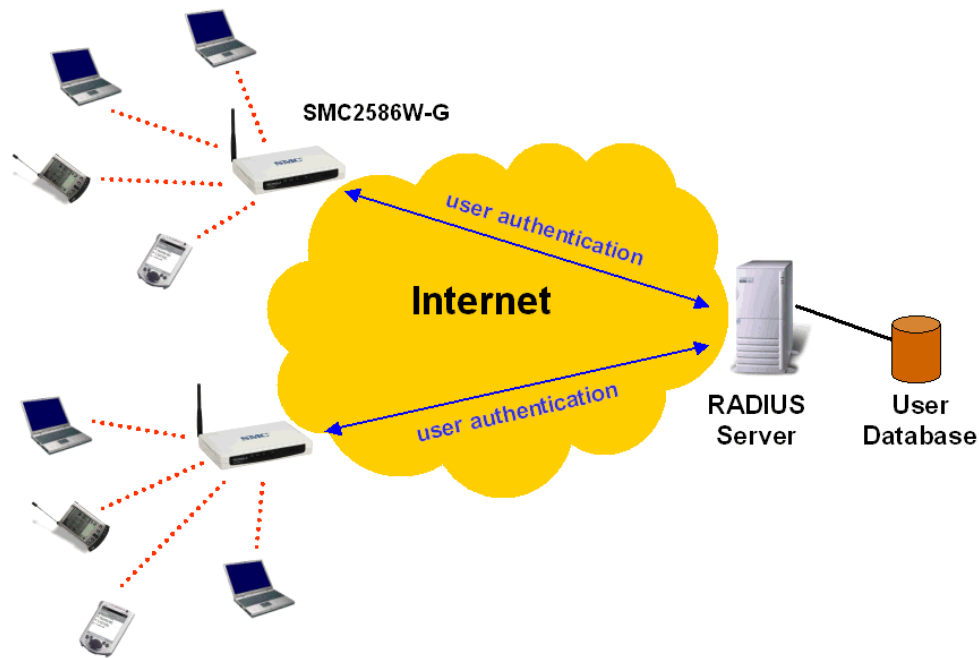
Fig. 49. IEEE 802.1x and RADIUS.

SMC2585W-G supports IEEE 802.1x and can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, SMC2585W-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 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.

Fig. 50. IEEE 802.1x/RADIUS settings.

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

The SMC2585W-G provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: whether this filtering capability is enabled or disabled.

Policy for matched packets: how a matched packet is processed—discard or pass.

To enable a filtering rule: select the check box to the left of the rule.

3.6.1.1. Ethernet Type Filters

Fig. 51. Ethernet type filters settings.

The Ethernet type filed of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal Ethernet type number and give the rule a name.

3.6.1.2. IP Protocol Filters

Fig. 52. IP protocol filters settings.

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

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 result source IP address range is 192.168.0.0 to 192.168.0.255.

3.6.1.3. TCP/UDP Port Filters

Fig. 53. TCP/UDP port filters settings.

The destination port field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

3.6.2. Management

3.6.2.1. Basic

Fig. 54. Basic management settings.

The SMC2585W-G can be managed by Telnet. This functionality can be either enabled or disabled.

As the SMC2585W-G allows only one administrator to log on for management, you have to log off before another can log on. If you forget to log off or have not interacted with the Web management interface for a period specified by the **Web admin idle timeout** setting (default: 5 minutes), you'll be automatically logged off by the SMC2585W-G.

3.6.2.2. UPnP

Fig. 55. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices. When the UPnP functionality is enabled, you can see the SMC2585W-G in My Network Places of Windows XP. The SMC2585W-G can be given a user-friendly name that will be shown in My Network Places. Double-clicking the icon in My Network Places that refers to the SMC2585W-G will launch the Web browser for you to configure the SMC2585W-G.

NOTE: Make sure you have installed the necessary Windows UPnP components on your Windows XP computer.

3.6.2.3. System Log

Fig. 56. System log settings.

System events can be logged to the on-board RAM of the SMC2585W-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 SMC2585W-G via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (disabled by default).

3.6.2.4. SNMP

Fig. 57. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and 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.

Appendix A: Default Settings

TIP: Press the **Default** button on the powered-on SMC2585W-G to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	admin
Password	smcadmin
Host Name	SMC2585W-G
IEEE 802.11g	
Operational Mode	Access Point
Policy	Mixed (Both IEEE 802.11b- and IEEE 802.11g-based wireless clients are supported.)
Regulatory Domain	FCC (U.S.) or ETSI (Europe)
Channel Number	6/11
SSID	SMC1/2
SSID Broadcasts	Enabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the housing of the SMC2585W-G.
Security Mode	Open System
WEP Key Length	64 Bits
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
Link Integrity	Disabled
LAN Interface	
Method of obtaining an IP Address	DHCP Client enabled
IP Address	192.168.2.50 (If a DHCP server cannot be found.)
Subnet Mask	255.255.255.0 (If a DHCP server cannot be found.)
Default Gateway	0.0.0.0
DHCP Server	Disabled
Management	
Web Admin Idle Timeout	5 min
UPnP	Enabled
Device Friendly Name	SMC2585W-G
System Log	Local Log
SNMP	Enabled
SNMP Read Community	public
SNMP Write Community	private
Telnet	Disabled

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the SMC2585W-G is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the SMC2585W-G.

- Make sure that the LED ALV of the SMC2585W-G is blinking to indicate the SMC2585W-G is working.

- Make sure the types of the Ethernet cables are correct. Recall that there are two types—straight-through and crossover.

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with an SMC2585W-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 SMC2585W-G?

        - Check the SSID setting of the WLAN NIC and of the SMC2585W-G.

    - Is the WEP functionality of the prospective SMC2585W-G enabled?

        - Make appropriate WEP settings of the client computer to match those of the SMC2585W-G.

    - Is the prospective SMC2585W-G within range of wireless communication?

        - Check the signal strength and link quality sensed by the WLAN NIC.

B-2: TCP/IP Settings Problems
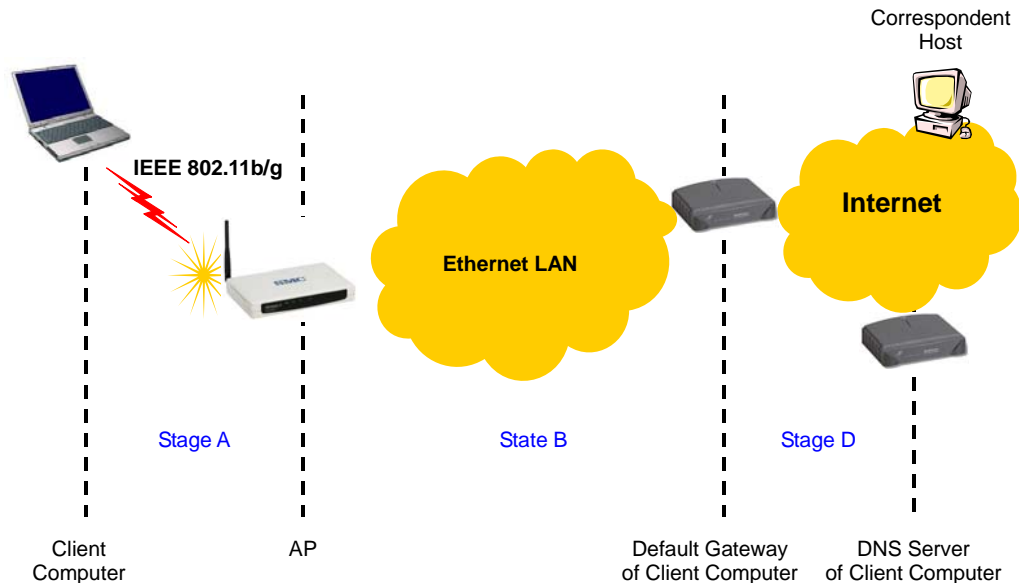
Fig. 58. Communication stages for a client to reach its correspondent host.

For a wireless client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. http://www.wi-fi.com), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, then the AP relays this request to the default gateway of the client computer. Finally, this request is forwarded by the 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 address.

As illustrated in Fig. 58, 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:

- **My SMC2585W-G does not respond to ping from the client computer.**

  - Are two or more NICs installed on the client computer?

    - Use Windows-provided **Device Manager** to disable unnecessary NICs.

  - Is the underlying link (Ethernet or IEEE 802.11g) established?

    - Make sure the Ethernet link is OK.

    - Make sure the wireless settings of the wireless client computer and of the

43

SMC2585W-G match.

- ■ Are the IP address of the client computer and the IP address of the SMC2585W-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 SMC2585W-G are in the same IP subnet.

  - ◆ **TIP:** If you forget the current IP address of the SMC2585W-G, use Wireless Router/AP Browser to get the information (see Appendix B-3).

- ● **The default gateway of the client computer does not respond to ping from the client computer.**

  - ■ Solve the preceding problem first.

  - ■ Are the IP address of the SMC2585W-G and the IP address of the client computer in the same IP subnet?

  - ■ If you cannot find any incorrect settings of the SMC2585W-G, the default gateway may be really down or there are other communication problems on the network backbone.

- ● **The DNS server(s) of the client computer do not respond to ping from the client computer.**

  - ■ Solve the preceding problems first.

  - ■ If you cannot find any incorrect settings of the SMC2585W-G, the default gateway of the SMC2585W-G may be really down or there are other communication problems on the network backbone.

B-3: Other Problems

- ● **My SMC2585W-G has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?**

  - ■ Use the SMC2585W-G Scan Utility (**WLBrwsr.exe**), which is included in the SMC2585W-G Installation CD. This utility can discover nearby SMC2585W-Gs and show their MAC addresses and IP addresses. In addition, it can launch the Web browser on your computer.

NOTE: On Windows 2000/XP, SMC2585W-G Scan Utility can only be run by a user with administrator privilege.

NOTE: SMC2585W-G Scan Utility does not scan the SMC2682W.
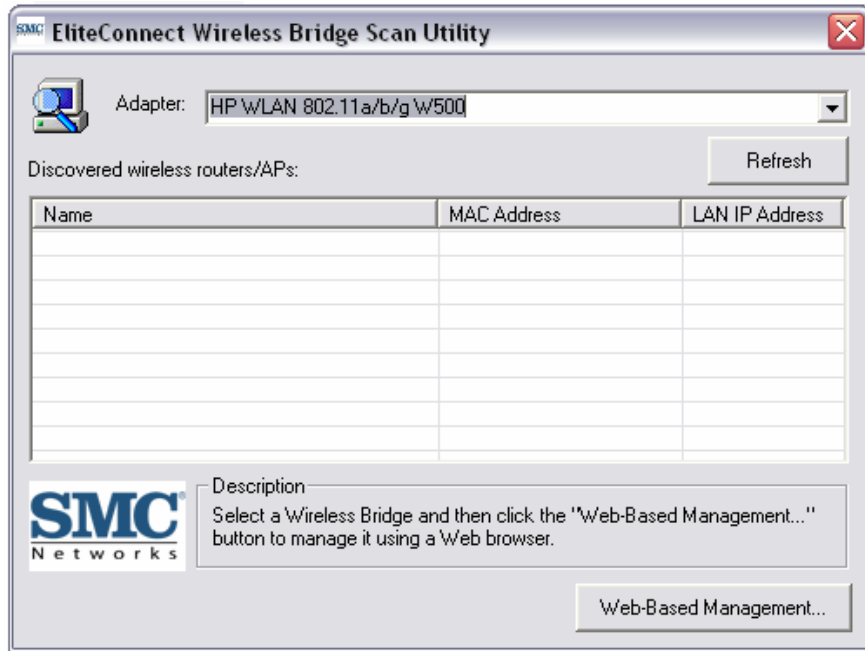
Fig. 59. SMC2585W-G Configuration Utility.

- **My SMC2585W-G stops working and does not respond to Web management requests.**

    ■ The firmware of the SMC2585W-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 SMC2585W-G.

        ◆ Contact our technical support representatives to report this problem, If this happens after a failed firmware upgrade process, the firmware of the SMC2585W-G may have been corrupted.

    ■ If the SMC2585W-G still does not work after restarting, there may be hardware component failures in the SMC2585W-G.

        ◆ Contact our technical support representatives for repair.

45

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: SMC2585W-G Wireless Bridge

Standards:
> 802.11b
> 802.11g
> 802.3
> 802.3u
> 802.3af

Data rate & modulation:
> OFDM@54Mbps, CCK@11/5.5Mbps, DQPSK@2Mbps and DBSK@1Mbps

Radio Technology:
> OFDM
> DSSS

Operating Range:
> Up to 1,155 feet

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:
> Bridge Repeater, AP Repeater, Dual AP

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
Disabled SSID broadcast
Wireless client isolation

Configuration and Management

Web-browser
Telnet
TFTP
SNMP
Syslog
Event Logging

LEDs

Power
LAN
RF 1
RF 2
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):
8.5" x 5.5 " x 1.25"

Weight:
0.96 lbs

D-2: SMCPWR-INJ3 Power Injector

Input Power Requirements
AC Input Voltage   : 90 – 264Vac
AC Frequency   : 47 – 63 Hz
AC Input Current   : 2A at 100Vac, 1A at 240Vac, (-48Vdc)

Power over LAN output Specification
Pin Assignments and Polarity: (＋) 4/5   (－) 7/8
Output Voltage   : Aggregate Power:50W (48Vdc)

Mechanical Requirement
Dimensions   :   4" x 5.5" x 1.5"

Weight   : 1.38 Lbs
Indicators
   System Indicator:
        AC Power (Green)
        Power Active (Red) $0.05\ A < Io < 0.8\ A$
        Over Current Protection (Red, Flash) $Io > 1.0\ A$
Connectors Shielded Rj-45

Environmental Conditions
Operating Temperature   : 32° to 104° F (0° to 40° C)
Operating Humidity   : Maximum 90% Non-condensing
Storage Temperature   : -13° to 185° F (-25° to 85° C)
Storage Humidity   : Maximum 95%, Non-condensing
Operating Altitude   : -1000 to 10,000 ft. (-304.8 to 3048 m)

Safety Approval
 UL 1950
 CSA A22.2 No. 950
 EN 60950
 CB

Regulatory Compliance
CE Compliance

Electromagnetic Emission and Immunity
   A.   FCC Part 15 Class B

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.

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.com

INTERNET
E-mail address:
   techsupport@smc.com

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

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

Model Number: SMC2585W-G

SMC®
N e t w o r k s

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