



User Manual:
EZ Connect N
Draft 11n Wireless Access Point/ Ethernet Client
Model No: SMCWEB-N

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 website. 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, NEGLIGENCE, 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.
20 Mason
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 radiate 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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

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

- EN 300 328
- EN 301 489-1
- EN 301 489-17
- EN 60950-1

A copy of the CE Declaration of Conformity is available for download at: <http://www.smc.com>

Intended for indoor use in the following countries:

AT, BE, CZ, CY, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LT, LU, MT, NL, NO, PL, PT, SI, SK, ES, SE, CH, UK.

Table of Contents

Getting Started with the SMCWEB-N	2
Package Contents	2
Minimum System Requirements	2
Wireless LAN Networking	3
Introduction	4
Features	4
Hardware Overview	5
Back/Side Panel	5
Front Panel LED's	6
Installation Considerations	7
Getting Started	7
Using the Configuration Menu in AP Mode	8
Basic	9
Advanced	17
Tools	25
Status	30
Using the Configuration Menu in Client Mode	37
Basic	38
Advanced	43
Tools	49
Status	53
Glossary	59

Getting Started with the SMCWEB-N

Congratulations on purchasing the SMCWEB-N! This manual provides information for setting up and configuring the SMCWEB-N. This manual is intended for both home users and professionals.

Package Contents

- EZ Connect™ N Wireless Access Point/Ethernet Client (SMCWEB-N)
- Yellow RJ-45 Ethernet Cable
- Power Adapter (12V, 1A)
- Documentation CD
- Quick Installation Guide
- Warranty Information Card

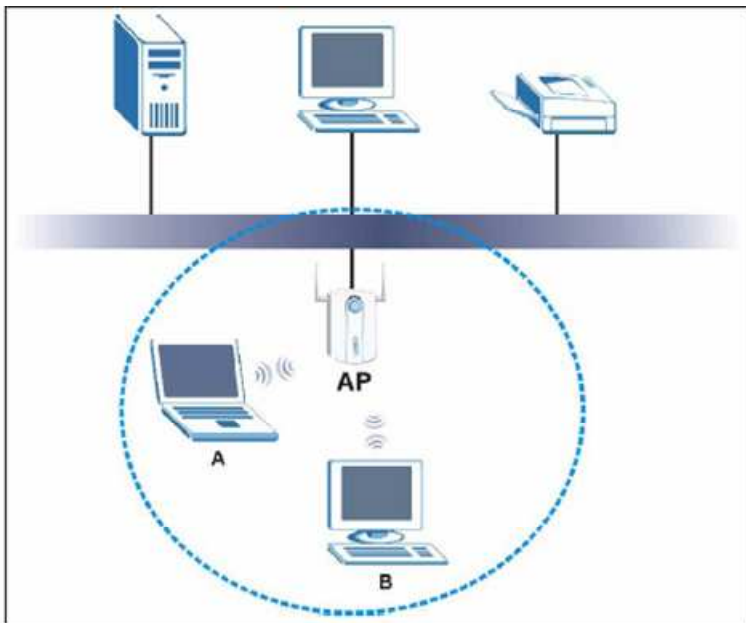
Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

Minimum System Requirements

- 2.4GHz 802.11n draft wireless adapter or 2.4GHz 802.11b/g wireless adapter or Ethernet Adapter installed on each PC.
- Internet Explorer 5.5 or above, Netscape 4.7 or above, Mozilla Firefox 1.0 or above

Wireless LAN Networking

The following figure provides an example of a wireless network with an AP.



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless client. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with Internet. Every wireless network must follow those basic guidelines.

1. Every device in the same wireless network must use the same SSID. The SSID is the name of the wireless network. It stands for Service Set Identity.
2. If two wireless network overlap, they should use a different channel. Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
3. Every device in the same wireless network must use security compatible with the AP or peer computer.

Introduction

The SMCWEB-N is a multi-function Wireless-N (802.11n draft) networking device: Access Point and Ethernet Client modes. Designed for multimedia applications SMCWEB-N can be used in Access Point mode to add high-speed wireless connectivity to your network, or Client mode to simultaneously connect multiple Ethernet enabled devices such as a game console, digital media player or Network Attached Storage.

The SMCWEB-N is 802.11n draft v2.0 compliant while maintaining full backwards compatibility with the Wireless-G (802.11g) and Wireless-B (802.11b) standards. This next generation wireless networking standard utilizes advanced MIMO (Multiple-In, Multiple-Out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps and extended coverage, there is enough bandwidth to simultaneously stream video and audio, play online games, transfer large files, make VoIP calls and surf the Internet. With security being a key consideration, SMCWEB-N supports the latest WPA and WPA2 wireless encryption standards, which prevent unauthorized access to wireless networks and ensure data is secure. Wireless security can also be set up easily using Wi-Fi Protected Setup™ (WPS) that enables push button or PIN configuration.

For an enhanced multimedia experience Wireless Intelligent Stream Handling technology automatically manages and prioritizes the flow of time-sensitive data in your wireless network, without the need for end user configuration. As a result time-sensitive applications like online gaming, voice and video, run smoothly without lag and breakup problems. Finally, configuration is made simple and straightforward with the Installation Wizard, intuitive web-based management interface and slide switch for easily selecting operating mode.

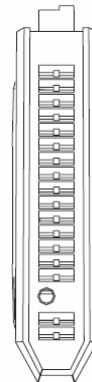
Features

- Wi-Fi Compliant with IEEE 802.11n (draft) and IEEE 802.11b/g Standards
- 2.412 to 2.462GHz frequency band operation
- Compliant with IEEE 802.3 & 3u standards
- Support OFDM and CCK modulation
- High-Speed up to 300Mbps Data Rate using IEEE 802.11n (draft) connection
- 64/128-bits WEP and WPA/WPA2 Personal/Enterprise security support
- Wi-Fi Protected Setup™ (WPS)
- DHCP Server Support up to 252 leases, and up to 24 reservations (AP mode only)
- MAC address filtering support up to 24 filtering entries
- Support WEB UI management, firmware upgrade and configuration backup and restore
- Support 4 x 10/100Mbps Auto-MDIX LAN ports

- Built-in 3 External Antennas to support high speed performance and great coverage
- AP and Client modes selectable with slide switch
- Wireless Intelligent Stream Handling Technology

Hardware Overview

Back/Side Panel



POWER

The Power input connector is a single jack socket to supply power to the SMCWEB-N. Please use the Power Adapter provided in the SMCWEB-N package.

RESET

Pressing the reset button for 10 seconds restores the SMCWEB-N to its original factory default settings.

AP / Client Slide Switch

Select AP or Client operating modes

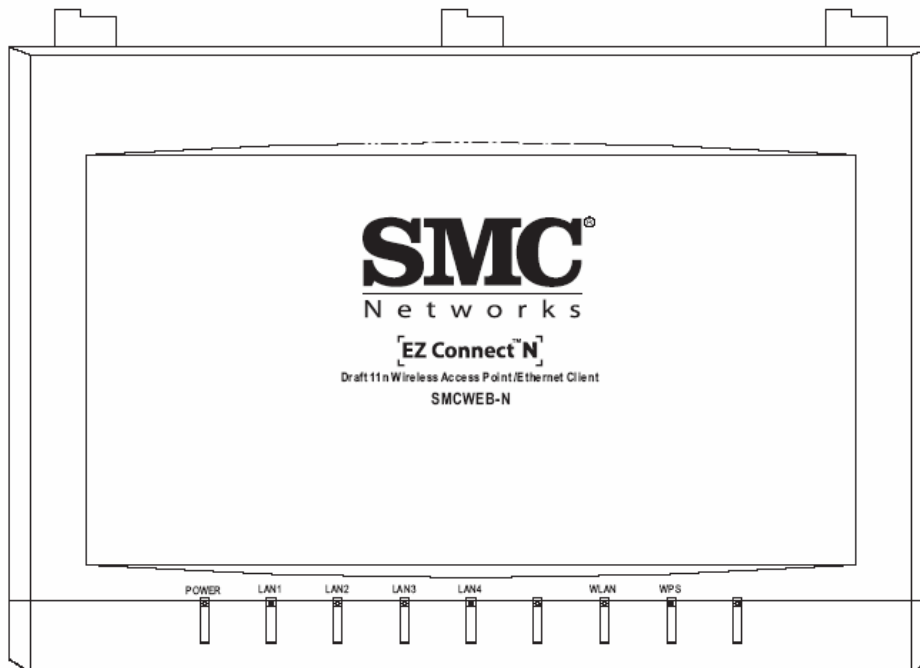
LAN1-4 (Auto MDI/MDIX)

The LAN ports are used for connecting networking devices such as PC's, Printers & Switches. The LAN ports automatically sense the cable type when connecting to Ethernet enabled computers.

WPS

Press and hold the WPS button for 4 seconds to automatically configure wireless security. If the client device supports WPS Push Button Configuration (PBC) you will need to press the button within 60 seconds to automatically configure security on the client. **Note:** WPS LED will start to flash after pressing WPS button for 4 seconds. When a client joins the network successfully the LED will stop blinking and become solid until the next WPS action or the device is rebooted. If no client joins the LED will stop blinking and switch off after 4 minutes.

Front Panel LED's



POWER

A solid green LED indicates the SMCWEB-N is receiving power – normal operation. If the LED is off there is no power to device or failure.

LAN1-4

A solid green LED indicates the corresponding LAN port connection is established. The LED blinks when data is transmitted. If the LED is off there is no link for corresponding LAN port.

WLAN

A solid green LED indicates the wireless AP is ready. The LED blinks when wireless data is transmitted.

WPS

After pressing the WPS button for 4 seconds the WPS LED will blink continually. When a client joins the network successfully the LED will stop blinking and become solid until the next WPS action or the device is rebooted. If no client joins the LED will stop blinking and switch off after 4 minutes.

Installation Considerations

The SMCWEB-N lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- 1 Keep the number of walls and ceilings between the SMCWEB-N and other network devices to a minimum - each wall or ceiling can reduce your wireless product's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- 2 Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- 3 Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- 4 Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.

Getting Started

For a typical wireless setup please do the following:

1. Select desired operation mode using the slide switch on the back panel. AP mode configures the SMCWEB-N to function as a wireless access point. Client mode configures the SMCWEB-N to function as an Ethernet to wireless bridge. Client mode is used for connecting Ethernet devices such as a game console, digital media player or Network Attached Storage. You can directly connect up to 4 devices. **Note:** The default mode is AP.
2. Using the yellow RJ-45 cable connect port **LAN1** on the SMCWEB-N to your network or Ethernet client device(s). Now connect the power supply. Ethernet LAN ports of the SMCWEB-N are Auto MDI/MDIX and will work with both Straight-through and Cross-Over cable.
3. To access the default management IP address your PC must have an IP address in the range 192.168.2.3-254, with subnet mask 255.255.255.0.
4. Start web browser and enter address <http://192.168.2.2> (default). When prompted enter password **smcadmin** then click [Log In]. **Note:** The User Name must be set to Admin.
5. Click [Wireless Network Setup Wizard] and follow the on screen instructions to complete the set-up and reboot.

Using the Configuration Menu in AP Mode

Whenever you want to configure your SMCWEB-N, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the SMCWEB-N. The SMCWEB-N's default IP Address is http://192.168.2.2.

- Open the Web browser.
- Type in the **IP Address** of the SMCWEB-N (http://192.168.2. 2).

The screenshot shows the web interface for SMC Networks. At the top, the SMC Networks logo is on the left, and the text 'Draft 11n Wireless AP/Ethernet Client SMCWEB-N' is on the right. Below this is a 'LOGIN' section with the heading 'Log in to the access point:'. It contains a 'User Name' dropdown menu with 'Admin' selected, a 'Password' input field, and a 'Log In' button. At the bottom of the page, the copyright notice 'Copyright © 2004-2007 SMC, Inc.' is displayed.

- Select **Admin** in the **User Name** field.
- Enter **Password:** smcadmin (default).
- Click **Login In**.

Basic

The Basic tab provides the following configuration options: Wireless Settings and Network Settings.

Basic_ Wireless Settings

The wireless section is used to configure the wireless settings for your access point. Note that changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC ADVANCED TOOLS STATUS HELP

BASIC

WIRELESS SETTINGS

NETWORK SETTINGS

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

ADD WIRELESS DEVICE WIZARD

This wizard is designed to assist you in connecting your wireless device to your access point. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

[Add Wireless Device Wizard](#)

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Network Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the access point.

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new access point manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Network Setup](#)

Copyright © 2004-2007 SMC, Inc.

Enable Wireless

This option turns off and on the wireless connection feature of the access point. When you set this option, the following parameters are in effect.

Wireless Network Name

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

Enable Auto Channel Scan

If you select this option, the access point automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the access point uses the channel that you specify with the following **Wireless Channel** option.

Wireless Channel

A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

802.11 Mode

If all of the wireless devices you want to connect with this access point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Channel Width

The "Auto 20/40 MHz" option is usually best. The other options are available for special circumstances.

Transmission Rate

By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

Number of Spatial Streams

Selecting more than one spatial stream can increase throughput, but can in some cases decrease signal quality. Select the option that works best for your installation.

Visibility Status

The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

WEP

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Example:

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

Note that, if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros.

WPA-Personal and WPA-Enterprise

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The **WPA Mode** further refines the variant that the access point should employ.

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the access point only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the access point tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the access point associates only with clients that also support WPA2 security.

Cipher Type: The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the access point negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Example:

Wireless Networking technology enables ubiquitous communication

WPA-Enterprise

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

MAC Address Authentication: If this is selected, the user must connect from the same computer whenever logging into the wireless network.

Advanced:

Optional Backup RADIUS Server

This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields **Second RADIUS Server IP Address**, **RADIUS Server Port**, **Second RADIUS server Shared Secret**, **Second MAC Address Authentication** provide the corresponding parameters for the second RADIUS Server

Basic_Network Settings

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC ADVANCED TOOLS STATUS HELP

BASIC

WIRELESS SETTINGS

NETWORK SETTINGS

NETWORK SETTINGS

Use this section to configure the internal network settings of your access point and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

[Save Settings](#) [Don't Save Settings](#)

ACCESS POINT SETTINGS

Use this section to configure the internal network settings of your access point. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN Connection Type: Static IP

Access Point IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Local Domain Name: (optional)

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server:

DHCP IP Address Range: 192.168.2.100 to 192.168.2.199

DHCP Lease Time: 1440 (minutes)

Always broadcast: (compatibility for some DHCP Clients)

NetBIOS announcement:

NetBIOS Scope: (optional)

NetBIOS node type:

- Broadcast only (use when no WINS servers configured)
- Point-to-Point (no broadcast)
- Mixed-mode (Broadcast then Point-to-Point)
- Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address: 0.0.0.0

Secondary WINS IP Address: 0.0.0.0

Access Point Settings

These are the settings of the LAN (Local Area Network) interface for the access point. The access point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

DHCP Server Settings

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Enable DHCP Server

Once your access point is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically".

When you set **Enable DHCP Server**, the following options are displayed.

DHCP IP Address Range

These two IP values (*from* and *to*) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see [DHCP Reservation](#) below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

Your access point, by default, has a static IP address of 192.168.2.2. This means that addresses 192.168.2.3 to 192.168.2.254 can be made available for allocation by the DHCP Server.

Example:

Your access point uses 192.168.2.2 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.2.3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.168.2.4. Therefore the starting IP address for your DHCP IP address range needs to be 192.168.2.5 or greater.

Example:

Suppose you configure the DHCP Server to manage addresses From 192.168.2.100 To 192.168.2.199. This means that 192.168.2.3 to 192.168.2.99 and 192.168.2.200 to 192.168.2.254 are NOT managed by the DHCP Server. Computers or devices that use addresses from these ranges are to be manually configured. Suppose you have a web server computer that has a manually configured address of 192.168.2.100. Because this falls within the "managed range" be sure to create a reservation for this address and match it to the relevant computer (see [Static DHCP Client](#) below).

DHCP Lease Time

The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

Always Broadcast

If all the computers on the LAN successfully obtain their IP addresses from the access point's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the access point's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the access point to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

NetBIOS Advertisement

Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allow LAN hosts to discover all other computers within the network, e.g. within Network Neighbourhood.

Primary WINS Server IP address

Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in Network Neighbourhood.

Secondary WINS Server IP address

Configure the IP address of the backup WINS server, if any.

NetBIOS Scope

This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate.

NetBIOS Registration mode

Indicates how network hosts are to perform NetBIOS name registration and discovery.

H-Node, this indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers.

M-Node (default), this indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN.

P-Node, this indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server.

B-Node, this indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first.

Add/Edit DHCP Reservation

This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the access point. The access point will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

Enable

Specifies whether the entry will be active or inactive.

Computer Name

You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way. Example: **Game Server**.

IP Address:

The LAN address that you want to reserve.

MAC Address

To input the MAC address of your system, enter it in manually or connect to the access point's

Web-Management interface from the system and click the **Copy Your PC's MAC Address** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the access point from the computer and click the **Copy Your PC's MAC Address** button to enter the MAC address.

As an alternative, you can locate a MAC address in a specific operating system by following the steps below:

Windows 98
Windows Me

Go to the Start menu, select Run, type in **winipcfg**, and hit Enter. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address. This is the MAC address of the device.

Windows 2000 Windows XP	Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type ipconfig /all and hit Enter. The physical address displayed for the adapter connecting to the access point is the MAC address.
Mac OS X	Go to the Apple Menu, select System Preferences, select Network, and select the Ethernet Adapter connecting to the access point. Select the Ethernet button and the Ethernet ID will be listed. This is the same as the MAC address.

Save/Update

Record the changes you have made into the following list.

Clear

Re-initialize this area of the screen, discarding any changes you have made.

DHCP Reservations List

This shows clients that you have specified to have reserved DHCP addresses. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing.

Number of Dynamic DHCP Clients

In this section you can see what LAN devices are currently leasing IP addresses.

Revoke

The **Revoke** option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking **Revoke** cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

Reserve

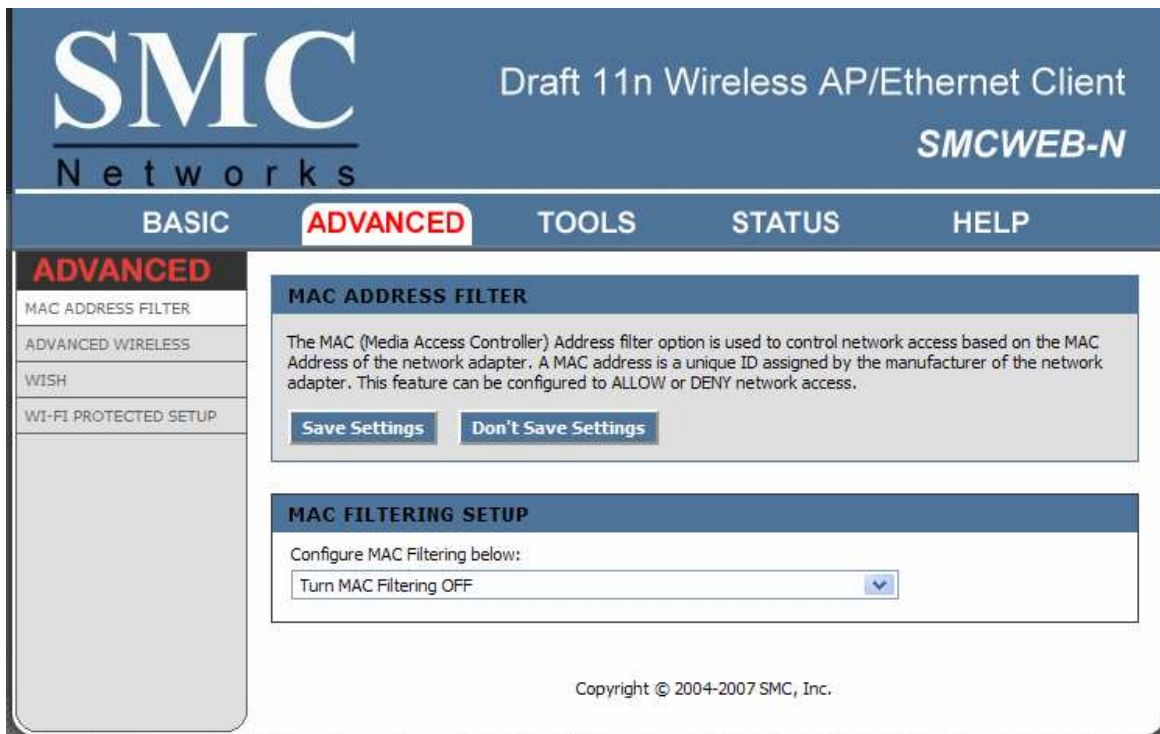
The **Reserve** option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

Advanced

The Advanced tab provides the following configuration options: **MAC Address Filter**, **Advanced Wireless**, **WISH**, **Wi-Fi Protected Setup**

Advanced_ MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.



16 -- MAC Filtering Rules

Configure MAC Filtering

When "OFF" is selected, MAC addresses are not used to control network access. When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "DENY" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

MAC Address

Enter the MAC address of the desired. Computers that have obtained an IP address from the access point's DHCP server will be in the DHCP Client List. Select a device from the drop down menu, then click the arrow to add that device's MAC address to the list.

Clear

Click the **Clear** button to remove the MAC address from the MAC Filtering list.

Advanced_Advanced Wireless

The screenshot shows the SMC Networks configuration interface for a Draft 11n Wireless AP/Ethernet Client. The page is titled "SMC Networks" and "Draft 11n Wireless AP/Ethernet Client SMCWEB-N". The navigation menu includes "BASIC", "ADVANCED" (selected), "TOOLS", "STATUS", and "HELP". The "ADVANCED" section is expanded to show "ADVANCED WIRELESS" settings. A warning message states: "If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings." Below this are "Save Settings" and "Don't Save Settings" buttons. The "ADVANCED WIRELESS SETTINGS" section includes the following options:

Transmit Power :	High	(v)
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
802.11d Enable :	<input type="checkbox"/>	
Wireless Isolation :	<input type="checkbox"/>	
WMM Enable :	<input checked="" type="checkbox"/>	
WDS Enable :	<input type="checkbox"/>	
Short GI :	<input checked="" type="checkbox"/>	

Copyright © 2004-2007 SMC, Inc.

Transmit Power

Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

Beacon Period

Beacons are packets sent by a wireless access point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

RTS Threshold

When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.

Fragmentation Threshold

Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.

DTIM Interval

A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Wireless Isolation

Enabling Wireless Isolation prevents associated wireless clients from communicating with each other.

WMM Enable

Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

Short GI

Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

Extra Wireless Protection

Extra protection for neighboring 11b wireless networks. Turn this option off to reduce the adverse effect of legacy wireless networks on 802.11ng performance. This option is available only when **802.11 Mode** is set to an **11n Only** option. (Refer to the [Basic → Wireless](#) page.)

WDS Enable

When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.

WDS AP MAC Address

Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP. Enter a MAC address for each of the other APs that you want to connect with WDS.

Advanced_ WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

The screenshot shows the SMC Networks configuration interface for a Draft 11n Wireless AP/Ethernet Client. The page is titled "SMC Networks" and "Draft 11n Wireless AP/Ethernet Client SMCWEB-N". The navigation menu includes "BASIC", "ADVANCED" (selected), "TOOLS", "STATUS", and "HELP". The left sidebar shows "ADVANCED" selected, with sub-items: "MAC ADDRESS FILTER", "ADVANCED WIRELESS", "WISH", and "WI-FI PROTECTED SETUP".

The main content area is titled "WISH" and contains the following sections:

- WISH**: A description of WISH (Wireless Intelligent Stream Handling) and two buttons: "Save Settings" and "Don't Save Settings".
- WISH**: A section with "Enable WISH :
- PRIORITY CLASSIFIERS**: A section with three options: "HTTP : " (checked), "Windows Media Center : " (checked), and "Automatic : (default if not matched by anything else)".
- ADD WISH RULE**: A form with fields for "Enable : " (unchecked), "Name : " (empty), "Priority : Background (BK) " (dropdown), "Protocol : Other " (dropdown), "Host 1 IP Range : - " (text), "Host 1 Port Range : - " (text), "Host 2 IP Range : - " (text), and "Host 2 Port Range : - " (text). There are "Save" and "Clear" buttons at the bottom.
- WISH RULES**: A table with columns: "Name", "Priority", "Host 1 IP Range", "Host 2 IP Range", and "Protocol / Ports". The table is currently empty.

Copyright © 2004-2007 SMC, Inc.

WISH

Enable WISH

Enable this option if you want to allow WISH to prioritize your traffic.

Priority Classifiers

HTTP

Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center

Enables the access point to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic

When enabled, this option causes the access point to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

Add/Edit WISH Rule

A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Enable

Specifies whether the entry will be active or inactive.

Name

Create a name for the rule that is meaningful to you.

Priority

The priority of the message flow is entered here. Four priorities are defined:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Protocol

The protocol used by the messages.

Host 1 IP Range

The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range

The rule applies to a flow of messages for which host 1's port number is within the range set here.

Host 2 IP Range

The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

Host 2 Port Range

The rule applies to a flow of messages for which host 2's port number is within the range set here.

Save/Update

Record the changes you have made into the following list.

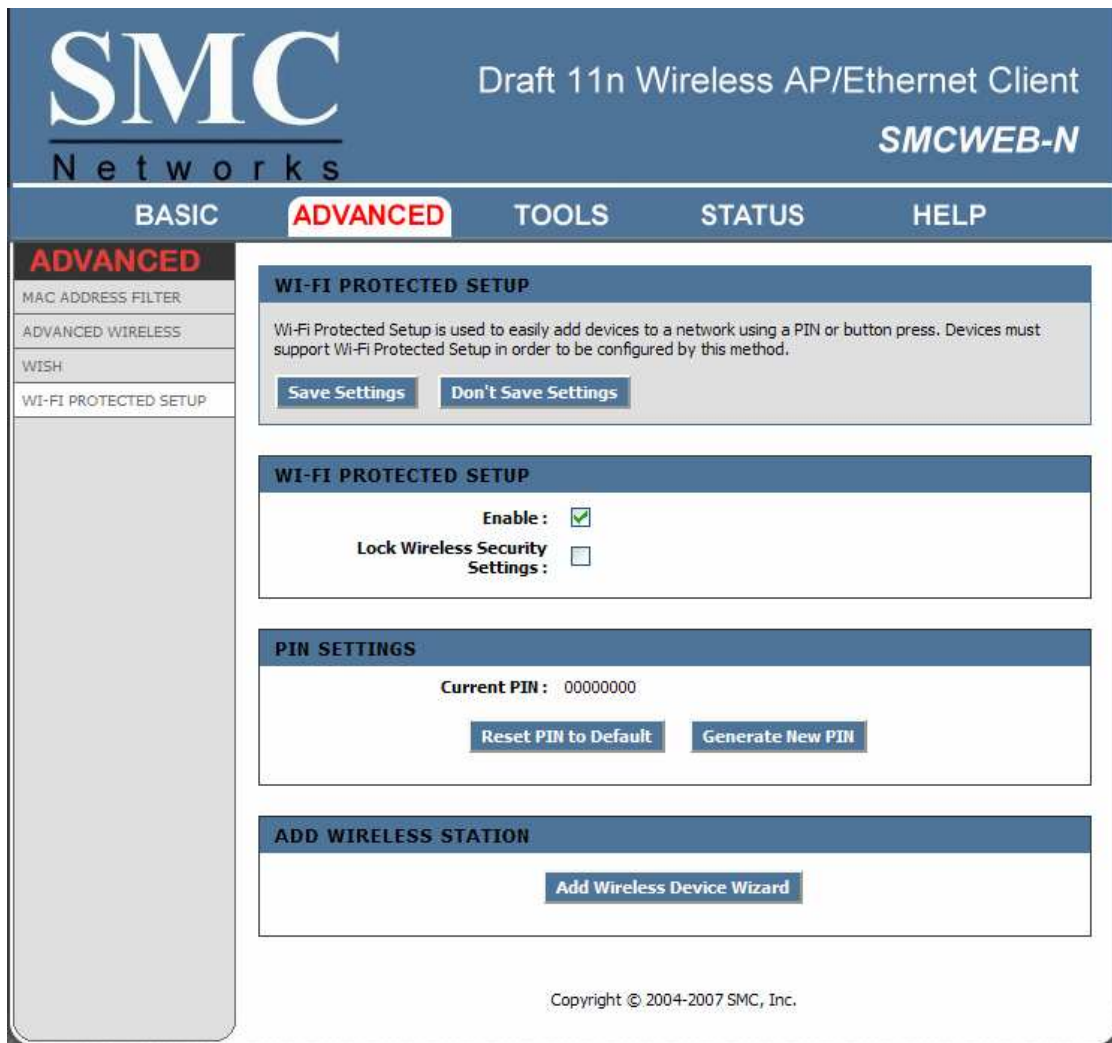
Clear

Re-initialize this area of the screen, discarding any changes you have made.

WISH Rules

This section lists the defined WISH Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit WISH Rule" section is activated for editing.

Advanced_ Wi-Fi Protected Setup



Wi-Fi Protected Setup

Enable

Enable the Wi-Fi Protected Setup feature.

Lock Wireless Security Settings

Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup. It is still possible to change wireless network settings with [Manual Wireless Network Setup](#), [Wireless Network Setup Wizard](#), or an existing external WLAN Manager Registrar.

PIN Settings

A PIN is a unique number that can be used to add the access point to an existing network or to create a new network. The default PIN is printed on the bottom of the access point. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

Current PIN

Shows the current value of the access point's PIN.

Reset PIN to Default

Restore the default PIN of the access point.

Generate New PIN

Create a random number that is a valid PIN. This becomes the access point's PIN. You can then copy this PIN to the user interface of the registrar.

Add Wireless Station

This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the access point within 60 seconds. The status LED on the access point will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. Access to the wireless network is controlled by a "registrar". A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The access point acts as a registrar for the network, although other devices may act as a registrar as well.

Tools

The Tools tab provides the following configuration options: **Admin, Time, System, Firmware**

Tools_Admin

The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new access point secure.

The screenshot displays the SMC Networks web management interface. The header includes the SMC Networks logo and the device model 'Draft 11n Wireless AP/Ethernet Client SMCWEB-N'. A navigation bar contains tabs for 'BASIC', 'ADVANCED', 'TOOLS' (which is selected), 'STATUS', and 'HELP'. On the left, a vertical menu lists 'TOOLS', 'ADMIN', 'TIME', 'SYSTEM', and 'FIRMWARE'. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS**: A text block explaining that 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. It notes that by default there is no password configured and recommends creating one for security. Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'.
- INACTIVITY TIME OUT**: A section with the instruction 'The number of minutes of no activity before your login is cancelled.' and a text input field for 'Inactivity Time Out' containing the value '15'.
- ADMIN PASSWORD**: A section with the instruction 'Please enter the same password into both boxes, for confirmation.' It features two password input fields labeled 'Password' and 'Verify Password', both containing masked characters (asterisks).
- USER PASSWORD**: A section with the instruction 'Please enter the same password into both boxes, for confirmation.' It features two password input fields labeled 'Password' and 'Verify Password', both containing masked characters (asterisks).
- SYSTEM NAME**: A section with a text input field for 'Device Name' containing the value 'SMCWEB-N'.

At the bottom of the page, the copyright notice reads: 'Copyright © 2004-2007 SMC, Inc.'

Inactivity Time Out

If the router does not detect any administrative activity during this number of minutes, it logs the administrator off.

Admin Password

Enter a password for the user "admin", who will have full access to the Web-based management interface.

User Password

Enter a password for the user "user", who will have read-only access to the Web-based management interface.

Device Name

The name of the access point can be changed here.

Tools_Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the access point's internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight saving can also be configured to automatically adjust the time when needed.

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC ADVANCED **TOOLS** STATUS HELP

TOOLS

- ADMIN
- TIME
- SYSTEM
- FIRMWARE

TIME

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Save Settings Don't Save Settings

TIME CONFIGURATION

Current Time: 31 January 2004 10:50:15

Time Zone: (GMT-08:00) Pacific Time (US/Canada), Tijuana

Enable Daylight Saving:

Daylight Saving Offset: +1:00

Daylight Saving Dates:

	Month	Week	Day of Week	Time
DST Start	Apr	1st	Sun	2 am
DST End	Oct	5th	Sun	2 am

AUTOMATIC TIME CONFIGURATION

Enable NTP Server:

NTP Server Used: << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time:

Year	2004	Month	Jan	Day	31
Hour	10	Minute	50	Second	09 AM

Copy Your Computer's Time Settings

Copyright © 2004-2007 SMC, Inc.

Time Configuration

Current Time

Displays the time currently maintained by the access point. If this is not correct, use the following options to configure the time correctly.

Time Zone

Select your local time zone from pull down menu.

Enable Daylight Saving

Check this option if your location observes daylight saving time.

Daylight Saving Offset

Select the time offset, if your location observes daylight saving time.

DST Start and DST End

Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."

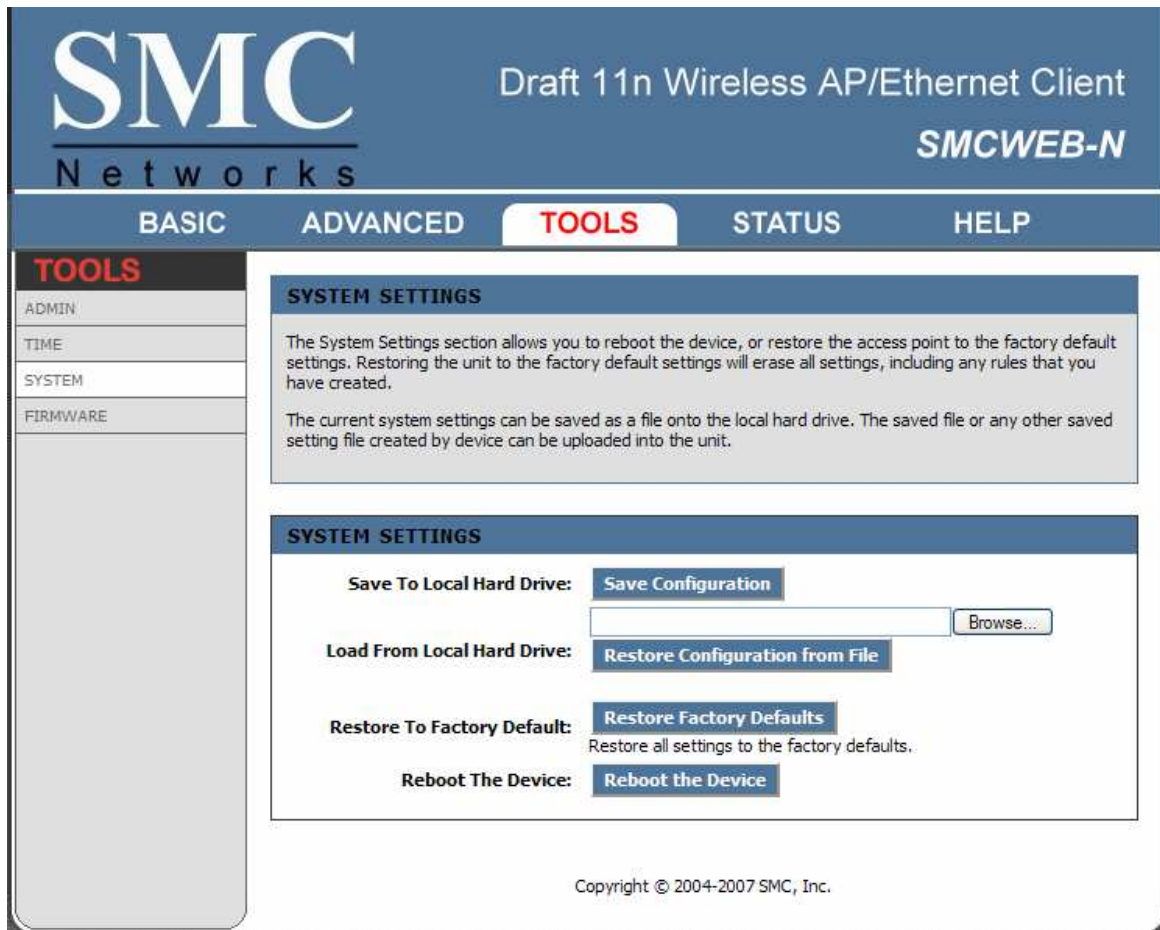
Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your access point here, or you can click the [Copy Your Computer's Time Settings](#) button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

Note: If the access point loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the access point, or you must enable the NTP Server option.

Tools_System

This section allows you to manage the access point's configuration settings, reboot the access point, and restore the access point to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.



Save To Local Hard Drive

This option allows you to save the access point's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

Load From Local Hard Drive

Use this option to restore previously saved access point configuration settings.

Restore To Factory Default

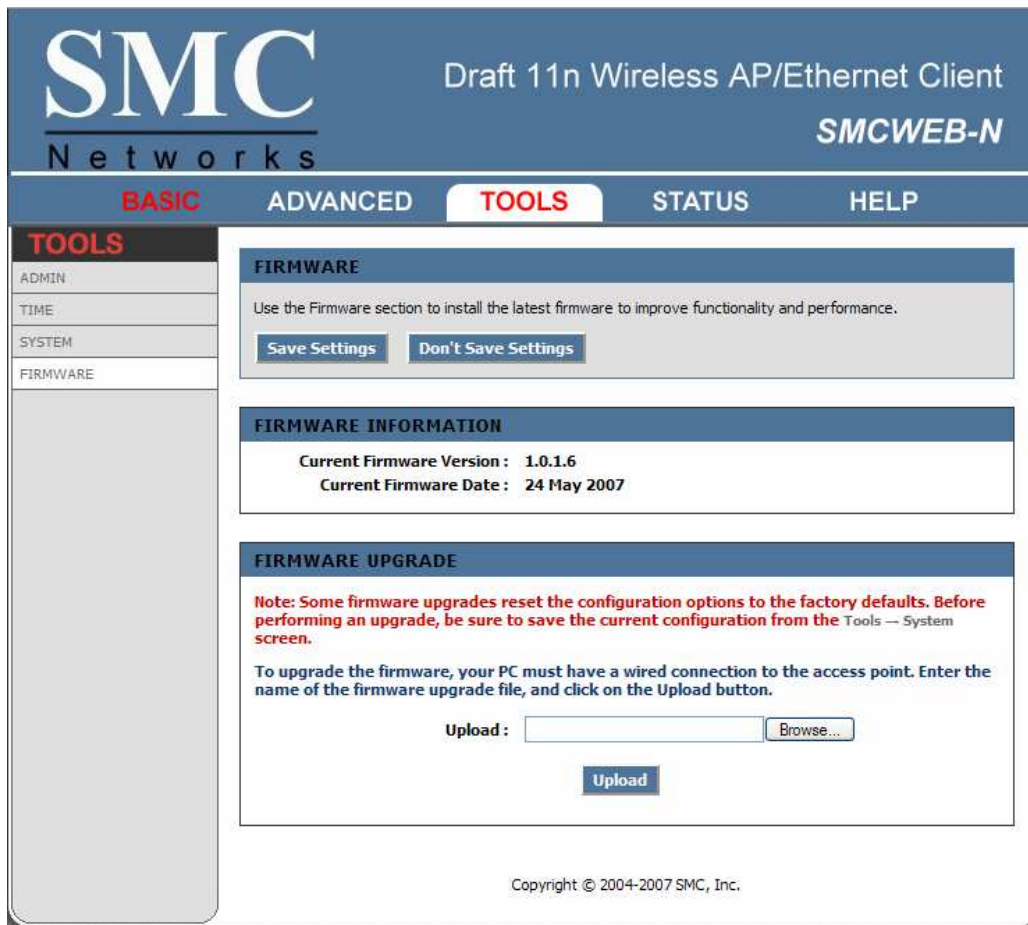
This option restores all configuration settings back to the settings that were in effect at the time the access point was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your access point configuration settings, use the Save Settings option above.

Reboot The Device

This restarts the access point. Useful for restarting when you are not near the device.

Tools_Firmware

Use the Firmware section to install the latest firmware to improve functionality and performance.



To upgrade the firmware, follow these steps:

1. Click the **Browse** button to locate the upgrade file on your computer.
2. Once you have found the file to be used, click the **Upload** button below to start the firmware upgrade process. This can take a minute or more.
3. Wait for the access point to reboot. This can take another minute or more.
4. Confirm updated firmware revision on status page.

Firmware Information

Here are displayed the version numbers of the firmware currently installed in your access point and the most recent upgrade that is available.

Firmware Upgrade

Note: Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the access point by wire.

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the [Tools → System](#) screen.

Upload

Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point.

Status

The Status tab provides the following configuration options: **Device Info, Wireless, Logs, Statistics and WISH Sessions.**

Status_Device info

All of your network connection details are displayed on the Device Info page. The firmware version is also displayed here.

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

STATUS

- DEVICE INFO
- WIRELESS
- LOGS
- STATISTICS
- WISH SESSIONS

DEVICE INFORMATION

All of your network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 31 January 2004 10:59:59
Firmware Version : 1.0.1.6, 24 May 2007

LAN

Connection Type : Static IP
MAC Address : 00:11:E0:05:01:01
IP Address : 192.168.2.2
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
DHCP Server : Disabled

WIRELESS LAN

Wireless Radio : Enabled
WISH : Active
MAC Address : 00:11:E0:05:01:01
Network Name (SSID) : SMC
Channel : 11
Security Mode : Disabled
Wi-Fi Protected Setup : Enabled/Not Configured

LAN COMPUTERS

IP Address	Name (if any)	MAC
------------	---------------	-----

Copyright © 2004-2007 SMC, Inc.

Wireless LAN

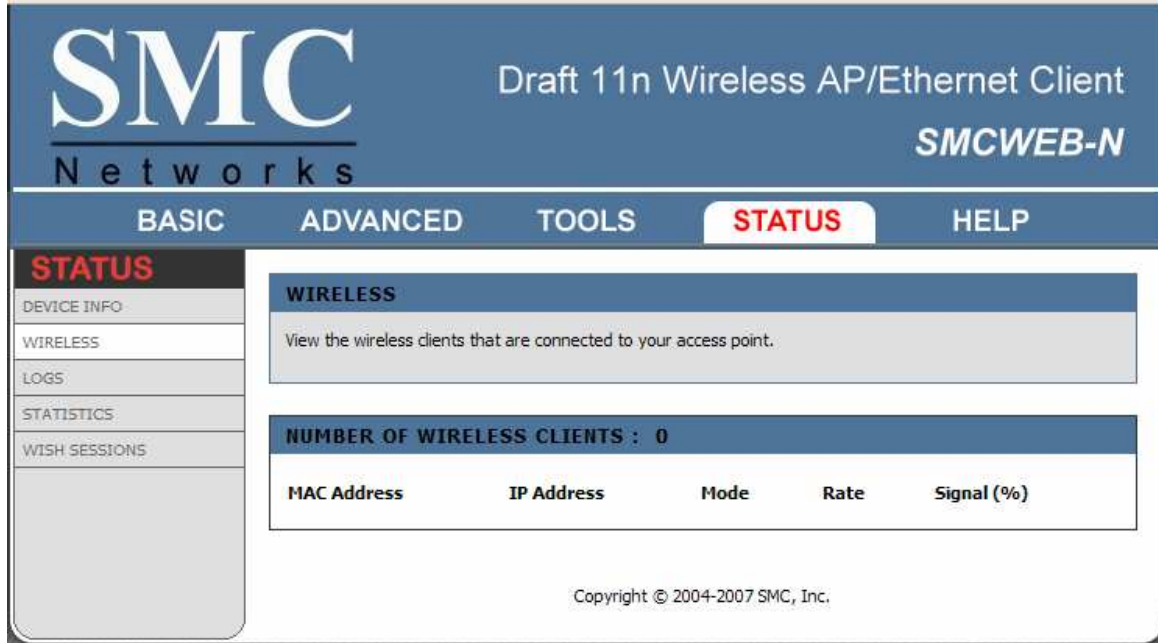
This area of the screen reflects configuration settings from the [Setup → Wireless Settings](#) page and the [Advanced → WISH](#) page. The **MAC Address** is the factory-assigned identifier of the wireless card.

LAN Computers

This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your access point. The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to "Automatically obtain an address") supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not.

Status_Wireless

The wireless section allows you to view the wireless clients that are connected to your wireless access point.



MAC Address

The Ethernet ID (MAC address) of the wireless client.

IP Address

The LAN-side IP address of the client.

Mode

The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.

Rate

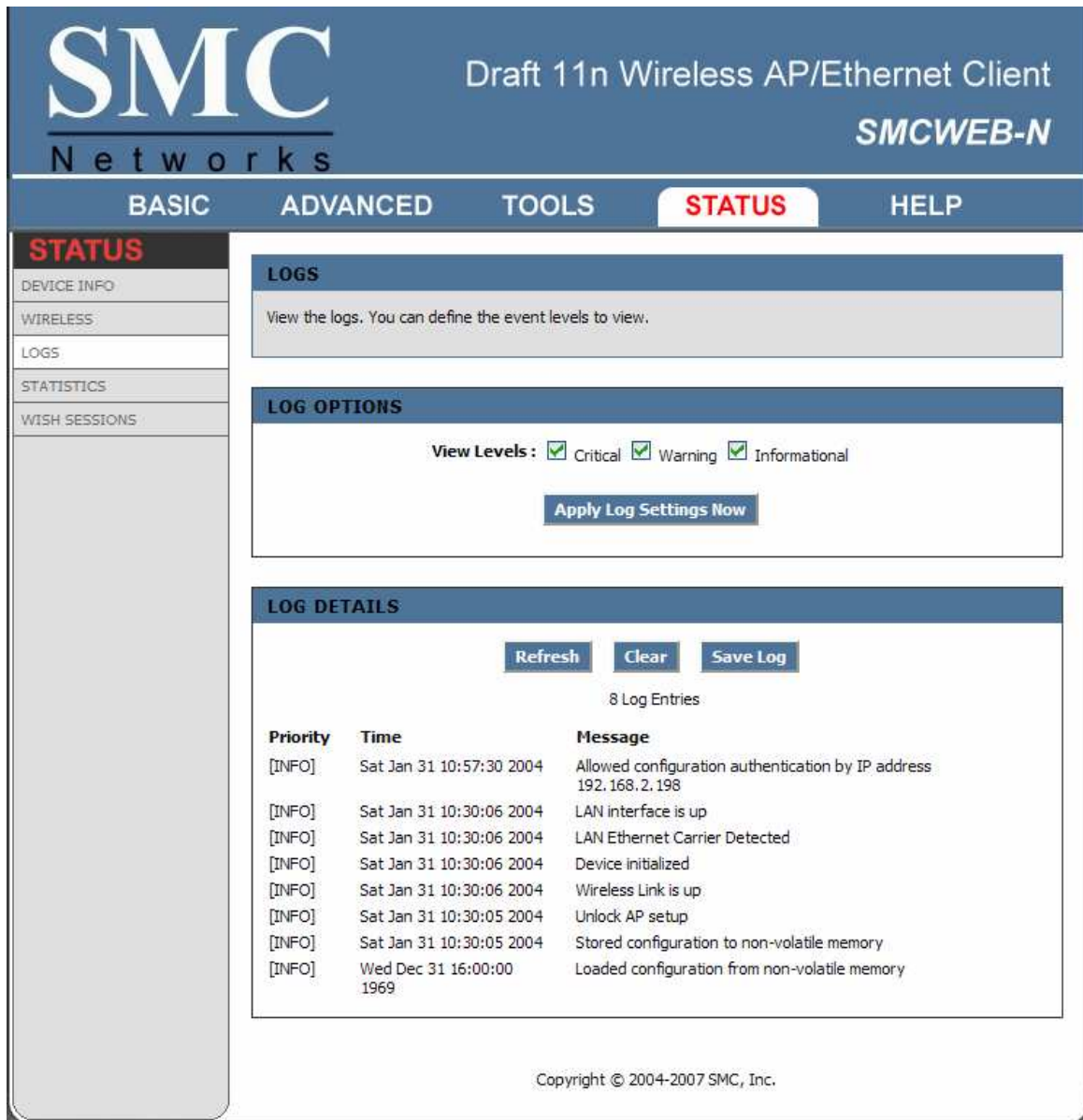
The actual transmission rate of the client in megabits per second.

Signal

This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the access point and the wireless device.

Status_Logs

The access point automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to define the level of events to view.



View Levels

Select the level of events that you want to view.

- Critical
- Warning
- Informational

Apply Log Settings Now

Click this button after changing Log Options to make them effective and permanent.

Refresh

Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear

Clicking this button erases all log entries.

Save Log

Select this option to save the access point log to a file on your computer.

Status_Statistics

The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.

The screenshot shows the SMC Networks SMCWEB-N interface. The top navigation bar includes BASIC, ADVANCED, TOOLS, STATUS (highlighted), and HELP. The left sidebar contains links for STATUS, DEVICE INFO, WIRELESS, LOGS, STATISTICS, and WISH SESSIONS. The main content area is divided into three sections: TRAFFIC STATISTICS, LAN STATISTICS, and WIRELESS STATISTICS. The TRAFFIC STATISTICS section includes a description and buttons for Refresh Statistics and Clear Statistics. The LAN STATISTICS section shows Sent: 492, Received: 9441, TX Packets Dropped: 0, RX Packets Dropped: 0, and Collisions: 0. The WIRELESS STATISTICS section shows Sent: 9007, Received: 0, TX Packets Dropped: 0, RX Packets Dropped: 0, and Errors: 0. The footer contains the copyright notice: Copyright © 2004-2007 SMC, Inc.

LAN STATISTICS	
Sent :492	Received :9441
TX Packets Dropped :0	RX Packets Dropped :0
Collisions :0	Errors :0

WIRELESS STATISTICS	
Sent :9007	Received :0
TX Packets Dropped :0	RX Packets Dropped :0
	Errors :0

Sent

The number of packets sent from the access point.

Received

The number of packets received by the access point.

TX Packets Dropped

The number of packets that were dropped while being sent, due to errors, collisions, or access point resource limitations.

RX Packets Dropped

The number of packets that were dropped while being received, due to errors, collisions, or access point resource limitations.

Collisions

The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).

Errors

The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.

Status_WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your access point when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

The screenshot shows the SMC Networks Draft 11n Wireless AP/Ethernet Client SMCWEB-N interface. The top navigation bar includes BASIC, ADVANCED, TOOLS, STATUS (highlighted), and HELP. The left sidebar contains links for STATUS, DEVICE INFO, WIRELESS, LOGS, STATISTICS, and WISH SESSIONS. The main content area displays the WISH SESSIONS page, which includes a descriptive paragraph and a table with columns for Originator, Target, Protocol, State, Priority, and Time Out. The footer of the page reads 'Copyright © 2004-2007 SMC, Inc.'

Originator

The IP address and, where appropriate, port number of the computer that originated a network connection.

Target

The IP address and, where appropriate, port number of the computer to which a network connection has been made.

Protocol

The communications protocol used for the conversation.

State

State for sessions that use the TCP protocol.

- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- the server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Priority

The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Time Out

The number of seconds of idle time until the access point considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

300 seconds

UDP connections.

240 seconds

Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

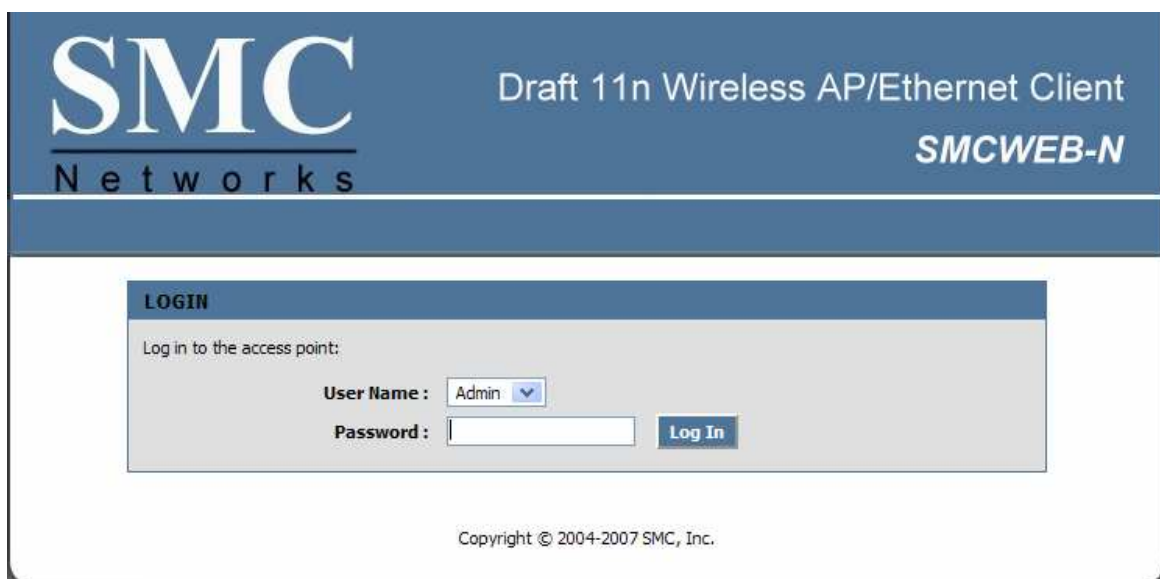
7800 seconds

Established or closing TCP connections.

Using the Configuration Menu in Client Mode

Whenever you want to configure your SMCWEB-N, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the SMCWEB-N. The SMCWEB-N's default IP Address is http://192.168.2.2.

- Open the Web browser.
- Type in the **IP Address** of the Client (http://192.168.2. 2).



The screenshot shows the SMC Networks login interface. At the top, the SMC Networks logo is on the left, and the text 'Draft 11n Wireless AP/Ethernet Client SMCWEB-N' is on the right. Below this is a 'LOGIN' section with a header 'Log in to the access point:'. The 'User Name' field is a dropdown menu currently showing 'Admin'. The 'Password' field is an empty text box. To the right of the password field is a blue 'Log In' button. At the bottom of the page, the copyright notice 'Copyright © 2004-2007 SMC, Inc.' is displayed.

- Select **admin** in the **User Name** field.
- Enter **Password:** smcadmin (default).
- Click **Login In**.

Basic

The Basic tab provides the following configuration options: **Wizard, Wireless, Network Settings**

Basic_Wizard

If you want to connect a new wireless network, click on **Setup Wizard** and the bridge will guide you through a few steps to get your network up and running.

SMC Networks
Draft 11n Wireless AP/Ethernet Client
SMCWEB-N

BASIC ADVANCED TOOLS STATUS HELP

BASIC
WIZARD
WIRELESS
NETWORK SETTINGS

SETUP WIZARD
The following Web-based wizards are designed to assist you in your wireless network setup.

WIRELESS NETWORK SETUP WIZARD
This wizard is designed to assist you to configure the wireless settings for your client. It will guide you through step-by-step instructions on how to setup wireless network. Click the button below to begin.

Wireless Setup Wizard

Copyright © 2004-2007 SMC, Inc.

Basic_Wireless

The wireless section is used to configure the wireless settings for your bridge. Note that some options in this section must agree with options selected for your wireless access point or wireless router.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC ADVANCED TOOLS STATUS HELP

BASIC

WIZARD
WIRELESS
NETWORK SETTINGS

WIRELESS

Wireless Network Settings

Use this section to configure the wireless settings for your wireless client. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Save Settings **Don't Save Settings**

WIRELESS NETWORK SETTINGS

Enable Wireless:

Wireless Network Name: SMCWGBR14-N_cb02dfe (Also called the SSID)

Enable Auto Channel Scan:

Wireless Channel: 2.437 GHz - CH 6

802.11 Mode: Mixed 802.11n, 802.11g and 802.11b

Transmission Rate: Best (automatic) (Mbit/s)

Channel Width: Auto 20/40 MHz

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode: WPA-Personal

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy APs are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode: Auto (WPA or WPA2)

Cipher Type: TKIP or AES

PRE-SHARED KEY

Pre-Shared Key: *****

Enable Wireless

This option turns off and on the wireless connection feature of the bridge. When you set this option, the following parameters are in effect.

Wireless Network Name

This is the name of the wireless access point that this station will associate to. Leave this field blank to associate to any access point.

Enable Auto Channel Scan

If you select this option, the bridge automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the bridge uses the channel that you specify with the following **Wireless Channel** option.

Wireless Channel

A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Your wireless bridge will use the channel that is used by the access point it associates with. But here you can select your channel preference to help optimize the performance and coverage of your wireless network.

802.11 Mode

If all of the wireless devices in your wireless network can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Channel Width

The "Auto 20/40 MHz" option is usually best. The other options are available for special circumstances.

Transmission Rate

By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

Number of Spatial Streams

Selecting more than one spatial stream can increase throughput, but can in some cases decrease signal quality. Select the option that works best for your installation.

Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

WEP

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Example:

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

Note that, if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros.

WPA-Personal and WPA-Enterprise

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The **WPA Mode** further refines the variant that the bridge should employ.

WPA Mode: WPA is the older standard; select this option if the Access Point that will be used with the bridge only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the **WPA2** option, the bridge tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the bridge associates only with clients that also support WPA2 security.

Cipher Type: The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. With the **TKIP or AES** option, the bridge negotiates the cipher type with the access point, and uses AES when available.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK). The WPA Mode further refines the variant that the bridge should employ. This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Example:

Wireless Networking technology enables ubiquitous communication

WPA-Enterprise

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this bridge.

EAP Type: The EAP type which is used for the authentication. These types are EAP-TLS, EAP-TTLS and PEAP.

Inner Authentication Method for TTLS: If the authentication type is selected as EAP-TTLS, it uses an inner authentication method after the TLS-secured tunnel is established between the client and server. The supported inner authentication types for EAP-TTLS are PAP, CHAP and MS-CHAPv2.

Inner Authentication Method for PEAP: If the authentication type is selected as PEAP, it uses an inner authentication method after the TLS-secured tunnel is established between the client and server. The supported inner authentication type for PEAP is MS-CHAPv2.

EAP Username: The username of the wireless client for the tunnel establishment and the inner authentication method.

EAP Password: The password of the wireless client for EAP-MD5 or the inner authentication methods of PEAP and EAP-TTLS.

EAP Certificate Password: The password of the user certificate file.

EAP User Certificate: The user certificate file. It is mandatory for EAP-TLS, but optional for PEAP and EAP-TTLS. If it is not uploaded for PEAP and EAP-TTLS, the bridge may establish a relatively unsecure system. We support .p12 and .pfx formats with a maximum size of 8192 bytes.

EAP Root Certificate: The root certificate file. It is mandatory to upload a root certificate to be able to authenticate the server certificate. We support .der and .cer formats with a maximum size of 8192 bytes.

Basic_Network Settings

SMC Networks Draft 11n Wireless AP/Ethernet Client **SMCWEB-N**

BASIC ADVANCED TOOLS STATUS HELP

BASIC
WIZARD
WIRELESS
NETWORK SETTINGS

NETWORK SETTINGS

Use this section to configure the internal network settings of your client and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

[Save Settings](#) [Don't Save Settings](#)

LAN SETTINGS

Use this section to configure the internal network settings of your client. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

IP Address Mode : Static DHCP

IP Address:

Subnet Mask:

Default Gateway:

Copyright © 2004-2007 SMC, Inc.

LAN Settings

These are the settings of the LAN (Local Area Network) interface for the bridge. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

IP Address Mode

Select **DHCP** to get the IP settings from a DHCP server on your network. Select **Static** to use the IP settings specified on this page.

IP Address

The IP address of your bridge on the local area network. For example, 192.168.1.24 The address you choose must be consistent with the LAN settings of your router.

Subnet Mask

The subnet mask of the local area network.

Default Gateway

This is the IP address of the gateway or router that connects you to the internet.

Advanced

The Advanced tab provides the following configuration options: **Advanced Wireless, WISH, Wi-Fi Protected Setup**

Advanced_Advanced Wireless

The screenshot shows the SMC Networks web interface for a Draft 11n Wireless AP/Ethernet Client. The page title is "SMC Networks Draft 11n Wireless AP/Ethernet Client SMCWEB-N". The navigation menu includes "BASIC", "ADVANCED" (highlighted), "TOOLS", "STATUS", and "HELP". The left sidebar shows "ADVANCED" selected, with sub-options for "ADVANCED WIRELESS", "WISH", and "WI-FI PROTECTED SETUP". The main content area is titled "ADVANCED WIRELESS" and contains a warning message: "If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings." Below the warning are "Save Settings" and "Don't Save Settings" buttons. The "WIRELESS MAC CLONING" section has a "Cloning Mode" dropdown set to "WLAN Card" (selected) and "Ethernet Client". The "ADVANCED WIRELESS SETTINGS" section includes: "Transmit Power" set to "High", "802.11d Enable" (unchecked), "WMM Enable" (checked), and "Short GI" (checked). The footer contains "Copyright © 2004-2007 SMC, Inc."

MAC Cloning Mode

This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless). If set to **Ethernet Client**, the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC Address is being used. If set to **WLAN Card**, the MAC Address of the WLAN Card (typically written on the back of the card) will be used. When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change.

Transmit Power

Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

RTS Threshold

When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.

Fragmentation Threshold

Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. Setting the Fragmentation value too low may result in poor performance.

WMM Enable

Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

Short GI

Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

Advanced_Wish

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

The screenshot shows the SMC Networks web interface for a Draft 11n Wireless AP/Ethernet Client. The page is titled "Draft 11n Wireless AP/Ethernet Client" and "SMCWEB-N". The navigation menu includes "BASIC", "ADVANCED" (selected), "TOOLS", "STATUS", and "HELP". The left sidebar shows "ADVANCED" selected, with sub-items "ADVANCED WIRELESS", "WISH", and "WI-FI PROTECTED SETUP".

The main content area is titled "WISH" and contains the following sections:

- WISH**: A description of WISH (Wireless Intelligent Stream Handling) and two buttons: "Save Settings" and "Don't Save Settings".
- WISH**: A section with "Enable WISH :
- PRIORITY CLASSIFIERS**: A section with three options: "HTTP : " (checked), "Windows Media Center : " (checked), and "Automatic : (default if not matched by anything else)" (unchecked).
- ADD WISH RULE**: A section with fields for "Enable: " (unchecked), "Name: " (empty), "Priority: Background (BK) ", "Protocol: << Other ", "Host 1 IP Range: - " (empty), "Host 1 Port Range: - " (empty), "Host 2 IP Range: - " (empty), "Host 2 Port Range: - " (empty), and "Save" and "Clear" buttons.
- WISH RULES**: A table with columns: Name, Priority, Host 1 IP Range, Host 2 IP Range, Protocol / Ports.

Copyright © 2004-2007 SMC, Inc.

WISH

Enable WISH

Enable this option if you want to allow WISH to prioritize your traffic.

Priority Classifiers

HTTP

Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center

Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic

When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

WISH Rules

A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Name

Create a name for the rule that is meaningful to you.

Priority

The priority of the message flow is entered here. Four priorities are defined:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Protocol

The protocol used by the messages.

Host 1 IP Range

The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range

The rule applies to a flow of messages for which host 1's port number is within the range set here.

Host 2 IP Range

The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

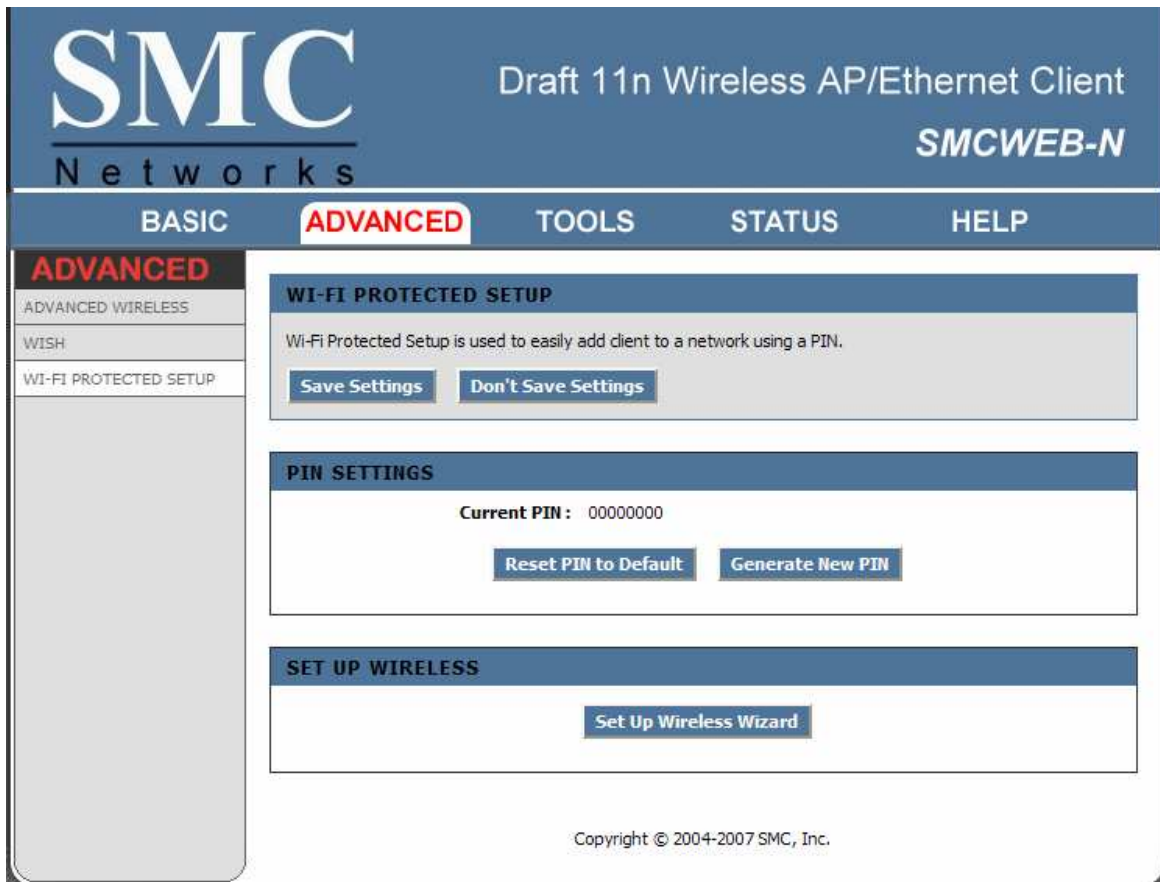
Host 2 Port Range

The rule applies to a flow of messages for which host 2's port number is within the range set here.

-- WISH Rules

This section is where you define WISH Rules. Enable or disable defined rules with the checkboxes at the left.

Advanced_Wi-Fi Protected Setup



PIN Settings

A PIN is a unique number that can be used to add the SMCWEB-N to an existing network or to create a new network. The default PIN is printed on the bottom of the unit. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

Current PIN

Shows the current value of the bridge's PIN.

Reset PIN to Default

Restore the default PIN of the bridge.

Generate New PIN

Create a random number that is a valid PIN. This becomes the bridge's PIN. You can then copy this PIN to the user interface of the registrar.

Set Up Wireless

This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then pressing the button on the router within 120 seconds. Each device

has an LED, and the LED will start flashing if the button is pressed. The LED on the router will turn solid ON if the device has been successfully added to the network. If something goes wrong during configuration, the flashing pattern of the LED changes.

There are several ways to add a wireless device to your network. Access to the wireless network is controlled by a “registrar”. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

After the device is in WiFi Protected Setup configured state, holding the button for more than 5 seconds will reset the device to unconfigured state, and the device will discard the current wireless security settings and will start to run WiFi Protected Setup protocol to find the new security settings.

Set UP Wireless Wizard

Start the wizard.

Tools

The Tools tab provides the following configuration options: **Admin, System, Firmware**

Tools_Admin

The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new bridge secure.

The screenshot shows the SMC Networks web management interface for a Draft 11n Wireless AP/Ethernet Client (SMCWEB-N). The interface has a blue header with the SMC Networks logo and the product name. Below the header is a navigation menu with tabs for BASIC, ADVANCED, TOOLS (selected), STATUS, and HELP. On the left side, there is a sidebar with a 'TOOLS' section containing links for ADMIN, SYSTEM, and FIRMWARE. The main content area is divided into several sections:

- ADMINISTRATOR SETTINGS:** A section with a blue header. It contains text explaining that 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. It also states that by default there is no password configured and it is highly recommended to create a password for security. At the bottom of this section are two buttons: 'Save Settings' and 'Don't Save Settings'.
- ADMIN PASSWORD:** A section with a blue header. It contains the instruction 'Please enter the same password into both boxes, for confirmation.' Below this are two input fields: 'Password : [password mask]' and 'Verify Password : [password mask]'.
- USER PASSWORD:** A section with a blue header. It contains the instruction 'Please enter the same password into both boxes, for confirmation.' Below this are two input fields: 'Password : [password mask]' and 'Verify Password : [password mask]'.
- ADMINISTRATION:** A section with a blue header. It contains two input fields: 'Bridge Name : SMCWEB-N' and 'Web Idle Timeout : 15'.

At the bottom of the page, there is a copyright notice: 'Copyright © 2004-2007 SMC, Inc.'

Admin Password

Enter a password for the user **admin**, who will have full access to the Web-based management interface.

User Password

Enter a password for the user **user**, who will have read-only access to the Web-based management interface.

Bridge Name

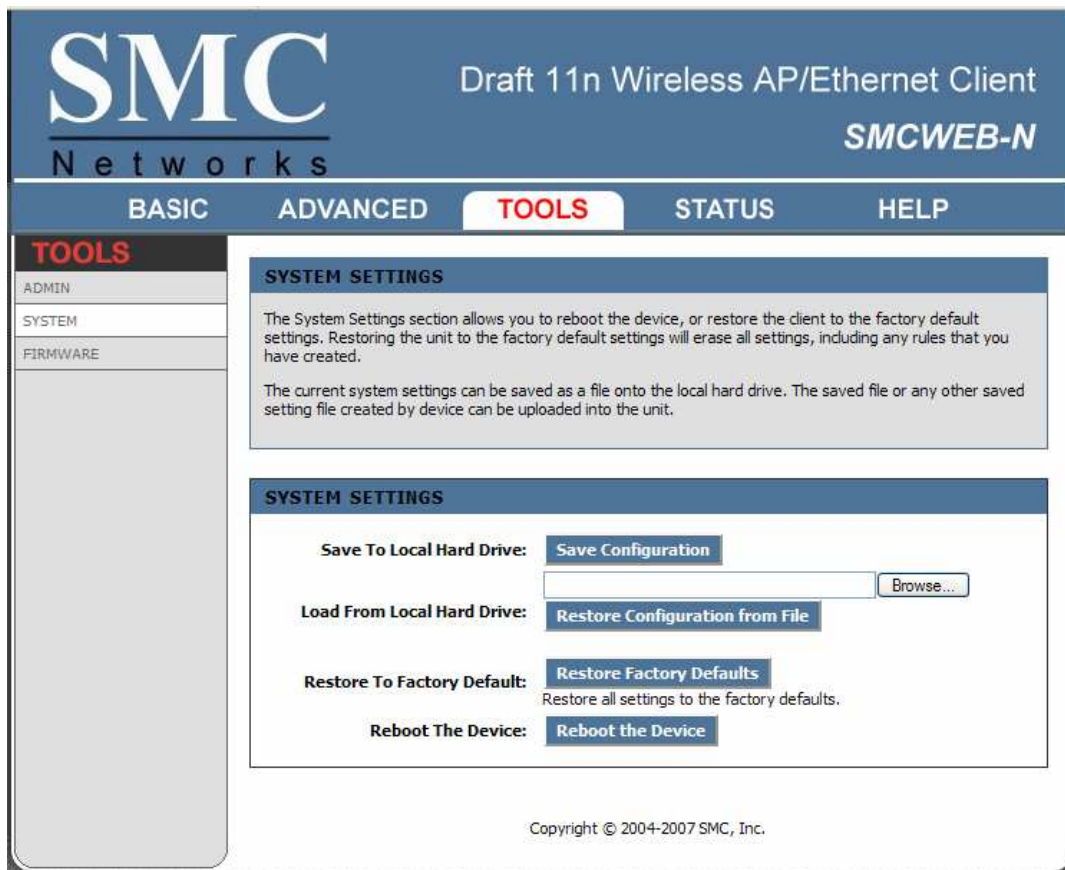
The name of the bridge can be changed here.

Web Idle Timeout

The maximum number of minutes that the web administration can be inactive before the administrator is automatically logged out.

Tools_System

This section allows you to manage the bridge's configuration settings, reboot the bridge, and restore the bridge to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.



Save To Local Hard Drive

This option allows you to save the bridge's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

Load From Local Hard Drive

Use this option to restore previously saved bridge configuration settings.

Restore To Factory Default

This option restores all configuration settings back to the settings that were in effect at the time the bridge was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your bridge configuration settings, use the Save Settings option above.

Reboot The Device

This restarts the bridge. Useful for restarting when you are not near the device.

Tools_Firmware

The Firmware section can be used to update to the latest firmware to improve functionality and performance.

The screenshot displays the SMC Networks web interface for a Draft 11n Wireless AP/Ethernet Client (SMCWEB-N). The interface has a blue header with the SMC Networks logo and the device name. Below the header is a navigation menu with tabs for BASIC, ADVANCED, TOOLS (selected), STATUS, and HELP. On the left, a sidebar menu lists TOOLS, ADMIN, SYSTEM, and FIRMWARE. The main content area is titled 'FIRMWARE' and contains three sections: 'FIRMWARE Upgrade' with a description and 'Save Settings'/'Don't Save Settings' buttons; 'FIRMWARE INFORMATION' showing 'Current Firmware Version : 1.0.1.6' and 'Current Firmware Date : 24 May 2007'; and 'FIRMWARE UPGRADE' with a note about factory defaults, instructions for wired connection, an 'Upload' field with a 'Browse...' button, and an 'Upload' button. The footer contains the copyright notice 'Copyright © 2004-2007 SMC, Inc.'

To upgrade the firmware, follow these steps:

1. Click the **Browse** button to locate the upgrade file on your computer.
2. Once you have found the file to be used, click the **Upload** button below to start the firmware upgrade process. This can take a minute or more.
3. Wait for the bridge to reboot. This can take another minute or more.
4. Confirm updated firmware revision on status page.

Firmware Information

Here are displayed the version numbers of the firmware currently installed in your bridge and the most recent upgrade that is available.

Firmware Upgrade

Note: Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the bridge by wire.

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the [Tools → System](#) screen.

Upload

Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the bridge.

Status

The Status tab provides the following configuration options: **Device Info, Wireless, Logs, Statistics, WISH Sessions**

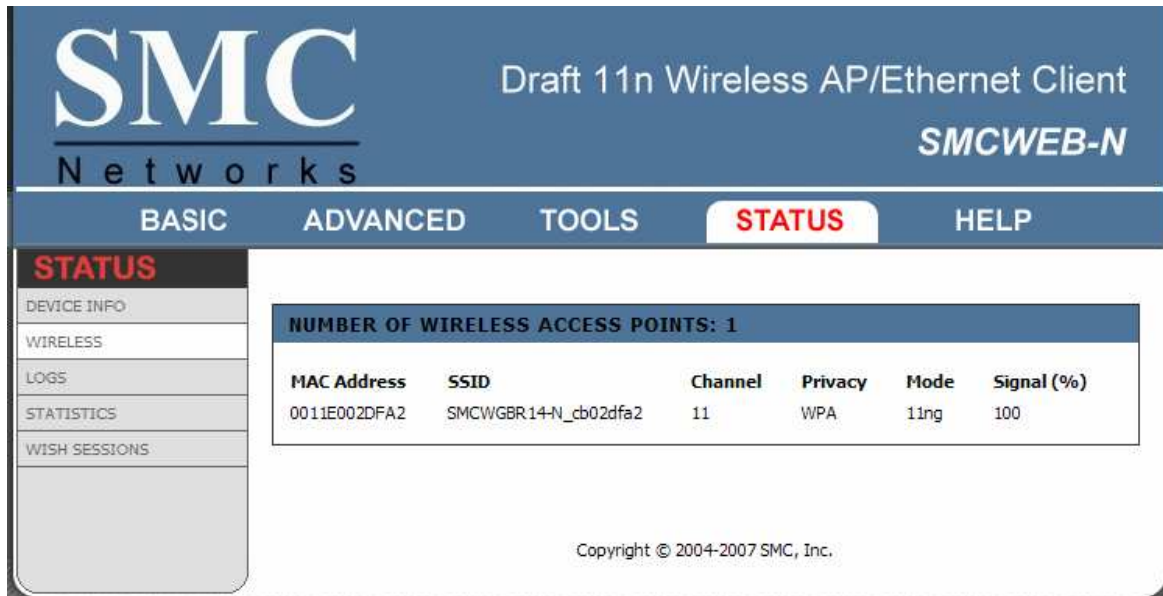
Status_Device Info

All of your network connection details are displayed on the Device Info page. The firmware version is also displayed here.

The screenshot displays the SMC Networks web interface for a Draft 11n Wireless AP/Ethernet Client (SMCWEB-N). The interface has a blue header with the SMC Networks logo and the device name. Below the header is a navigation menu with tabs for BASIC, ADVANCED, TOOLS, STATUS (selected), and HELP. On the left side, there is a sidebar menu with options: STATUS (selected), DEVICE INFO, WIRELESS, LOGS, STATISTICS, and WISH SESSIONS. The main content area is divided into three sections: DEVICE INFORMATION, GENERAL, LAN, and WIRELESS LAN. The DEVICE INFORMATION section contains a message: "All of your and network connection details are displayed on this page. The firmware version is also displayed here." The GENERAL section shows the Firmware Version as 1.0.1.6, dated 24 May 2007. The LAN section displays network details: MAC Address (00:11:E0:05:01:01), IP Address (192.168.2.2), Subnet Mask (255.255.255.0), and Default Gateway (192.168.2.1). The WIRELESS LAN section shows the Wireless Radio is Enabled, and provides details for the associated network: Status (Associated with SMCWGBR14-N_cb02dfa2), WISH (Active), MAC Address (00:11:E0:05:01:01), Network Name (SMCWGBR14-N_cb02dfa2), SSID, Channel (11), Wi-Fi Protected Setup (Configured), and Security Mode (WPA/WPA2 - Personal). The footer of the page contains the copyright notice: Copyright © 2004-2007 SMC, Inc.

Status_Wireless

The wireless section allows you to view all the access points that can be heard by your wireless bridge.



MAC Address

The Ethernet ID (MAC address) of the access point.

SSID

The network name that is used by this access point

Channel

The wireless channel that this access point is operating on.

Mode

The transmission standard being used by the access point. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.

Privacy

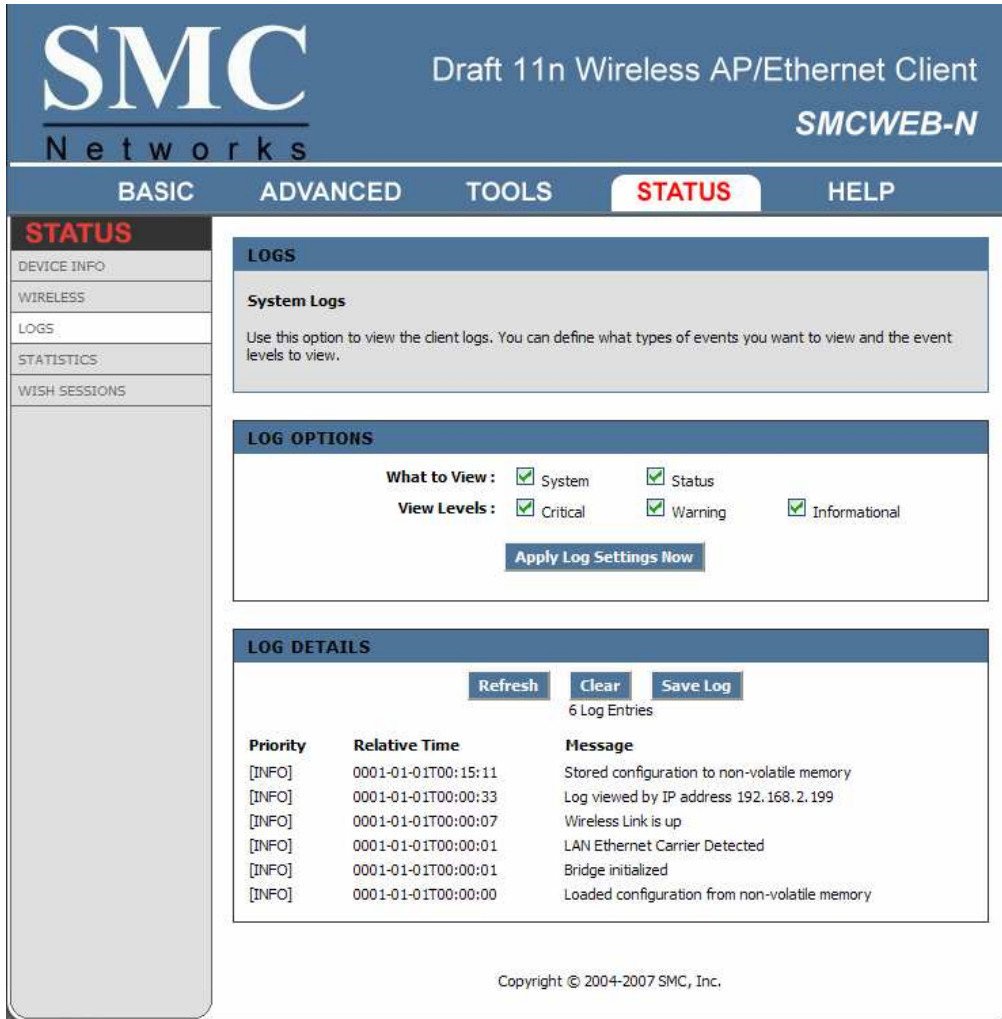
The wireless security mode of the access point.

Signal

This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the bridge and the access point.

Status_Logs

The bridge automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the bridge logs. You can define what types of events you want to view and the level of events to view. This bridge also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.



What to View

Select the kinds of events that you want to view.

- System
- Status

View Levels

Select the level of events that you want to view.

- Critical
- Warning
- Informational

Apply Log Settings Now

Click this button after changing Log Options to make them effective and permanent.

Refresh

Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear

Clicking this button erases all log entries.

Save Log

Select this option to save the bridge log to a file on your computer.

Status_Statistics

The Statistics page displays all of the LAN, and Wireless packet transmit and receive statistics.

The screenshot shows the SMC Networks web interface for a Draft 11n Wireless AP/Ethernet Client. The page is titled "STATUS" and is part of the "SMCWEB-N" interface. The navigation menu includes "BASIC", "ADVANCED", "TOOLS", "STATUS", and "HELP". The "STATUS" page is divided into three main sections: "TRAFFIC STATISTICS", "LAN STATISTICS", and "WIRELESS STATISTICS".

TRAFFIC STATISTICS

Network Traffic Stats

Traffic Statistics display Receive and Transmit packets passing through your client.

[Refresh Statistics](#) [Clear Statistics](#)

LAN STATISTICS

Sent :8800	Received :1946
TX Packets Dropped :0	RX Packets Dropped :0
Collisions :0	Errors :0

WIRELESS STATISTICS

Sent :1314	Received :7469
TX Packets Dropped :0	RX Packets Dropped :0
	Errors :150

Copyright © 2004-2007 SMC, Inc.

Sent

The number of packets sent from the router.

Received

The number of packets received by the router.

TX Packets Dropped

The number of packets that were dropped while being sent, due to errors, collisions, or router resource limitations.

RX Packets Dropped

The number of packets that were dropped while being received, due to errors, collisions, or router resource limitations.

Collisions

The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).

Errors

The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.

Status_WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your bridge when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

The screenshot shows the SMC Networks SMCWEB-N interface. The top navigation bar includes 'BASIC', 'ADVANCED', 'TOOLS', 'STATUS' (highlighted), and 'HELP'. A left sidebar contains 'STATUS' (highlighted), 'DEVICE INFO', 'WIRELESS', 'LOGS', 'STATISTICS', and 'WISH SESSIONS'. The main content area is titled 'WISH SESSIONS' and contains a descriptive paragraph and a table of active sessions.

WISH SESSIONS

The WISH Sessions page displays full details of active local wireless sessions through your client when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

Originator	Target	Protocol	State	Priority	Time Out
192.168.2.199:36798	62.153.213.28:30991	UDP	-	BE	289
192.168.2.199:36798	84.110.214.248:2369	UDP	-	BE	282
192.168.2.199:36798	84.57.177.178:30601	UDP	-	BE	275
192.168.2.199:36798	80.5.75.128:1884	UDP	-	BE	257
192.168.2.199:36798	74.102.44.43:22509	UDP	-	BE	257
192.168.2.199:36798	71.57.5.214:11151	UDP	-	BE	245
192.168.2.199:36798	84.109.22.66:3335	UDP	-	BE	238
192.168.2.199:36798	80.221.251.203:19030	UDP	-	BE	226
192.168.2.199:36798	84.196.34.254:35004	UDP	-	BE	219
192.168.2.199:36798	213.167.109.66:9110	UDP	-	BE	211
192.168.2.199:36798	212.158.147.169:4706	UDP	-	BE	204
192.168.2.199:36798	90.157.163.172:50949	UDP	-	BE	199
192.168.2.199:36798	85.228.172.153:29577	UDP	-	BE	181
192.168.2.199:36798	195.24.93.248:61292	UDP	-	BE	168
192.168.2.199:36798	84.234.22.68:61342	UDP	-	BE	187
192.168.2.199:36798	68.4.221.44:24026	UDP	-	BE	156
192.168.2.199:36798	216.15.36.57:41929	UDP	-	BE	150
192.168.2.199:36798	69.138.237.44:26879	UDP	-	BE	144
192.168.2.199:36798	80.62.108.138:21789	UDP	-	BE	144
192.168.2.199:36798	70.83.82.254:25149	UDP	-	BE	138
192.168.2.199:1025	192.168.70.1:161	UDP	-	BE	149
192.168.2.199:1025	192.168.2.1:161	UDP	-	BE	130
192.168.2.199:1025	192.168.10.1:161	UDP	-	BE	130
192.168.2.199:36798	172.215.149.57:1520	UDP	-	BE	125
192.168.2.199:56159	192.168.2.1:4444	TCP	TW	BE	57

Originator

The IP address and, where appropriate, port number of the computer that originated a network connection.

Target

The IP address and, where appropriate, port number of the computer to which a network connection has been made.

Protocol

The communications protocol used for the conversation.

State

State for sessions that use the TCP protocol.

- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- the server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Priority

The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Time Out

The number of seconds of idle time until the bridge considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

300 seconds

UDP connections.

240 seconds

Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

7800 seconds

Established or closing TCP connections.

Glossary

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B**Backward Compatible**

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C**Cable modem**

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 pin male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the same time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

K

Kbps

Kilobits per second

Kbyte

Kilobyte

L

L2TP

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

M

MAC address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q**QoS**

Quality of Service

R**RADIUS**

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload its operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend its coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S**Server**

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T**TCP**

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between your computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W

Wake on LAN

Allows you to power up a computer through its Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location