WI4NET

FlexiRadio FR100 Users Guide

WI4NET

FlexiRadio Users Guide

Revision History

Revision	Desrription	Date
1.1	Initial release	June 07

1835 Alexander Bell Drive• Suite 200
Phone 703.259.4047 • Fax 703.476.8964

Table of Contents

Conditions Of Use:

This manual is intended for information provided by CelPlan Technologies Inc or authorized parties. Please read this entire document, including the Regulatory Statements section before attempting to install or operate the module.
Warning: Any use of FR100 Module any manner which is not expressly specified within this manual or specifically approved by CelPlan Technologies Inc or its authorized agents will void the user's right to operate this module, and is expressly forbidden by CelPlan Technologies Inc. This includes any modification of the module, installation of the module in a configuration or used with an antenna which is not expressly listed in this document or approved by CelPlan Technologies Inc.

Notice to OEM Integrators:

This device is intended only for installation by authorized personnel under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users. For laptop installations, the antenna must be installed to ensure that the proper spacing is maintained in the event the users places the device in their lap during use (i.e. positioning of antennas must be placed in the upper portion of the LCD panel only to ensure 20 cm will be maintained if the user places the device in their lap for use) and

2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as the 2 conditions above are met, further transmitter testing will not be required. However, the authorized agents/OEM integrators are responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

Important Note: FCC approval is contingent on proper radio configuration for proper end-use operation as follows:

Radios that have the UNI 5.2GHz band enabled shall only be installed in indoor enclosures. Outdoor operation in the 5.2GHz UNII band is strictly prohibited.

The user's manual for the end user **must** contain the following statement, 'Use of this device in the 5.15-5.25GHz range is restricted to indoor use only.'

Important Note

In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

Note

The end user should NOT be provided any instructions on how to remove or install the device

RF Exposure Information Notice:

Important Note

To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Regulatory Notice – FCC Class B 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 or more of the following measures:

- Reorient or relocate the receiving antenna;
- Increase the separation between the equipment and the 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 technician for help.

Labeling:

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ASDL modems, certain laptop configurations, and similar equipment). One or more labels are applied to the final assembly during manufacture, including a label which identifies the FCC identification numbers as follows:

Contains FCC ID: TFF-FR-100.

Do not attempt to remove any labels from the module.

FCC Output Power Restrictions

License-free operation in the industrial, scientific, and medical band is documented in FCC Rules Part 15.247. This radio is approved for license-free operation in the 2.4 and 5.8GHz bands. It is the responsibility of the individuals designing and implementing the radio system to ensure compliance with any pertinent FCC Rules and Regulations.

Installation Instructions

This device must be professionally installed. The FCC specifies the maximum transmitter power used for antennae of a given gain. FCC Rules Part 15, Subpart 247 allow for a maximum power of 1 watt (30 dBm) into antennae of a gain less than or equal to 6 dBi..

1

Equipment Description

FlexiRadio is a professional radio conceived and primarily designed for public safety and homeland security networks. Commercial applications, however, can also benefit from the advanced concepts introduced in this equipment.

FlexiRadio provides professional outdoor equipment for wireless broadband networks (up to 108 Mbps). Operating in the licensed and unlicensed bands, the radio is engineered to make optimal use of the available spectrum, providing unparalleled data throughput, while respecting FCC regulations. The equipment allows the configuration of fixed and mobile networks using the cellular concept. Its flexible configuration minimizes installation requirements and provides different possibilities of network architecture.

An Introduction to FlexiRadio

The FlexiRadio software is 802.11a compatible and provides specific features to support different applications.

All Wi4Net radios are compatible to commercially available off-the-shelf 802.11 PC cards; however, specific applications, such as public safety networks, require special features, due to the additional security required, that do not allow the use of regular devices.

The FlexiRadio design addresses wireless broadband issues by providing unequaled range of operating frequencies and reliability, while complying with FCC maximum limits for professional installation.

OFDM is the technology of choice because it provides multipath interference (fast fading) protection for high data rates. The equipment also adopts a modular approach, hence the flexibility implied on its name. This modular approach allows easier maintenance, replacement and upgrade possibilities, even permitting any of its parts to be supplied by different vendors.

FlexiRadio Enclosures

FlexiRadio can be configured using up to four enclosures: radio, antenna, power, and RF head.

Energy Enclosure

The energy enclosure implements an un-interruptible power supply, using and AC rectifier/charger and a battery. It can be configured for different periods of autonomy time. Because it is a separate enclosure, designers have the flexibility of choosing the most effective dimensioning for their application.

The use of this enclosure is optional because the radio enclosure may also be directly connected to an external power supply.

Radio Enclosure

The radio enclosure holds the processor and up to two radios. In case the UPS is not used, it can be equipped with an AC/DC power supply (ACPS), and a coaxial power injector. Processor control signals can also be injected on the coaxial cable. Two RF heads can optionally be mounted in this enclosure.

The environmentally sealed radio enclosure has a low thermal resistance to the environment, minimizing the difference between internal and external temperatures. The installation fixture provides a sunshade that further enhances the enclosure's capabilities.

It can be mounted separately from the RF heads where additional environmental shielding can be provided, increasing the network reliability even more. Optionally, RF heads can be mounted inside this enclosure to make better use of space and heat extraction capabilities. The enclosure is made of aluminum and all parts get a chromate conversion coating to guarantee conductivity.

The unit has an advanced processor board with a 5x6 CPU with 266 MHz, 64 MB of SDRAM and 256 MB of flash RAM. This CPU provides enough processing power for the foreseen applications and can also be easily upgraded if required.

The two Internet ports available allow interconnection of local IP equipment, such as cameras and sensors. The processor board has two plug-in interfaces (mini PCI) for radio boards. Radio upgrades consist of simply removing old radios and plugging-in the new ones. A remote software load is required to configure the new radios. WiMax is a good example of upgrade opportunity.

This enclosure supports access points (AP), stations (STA) and backhaul applications (BH), so the same box can be used for all applications. The following chapter describes some of the possible configurations for each of these elements.

RF Head Enclosure

The RF Head Enclosure holds up to four RF Heads (one per antenna), the power and control signal extractor, and a DC/DC power supply (DCPS). It also allows the addition of remotely controlled cameras and a variety of sensors (radioactive, chemical or environmental). These sensors are connected to the Ethernet port of the processor and can be accessed through backhaul links, thus not loading local wireless cells.

The RF head module provides TX and RX diversity and offers a higher output power and a less noisy input receiver. This significantly increases link throughput and range.

The installation of the RF head at the antenna greatly reduces the cable loss even when thin coaxial cables are used. Each module can be turned on or off by a remote command from the processor. The DC power and the command signals are injected on the coaxial cable at the radio enclosure and extracted at the RF Head, so no additional cabling is required.

The RF head enclosure is mounted directly below the antenna. The special mounting kit provided can be attached to vertical or horizontal poles. Surge arrestors (SP) can be mounted between the antenna and the RF Head electronics.

Antenna Enclosure

The antenna enclosure holds up to four 90° panels or one omni antenna. The omni antenna (O514) has 14-dBi of gain and covers the band from 4.9 GHz to 5.9 GHz. This antenna has a fill-in lobe that provides coverage in areas close to the antenna.

Each directional antenna (P520) has 20-dBi of gain and also covers the band from 4.9 GHz to 5.9 GHz. The panels are oriented at 90° angles but the whole set can be rotated to adjust the group azimuth. A fine adjustment can also be performed for each panel.

Spatial diversity is extremely important when working when working at high frequencies (e.g. 5 GHz). The 802.11 standard uses TDD, what makes the provision of diversity a complex task; thus most vendors do not support this feature. FlexiRadio supports both, TX and RX, diversity. By mounting the RF heads to each antenna, FlexiRadio allows the antennas to be up to 30 meters apart without performance degradation, that is, diversity antennas could even be mounted on opposite sides of the street.

FlexiRadio Models

The FlexiRadio is available in three different models: FR500, FR1000, and FR 500. All of them are available in multiple channel bandwidths (1, 5, 10, and 20 MHz) and cover the 4.9 to 5.9 GHz bands. FR1000 also covers the ISM band (2,400 to 2,484 MHz).

The FR500 offers a lower throughput and is ideal for small networks, due to the size restriction of its cells. FR1000 and FR 500 are designed for larger networks and offer higher throughput and larger coverage areas. The next chapters present the technical specification and possible configuration of each of the radios.

The following table presents the main characteristics of the FlexiRadio family. The over-the-air data throughput can be as high as 108 Mbps for a 20 MHz bandwidth.

General Characteristics

The radio is configured to use a specific band via software. Within a band, this software selects the best available channel or follows a master frequency plan. The channel bandwidth can also be selected via software (5, 10, 15, 20, and 40 MHz). The software supports extended range technology, allowing the reception of data up to 256 kbps, significantly increasing the range of the network.

> **Note**
>
> The radio firmware is factory programmed to limit the transmission power to regulatory power limits and to keep the performance compliant with masks. The user has no control to change the power settings.

The actual transmitted power is automatically adjusted to comply with the desired data rate, minimizing interference. The antennas should be installed by a professional and should comply with the maximum regulatory radiation limits. Receive diversity is available in all radios. Some models also offer transmit diversity. An additional 3 dB output power gain is obtained for models FR 500 and FR2000 due to the antenna diversity configuration.

Network Architecture

FlexiRadio can be installed on poles, traffic lights, building walls, or bridges. Because of its multi-radio capability, FlexiRadio allows flexible configurations to best suit each application, considering spectrum availability and throughput requirements. The network architecture is also flexible and can be implemented with several levels of hierarchy.

Single Level Hierarchical Network

This is the typical ad-hoc configuration. The best channel available is chosen for each connection.

FIGURE 1 SINGLE LEVEL HIERARCHICAL NETWORK

Two-Level Hierarchical Network

In this networks, multiple stations connect to a RAN with cabled backhaul access. The same channel is used at each RAN.

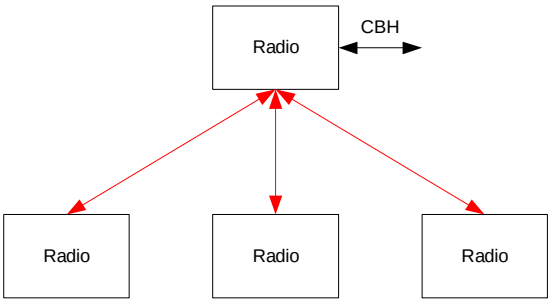

FIGURE 2 TWO-LEVEL HIERARCHICAL NETWORK

Three-Level Hierarchical Network

In a three-level hierarchical network, a separate layer is used for backhaul. This setup requires more available channels than the networks with less hierarchical levels.

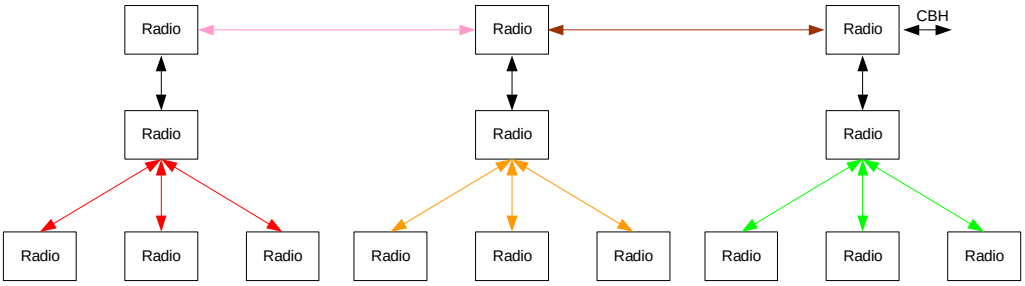

FIGURE 3 THREE-LEVEL HIERARCHICAL NETWORK

Cross-Level Hierarchical Network

This configuration avoids the need of separate channels for the backhaul.

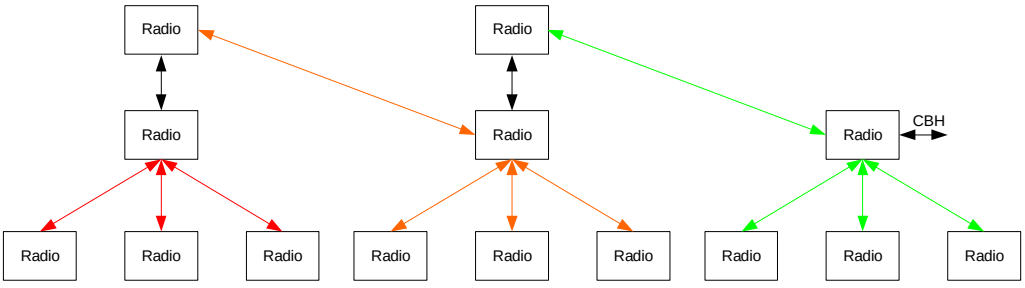

FIGURE 4 CROSS-LEVEL HIERARCHICAL NETWORK

Combined Hierarchical Network

The following figure illustrates the multiple configurations that can co-exist within a single network.

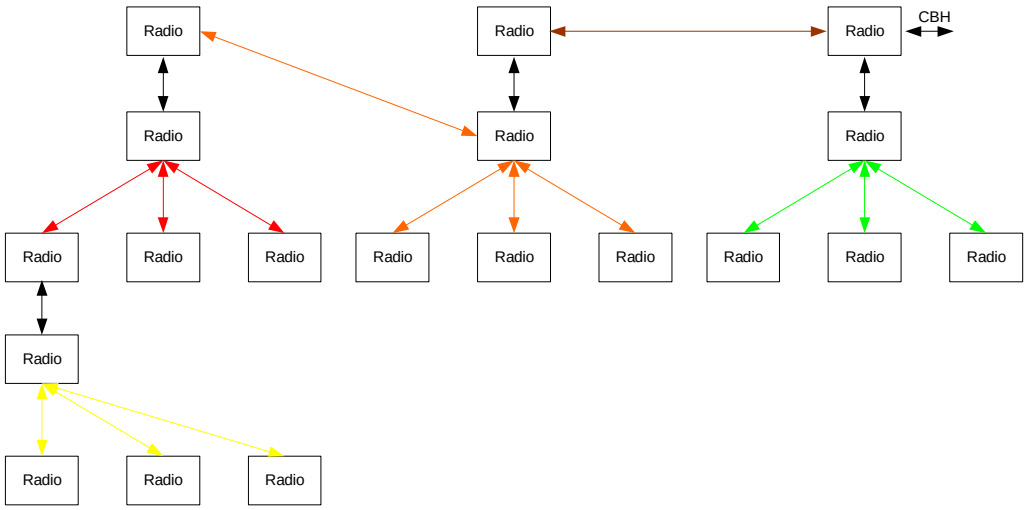

FIGURE 5 COMBINED HIERARCHICAL NETWORK

An example of such a network is a PAN (Personal Area Network), in which a network is established around a vehicle, for example, for the personnel around it to be able to use their personal devices to access the network. This network may use a particular band such as ISM. The vehicle than connects to the best server RAN, but, at the same time, a shadow radio registers with the second best server, thus the connection can be kept if the vehicle moves from one cell to the other. The backhaul of this example could be done using cross-level or separate levels hierarchical connections.

2

Software Structure

The software to program FlexiRadios is fully structured and uses proven modules to provide the required functionalities

The security layer implements state of the art security functions. The grid management layer allows many different network configurations. This software fully supports IP based applications, allowing the deployment of video, video conferencing, VoIP, ftp, web, and other IP based services. Broadcasting and multicasting are also possible.

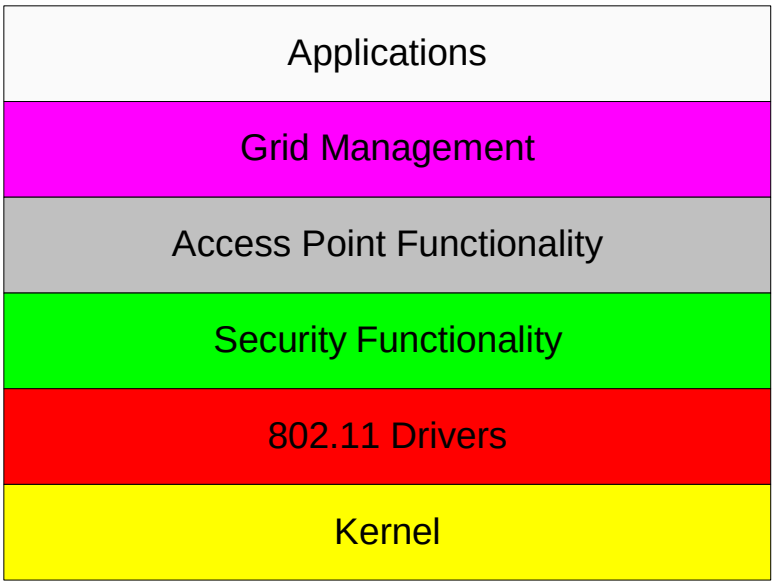

FIGURE 6 SOFTWARE STRUCTURAL LAYERS

Users can configure FlexiRadio through a serial port or a web interface, which can be cabled of wireless. A powerful command line interface is also available through telnet.

Access Point Web Server

The web server is located in the AP and can be accessed from any station connected to this AP's network. The web server configuration windows provide a user-friendly interface to aid users in setting up the AP.

Users must press the Update button to save any changes made to the configuration. The AP must be rebooted to apply the changes. The web server looses connectivity as the AP reboots. Users can restore that connection one the AP has completed rrebooting.

There are four groups of pages to be configured: script, firmware, configuration, and statistics. The configuration pages are subdivided into system and radio (2.4 and 5.0 GHz). The following sections describe how to access the web server and configure each of these pages.

The following steps describe how to configure the AP through the web. For the web server configuration pages to work properly, the web browser must support frames and have Java scripts enabled.

Accessing the Web Server

To access the web server from the host PC, open a web browser, such as Internet Explorer, and type in the IP address assigned to the desired AP, such as, http://192.168.1.20/index.htm. The Access Point Web Server homepage is displayed.

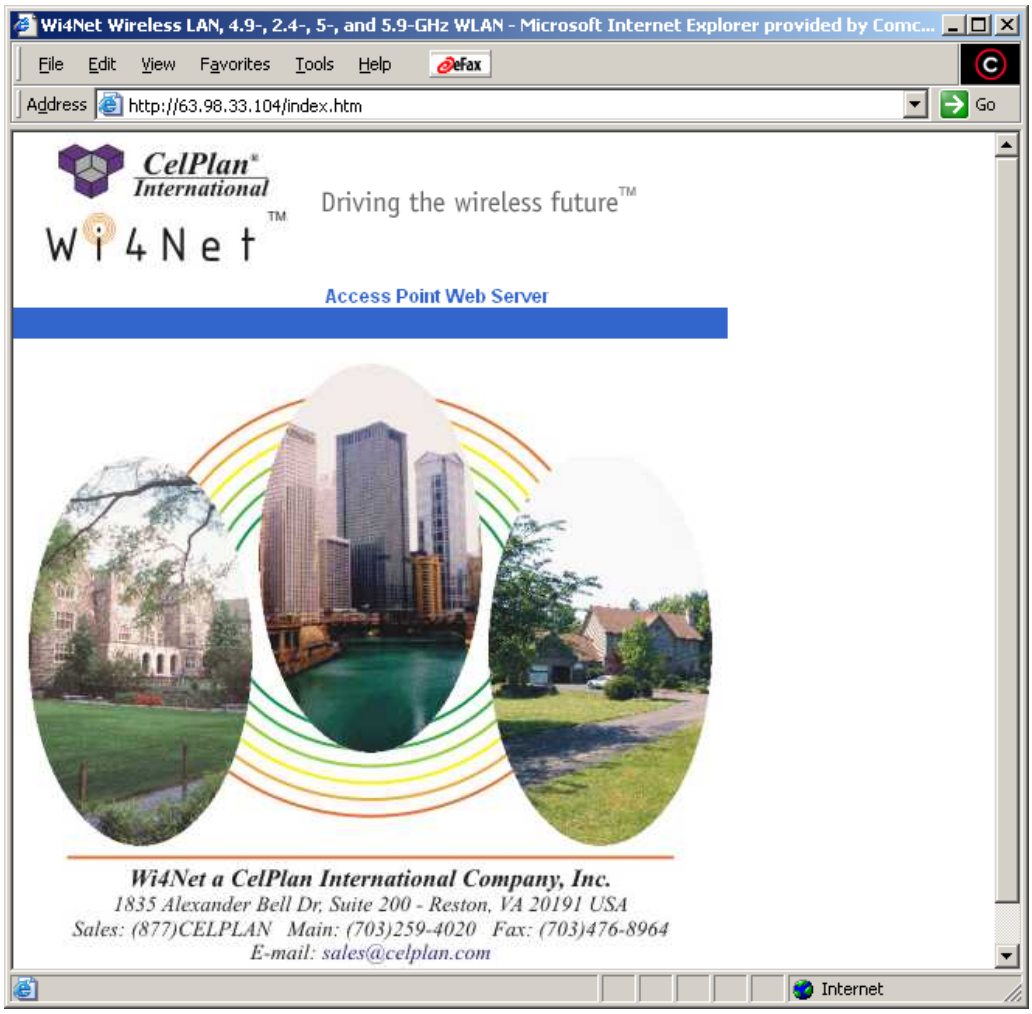

FIGURE 7 AP WEB SERVER HOMEPAGE

To access the configuration pages users must click on the picture and then fill in the information requested to obtain login authorization. Both user name and password are case sensitive. The following information can be used for login:

- User Name: **Admin**
- Password: **5up**

FIGURE 8 LOGIN INFORMATION

When users click OK, the Top-level AP Statistics window is displayed (Figure 9).

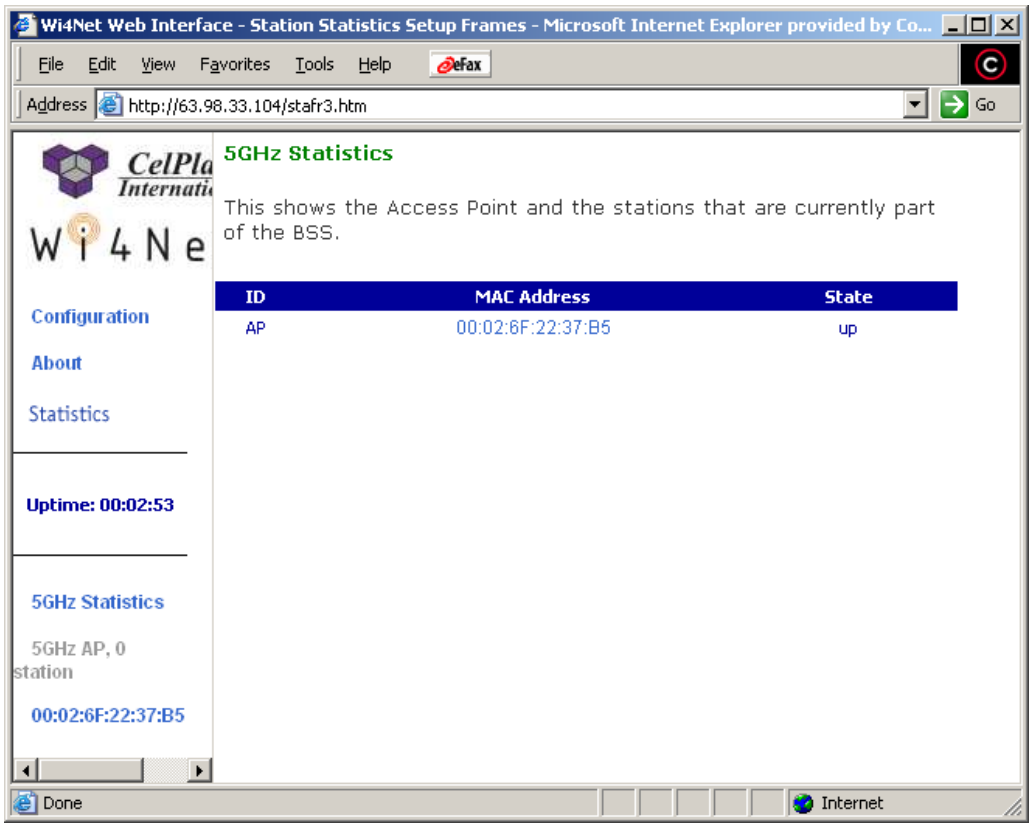

FIGURE 9 TOP-LEVEL STATISTICS WINDOW

Configuration Pages

The left panel of the web server pages contains links for the main configuration windows. Auxiliary configuration windows can be accessed through these main pages. The link for the configuration pages is at the left panel of all AP web server pages.

There are two main types of configuration pages: system and radio. This document starts by describing the system configuration. Users can switch between system and radio configuration using the links under Setup on the left panel. The system configuration page allows users to define the general operating settings for the access point.

System Configuration Page

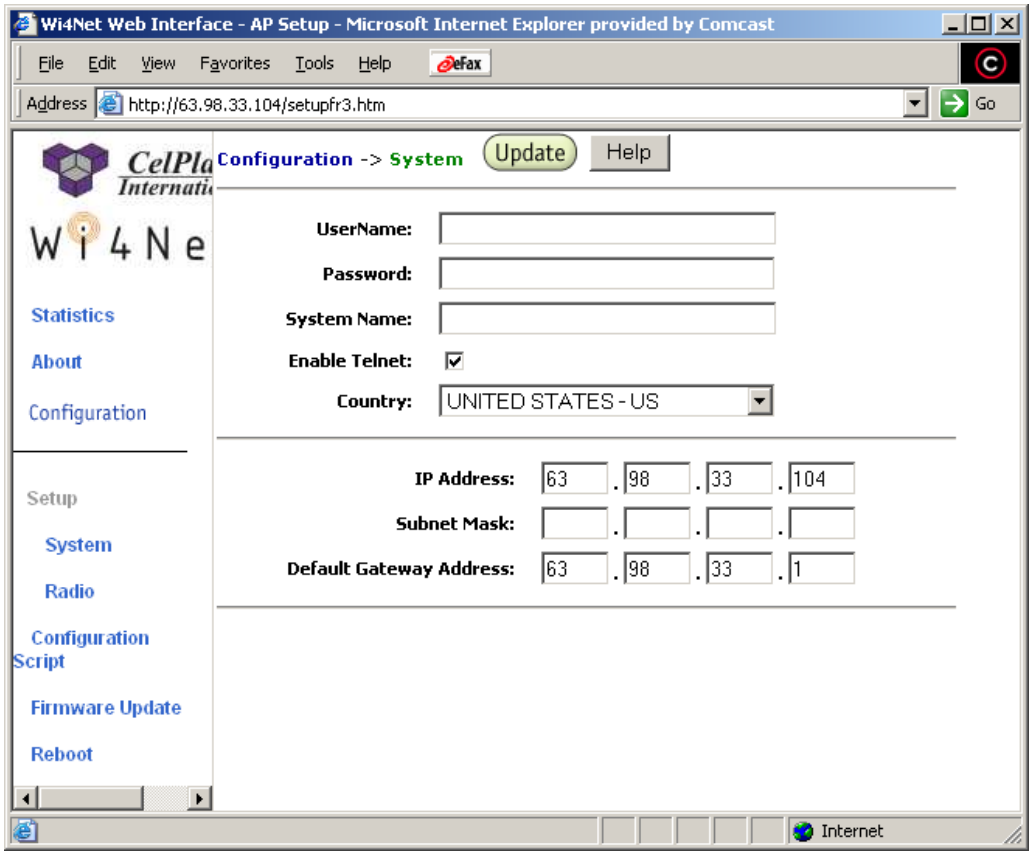

FIGURE 10 SYSTEM CONFIGURATION PAGE

In this window, users must type in the user name and password and specify a unique name for the AP (system name - up to 32 characters in length). Users select the country where the AP is operating through the drop-down list.

Users must also configure the IP Address, Subnet Mask and Default Gateway Address for the AP. To use command lines through telnet, users must select the "Enable Telnet" check box.

After configuring the system page, users must define the radio parameters. The link to access this screen (Radio) is located at the left panel, under Setup.

Radio Initial Setup Page

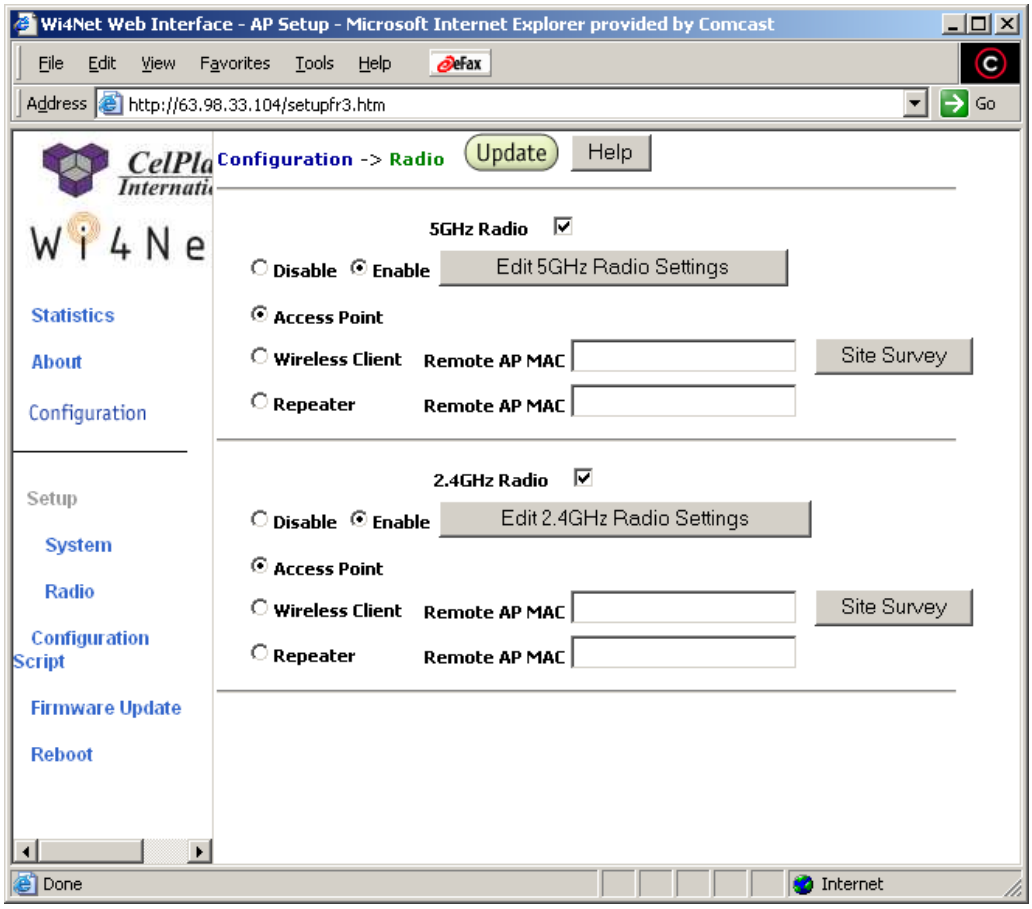

FIGURE 11 RADIO INITIAL SETUP

This window allows users to configure the 5 GHz and/or 2.4 GHz radios. The check boxes on the top of each section determine whether a radio is operational or not. Radios can be disabled/enabled at any time through this screen.

Users must also select which operation mode the radio is operating in: Access Point, Wireless Client, or Repeater. If operating as a wireless client, users must also fill in the remote AP MAC address. Radios in this mode provide wireless access for devices to a remote AP. STAs cannot associate to radios in this mode.

If the radio is operating as a repeater, users must also fill in the Remote AP MAC address. Wireless repeaters relay signals between STAs and an AP. An AP in repeater mode scans for a root AP and, once associated, acts like a point-to-point bridge between clients associated to the repeater and the root AP.

The Site Survey button triggers a 5GHz or 2.4 GHz site survey, displaying a list of every AP available.

Users can edit radio configuration through the Edit Radio Settings buttons. A Radio Configuration window is displayed allowing users to start editing radio settings. Several other configuration windows, such as security and WAP settings, can be accessed through this main window.

All configuration windows are the same for both types of radio; the advanced configuration window, however, presents additional fields for 2.4 GHz radios. Each of these windows is described next.

Radio Settings Page

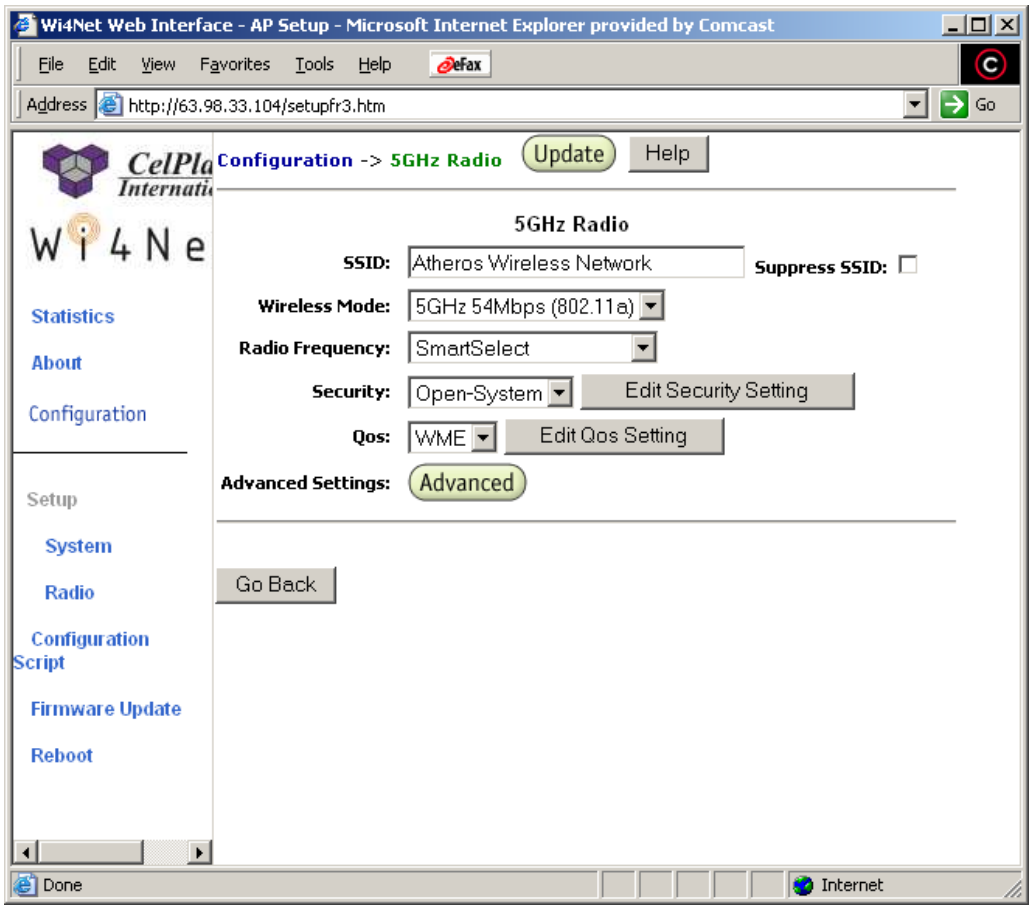

FIGURE 12 RADIO SETTINGS PAGE

The radio configuration window allows users to set generic radio operating information for the AP. In this window, the SSID represents the identification of the AP. This could be a number or address, between 1 and 32 characters in length, that the STAs associate with in infrastructure mode. This SSID can be used for more than one AP, therefore, users must use the System Name field (System Configuration dialog box) to uniquely identify the each AP. When operating as a wireless client or repeater, the SSID identifies the remote AP to which the device is associated.

The Suppress SSID check box prevents the broadcast of the AP's SSID in beacons; when enabled, only the STAs with previous knowledge of an AP's SSID can associate to that AP.

In the wireless mode drop-down list, users must select the frequency range and data rate for operation. The Radio Frequency allows the selection of the desired operation frequency. The frequencies on the drop-down list depend on the wireless mode selected. The option "Smart Select" automatically searches through the frequency list to find a valid and less congested channel.

The Security drop-down list allows users to choose between open-system, WPA-only, WPA2-only, and WPA2-auto. WPA (Wired Protection Access) modes have a special page for configuring security settings. The WPA security configuration page (Figure 16) can be accessed by pressing the Edit Security Settings button. If WPA is not used, the button shows the general security settings page (Figure 17).

Users can also select determine whether QoS (Quality of Service) is not defined (none) or is WME (Wireless Media Extension). The Edit QoS Setting button allows users to provide detailed QoS configuration (Figure 13).

The Advanced Settings button displays a window for more detailed operating configuration.

QoS Configuration Page

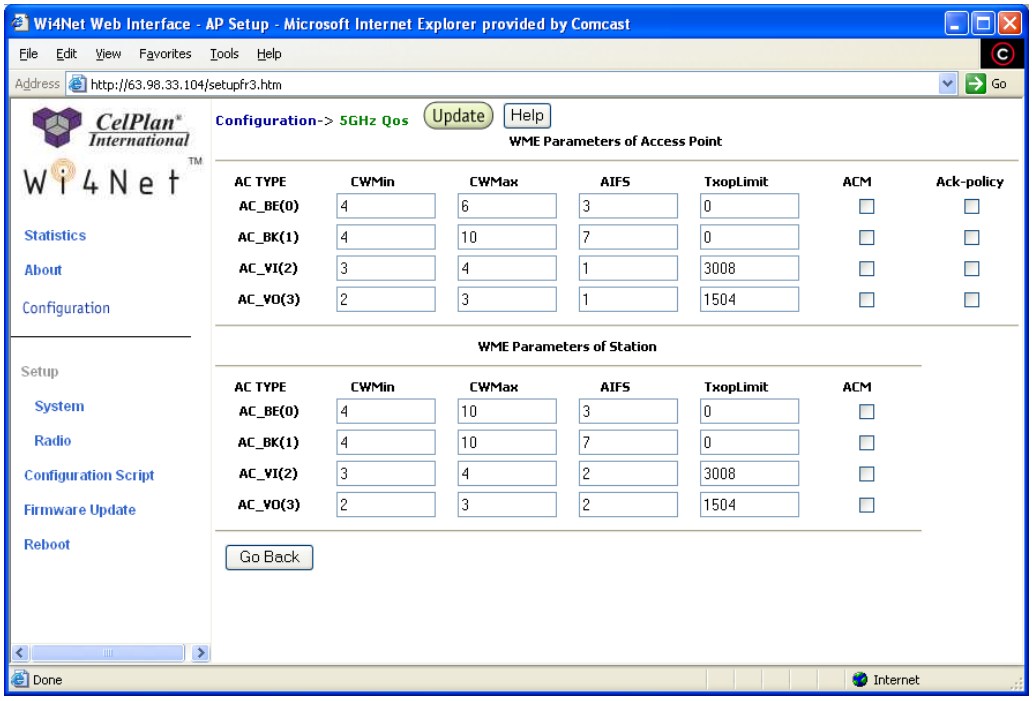

FIGURE 13 QOS CONFIGURATION PAGE

Advanced Radio Settings Page

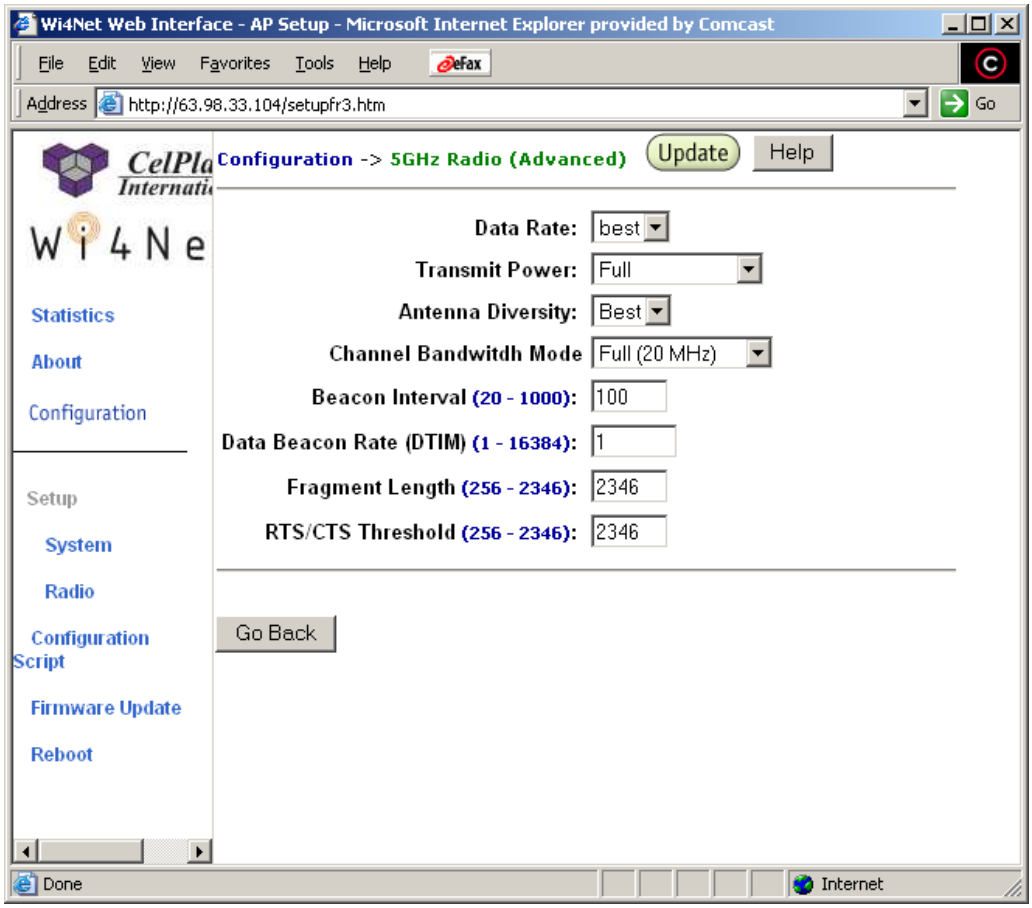

FIGURE 14 ADVANCED RADIO SETTINGS PAGE

In the advanced settings page, users must select the data transmission rate from the drop-down list. The option "best" adapts the rate to the best available.

The transmit power level is also selected from a drop-down list. Users should decrease the power if more than one AP is co-located and operating in the same frequency channel.

For antenna diversity, users can choose to use antenna 1, antenna 2, or the best available.

Users can defined the channel bandwidth mode as quarter (5 MHz), half (10 MHz), or full (20 MHz).

The Beacon Interval is defined between 20 and 1000, whereas the data beacon rate, which specifies the delivery traffic indication message (DTIM), is limited between 1 and 16384.

The Fragment Length and RTS/CTS Threshold are both limited between 256 and 2346.

This page presents additional parameters when configuring 2.4 GHz radios (Figure 15).

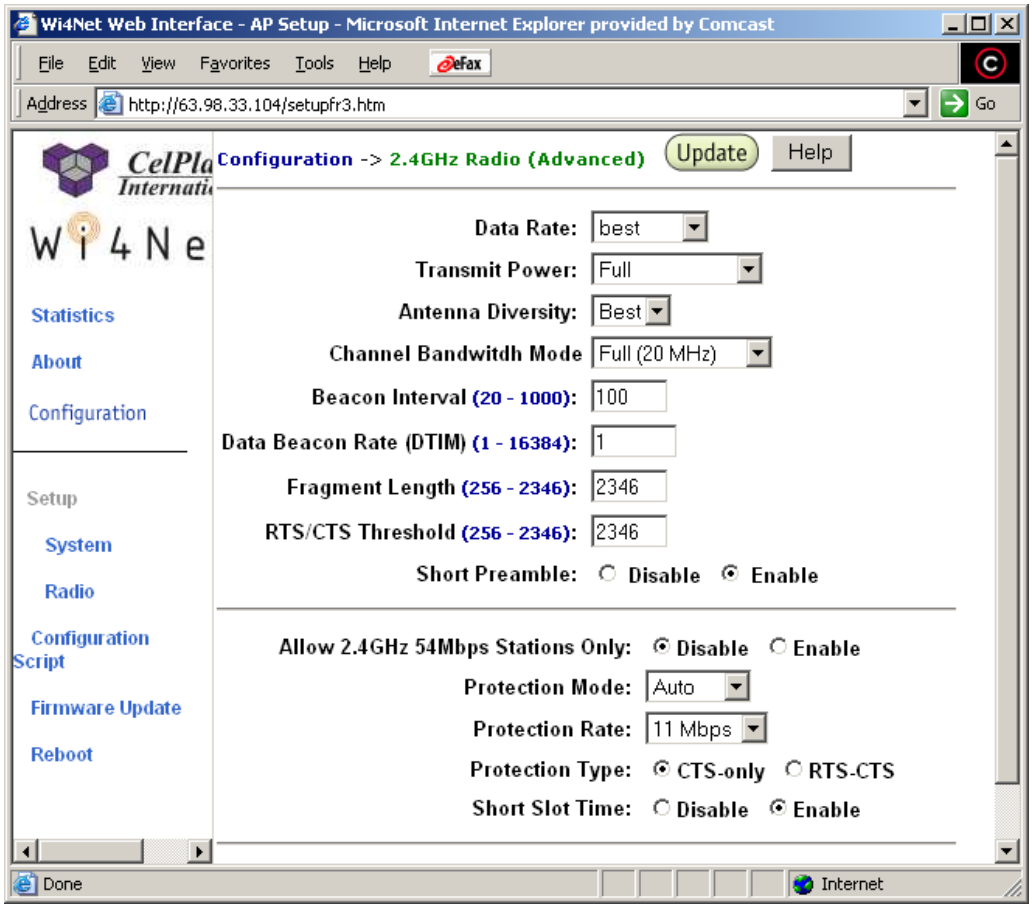

FIGURE 15 ADVANCED RADIO SETTINGS PAGE – 2.4 GHZ RADIO

Radio buttons allow users to specify the short preamble (11b) usage. When enabled, both short and long preambles are used. When disabled, only long preambles are used.

Users can also disable or enable the association of 2.4 GHz 54 Mbps STAs only.

The protection mode drop-down list allows defining the CTS protection mode as never on (none), always on, or automatic. Users can set the CTS protection rate to 1,2, 5.5, or 11 Mbps. The protection type can be CTS only or RTS-CTS.

Radio buttons also allows users to enable or disable short slot time usage.

Security Settings

The WPA page only has to be configured when the WPA mode is enabled in the Radio Settings page (Figure 12). In this case, users can access the WPA Security Configuration page (Figure 16) through the Edit Security Settings button.

WPA Configuration Page

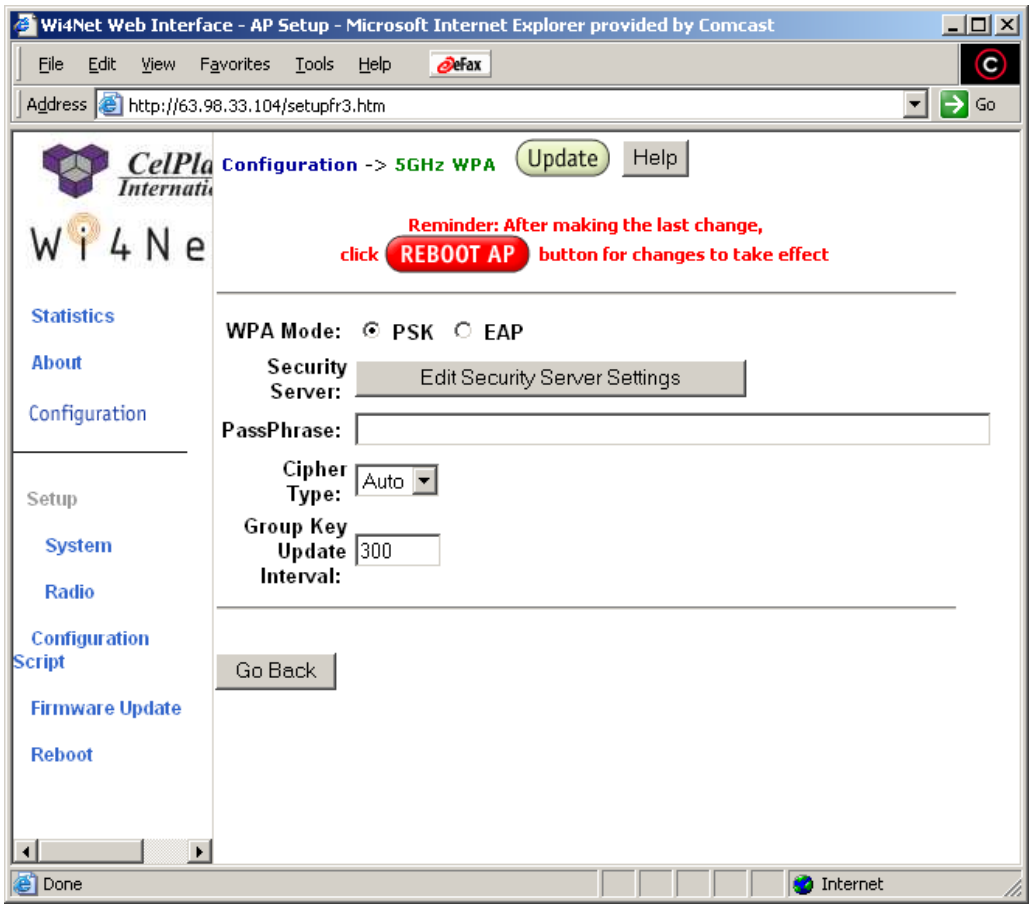

FIGURE 16 WPA CONFIGURATION PAGE

The radio button on top of the page allows users to specify either PSK (pre-shared key) or EAP (802.1x) mode. Choose EAP for WPA-TLS, or PSK for WPA-PSK authentication.

The PassPhrase field is a password phrase from 8 to 63 ASCII characters in length, or a hexadecimal phrase with exactly 64 characters. This phrase is only required if using WPA-PSK

If using WPA-TLS, after configuring this page, users must configure the RADIUS security server (Figure 18) by pressing the Edit Security Server Settings button.

The Cipher Type can be TKIP, AES, or Auto. The Group Key Update Interval is an internal value between 15 and 300 seconds. Users can also configure this value as 0, representing that it is disabled.

Security Settings Page

If WPA is not enabled, users must configure the general security settings page (Figure 17), which can be accessed through the Edit Security Settings button in the Radio Settings page (Figure 12). The radio buttons on top of the general security settings page allows users to configure the security mode: disabled, pre-shared key, or dynamic. The key entry method can be hexadecimal or ASCII text.

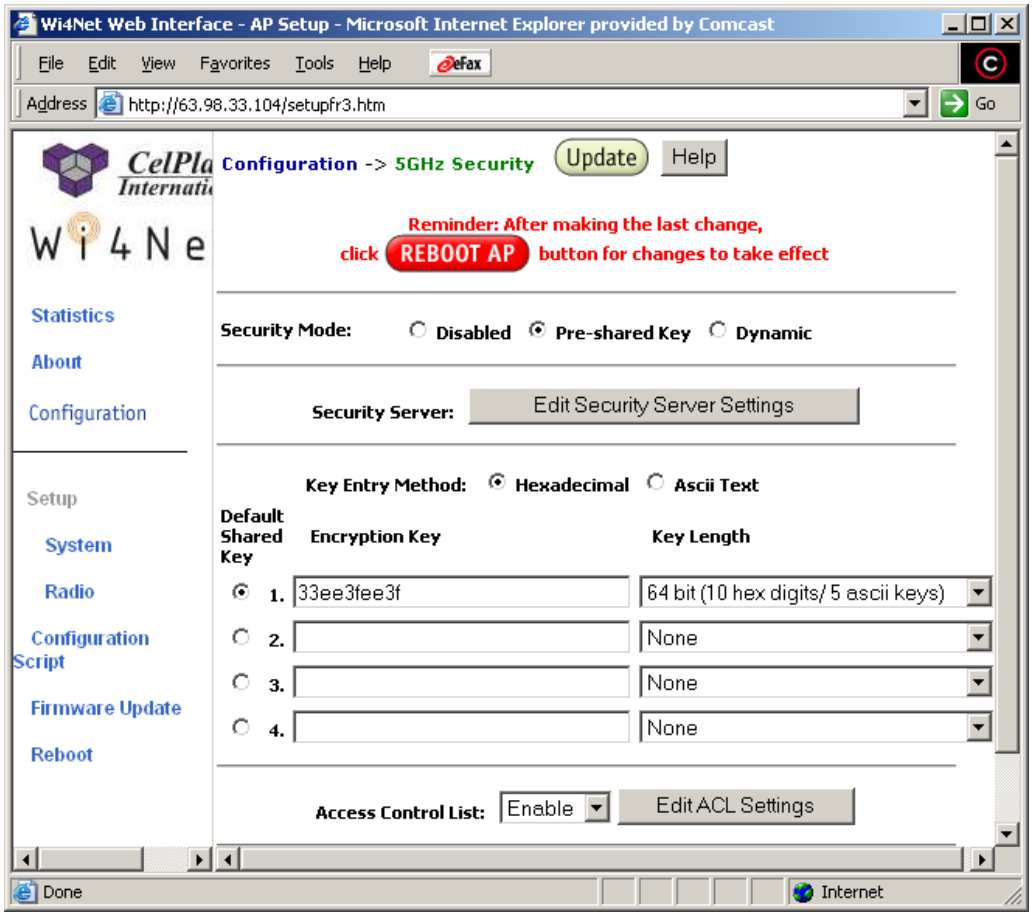

FIGURE 17 SECURITY SETTINGS PAGE

Users can configure up to four Encryption keys to be used for broadcast/multicast frames. The key length can be 10, 26, or 32 hexadecimal digits or, respectively, 5, 13, or 16 ASCII characters. Radio buttons allow users to pick the key to be used as default shared key.

Users can also specify the state of the Access Control List (ACL) using the drop-down menu. Three options are available: 1) disable, which offers unrestricted access. By default, while checking of whether the ACL is enabled, the access control list itself is empty. This is the same as disabling the checking on the ACL; 2) enable, which offers restricted access. An ACL entry must exist before ACL can be enabled. While ACL is enabled, stations with valid shared keys and stations with matching "allow" entries on the ACL are authenticated; 3) strict, which offers restricted access with ACL match. This mode requires an ACL entry that specifies the station's assigned unique key or the station is denied association. In the strict mode, stations with valid share keys and not on the ACL are not authenticated. The stations must have unique keys defined and matching "allow" ACL entries specified to associate to the AP.

RADIUS Security Server details (Figure 18) can be configured through the Edit Security Server Settings button.

RADIUS Security Server Configuration Page

The IEEE 802.1x protocol is designed to support port-based authentication and secure key distribution, as well as unique encryption keys distribution for an entire BSS. This system provides AP and STA support for this protocol.

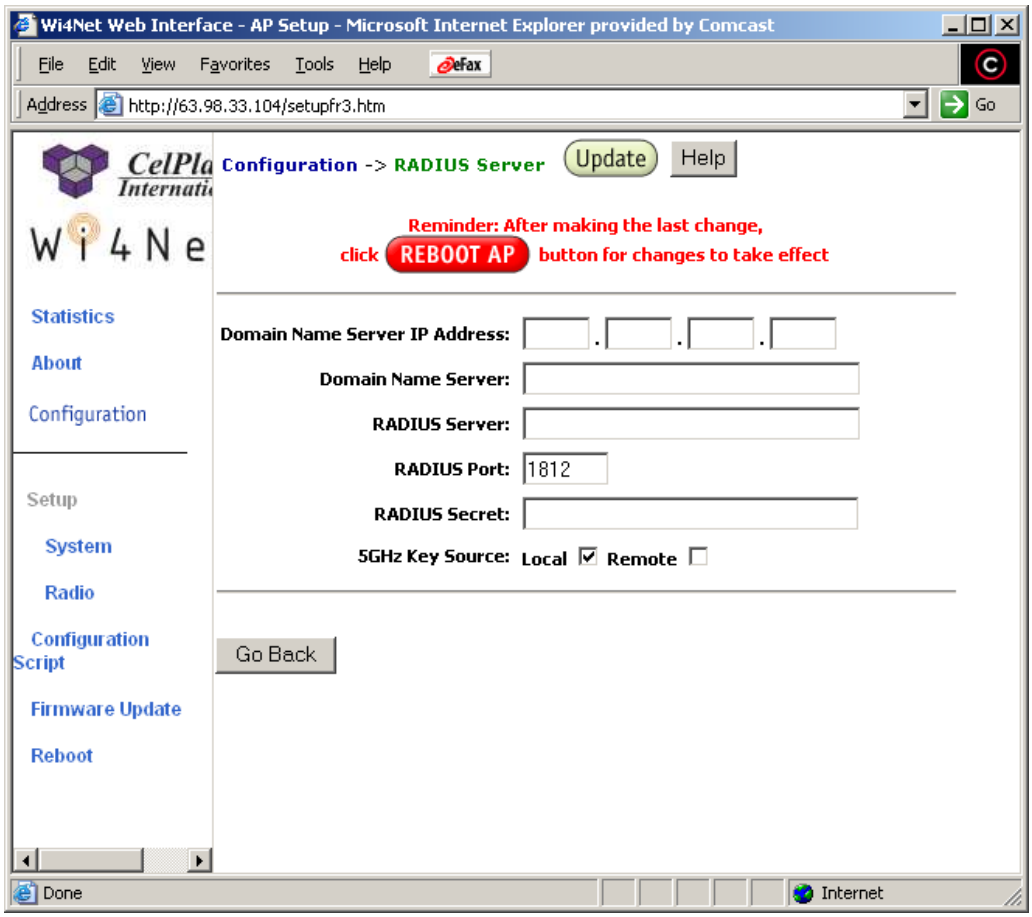

FIGURE 18 RADIUS SERVER SETTINGS PAGE

The RADIUS server security settings include the definition of the domain name server and its IP address. Users must also specify the RADIUS IP address, port and password (secret). The Key Source determines the location of the RADIUS keys: "local" indicates that the keys are in the AP; "remote", that they are in the RADIUS server. To enable 802.1x on the AP, users must configure this page and select the key source as remote.

ACL Configuration Pages

Users can access this configuration page (Figure 19) through the Edit ACL Settings button in the General Security Configuration page (Figure 17).

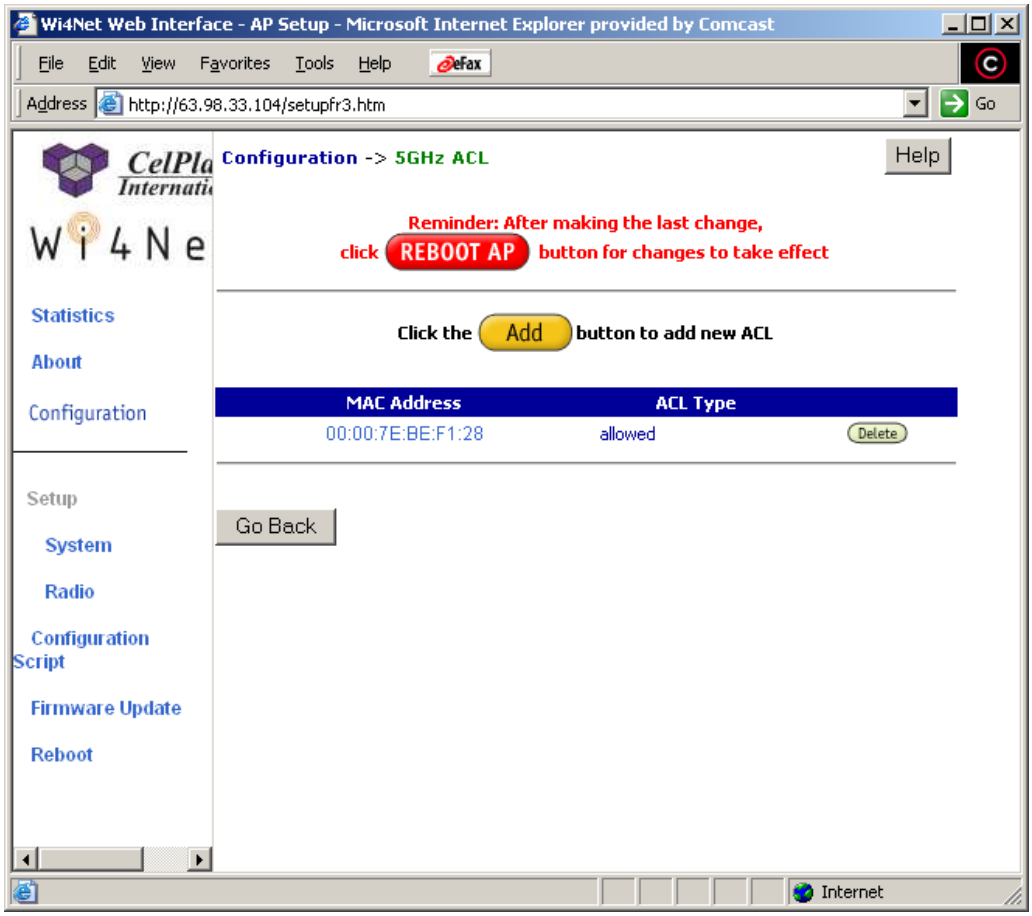

FIGURE 19 ACL CONFIGURATION PAGE

Users can add and remove ACLs from the list using the Add and Delete buttons respectively. The access control list (ACL) allows an administrator to perform security actions based on the client station MAC address. This selection allows or denies association with the AP and for unique, per station, WEP key assignment.

The Add button displays a new page (Figure 20) for configuring the ACL information. Users must specify three parameters for each ACL: the MAC address, the ACL type, and a unique key.

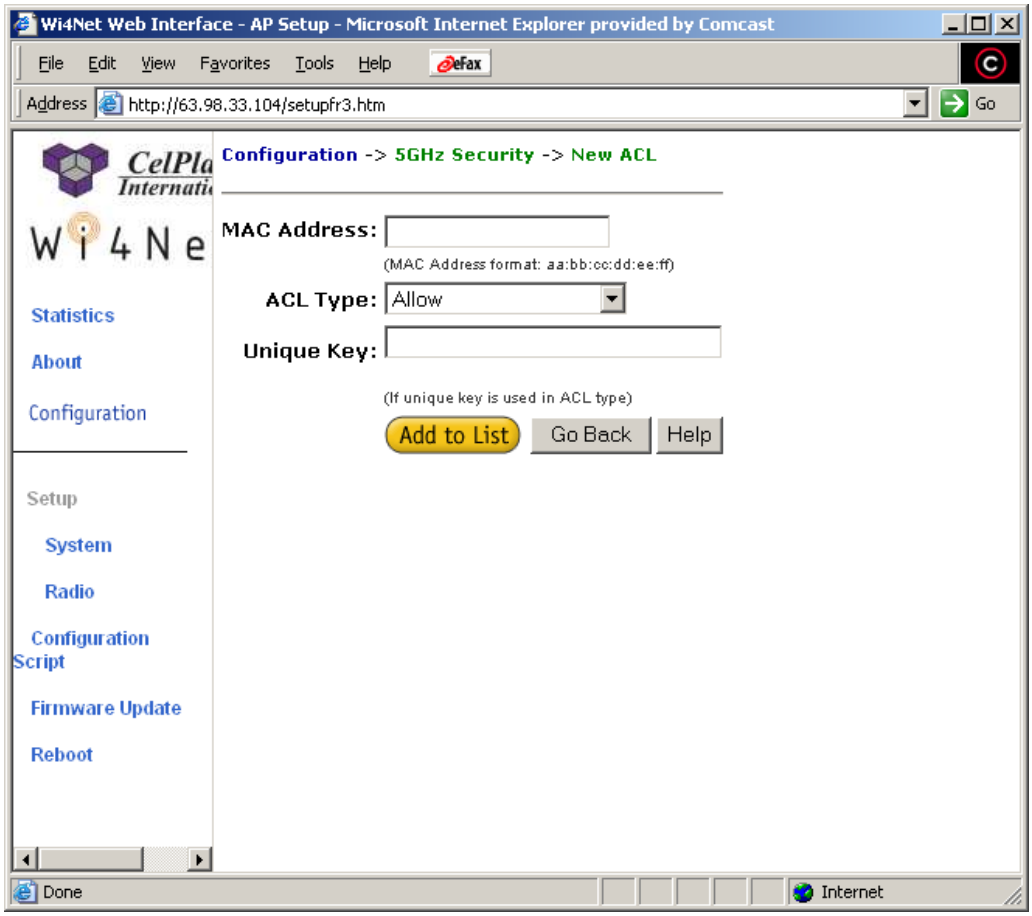

FIGURE 20 NEW ACL PAGE

The MAC address specifies the STA to be included in the ACL, whereas The ACL type specifies the current state of each STA:

- Allow – enables access for the MAC address to the ACL
- Deny – denies access for the MAC address to the ACL
- Default shared key – the MAC address uses the default shared key
- 64/128/256 bits – specifies lengths for shared keys

After configuring the ACL, users must press the Add to List button. The delete button can be used to remove an item from the list.

After creating ACL entries, users can click on each MAC address presented in the ACL list (Figure 19) to edit the permissions for that list item. The page displayed (Figure 21) is similar to the page for adding new entries, except that here the MAC address is already known.

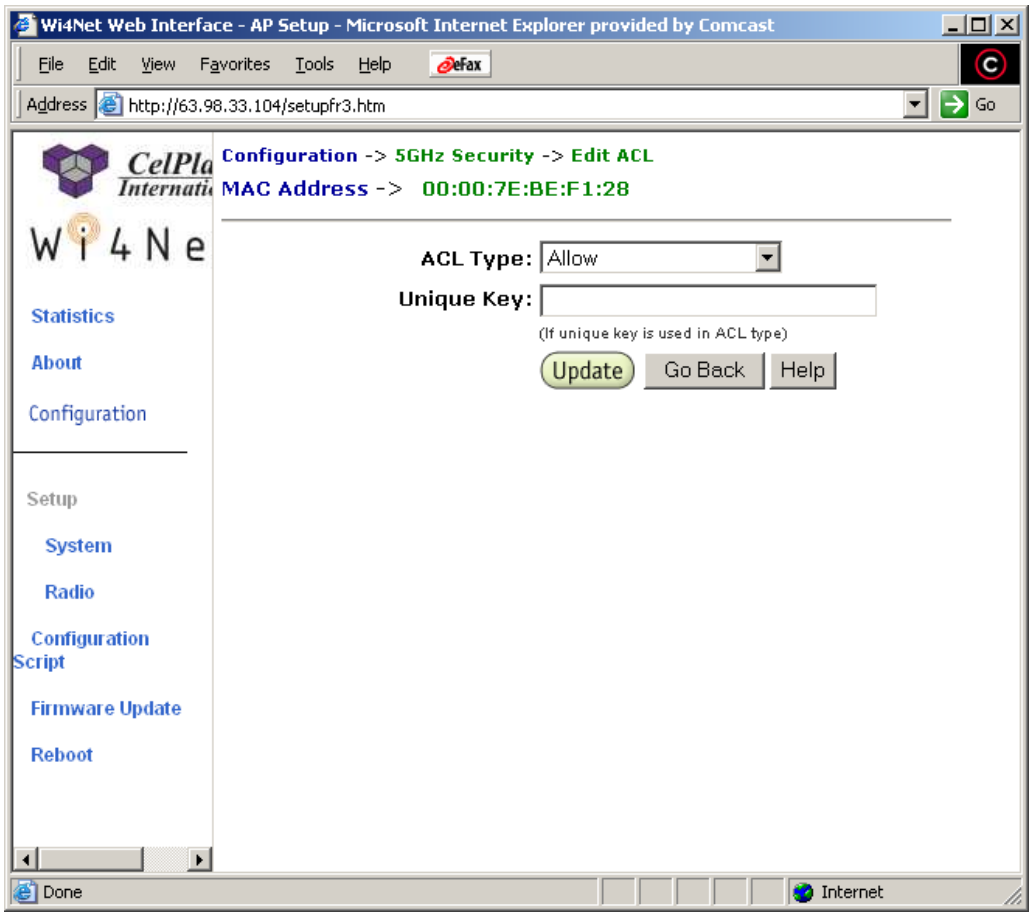

FIGURE 21 EDIT ACL PAGE

Script Configuration

The Script Configuration window (Figure 22) allows execution of text scripts of CLI commands (e.g. construction of a text script to enter the shared keys for stations). All set commands can be used in scripts, except for the following: "set security", "set password", "find bss", "ftp", "password", and "ping".

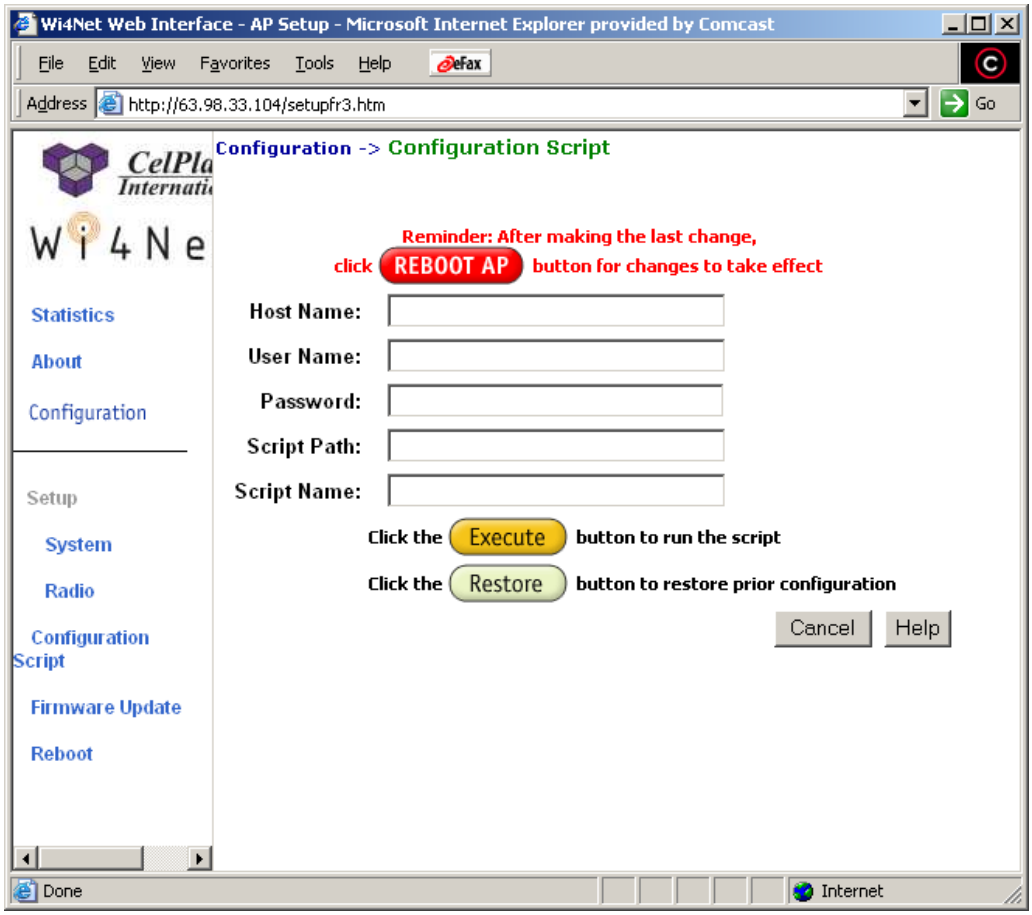

FIGURE 22 SCRIPT CONFIGURATION PAGE

To use scripts, users must first develop the scripts for the application. Then use this window to enter the host name where the script resides. Users must also type in the user name and password for this host. The Script path and name fields determine where the script is located.

Users must press the Execute button to run the script. The Restore button reverts to the previous configuration.

Firmware Update Configuration

The Firmware Update Basic configuration window (Figure 23) displays the current File Transfer Protocol (FTP) location of new firmware. The AP uses the FTP to download the operating image from the HPC. An FTP server utility is required to perform the data transfer between the AP and the HPC.

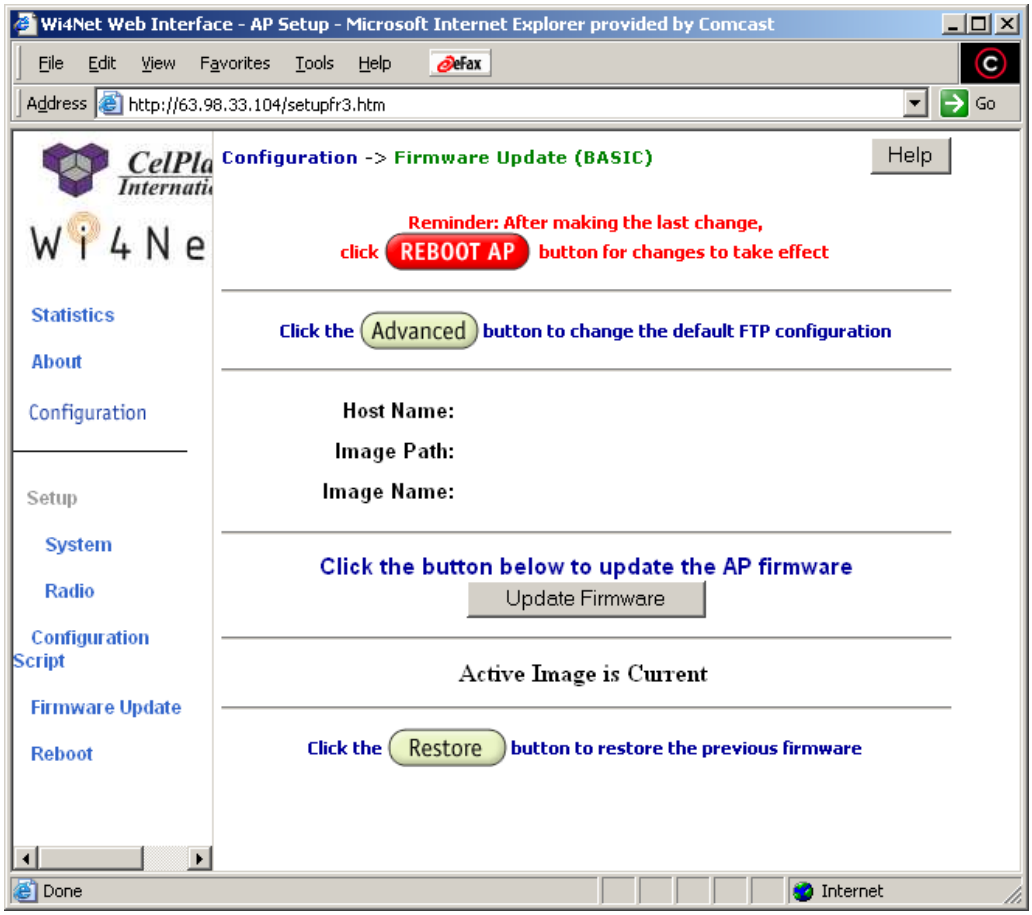

FIGURE 23 FIRMWARE UPDATE BASIC CONFIGURATION PAGE

Before users configure this FTP location, the page displays the default values for the Host Name, Image Path, and Image Name. This window is accessed through the navigation bar, Firmware Update option. To change the default configuration users must press the Advanced button. The AP Firmware Update Advanced Configuration window (Figure 24) is displayed.

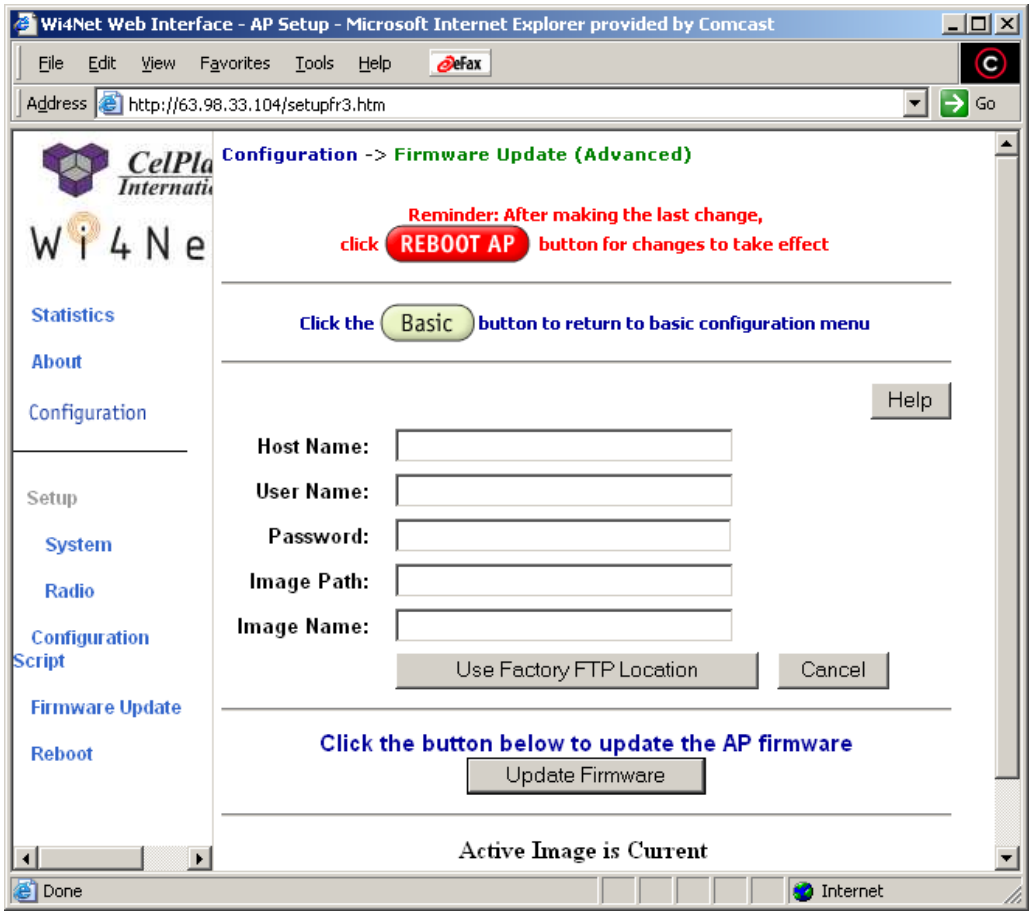

FIGURE 24 FIRMWARE UPDATE ADVANCED CONFIGURATION PAGE

This advanced window allows the configuration of new information on the FTP location of new firmware or filename of the firmware.

Users must enter the Host Name, or host's PC's IP address, User Name, Password, Image Path, and Image Name. The button "Use Factory FTP Location" reverts the settings to the default vendor values. Users must press the Update Firmware button to store the firmware changes.

If the Flash memory contains two images, the Restore button toggles between them. If it contains only one image, the Restore button has no effect.

Statistics Window

Users can access the AP Statistics window at any time through the Statistics link displayed on the left panel of the web page. This window (Figure 25) displays the assigned ID, MAC address, and current state of the AP and all stations currently part of its Basic Service Set (BSS). This window automatically updates itself each minute.

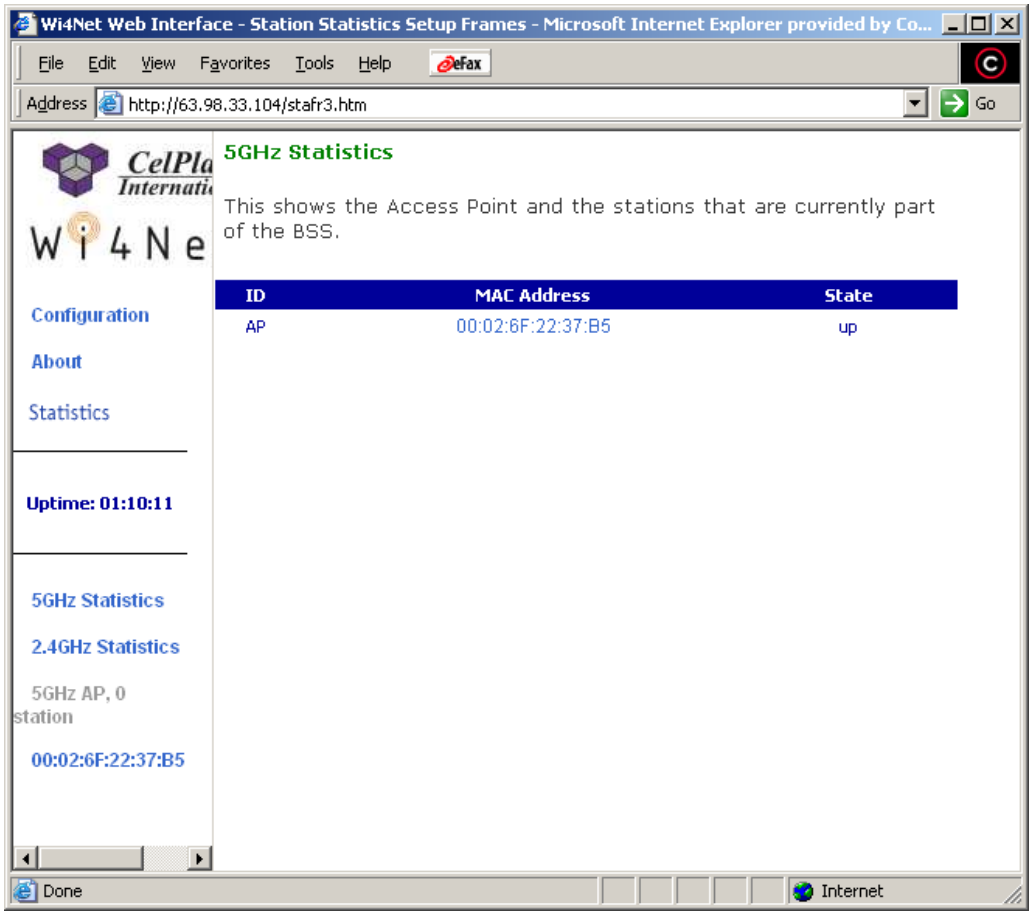

FIGURE 25 TOP-LEVEL STATISTICS WINDOW

Users can view the statistics on the AP by clicking on the MAC address hyperlink for the desired AP. Figure 26 shows an example of a BSS Stats window.

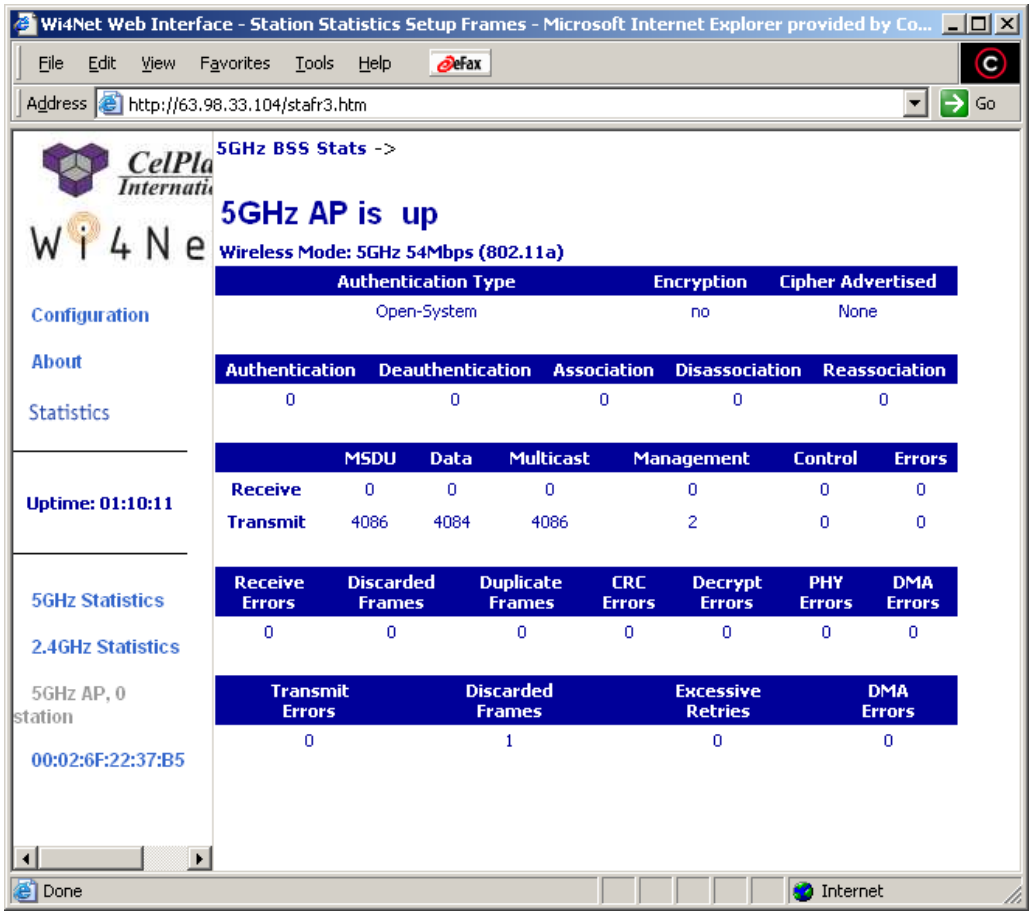

FIGURE 26 BASIC SERVICE SET (BSS) STATISTICS WINDOW FOR AN AP

The BSS Stats window is divided into sections that provide the AP configuration, AP SME statistics (station association information), or AP transmit and receive statistics. The AP stats window automatically updates itself every five seconds.

The title of the window indicates the current state of the AP (e.g. "5GHz AP is up"). The first row indicates the authentication type (open-system or shared key), encryption (enabled or disabled), and the current state of advertised cipher negotiations (AES and/or WEP, or none).

The second row indicates how many times an STA has attempted authentication, deauthentication, association, deassociation, and reassociation.

The third row describes packet information. The MSDU (Maximum Service Data Unit) column specifies the number of packets sent and received by the AP. Packets can be data, control, or management. The Data/Management/Control columns specify the number of packets sent and received for each. The last two columns specify,

respectively, the number of multicast packets and error count for both transmit and receive directions.

The last two rows indicate, respectively, reception and transmission errors. Receive errors are categorized as discarded frames, duplicate frames, CRC errors, PHY errors, and DMA errors. Transmit are categorized as discarded frames, excessive retries and DMA errors.

Users can also visualize statistics for a station by clicking on the MAC address hyperlink for the desired station in the top-level Statistics window (Figure 25). Figure 27 shows an example of a BSS Stats window for a station.

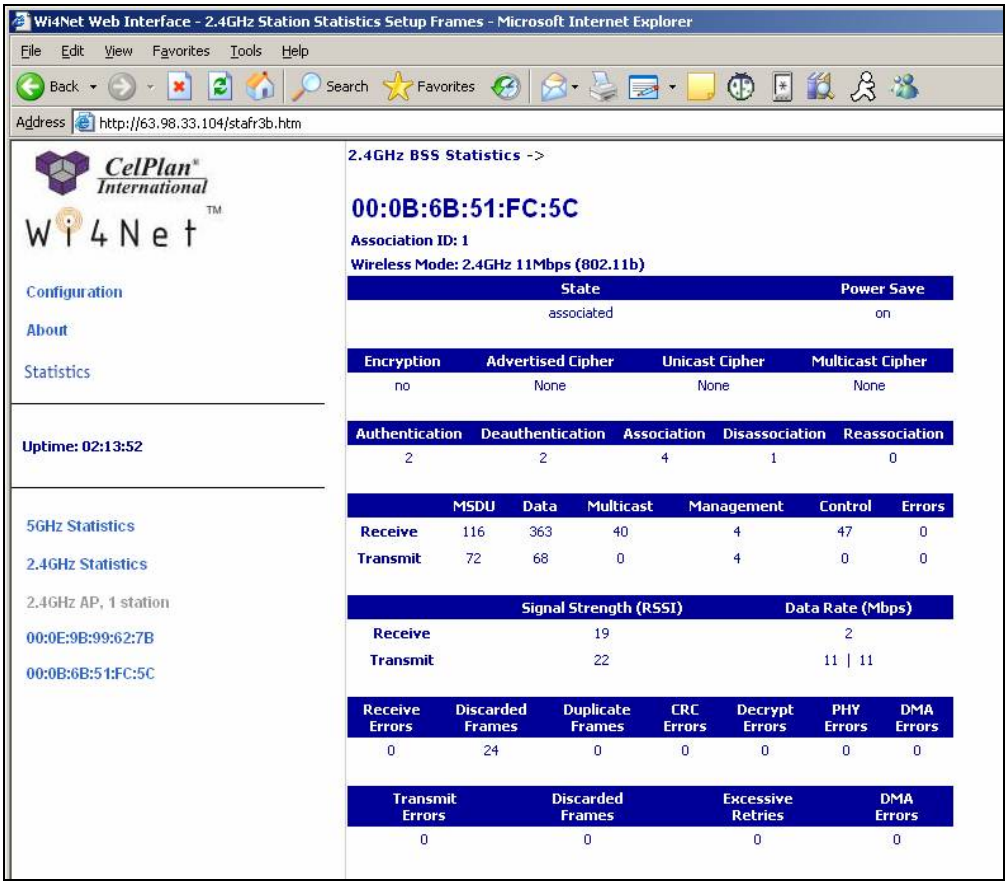

FIGURE 27 BASIC SERVICE SET (BSS) STATISTICS WINDOW FOR A STATION

This window displays station configuration and statistics for the selected station. The Association ID shows the ID of the STA. The first row indicates whether the power save option is enabled or disabled and which type of encryption is used (AES, WEP, none).

The second row shows ciphering configuration, indicating supported cipher types and current unicast and multicast cipher used.

The third row indicates how many times an STA has attempted authentication, deauthentication, association, deassociation, and reassociation.

The fourth row describes packet information. The MSDU (Maximum Service Data Unit) column specifies the number of packets sent and received by the AP. Packets can be data, control, or management. The Data/Management/Control columns specify the number of packets sent and received for each. The last two columns specify, respectively, the number of multicast packets and error count for both transmit and receive directions.

The fifth row shows signal strength (in dBm) and data rate (in Mbps) for both transmit and receive direction.

The last two rows indicate, respectively, reception and transmission errors. Receive errors are categorized as discarded frames, duplicate frames, CRC errors, PHY errors, and DMA errors. Transmit are categorized as discarded frames, excessive retries and DMA errors.

Acronyms

AC – Alternating Current

ACPS - AC Power Supply

AP – Access Point

BH - Backhaul

CPU – Central Processing Unit

DC – Direct Current

DCPS – DC Power Supply

DSRC - Dedicated Short Range Communications

EEPROM – Electronic Erasable Programmable Read Only Memory

FCC – Federal Communications Commision

IEEE - Institute of Electrical and Electronics Engineers

IP – Internet Protocol

ITS - Institute for Telecommunication Sciences

LNA – Low Noise Amplifier

MIPS – Millions of Instructions per Second

OBU – On Board Unit

OFDM – Orthogonal frequency division multiplexing

PA – Power Amplifier

PAN – Personal Area Network

PC – Personal Computer

PCI – Peripheral Component Interconnect

PCMCIA - Personal Computer Memory Card International Association

PRE – Pre-amplifier

RAM - Random Access Memory

RAN – Radio Access Node

RF – Radio Frequency

RSU – Road Side Unit

RX – Receiver, reception

SDRAM – Synchronous Dynamic RAM

STA – Station

SW – Switch

TDD – Time Division Duplexing

TX – Transmitter, transmission

UNII - Unlicensed National Information Infrastructure

UPS – Uninterruptible Power Supply