

Cicada

manual version 1.2



Contents

CICADA ACCESSORIES.....	3
CICADA KEYPAD.....	3
GETTING STARTED.....	3
AP MEASUREMENT SCREENS.....	4
MAIN MENU.....	5
AP ANALYSIS.....	5
AP FOLLOWING.....	5
SPECTRUM.....	6
PEAK HOLD.....	6
CICADA SETUP.....	6
INFO SCREEN.....	7
GPS : ON.....	7
INITIALIZE CARD.....	8
SELECT REGION.....	8
CONTRAST ADJUSTMENT.....	9
BACKLIGHT ADJUSTMENT.....	9
WEP ENCRYPTION DETECTION.....	9
NETWORKING BASICS.....	10
CICADA ACCESSORIES.....	12
DIRECTION FINDING ANTENNA SETUP.....	13
CICADA SERIAL INTERFACE (DATA LOGGER).....	14
SYSTEM REQUIREMENTS.....	14
GPS SCREEN.....	15
SERIAL PORT SCREEN.....	15
UNIT SETUP SCREEN.....	16
DOLPHIN REAL TIME PLOTTER SCREEN.....	16
MENU SELECTIONS.....	17
AP ANALYSIS SCREEN.....	19
FOLLOW SCREEN.....	19
SPECTRUM SCREEN.....	20
CHAMELEON WLAN DATA CONVERSION APPLICATION.....	21
GLOSSARY OF ACRONYMS.....	23
GENERAL SAFETY	
ANTENNA RADIATION PATTERNS	
CICADA DATA SHEET	

INTRUDER ALERT: Recognizing WLAN Attacks & Locating the Culprits (MPD August, 2002)
802.11a Measurement Techniques and Network Issues (MPD November, 2003)
TAKE THE WLAN TEST CHALLENGE (COMMUNICATION NEWS April, 2002)

Cicada™ is a handheld, wireless receiver designed specifically for sweeping and optimizing Local Area Networks. The instrument measures coverage of direct sequence CDMA networks which operate on the IEEE 802.11b standard allowing the user to measure and determine the AP (Access Point), PER (Packet Error Rate), and RSSI signal levels and access points throughout a building. **Cicada** detects and differentiates from narrow-band multipath interferences such as microwave ovens and direct sequence systems and features a built-in display, keypad and removable battery pack for true portability.

Cicada's battery pack uses common AA battery cells found in any convenience store. Ni-Cad, Alkalines, Ni-MH and Li-Ion cells may all be used. **Cicada** does require 5 AA cells with at least 1500 mAh per cell. BVS supplies 2 battery packs complete with 10 Ni-MH battery cells to get users working right out of the box. Ni-MH cells are recommended for best performance from your **Cicada**.

Cicada also includes a simple 2.4 GHz threaded antenna that screws right into the top of the unit. Additional antennas may be ordered from BVS through BVS.

At the top of the **Cicada** rests the GPS connector, antenna connector and upload port. The **GPS antenna connector** (left) is a small male connector. The **antenna connector** (center) is a 2.4 GHz SMA Female 50 ohm. The provided antenna easily screws and unscrews from this connector. Be sure to unscrew antennas when transporting the **Cicada**. The **upload port** (right) is used as a one way communications port for uploading new firmware to the **Cicada**. The port uses the provided cable which employs a standard RJ-11 phone jack on one end and DB-9 PC serial cable on the other end.

See **UPDATING CICADA FIRMWARE** in this manual for firmware updating procedures.



CICADA ACCESSORIES

Your Cicada includes all basic operational accessories including the following: 2.4 GHz antenna, GPS antenna, 16MB compact flash card, compact flash card reader, 2 (Ni-MH) battery packs, AC/DC power cable, carrying case and upload cable. Insert depleted battery pack into charger and plug charger into AC outlet. See rear of charger for LED status indicator lights. Approximate charging time for included Ni-MH battery pack is just over one hour. Run time using these same batteries is just over two hours.

NOTE: The included charger may only be used to charge the included Ni-MH batteries or other AA Ni-MH batteries. **NOT** Ni-CAD batteries. Batteries are automatically conditioned in the charger before starting a rapid charge. The charge and runtime are balanced so that the charge is usually complete before the Cicada displays low battery indication. This is an average estimate since the current consumed by Cicada and runtime depend substantially on the mode of operation. Expect over 500 cycles from each Ni-MH pack.



CICADA KEYPAD

Cicada uses a raised plastic keypad as its only interface. Below are simple descriptions of the buttons and their features:

LOGGING - indicates if unit is logging to compact flash

RECEIVE - indicates if any signals are being received

GPS POWER - indicates internal GPS ON / OFF status

1 - toggles backlight ON & OFF

POWER - toggles Cicada ON & OFF

4 - toggles highest signal strength metering ON & OFF

5 - toggles data logging ON & OFF to compact flash

SETUP - enters the setup menu screen

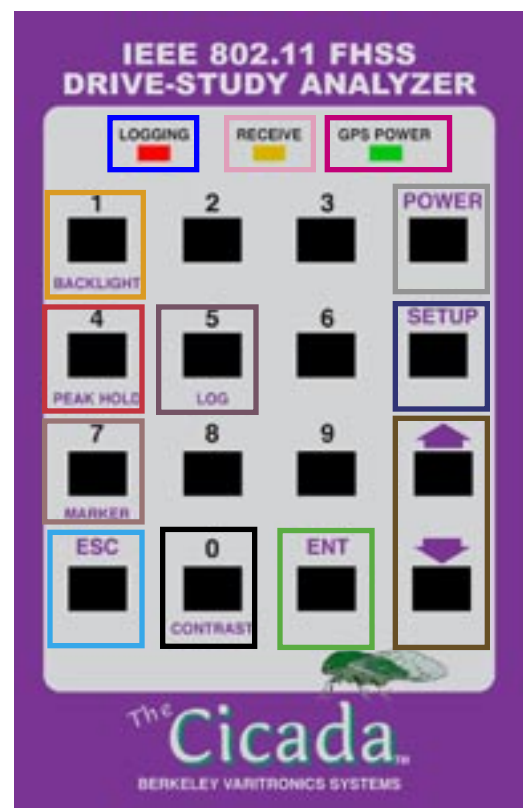
7 - incrementally time stamps

ESC - exits current menu screen

0 - displays contrast screen

ENT - executes currently selected option

UP/DOWN ARROWS - scroll through selections



GETTING STARTED

Operation of the Cicada is straightforward. Insert 5 fresh battery cells into removable pack. Close the bottom back up and power on the Cicada by holding down the POWER button for about 2 seconds.

AP MEASUREMENT SCREENS

This is the main measurement screen used for monitoring and selecting any valid FHSS (Frequency Hopping Spread Spectrum) APs (Access Points). This screen displays AP parameters such as signal strength in dBm, WEP encryption, current GPS time/position/satellites of Cicada and MAC address list. The MAC address list consists of all FHSS MAC addresses detected. Multiple addresses may be listed and monitored simultaneously here. Use the UP/DOWN ARROW keys to toggle between all of these selections and ENT to choose one. Upon choosing an AP, the user will be taken to the AP Following Screen (below) providing detailed parameters for the chosen AP.

AP ANALYSIS SCREEN

NAEur - indicates current region selection for measure

The AP address window at the bottom indicates all IEEE addresses identified. (the arrow to the left indicates the address that is currently selected)

dBm - indicates the signal strength of the last packet measured.

W - indicates WEP (Wireless Equivalent Privacy). "P" indicates encryption is detected.

LAT - GPS Latitude coordinates

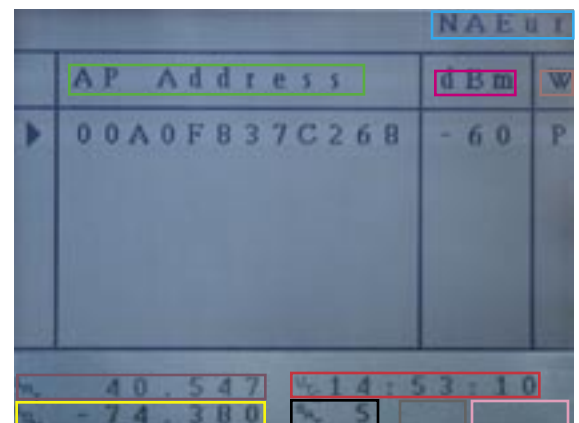
UTC - GPS time stamp

LON - GPS Longitude coordinates

SAT - number of satellites in view

Indicates compact flash has been formatted for Cicada

Indicates data storage remaining in compact flash card



AP FOLLOWING SCREEN

AP: the selected AP's MAC address

RSSI: last packet's signal strength measurement in dBm

Hop Set: indicates set number of sets 1,2 or 3

Hop Pattern: indicates pattern number of patterns 1-79 (note: this number corresponds to the IEEE 802.11 spec)

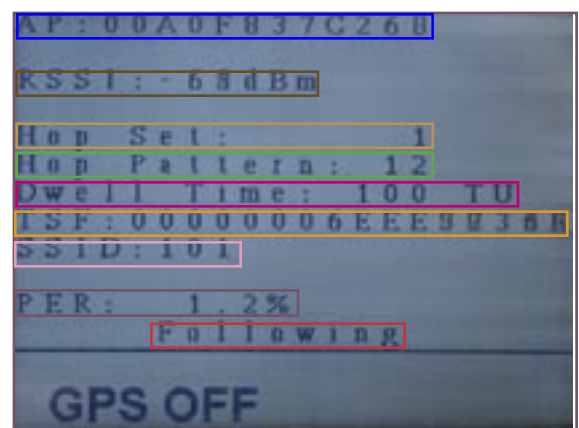
Dwell Time: indicates how long the AP stays on a channel before it jumps to another channel in TU (Time Units defined as 1024 microseconds)

TSF: Timing Synchronization Function indicates the AP's absolute time that counts down to the next channel hop

SSID: currently selected AP's Service Set Identification

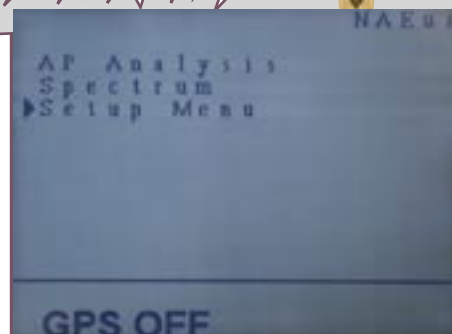
PER: Packet ErrorRate percentage for the selected AP

Following - Cicada continues to follow AP as it hops



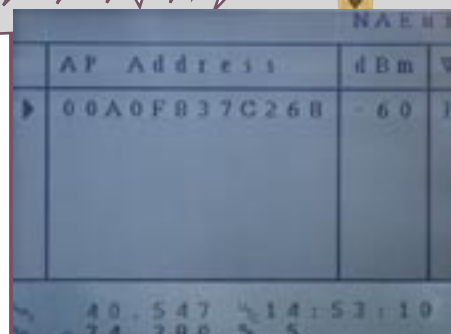
MAIN MENU

Press the ESC key at any time to enter the MAIN MENU. This menu allows access to all controls and parameters found in the Cicada. Use the UP/DOWN ARROW keys to choose and press ENT to make the selection.



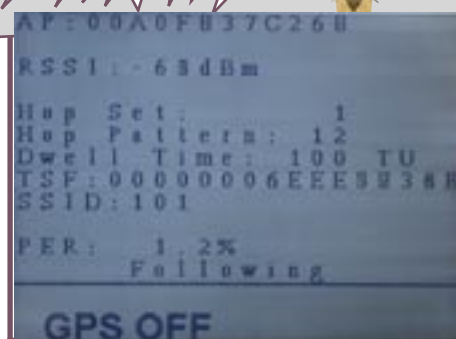
AP ANALYSIS

This selection places a cursor at the bottom of the screen to the left of the AP addresses. By pushing ENT, the user selects (indicated by the arrowhead) a specific AP address to monitor. Use Select AP and the UP / DOWN ARROW keys to toggle through all received addresses. In this screen, the user may access up to 16 unique, detected AP addresses by scrolling through the list and selecting one.



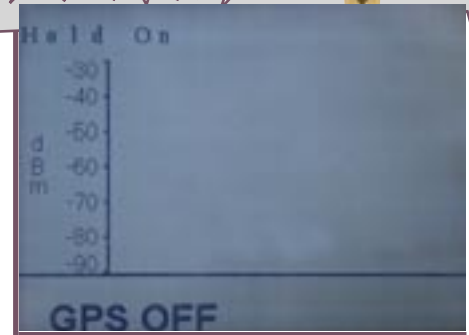
AP FOLLOWING

By selecting an AP to monitor off the AP analysis screen, the user will prompt this screen to appear. This screen allows monitoring of the selected AP's beacon timing channel. After a few moments of searching, Cicada will "lock on" and follow the AP's timing parameters. The parameters are listed on page 4 of this manual. Press ESC at any time to return to the AP analysis screen.



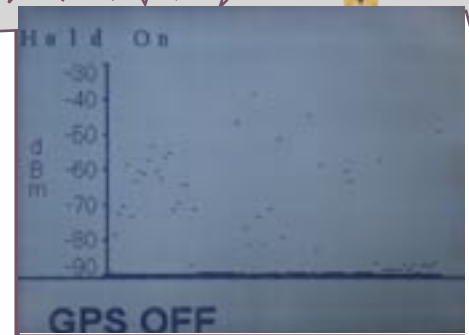
SPECTRUM

This RSSI screen indicates all received signals at 2.4 GHz in a 1 MHz bandwidth that Cicada continuously scans. The peak power is indicated graphically and numerically on this screen as well as the channel being scanned.



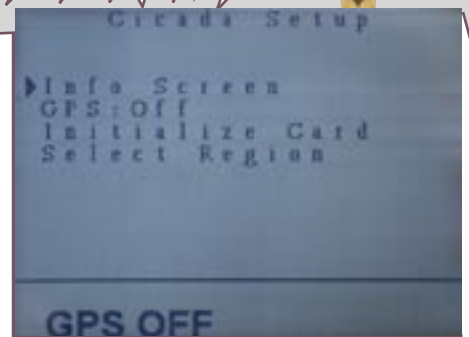
PEAK HOLD

Peak Hold is only activated and deactivated in the Spectrum Screen. Use Peak Hold when looking for interference sources with low duty cycles such as APs. Push the 4 key on the keypad to turn ON the Peak Hold. Push the 4 key again to turn the Peak Hold back OFF. Each small tick mark indicates a dBm peak for that portion of the 1 MHz scan. Remember the last signal displayed will reset when Peak Hold is toggled ON.



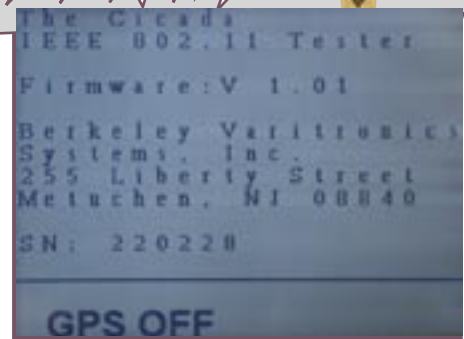
CICADA SETUP

Press the SETUP key at anytime to access the Setup Menu. While in the this menu, use the UP/DOWN ARROW keys to choose a setup option. From this menu, users may access and/or control features such as unit information, internal GPS, Compact Flash card and international region. Press ENTER to select or ESC to return to previous menu screen.



INFO SCREEN

This informational screen provides information on your Cicada unit such as firmware version, serial number and current GPS information.

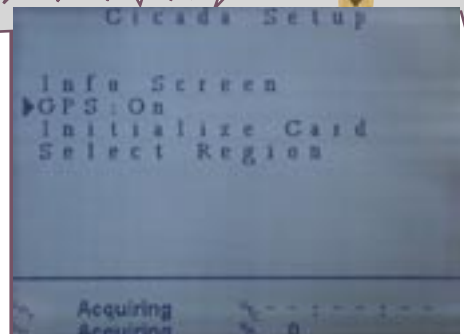


The Cicada
IEEE 802.11 Tester
Firmware: V 1.01
Berkeley Varitronics
Systems, Inc.
255 Liberty Street
Metuchen, NJ 08840
SN: 220220
GPS OFF

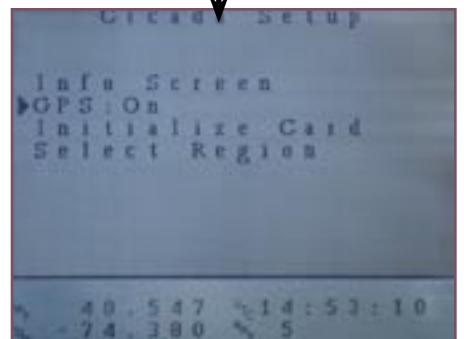
GPS : ON

Press ENTER to toggle the internal GPS ON and OFF. The GPS POWER LED indicator above the keypad will light up indicating the internal GPS is operational. Be sure that the GPS antenna is connected to the Cicada and not blocked from the satellites in the sky.

Allow a few minutes for the GPS antenna to acquire a few satellites and lock. Be sure to keep the GPS off if GPS data is not needed in WLAN studies as it will draw power and shorten the running time of your Cicada.



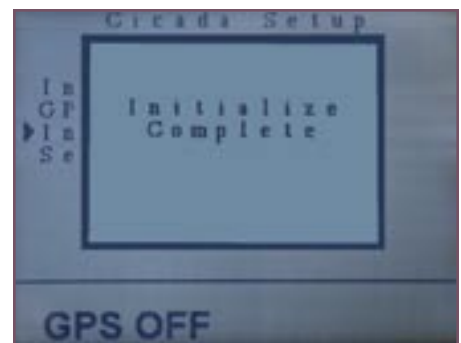
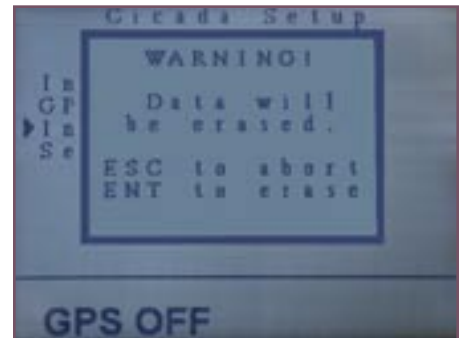
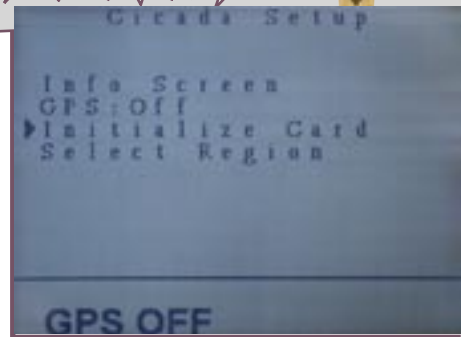
Cicada Setup
Info Screen
GPS: On
Initialize Card
Select Region
Acquiring
Searching



Cicada Setup
Info Screen
GPS: On
Initialize Card
Select Region
40.547 14:53:10
-74.380 5

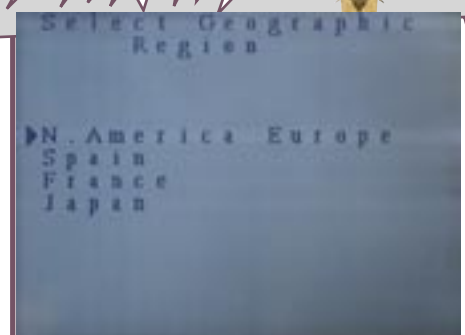
INITIALIZE CARD

Press ENTER to begin initialization of the compact flash card. A warning screen will then appear asking the user to press ESC or ENTER. Upon selecting ENTER, a new message will appear moments later indicating that the compact flash card is now formatted for use in your Cicada.



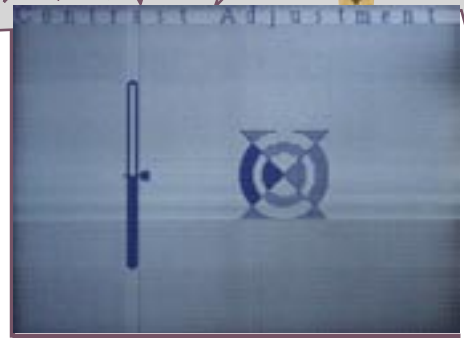
SELECT REGION

At anytime, press SETUP on the key pad to access the Select Geographic Region screen. Use the ARROW keys and ENT to select between one of the four IEEE allocated regions for scanning.



CONTRAST ADJUSTMENT

At anytime, press 0 on the key pad to access the Contrast Adjustment screen. Use the UP/DOWN ARROW keys to increase or decrease LCD contrast. When finished, press ESC to exit this screen.



BACKLIGHT ADJUSTMENT

At anytime, press 1 key to toggle the backlight off and on. Remember that using the Cicada without the backlight on will increase overall battery life.

WEP ENCRYPTION DETECTION

A “P” next to its associated AP address and signal strength indicates that WEP (Wireless Equivalent Privacy) is enabled and detected for that particular AP. An empty space indicates no WEP encryption.

A screenshot of the WEP Encryption Detection screen. It displays a table with the following columns: AP Address, dBm, and W. The first row shows an AP address of 00A0F837C268, a signal strength of -60, and a 'P' in the W column, indicating WEP is enabled. The screen also shows a status bar at the bottom with the text '40.547 14:53:10' and '74.380 5'.

AP Address	dBm	W
00A0F837C268	-60	P

Networking Basics

Packets and traffic

Information travels across a network in chunks called “packets.” Each packet has a header that tells where the packet is from and where it’s going, similar to what you write on the envelope when you send a letter. The flow of all these packets on the network is called “traffic.”

Hardware addresses

Your PC “listens” to all of the traffic on its local network and selects the packets that belong to it by checking for its hardware address in the packet header or MAC (Media Access Control). Every hardware product used for networking is required to have a unique hardware address permanently embedded in it.

IP addresses

Since the Internet is a network of networks (connecting millions of computers), hardware addresses alone are not enough to deliver information on the Internet. It would be impossible for your computer to find its packets in all the world’s network traffic, and impossible for the Internet to move all traffic to every network, your PC also has an IP (Internet Protocol) address that defines exactly where and in what network it’s located. IP addresses ensure that your local Ethernet network only receives the traffic intended for it. Like the hierarchical system used to define zip codes, street names, and street numbers, IP addresses are created according to a set of rules, and their assignment is carefully administered.

Put another way, the hardware address is like your name; it uniquely and permanently identifies you. But it doesn’t offer any clues about your location, so it’s only helpful in a local setting. An IP address is like your street address, which contains the information that helps letters and packages find your house.

Rules for Sending Information (Protocols)

A protocol is a set of rules that define how communication takes place. For instance, a networking protocol may define how information is formatted and addressed, just as there’s a standard way to address an envelope when you send a letter.

Networking Devices:

Bridges

A bridge joins two networks at the hardware level. This means that as far as other protocols are concerned, the two networks are the same.

Routers

A router connects two IP networks. In contrast to a bridge, which joins networks at the hardware level, a router directs network IP traffic based on information stored in its routing tables. A routing table matches IP addresses with hardware addresses. The router stamps each incoming IP packet with the hardware address that corresponds to that IP address. As a result, the packet can be picked up by the right computer on the hardware network.

DNS (Domain Name Server)

Networks (domains) on the Internet have names that correspond to their IP addresses. A Domain Name Server maintains a list of domain names and their corresponding addresses. This is why you can go to Berkeley’s Web site by entering www.bvsystems.com, instead of the IP address.

Networking Terms:

TCP/IP (Transport Control Protocol/Internet Protocol)

TCP/IP is a collection of protocols that underlies almost every form of communication on the Internet.

DHCP (Dynamic Host Control Protocol)

DHCP is a method of automatically assigning IP addresses. Instead of assigning addresses to individual users, addresses are assigned by the DHCP server when clients need them. This means that instead of entering several fields of long addresses, users need only to select DHCP as their configuration method for IP networking.

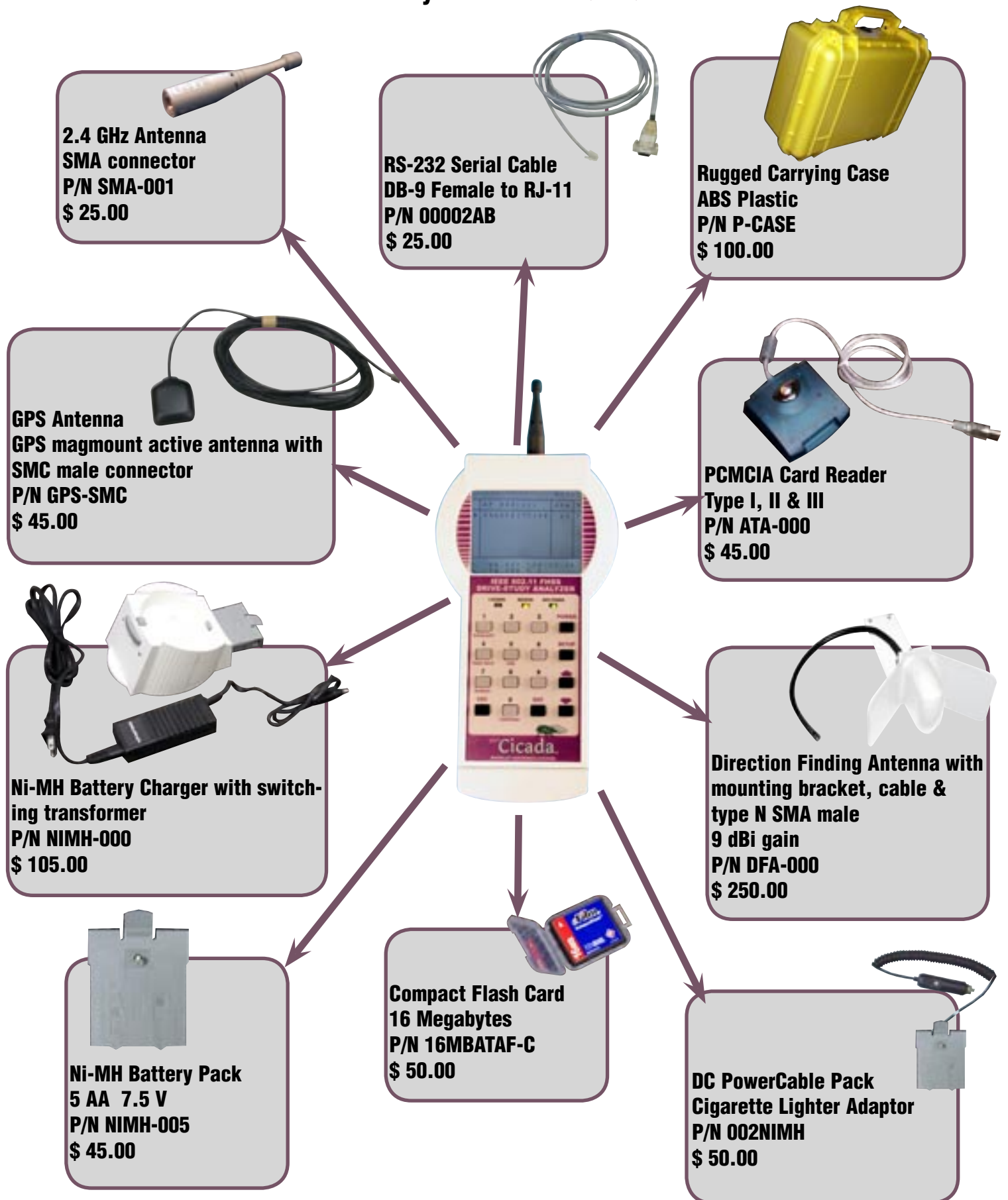
PPP (Point-to-Point Protocol)

PPP is the most common protocol for providing IP services over a modem.

NAT (Network Address Translation)

NAT is used to share one IP address among several computers. A device set up as a NAT router uses a collection of “private” IP addresses (in the range 10.0.1.2 to 10.0.1.254 for example) to allow several computers to access the Internet using one “public” IP address. When a computer using a private IP address requests information from the Internet, the NAT router keeps a record of the computer making the request, and sends the information to the Internet using its own IP address. When the response comes back from the Internet, the NAT router forwards the packet to the appropriate computer.

Accessories for your *Cicada*



Optional Direction Finding Antenna (DFA-000) Setup



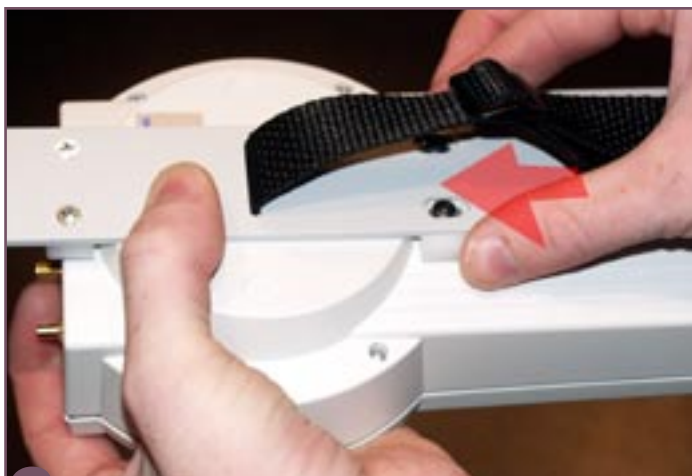
1 Remove cap from SMA connector on DF antenna.



4 Tighten both screws on bracket.



2 Hook antenna bracket into slit on top of unit.



3 Slide bracket plate into other slit.



5 Loop & screw in antenna cable to unit.

OVERVIEW

Cicada Program Requirements

V2.0 Cicada Data Logger requires the following:

Windows 98, Windows 2000 or Windows XP operating system

64 Meg (or more) RAM

Pentium II CPU

400 MHz or greater operating speed

100 MB (or more) free space on Hard Drive

At least 1 serial port for data logging (not required for replay)

Color Display 800 x 600 recommended

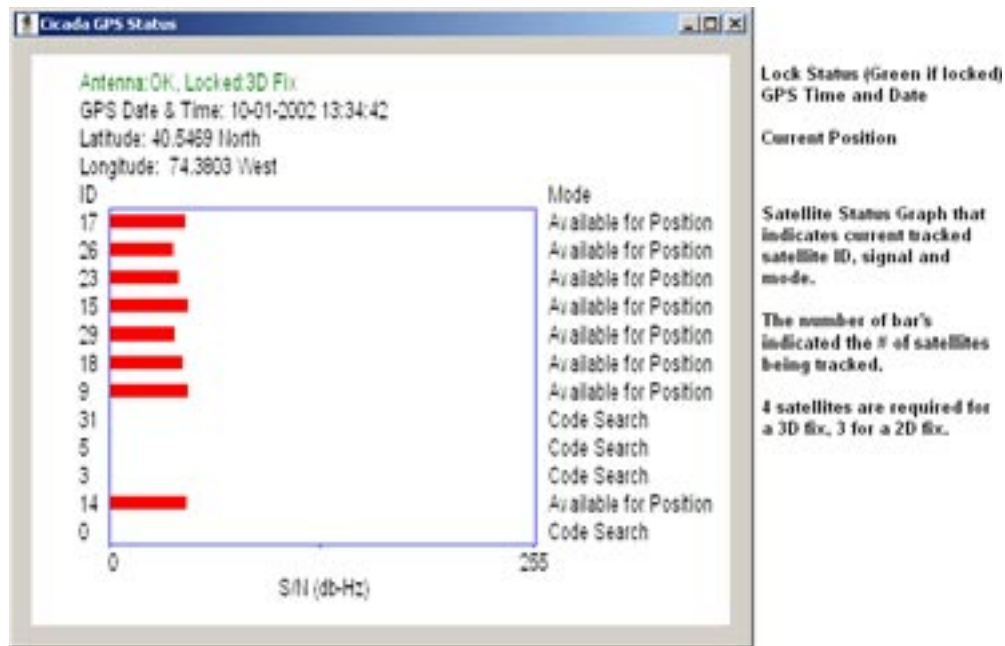
Optional PCMCIA card reader

The CICADA Serial Interface software allows complete control of the CICADA IEEE 802 scanner. All data displayed on the CICADA LCD is also displayed on the PC screen. Data received by the PC software can be saved in disk files for later replay and conversion. Each measurement screen of the CICADA is duplicated by the PC software. In addition, GPS and UNIT INFORMATION screens are provided to display additional information about the GPS receiver and the CICADA. When the PC software starts, data is displayed in a 640 by 480 format. To increase to 800 by 600, click the maximize button on the right side of the control bar. The PC used to run the CICADA application MUST be running the Windows 98 or Windows 2000 operating system. NO OTHER program should be running while the CICADA application is running.

The PC menu bar is used to select disk files for saving or replaying data files (SELECT DISK FILE). Instructions can be found using the HELP menu selection. Version and other information is available via the ABOUT selection. INCREMENT MARKER causes the CICADA connected to the PC to add one to the current marker value. PEAK HOLD is used to toggle the peak hold feature on and off during the spectrum or follow measurements. UNIT SETUP displays a screen that displays CICADA parameters. GPS displays the gps receiver information screen.

Cicada GPS Status screen.

To view this screen, click the GPS Status Tool Bar button.



GPS SCREEN

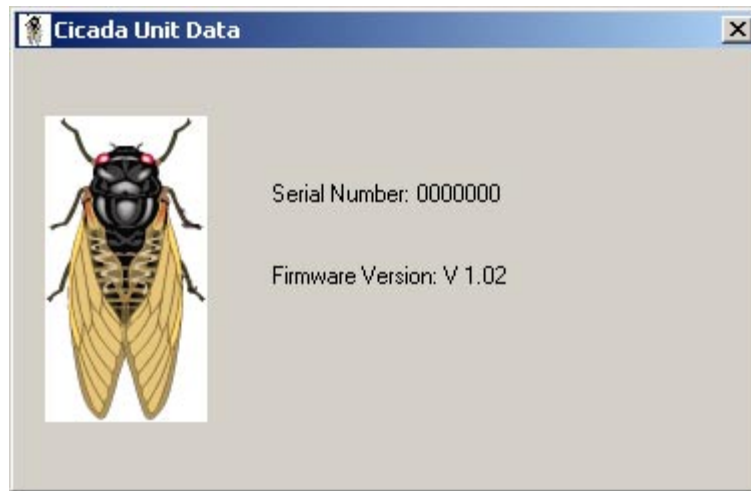
This screen is used to determine the number of satellites being tracked by the built in GPS receiver. At least 3 satellites are required for GPS lock. The tool bar GPS Status button indicates lock status with two indicators. These indicators are GREEN if the GPS is locked, RED if not. If the indicators are the same color as the button, the Cicada GPS is off.

This display is available during replay or while displaying real time data. It can be sized using the mouse and the lower right hand corner of the GPS display. The color of the top line of this display indicates GPS lock status. The same color is displayed by the indicators on the GPS Status tool bar button.



SERIAL PORT SCREEN

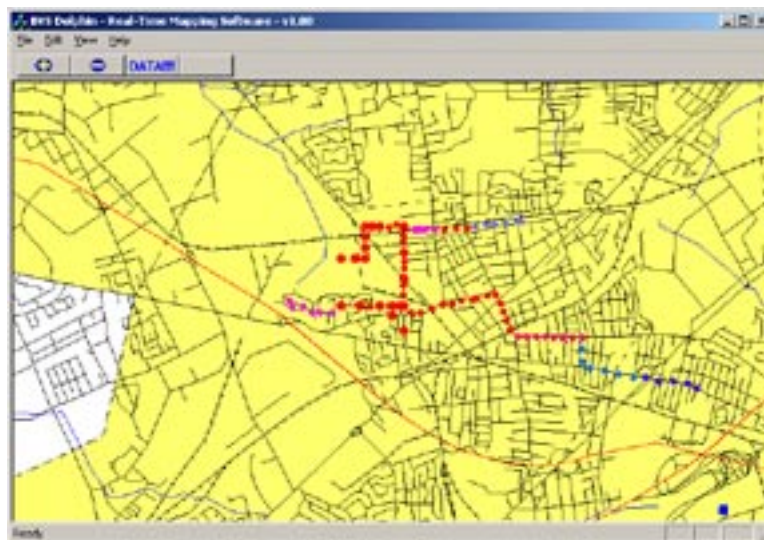
This is the first screen that the user will see when running Cicada Serial Interface. Simply connect the Cicada unit to any available PC serial port with the provided cable, select the appropriately numbered port on this menu screen and select OK. The Cicada is now connected to your PC for communications.



UNIT SETUP SCREEN

Clicking the menu View Unit Data button will cause the Cicada connected to the PC serial port to send its unit data which is displayed in a dialog.

When using BVS Dolphin plotting software, this information must be available. When making data files that will be replayed for plotting, display this dialog just after turning on Data save. Do the same to plot data in real time using Dolphin.



DOLPHIN REAL TIME PLOTTER SCREEN

When using the DOLPHIN plotter software with the CICADA, check the “Use BVS Dolphin” in the UNIT SETUP screen. DOLPHIN plots data in real time or from data files during replay.

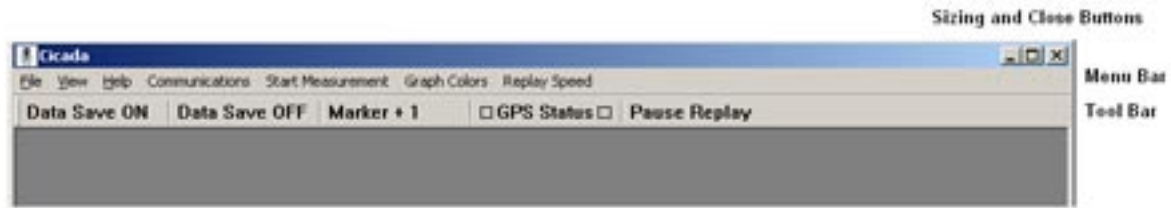
V2.0 Cicada PC Software Dolphin Support

Dolphin software requires that the Cicada serial number be recorded before it will operate. Use the following steps to ensure that the Dolphin software has the Cicada serial number.

- 1 Run the supplied copy of BVS Dolphin before starting Cicada v2.0.
- 2 Start Cicada v2.0

3 If connected to the Cicada via PC serial port, get the Cicada Setups by clicking the “View Unit Data ” menu button. If using Dolphin later with replay, make sure to do this just after turning on the data file save so that the Cicada serial number is recorded in the data save file.

4 Make sure the Cicada GPS is turned on.



Menu Selections

File: Use to select a Cicada data file to replay or to cancel the current disk file replay. The Exit selection closes the application in the same way as the Close Button in the upper right hand corner of the screen. Closing the application causes any open data files to be closed.

View: This selection can be used to turn on and off the tool bar. It is also used to get the Unit Data from the currently connected Cicada. Unit data is required when using the BVS Dolphin plotting software.

Help: Use this selection to view this help file and to display the version number of the PC software.

Communications: This selection is used to indicate to the PC which serial port is connected to the Cicada. Use this selection first when starting a data log session with the Cicada. After a data file replay, the serial port is disconnected. Use this selection after a file replay to reconnect the serial port to the Cicada.

Start Measurement: Use this selection to start a Cicada measurement.

Graph Colors: This selection is used to change graph colors.

Replay Speed: Use this selection to modify the rate of the disk file replay display.

Tool Bar Buttons

Data Save ON: Click this button to select a disk file to save Cicada data into. Once a file is selected, all packets from the Cicada will be written to the selected disk file. The file name and current file size is displayed in the Status Bar. If an existing file is selected, new data is appended to the end of the existing file.

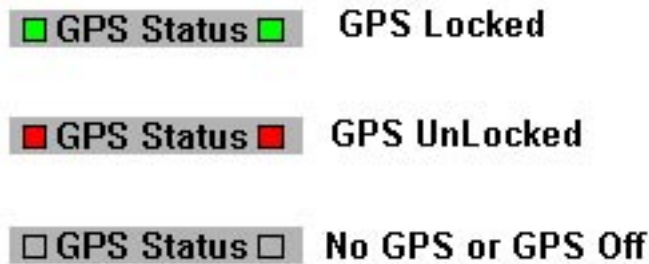
Clicking this button while data save is on is ignored.

Data Save OFF: Click this button to stop saving data and to close the current save file. Clicking this button when data save is off is ignored.

Marker + 1: Click this button to cause the Cicada marker value to be incremented. The Cicada must be connected to a PC serial port for this button to function. The marker value is displayed

in the Status Bar.

GPS Status: Click this button to view the GPS status screen. The indicators on the button show the current GPS status :



Pause Replay: Click this button to pause the current disk file replay.



The Cicada status bar is used to display current program status using 7 indicators as shown above.

1 -- Displays the current serial connection. It will indicate “Not Connected” if a serial port has not been selected and during file replay. Use the menu Communications selection to choose the PC serial port being used with the Cicada.

2-- Displays data save status. If data save is ON, the current size of the data file is displayed here.

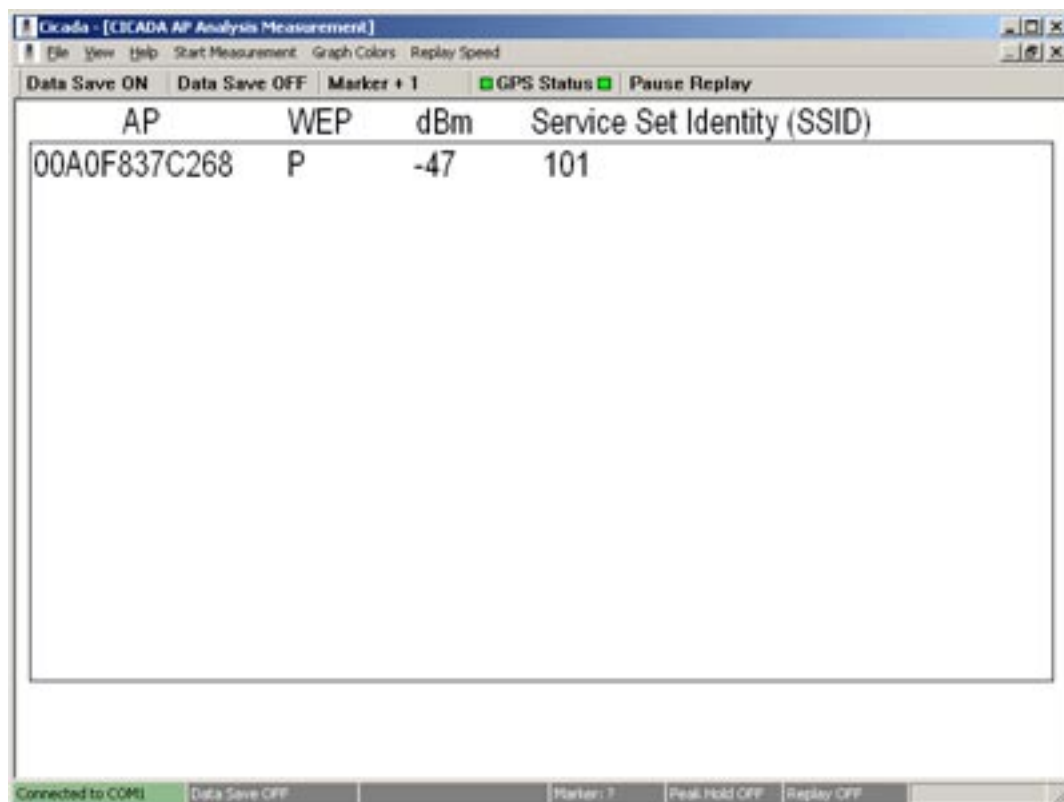
3-- Displays the name of the data save disk file if data save is on or it displays the name of the data file being replayed.

4-- Displays the current Cicada marker value.

5-- Peak hold status is displayed here (On or Off).

6-- Replay status is displayed here (On or Off).

7-- Replay Progress bar is displayed here during data file replay. This bar indicates the approximate position of the data in the file being displayed. The replay is complete when the bar reaches the right of the indicator.

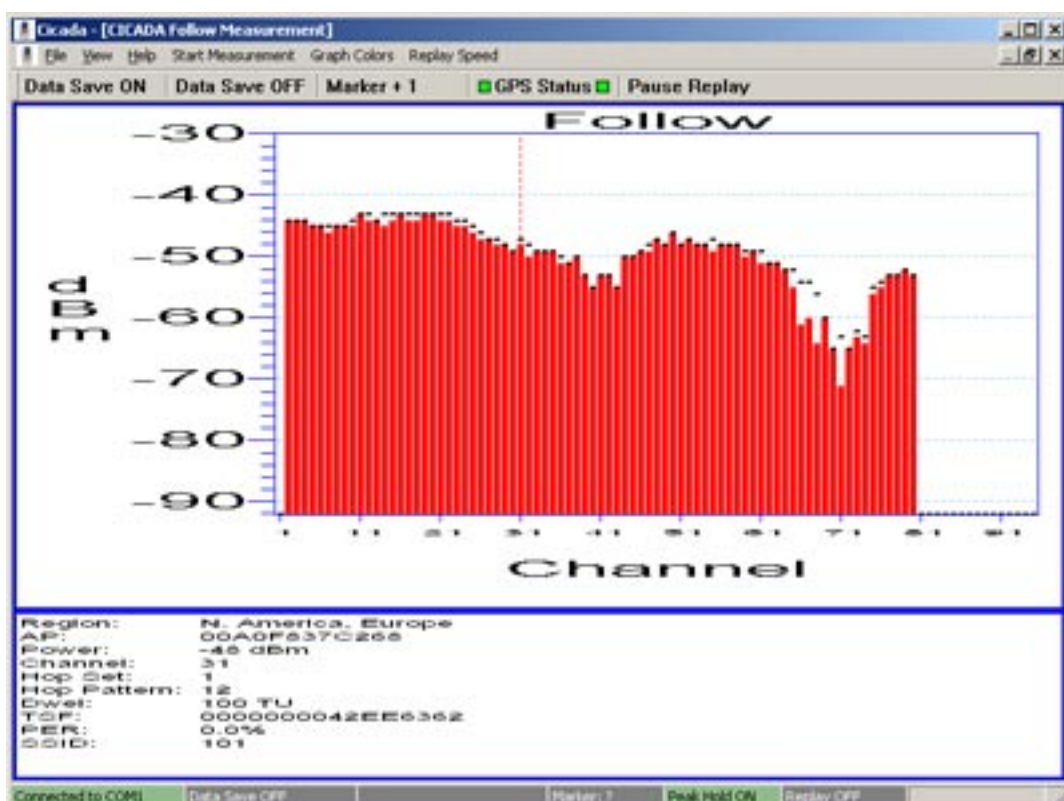


List of up to 64 detected AP's

Double click an AP in the list to start the Follow measurement.

AP ANALYSIS SCREEN

This measurement displays up to 64 detected AP's. Scroll bar's appear when more AP's are detected than can be displayed in the window. To follow a particular AP displayed in this list, double click it. The Cicada will enter the Follow measurement using the selected AP.



Top Section

Follow Channel's

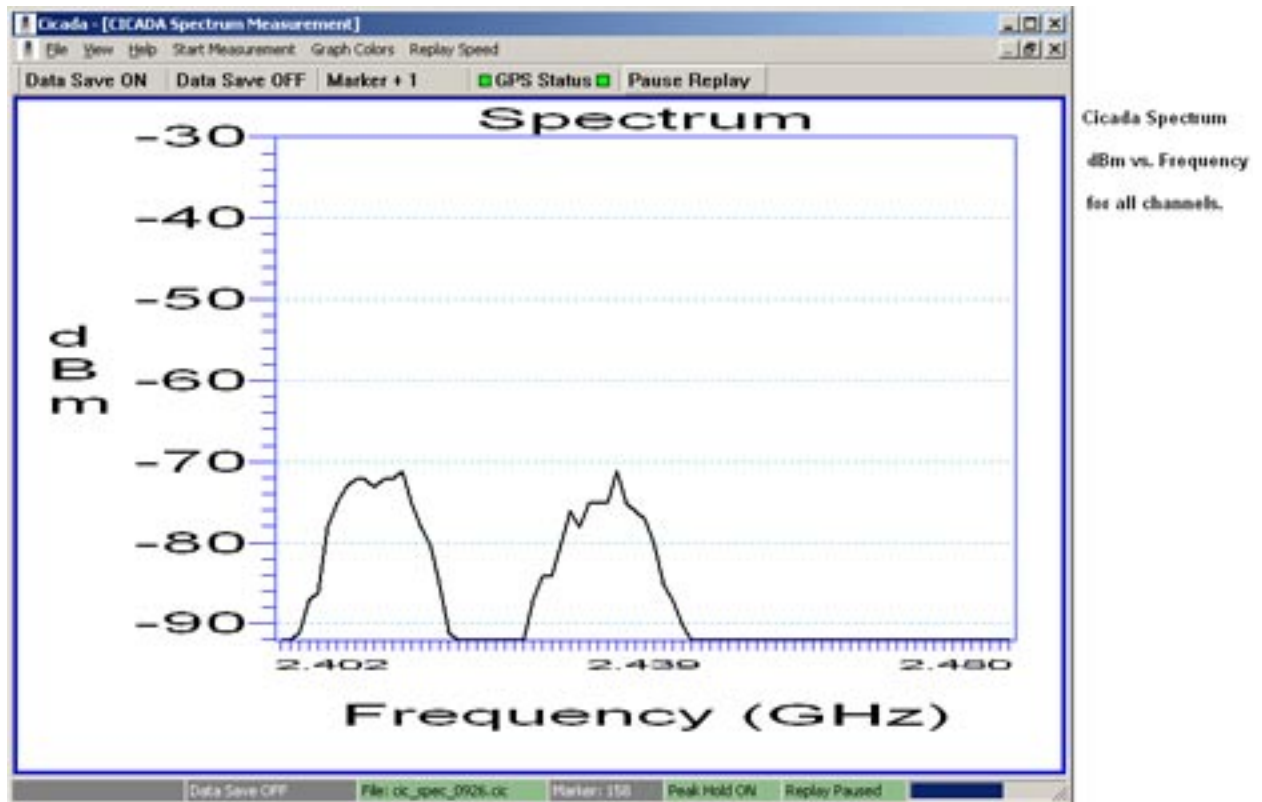
Current channel is marked by the dotted line.

Bottom Section

AP information

FOLLOW SCREEN

This measurement displays the channel hopping sequence of the selected AP. The current channel is indicated with a dotted line along with channel power in the top section of the display. The bottom section of the display indicates information about the AP.



SPECTRUM SCREEN

The Cicada sweeps across all channels and reports the power (dBm) for each.

BVS CHAMELEON DATA CONVERSION UTILITY

Introduction

The Chameleon application software is the universal data conversion and filtering tool for BVS Receivers.

The Chameleon was designed to greatly simplify the transfer of receiver data to many popular post-processing applications such as MapInfo and MS Excel.

The following sections of this document outline the various features of the Chameleon WLAN software.

Installation

Installation of Chameleon is straightforward. Use the enclosed CD and follow the instructions.

Starting the Application

Start Chameleon by clicking on the icon created by the installation utility. The main screen will show up. All steps for the conversion of data are taken from this screen.



Chameleon WLAN Main Screen

Input File

The first step is the choosing of files for input and output. Choose the data file that is to be converted. The Chameleon will automatically determine which product created the file. Chameleon will display the product on the top of the screen. Then choose the name of the file to store the conversion results. By default, the filename for input will be chosen with a “.out” extension.

Output Format

By selecting the appropriate post-processing application, the correct fields will be selected and placed in the field selection screen in the appropriate order. The user may also choose “none”. Whether or not the field titles are in the output can be selected.

Also, the delimiting character of the fields in the output file is chosen in this section.

Output Field Selection

This section enables the selection of those fields that are to be placed in the output file. The individual fields for the data types will appear in the far right box when the data type is selected in the “selected” box.

Conversion

The final step in the step-by-step process is the “conversion” section. Press the **CONVERT** button. The progress bar will be updated as the file is being processed. The speed of conversion will vary based on the size of the data file.

Glossary of Acronyms

AC	Alternating Current
A/D	Analog to Digital converter
AGC	Automatic Gain Control
AP	Access Point
Applet	a small Application
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
BW	Band Width
CDMA	Code Division Multiple Access (spread spectrum modulation)
DC	Direct Current
D/A	Digital to Analog
dB	decibel
dBm	decibels referenced to 1 milliwatt
DOS	Digital Operating System
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
FIR	Finite Impulse Response
GHz	GigaHertz
IF	Intermediate Frequency
I and Q	In phase and Quadrature
IBBS	Independent Basic Service Set
kHz	kiloHertz
LCD	Liquid Crystal Display
LO	Local Oscillator
MAC	Medium Access Control
Mbits	Megabits
MHz	MegaHertz
NIC	Network Interface Card
OFDM	Orthogonal Frequency Domain Multiplexing (802.11a)
PC	Personal Computer
PCS	Personal Communications Service (1.8 to 2.1 GHz frequency band)
PER	Packet Error Rate
PN	Pseudo Noise
QPSK	Quaternary Phase Shift Keying, 4-level PSK
RF	Radio Frequency
RSSI	Receiver Signal Strength Indicator
SSID	Service Set IDentification
UCT	Universal Coordinated Time
VAC	Volts Alternating Current
VGA	Video graphic
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network

IMPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- 1) Read and understand all instructions.
- 2) Follow all warnings and instructions marked on the product.
- 3) Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
- 4) Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool.
- 5) Do not place this product on an unstable cart, stand, or table. The product may fall, causing serious damage to the product.
- 6) Slots and openings in the cabinet and the back or bottom are provided for ventilation, to protect it from overheating these openings must not be blocked or covered. The openings should never be blocked by placing the product on the bed, sofa, rug or other similar surface. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
- 7) This product should be operated only from the type of power source indicated on the appliance. If you are not sure of the type of power supply to your home, consult your dealer or local power company.
- 8) Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- 9) Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- 10) Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
- 11) To reduce the risk of electric shock, do not disassemble this product, but take it to a qualified service facility when some service or repair work is required. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock when the appliance is subsequently used.
- 12) Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
 - A) When the power supply cord or plug is damaged or frayed.
 - B) If liquid has been spilled into the product.
 - C) If the product has been exposed to rain or water.
 - D) If the product does not operate normally by following the operating instructions. Adjust only those controls, that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal operation.
 - E) If the product has been dropped or the cabinet has been damaged.
 - F) If the product exhibits a distinct change in performance.
- 13) Avoid using the product during an electrical storm. There may be a remote risk of electric shock from lightning.
- 14) Do not use the telephone to report a gas leak in the vicinity of the leak.

INSTALLATION INSTRUCTIONS

1. Never install telephone wiring during a lightning storm.

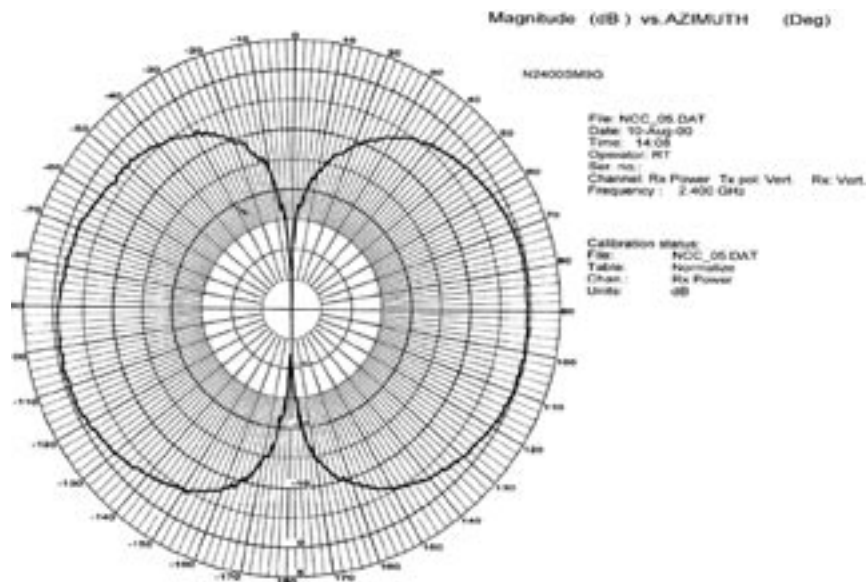
2. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
3. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
4. Use caution when installing or modifying telephone lines.

INSTRUCTION FOR BATTERIES

CAUTION: To Reduce the Risk of Fire or Injury to Persons, Read and Follow these Instructions:

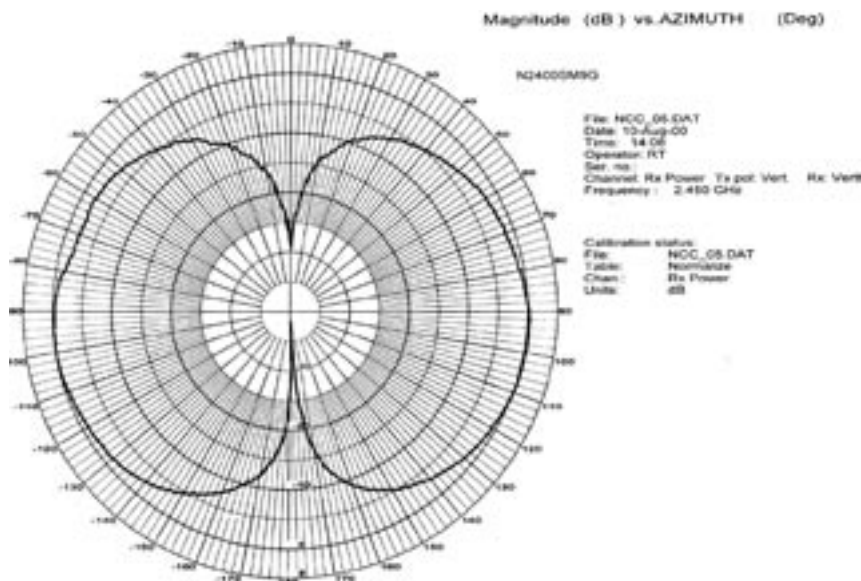
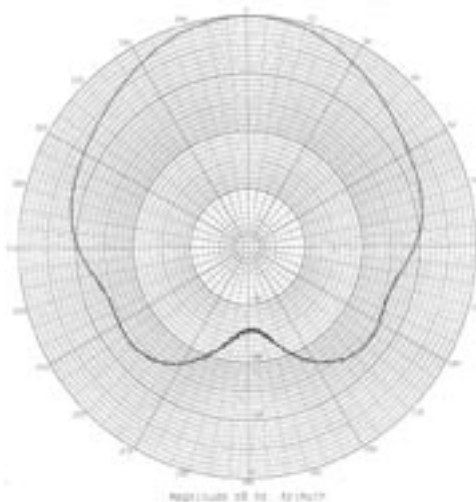
1. Use only the type and size of batteries mentioned in owner's manual.
2. Do not dispose of the batteries in a fire. The cells may explode. Check with local codes for possible special disposal instructions.
3. Do not open or mutilate the batteries. Released electrolyte is corrosive and may cause damage to the eyes or skin. It may be toxic if swallowed.
4. Exercise care in handling batteries in order not to short the battery with conducting materials such as rings, bracelets, and keys. The battery or conductor may overheat and cause burns.
5. Do not attempt to recharge the batteries provided with or identified for use with this product. The batteries may leak corrosive electrolyte or explode.
6. Do not attempt to rejuvenate the batteries provided with or identified for use with this product by heating them. Sudden release of the battery electrolyte may occur causing burns or irritation to eyes or skin.
7. When replacing batteries, all batteries should be replaced at the same time. Mixing fresh and discharged batteries could increase internal cell pressure and rupture the discharged batteries. (Applies to products employing more than one separately replaceable primary battery.)
8. When inserting batteries into this product, the proper polarity or direction must be observed. Reverse insertion of batteries can cause charging, and that may result in leakage or explosion. (Applies to product employing more than one separately replaceable primary battery.)
9. Remove the batteries from this product if the product will not be used for a long period of time (several months or more) since during this time the battery could leak in the product.
10. Discard "dead" batteries as soon as possible since "dead" batteries are more likely to leak in a product.
11. Do not store this product, or the batteries provided with or identified for use with this product, in high-temperature areas. Batteries that are stored in a freezer or refrigerator for the purpose of extending shelf life should be protected from condensation during storage and defrosting. Batteries should be stabilized at room temperature prior to use after cold storage.

Below are Radiation Patterns for the included N2400SMA1G Antenna (left) and BVS' optional DF corner reflector (right). The Antenna Under Test was measured against a 1/2 Wave Dipole, therefore; The Gain is measured in dBd (0 dBd = 2.14 dBi).



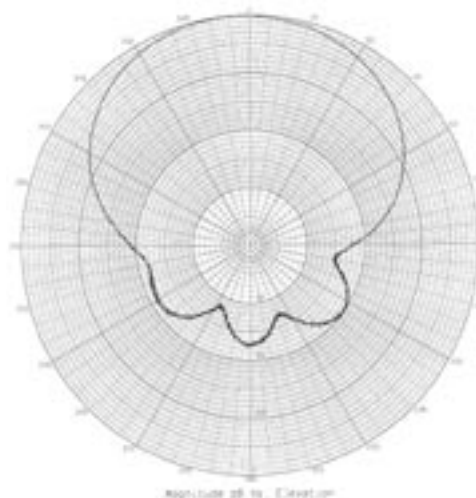
2.400 GHz Corner Reflector
FILENAME: 0076003.D00
FREQ: 2.400 GHz
RELATION: 0.00144

**BVS P/N DFA-001
&
DFA-000**



2.400 GHz Corner Reflector
FILENAME: 0076003.D00
FREQ: 2.400 GHz
RELATION: 0.00144

**BVS P/N DFA-001
&
DFA-000**



Cicada™

802.11 W-LAN TESTER

FHSS DRIVE-STUDY ANALYZER

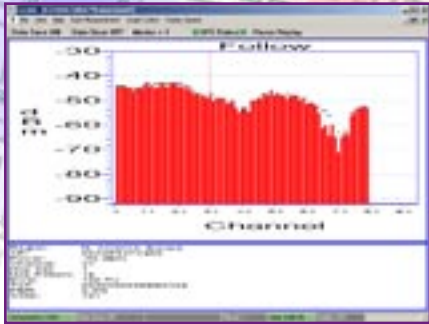
Cicada™ is a wireless receiver designed for sweeping and optimizing 2.4 GHz Local Area Networks for analysis in drive-studies. The instrument measures coverage of FHSS (Frequency Hopping Spread Spectrum) CDMA networks which operate on the **IEEE 802.11** standard allowing the user to measure and determine the AP (Access Point) location, PER (Packet Error Rate), SSID and RSSI signal levels aiding in locating the hub and access points throughout a drivetest. **Cicada™** provides measurements in real time and logs data for further post processing analysis. Users may detect and differentiate from narrowband multipath interferences using the provided internal 12-channel GPS receiver, drive-test vehicle, GPS antenna and serial output to a laptop PC.

RSSI✓

SSID✓

PER✓

GPS✓



- Measure 2.4 GHz coverage for frequency-hopping (FHSS) wireless networks (IF wideband 1 MHz) within the **IEEE 802.11** standard
- Internal 12-channel, 12 satellite GPS for support of most popular mapping/post processing applications
- Identifies MAC address and SSID of any FHSS Access Point
- Measures Packet Error Rate on selected APs
- Measures and displays RF power measurements: narrow band received signal strength (RSSI), total channel power
- Includes peak hold on display for accurate measurements
- Removable ATA Flash card (32 MB compact) stores collected data for post processing
- Removable battery pack (5 AA Ni-MH cells), also can be powered from 12VDC car cigarette lighter
- Built-in numeric keypad, backlit display with simple menu interface

The Cicada is just one of many exceptional design solutions from Berkeley Varitronics. Call us today for more information: (732) 548-3737 / Fax: (732) 548-3404 Internet: www.bvsystems.com E-mail: info@bvsystems.com



Cicada™

802.11 W-LAN TESTER



FHSS DRIVE-STUDY ANALYZER

BANDS SUPPORTED
RF SENSITIVITY
RSSI MEASUREMENT
TUNING INCREMENTS

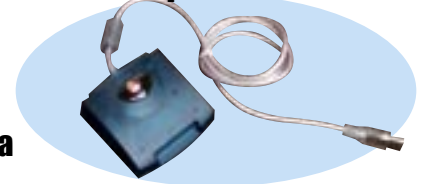
ISM: 2.402-2.480 GHz
-20 to -90 dBm
-30 to -90 dBm
1 MHz steps (IEEE 802.11 channels)

GENERAL SPECIFICATIONS

IF Bandwidth:	Wideband 1 MHz
Stability:	± 2.5 PPM Temp range 32° to 120 F°
Antenna:	SMA Female 50 ohm
Controls:	16 button keypad
Warm Up Time:	< 3 minutes
Power:	Internal battery pack (5 AA Ni-MH batteries) or 12VDC from car adaptor
Weight:	3 lbs.
Dimensions:	2" H x 4" W x 9" L (water resistant, high impact ABS plastic case)
Internal GPS (included)	Motorola 12-channel differential capable receiver
Serial Port	RS-232

Cicada includes all of the following accessories:

ATA compact flash reader



GPS active antenna (SMC male connector)



32 MB compact flash



Cicada includes a straight 3 dBi 2.4 GHz antenna (SMA Female 50 ohm), GPS mag-mount antenna, two removable battery packs (5 AA Ni-MH cells, 32 MB Compact Flash and 12V car power adaptor) charger, RS-232 cable all in a rugged carrying



carrying case



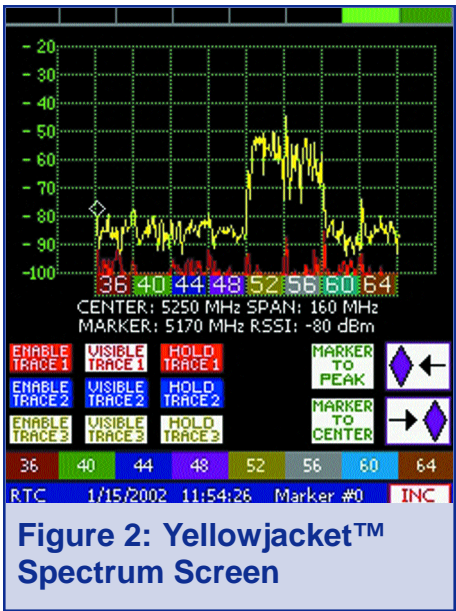
battery pack, charger & car cigarette power adaptor



Cicada Data Logger™ data supports output to Microsoft Excel® spreadsheets and MapInfo® post processing applications in Windows® environment.

Berkeley Varitronics Systems, Liberty Corporate Park, 255 Liberty Street, Metuchen, NJ 08840
Phone 732-548-3737 • Fax 732-548-3404 • www.bvsystems.com • E-mail: info@bvsystems.com

Excel and MapInfo are shown above and are the registered ® trademarks of Microsoft and MapInfo respectively.



BVS, Con’t from pg 48

security of the network.

Going into the AP Search screen, the unauthorized intruder can be located with the directional antenna. By fanning the antenna back and forth, the unauthorized MAC address would have a stronger RSSI value when in the direct path of the antenna. Once the direction is found, proceeding towards the MAC address would be produce even higher readings until the user is right on top of the intruder.

A game that the network hackers play is another denial-of service attack. Two clients set up within range of the network in question. They log

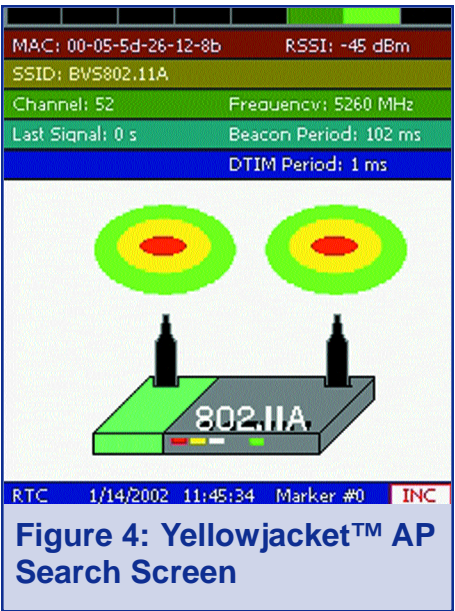


into their own network. They transfer high amounts of data as quickly as they can. This interferes and reduces throughput of any legal network traf- fic in the same area.

These culprits can be found in the same manner as the other ones. Use a directional antenna and the AP search screen to zero in on the intruder.

Performing site surveys is another important step in maintaining a wire- less network.

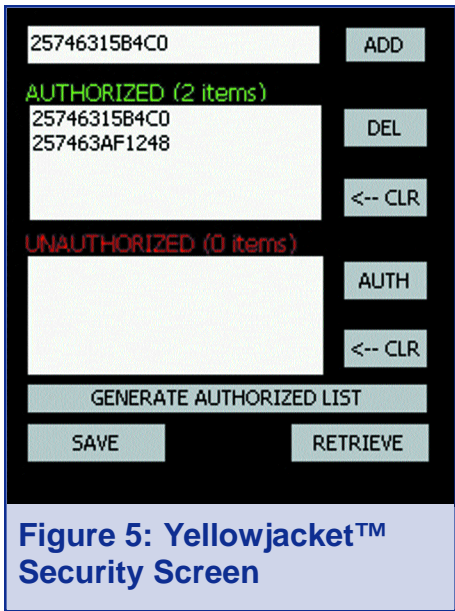
An associated software package that is an option with the YellowJacket is BirdsEye Site Initiator, Site Supervisor, and Site Investigator. This application package performs site sur-



veys and analyzes coverage issues in current network environments. The result is a printable color report of site coverage and interference.

There are three applications associ- ated with the BirdsEye™ package. The first is the Site Initiator applica- tion which runs on any Windows desktop or laptop. This program imports bitmapped floor plans for use in the site survey. Associated land- marks may be added to the drawing. These landmarks include AP’s, cord- less phones, microwaves, and text messages for different areas of the floor plan.

The finished site is saved and



imported into the Site Supervisor application. This application runs on the iPAQ Pocket PC that controls the YellowJacket hardware. The site is pulled up on the iPAQ. Then the user walks around the site, tapping the cur- rent point in the floor plan with the attached stylus. The YellowJacket per- forms a quick scan of all 8 channels at each point, recording any access points that are found. The user only has to make sure that enough sample points are taken throughout the site. A good rule of thumb is taking a point every 40-60 square feet.

After the survey has been complet-

BVS, Con’t on pg 60

BVS, Con't from pg 57

[illegible]

Figure 6: Yellowjacket™ Access Point MAC List

ed, the resulting data is transferred off of the iPAQ back onto the desktop or laptop. Here is where Site Investigator is used. This application will plot out the data from the Site Survey and prepare a visual and/or printed report of the coverage for the site in question. In the figure shown for Site Investigator, a typical analysis is shown. The different colors represent different access points.

As you can see from the diagram, access point markers were placed on the site using Site Initiator. The colors for the RSSI (Received Signal Strength Indicator) data for the associated access points get noticeably darker as they get closer to the markers of the actual location of the access points. The shade of the colors will get darker as the RSSI values increase. For example, a value of -40 dBm will result in a darker shade than a value of -80 dBm.

BirdsEye™ software with YellowJacket™ hardware combines to provide a network administrator with a tool to constantly monitor the wireless network environment. Coverage holes would show up in the resulting reports as colorless (white). Then the

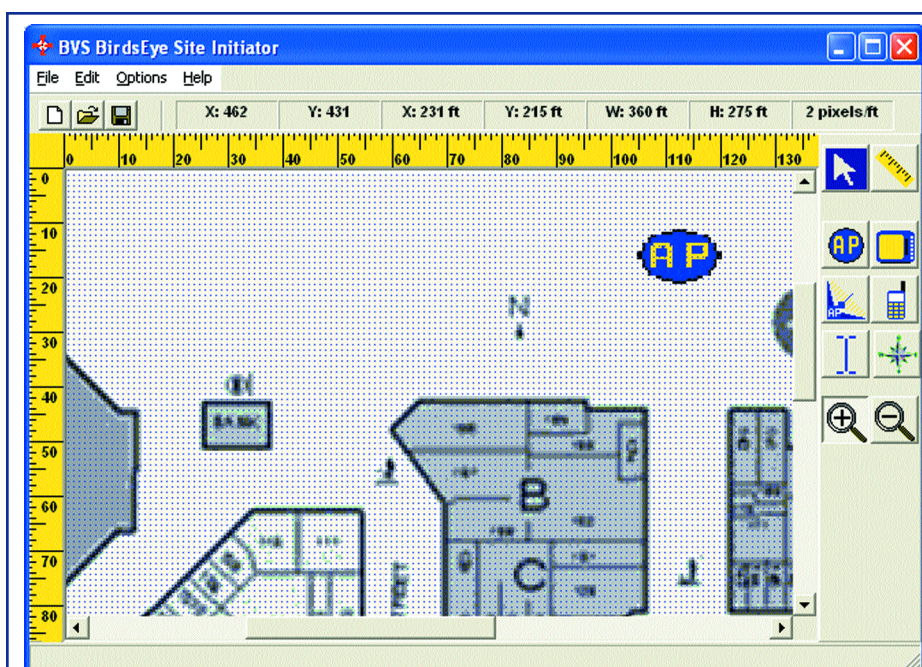


Figure 7: Birdseye™ Site Initiator

user could turn around and use the YellowJacket™ to determine why there is a network hole.

There could simply be a need for another access point. If it seems that a nearby access point should have covered the hole, outside RF interference could be the culprit. The user can take the YellowJacket™ spectrum screen to see if that is indeed the case.

There could be co-channel interference. BirdsEye™ can map the area by channel and it can be seen whether or not there are two adjoining access points that are using the same channel.

It could also be that certain clutter is preventing an access point signal from reaching the designated area. Clutter such as copper-lined walls could cause a signal to not propagate and simply reflect.

Combining BirdsEye™ with the

YellowJacket™ is one of the more effective tools in the battle against constantly changing RF environments for 802.11a networks.

There are a number of issues that must be considered when deciding how and when to deploy an 802.11a wireless network for home or corporate use. A test tool such as the YellowJacket™ is extremely useful in network setup and troubleshooting and can make an IT manager's daily work less strenuous as well provide a baseline archive of a wireless network's performance.

The key is being able to maintain your wireless network amidst constantly evolving security and environmental concerns. The right test tool helps reduce the amount of labor cost involved with network maintenance.

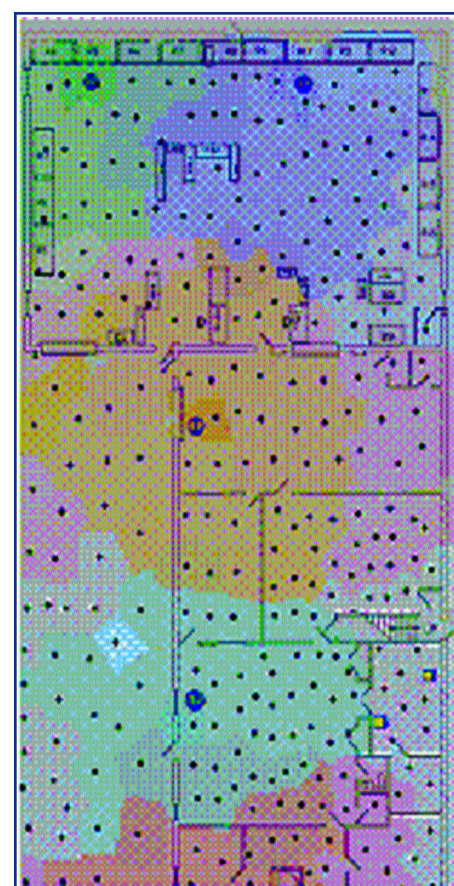


Figure 8: Birdseye™ Site Investigator

1. **BLUETOOTH** is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden.
2. **YellowJacket** and **BirdsEye** are trademarks of Berkeley Varitronics Systems, Inc. of Metuchen, NJ
732-548-3737
www.bvsystems.com
3. **iPAQ** is a trademark of Compaq Corporation

Take the W-LAN Test Challenge

A WLAN system's RF environment challenges designers, installers and administrators with planning re-use patterns, interference detection and system coverage in both installation and maintenance. These challenges are also found in seemingly more complicated cellular phone systems. Frequency re-use patterns, coverage mapping, interference from neighbors, locating unauthorized users and locating stolen equipment must be considered in addition to the standard PER and throughput metrics. Installing and maintaining a large WLAN system can rival the complexity of a cellular phone system. The author presents a comparison of equipment that is available to designers, installers and administrators to measure and overcome these challenges. Spectrum analyzers, standard WLAN cards and RF equipment specifically designed to measure 802.11 on the air are examined. Examples are drawn from the author's experience in designing WLAN test equipment; parallels are also drawn to methods and equipment that are found in the relatively mature cellular phone industry.

Introduction

The installation of an 802.11b Wireless LAN system to cover a large office setting can be very challenging and techniques found in cellular system engineering are often required. WLAN systems have the added complexity of operating in an unlicensed band where interference may not be under control of the WLAN manager, and the WLAN often operates in a harsher indoor RF environment.

Large WLAN installations will in many ways resemble a cellular phone system. Access Points (APs) are analogous to Base Stations. APs connect to the clients within their coverage area. APs have a "backhaul", Ethernet, which ties them together and into the network. Adjacent APs must be channelized so that they do not interfere with each other.

The most basic and readily available test tool is a laptop with an 802.11b card. The measurements vary with manufacturer, but the ability to measure signal strength and signal quality is common. These measurements are often relative, scaled 1–10. Specialized test tools are available that measure to traceable quantities, dBm, and have more types of measurements available. The tool or set of measurement tools should detect and measure interference, measure AP signal strength and Packet Error Rate (PER) from an AP.

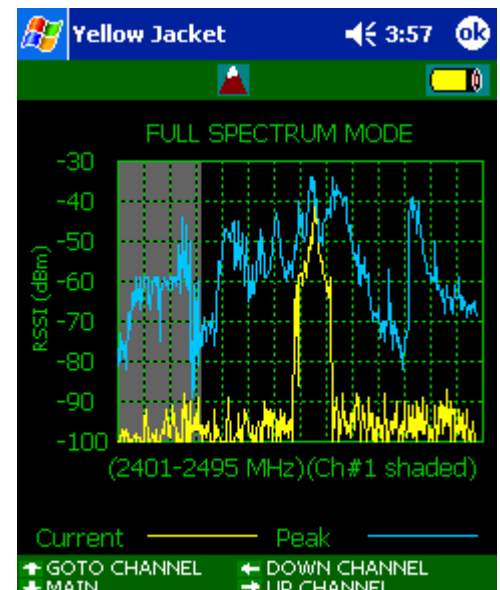
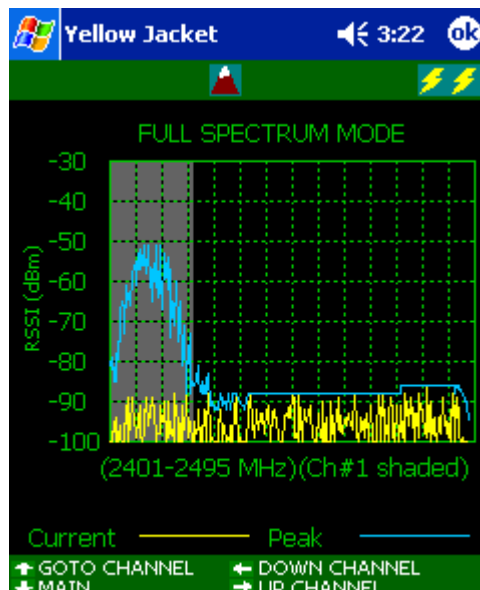
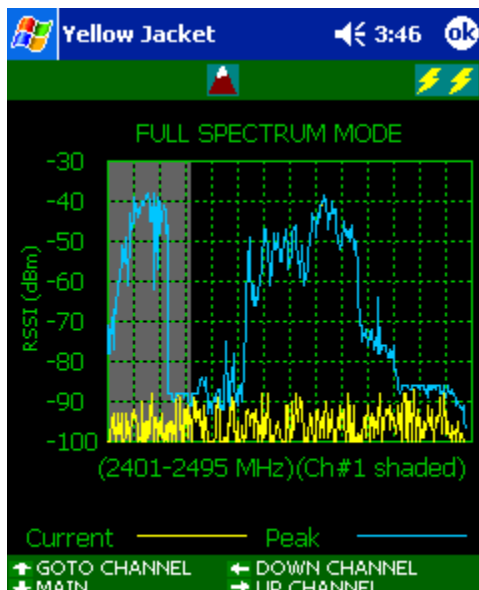
Measuring the Existing RF Environment for Interference

The place to start an 802.11 installation is to measure the existing interference. Microwave ovens, 2.4 GHz cordless telephones, other 802.11b WLANs, 802.11 frequency hoppers and bluetooth devices can all interfere with and degrade the performance of an 802.11b system.

Figure 1 illustrates a frequency sweep of an 802.11b channel with several types of common interference. A specialized WLAN test tool or spectrum analyzer is used to measure the interference and is moved throughout the coverage area of the WLAN system. A peak hold or logging of the data is essential to establish the "noise floor" that will be interfering with the WLAN in different areas. A more rigorous check would leave the instrument measuring for perhaps a day or more with data logging and then moved to different locations in the coverage area. The tool or spectrum analyzer should have a sensitivity of at least -90dBm.

The spectrum scan detects energy present in the band from all sources and is best to scan for all types of interference. A test tool or 802.11b card should also be used to demodulate any existing 802.11b interference on the air. Testing for 802.11b interference via demodulation yields more information about these interferers and is more sensi-

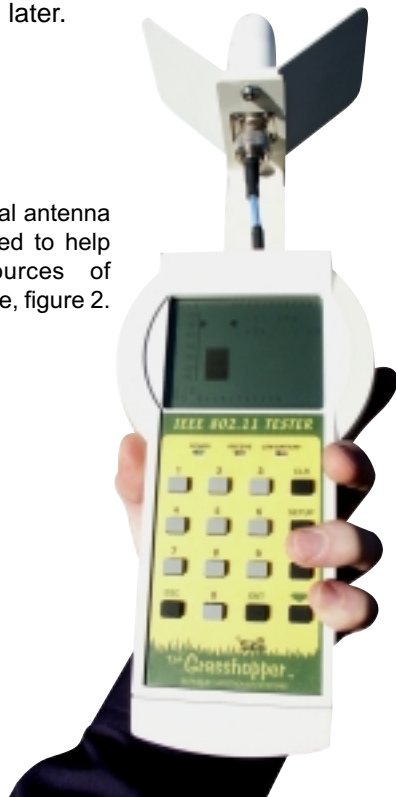
Figure 1 illustrates a frequency sweep of an 802.11b channel with several types of common interference. We see a frequency hopper (left), an 802.11b access point (center) and a microwave oven (right).



tive.

A directional antenna can be used to help locate sources of interference, shown in figure 2. As many interferers should be eliminated as possible. Microwave ovens may be moved, and bluetooth devices and cordless phones can be banned from the office. Some interference may be impractical to eliminate. A neighboring business may also have an 802.11 system or some other interfere. In these areas, plan to have a higher density of APs, spend more time planning channelization and use some special techniques that are discussed later.

A directional antenna can be used to help locate sources of interference, figure 2.



Measuring the Coverage of an Access Point

The coverage area of an Access Point is experimentally found by simply locating the AP at a candidate site and measuring the signal strength and PER with a test tool. A spectrum analyzer could be used, but it can only measure signal power in the channel; and this measurement may also include interference, other Access Points other than the one being measured or even energy from a different AP on an overlapping adjacent channel. A test tool with demodulation is desirable because it can measure the signal strength of the AP coverage under test and the signal to noise is indirectly measured by the PER.

A typical signal level required for adequate coverage is around -80 dBm or stronger. This level includes some margin for typical interference and signal fading. The signal strength required will be greater in areas with interference levels greater than -90 dBm. Figure 3 tabulates typical signal strengths required with varying amounts of interference.

BER	Min Eb/No Required	Eb (Min) required for thermal noise = -100 dBm	Eb (Min) required for interference = -90 dBm
10 ⁻⁴	10	-90 dBm	-80 dBm
10 ⁻⁵	12	-88 dBm	-78 dBm

Note: Figures estimated from Harris HFA3861B data sheet.

Figure 3: Required Received Power (Eb) for various Bit Error Rates (BER) and Noise/Interference Levels (NO).

Measuring Coverage and Co-Channel System Interference

After testing AP coverage in several locations, the APs required for adequate coverage and overlap can be located. This may require an educated estimate or specialized propagation software. Neither method is perfect, so additional APs may need to be added or locations adjusted with testing.

Channelization is required so that neighboring APs do not interfere with each other. Figure 4 depicts a typical hexagonal frequency reuse pattern for three frequencies. For continuous coverage, APs must overlap, and the frequencies in these overlap areas should be different for each AP to avoid interference in these overlap areas.

The installation site must be surveyed to insure that all areas have sufficient signal strength, good PER from at least one AP and is without significant co-channel interference. Co-channel interference is when energy on the same channel is received from different APs. Co-channel interference should be at least 15dB weaker than the stronger AP. This survey requires that 3 frequencies be measured for a reuse pattern of 3, figure 5.

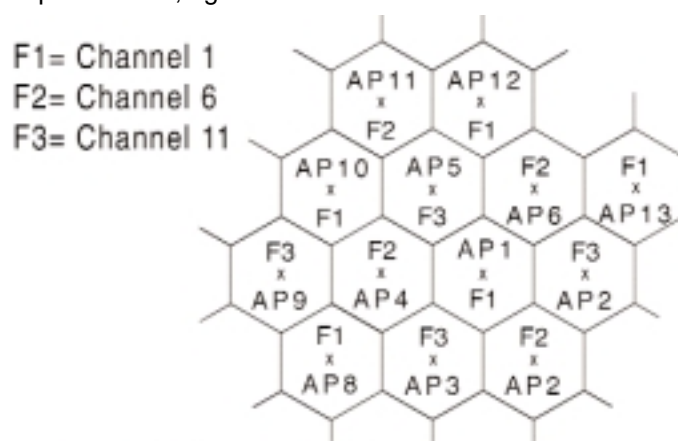


Figure 4: Coverage layout for 3 frequencies. Three frequencies were chosen because there are only 3 non-overlapping channels available for 802.11b in the U.S.. Co-channel interference near AP1 can be received from other APs transmitting on the same frequency (AP8, AP10, AP12,...).

Fixing Problem Areas

A site survey or the operation of the WLAN itself will probably reveal areas where coverage is not adequate. Adding or moving an AP closer to an area with high interference will boost the signal level. Directional antennas such

as corner reflectors can direct more energy to your coverage area and reduce the amount of received interference. This is a useful technique for existing with a neighboring WLAN system; use directional antennas on the AP to direct coverage into the coverage area and to reduce interference received from outside the coverage area. A directional antenna may also be used at the client.

is a plus), PER, and scanning of multiple channels is a plus. Best used to measure 802.11b interference, coverage of APs, channelization and co-channel interference.

Directional antenna: Can be used to locate interference or an unauthorized user.

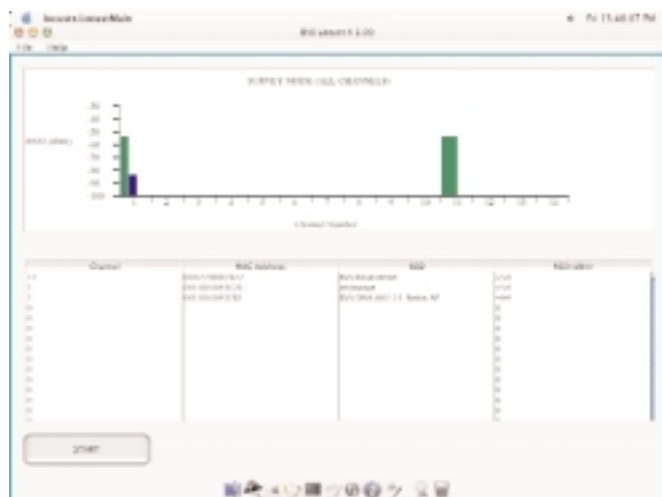


Figure 5: Site survey showing multiple frequencies and multiple APs. Note the co-channel interference on channel 1.

Keep the tools ready for Problems

Periodic checks and monitoring can avoid problems, but be prepared for a client with little or no throughput. Tools can quickly verify the RF link for signal level, PER and interference. The tools can help debug a new interfering AP a neighbor has set-up or to find the antenna that has been knocked over.

A directional antenna and receiver are very useful for locating interference or even an unauthorized user or stolen equipment. The directional set-up shown in figure 2 can be used to direction find a node with a specific MAC address.

Summary of tools and techniques

A microwave oven, a client with slightly weak signal strength or another interferer with short transmissions should not bring down the network or significantly degrade performance. The guidelines presented here are conservative, aim for them when planning and setting up a network. An outage or a drop in performance will justify the cost of WLAN RF test tools.

A laptop with an 802.11b card is a good test tool and may be adequate for small installations and maintenance of small systems where interference is not significant. For larger installations and maintenance or in areas with significant interference, a tool or set of tools with the following characteristics is recommended:

Spectrum Analysis: sensitivity at least -90dBm, with peak hold, and data logging is a plus. Best used to check for and measure interference of any type.

Demodulation Analysis: Signal strength (measured in dBm