





Contents

GETTING STARTED.....	2
MAIN SCREEN.....	2
MENU SCREEN.....	3
SET CHANNEL.....	3
SETTINGS.....	3
SELECT ALARMS.....	4
REVIEW LOG.....	4
ADJUST CONTRAST.....	5
HORNET INFO.....	5
HORNET OPERATION.....	5
HORNET PC INTERFACE SOFTWARE OPERATION.....	6
NETWORKING BASICS.....	12
DSSS INTERNATIONAL CHANNEL CHART.....	13
GLOSSARY OF ACRONYMS.....	14
GENERAL SAFETY.....	15
ANTENNA RADIATION PATTERNS	
HORNET DATA SHEET	

The **Hornet™** is a self-contained 802.11b WLAN Monitoring System that detects and responds to unauthorized access attempts and sources of channel interference on any local DSSS network. By continually running through a checklist of valid MAC addresses, Hornet™ is able to instantly identify unauthorized “hackers” and distinguish them from valid AP traffic on the network. Hornet is a wireless instrument but also contains a RS-232 serial port for wired updating and monitoring as well as an AC connection for secure monitoring 24 hours a day, 7 days a week.

Hornet includes a simple 2.4 GHz threaded antenna that screws right into the back / top of the unit. Additional antennas may be ordered from BVS through BVS. The antenna connector (middle) is an SMA Female 50 ohm. The provided antenna easily screws and unscrews from this connector. Be sure to unscrew antenna when transporting the Hornet.

Power is applied when the unit is plugged into the included transformer. There is no power switch. Simply unplug the power connector in the back to power down the unit.



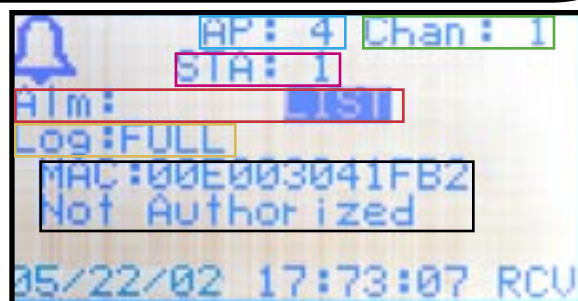
GETTING STARTED

Operation of the Hornet is straightforward. Power the unit up and turn the rotary knob to scroll through menu options and push in the knob to make the selections. The startup screen will display briefly followed by the main screen.



MAIN SCREEN

This is the main measurement screen used for monitoring APs or Access Points. The window to the upper right displays the received signal multipath in realtime of the currently selected AP. Any AP listed under the AP Address window is recognized as an IEEE 802.11b address. 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.

AP: indicates the Access Point number on list

Chan: 1 indicates channel being scanned (1-14)

STA: indicates STATION or card on list

Alm: indicates alarms being triggered

Log: indicates status of review log

MAC: indicates current MAC address and status

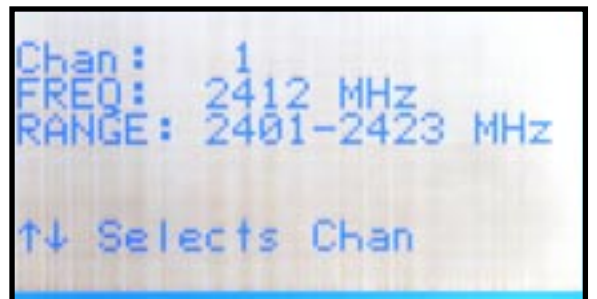
MENU SCREEN

This screen allows access to all Hornet function screens. Use the rotary knob to highlight the selection and then push in the knob to choose that selection. Select EXIT at anytime to access the Main screen.



SET CHANNEL

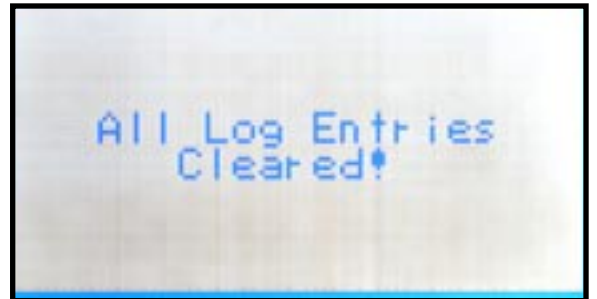
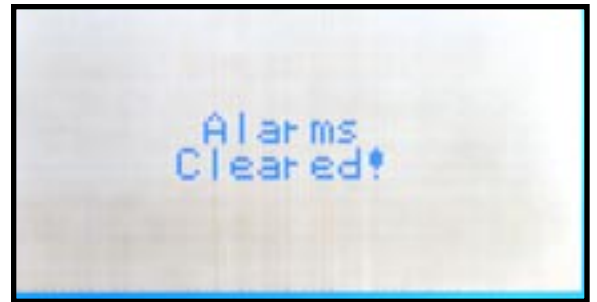
This selection allows the user to scroll through any of the 14 802.11b channels. The channel screen indicates all available channels and their corresponding frequencies. Refer to channel chart towards the end of this manual. Use the knob to scroll through channels and to make a specific channel selection.



SETTINGS

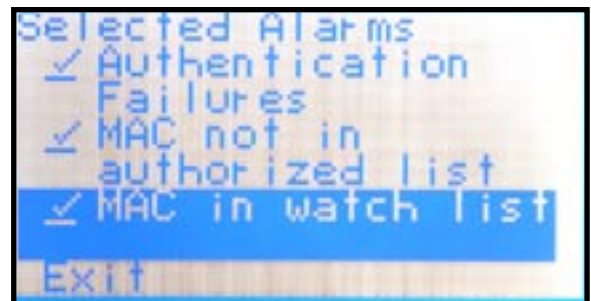
This screen allows the user to clear the alarm settings and log data that is stored internally in the Hornet. Simply select the category to be erased and push in the knob. The corresponding screen will follow indicating that the settings have been erased.





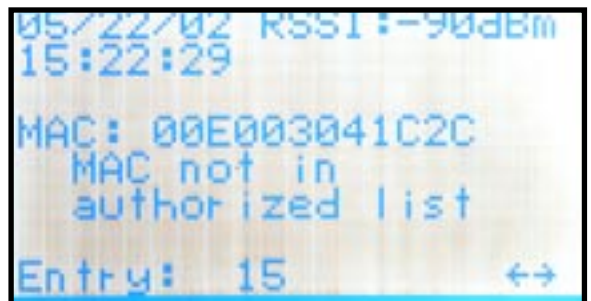
SELECT ALARMS

This screen lets the user select one or more alarms to be set. The **Authentication Failures** alarm alerts the user when an unsuccessful authentication attempt has been detected. The **MAC not in authorized list** alerts when a MAC is found that doesn't exist in the current authorized list. The **MAC in watch list** alerts when a MAC is found that is in the current watch list. Use the knob to check one, two or all three of these alarms. Chose EXIT to return to the Main Menu at anytime.



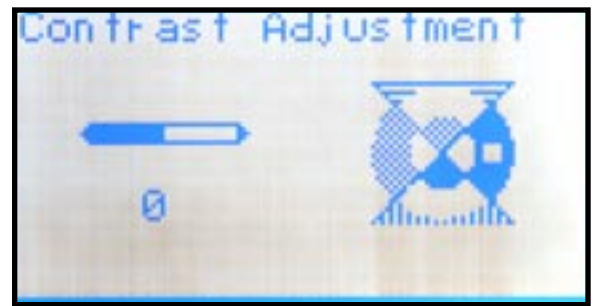
REVIEW LOG

This screen allows the user to review any alarm triggered as conditioned by the alarm settings. The log lists the date, RSSI signal strength, time of day, MAC address, specific alarm triggered and review log entry number. Any of these log entries may be accessed by scrolling with the rotary knob. Up to 2500 logs may be stored internally in the Hornet before memory runs out.



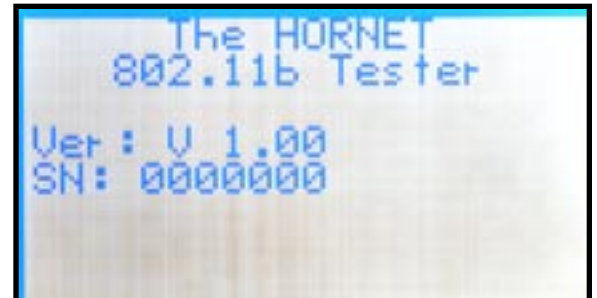
ADJUST CONTRAST

This screen allows adjustment of the LCDs display contrast. Use the knob to dial in the best looking contrast level and push in the knob when finished.



HORNET INFO

This screen displays the Hornet's current firmware and serial number. Push in the dial to return to the previous menu.



HORNET OPERATION

Hornet does not require a PC to operate in its basic mode which will only detect authentication failures. To utilize Hornet as a powerful guardian over an 802.11b network of access points, a PC with serial connectivity must be used in order to monitor and edit MAC lists for the Hornet to identify and verify.

Connect the supplied serial cable to your PC and the other end to the Hornet. Run the included Hornet software and choose the appropriate COM port. If Monitor is chosen from the Main PC screen, nothing on the Hornet's display will change. If the user chooses Data Retrieval or Mac Lists, the Hornet will lock out controls from the rotary knob and display a PC Control screen. When this screen is displayed, data may be downloaded from or uploaded to the Hornet via the PC. Please continue reading this manual for complete features included in your Hornet PC Interface Software.



HORNET PC INTERFACE MANUAL

PC Requirements

Windows 98, Me, 2000, or NT 4.0 operating system

Pentium II

500 MHz

64MB RAM

100MB free on Hard Drive

800x600 pixel resolution

CD-ROM (for installation)

Free RS-232 serial port between COM1: and COM4:

Overview

The Hornet PC Interface is a companion tool to the BVS Hornet. This tool facilitates the processing of different MAC lists as well as providing other utility features. There is also a reporting tool that allows the user to print out a report of information retrieved from the Hornet. The following sections outline the features of the interface tool.

Installation and Setup

Installation and setup of the PC interface to the Hornet is straightforward and takes only a couple of minutes. There is a software CD (usually red) that says "Software Installation". Place this CD in your CD-ROM drive. After a few seconds (up to 20-30 seconds), a setup application will appear. If not, run autorun.exe from the root directory of the CD.

Click on the button for "Install Windows Software/Drivers". Choose the Hornet button to install the Hornet PC Interface. Follow the instructions. The default directory is "c:\hornet".

After installation is complete, connect the Hornet to the PC using the serial cable provided.

Startup

To start the Hornet software, choose "START/PROGRAMS/BVS/Hornet PC Interface". The main screen will appear as shown in Figure 1.

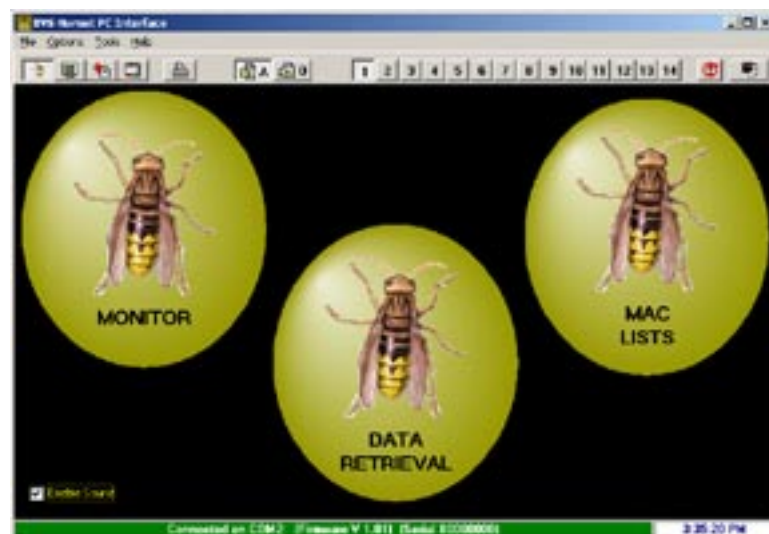
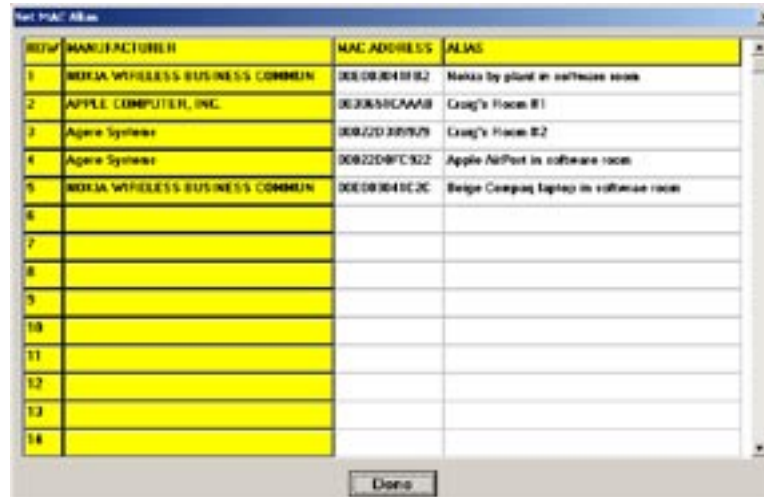


FIGURE 1 – HORNET MAIN SCREEN

Alias List

The alias list is an anchor repository of MAC addresses that can be used to drop into the authorized and watch lists to be sent to the Hornet. The alias list can be accessed by clicking on the button in the tool bar that contains an icon of a window with a tag. The screen appears as shown in Figure 2.



REF#	MANUFACTURER	MAC ADDRESS	ALIAS
1	NOKIA WIRELESS BUSINESS COMMUN	000000040002	Nokia by phone in software room
2	APPLE COMPUTER, INC.	000000000000	Craig's Floor #1
3	Agere Systems	000000000000	Craig's Floor #2
4	Agere Systems	000000000000	Apple Airport in software room
5	NOKIA WIRELESS BUSINESS COMMUN	000000040002	Beige Compaq laptop in software room
6			
7			
8			
9			
10			
11			
12			
13			
14			

FIGURE 2 – ALIAS SCREEN

Enter MAC addresses in the MAC address column. As the MAC address is entered, the manufacturer of the AP/Station will appear. After entering the MAC address, enter the alias name of the AP/Station. This alias can be used to identify the piece of equipment. It is more useful than the SSID in that it can describe the piece of equipment and its location, whereas the SSID only describes the network to which the piece of equipment is attached. Click 'DONE' to save the list.

Changing Channels

To tell the Hornet to monitor a different channel, press any of the numbered buttons between 1 and 14 on the tool bar. Each associated button will tell the Hornet to go to that channel.

MAC List Screen

The MAC List screen displays three different list types. The 'On Air' list shows the list of MAC addresses that the Hornet has seen since the list was cleared last. Press the 'GET FROM HORNET' button to retrieve the list from the Hornet. Press the 'CLEAR ON HORNET' to clear the current 'On Air' list. The entries on this list can be used to enter into the other two lists, as will be discussed.

The 'Authorized List' is a list of MAC addresses that are considered valid and no threat to the security of the network in question. The buttons associated with this list allow the user to import and export a list file, send the data to/from the Hornet, and clear the list as displayed. Pressing the 'CLEAR LIST' button only clears the list on the PC. To clear the list on the Hornet, the user must clear the list and then press the 'TO HORNET' button.

MAC addresses may also be pulled in from either the alias list or the on-air list. If the 'A' button is down on the toolbar, data will be pulled from the alias list. If the 'O' button is down, then the data can be pulled from the on-air list.



FIGURE 3 – MAC LIST SCREEN

To retrieve data from the alias or on-air list, right-click on a yellow section of the list box. A pop-up box will appear with a list of MAC addresses to choose as shown in Figure 4. Choose these addresses by placing a checkmark next to each address wished to be inserted. Then press the 'Add Selected' button. The checked MAC addresses will be appended to the current data in the list.



FIGURE 4 – MAC SELECT POP-UP BOX

The 'Watch List' has the same functionality as the 'Authorized List'. The difference is that the watch list tells the Hornet to trigger an alert whenever any MAC address in the list has been detected.

Log (Data Retrieval) Screen

The log screen (as shown in Figure 5) will display the log entries in the Hornet. The log screen is obtained by pressing the 'DATA RETRIEVAL' button from the main screen or by pressing the button on the toolbar with the icon of a piece of paper and an arrow. Press the 'FROM HORNET' button to retrieve the log. Entries are in a tree format separated out by alarm type and then MAC address. The level below the MAC address shows the time and date of the log entry as well as the RSSI value of the MAC address.



FIGURE 5 – LOG SCREEN

Real-Time Monitor Screen

The real-time monitor screen can be chosen by the leftmost button on the main screen or by choosing the button with the monitor icon on it from the toolbar. The screen is shown in Figure 6.

The monitor collects alarm data real-time from the Hornet. It displays alarm data in a tree-style format, using alarm type as the top level. The next level is by MAC address and the lowest level is the date/time stamp and the RSSI value of the last occurrence. Only one entry will be made per alarm per MAC address. The timestamp and RSSI will adjust to the last occurrence of the alarm.

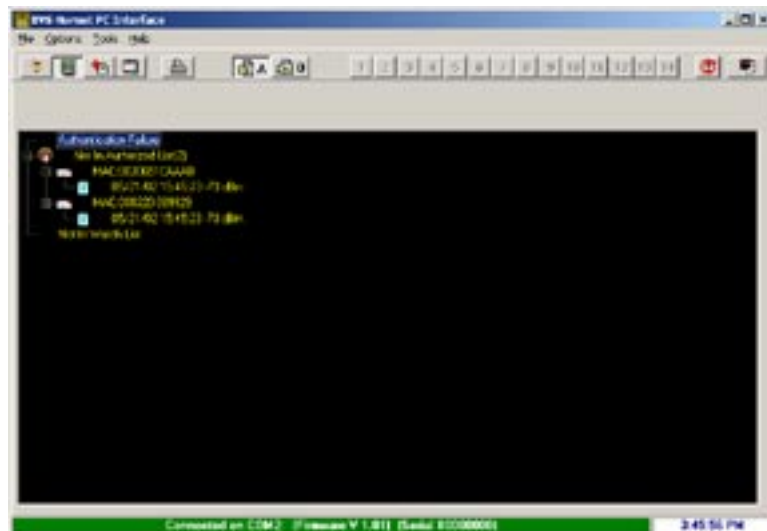


FIGURE 6 – MONITOR SCREEN

Options

There are utility options that can be chosen by selecting the 'OPTIONS' menu item.

SET DATE/TIME: Select the correct date and time to be set on the Hornet.



FIGURE 7 – SET DATE/TIME

SET ALARM MASK: Select the alarms to be used on the Hornet. The 'authentication failures' alarm alerts the user when an unsuccessful authentication attempt has been detected. The 'MAC not in authorized list' alerts when a MAC is found that doesn't exist in the current authorized list. The 'MAC in watch list' alerts when a MAC is found that is in the current watch list.



FIGURE 8 – SET ALARM MASK

CLEAR LOG: Clears the log stored on the Hornet.

RESET: Pressing the reset button on the toolbar reboots the Hornet.

Tools

Under the tools menu is an option for performing a MAC lookup. Choosing this option pulls up the dialog as shown in Figure 9.



FIGURE 9 – MAC Lookup Dialog

Enter a MAC address and then press the 'LOOKUP' button. If it is a valid MAC address, the manufacturer of the piece of equipment with the associated MAC address will be shown. Each manufacturer is assigned a prefix to be used with MAC addresses that consists of the first 6 hex digits.

Reports

Pressing on the printer icon button in the tool bar results in the report dialog appearing. Choose the appropriate options for types of data to produce in the report. When pressing the 'PRINT' button, the chosen report will be sent to the printer. Choose Save to File to create a Hornet.RPT file.

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.

DSSS INTERNATIONAL CHANNEL CHART

Channel Number	Frequency GHz	North America	Europe	Spain	France	Japan MKK
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

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
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.

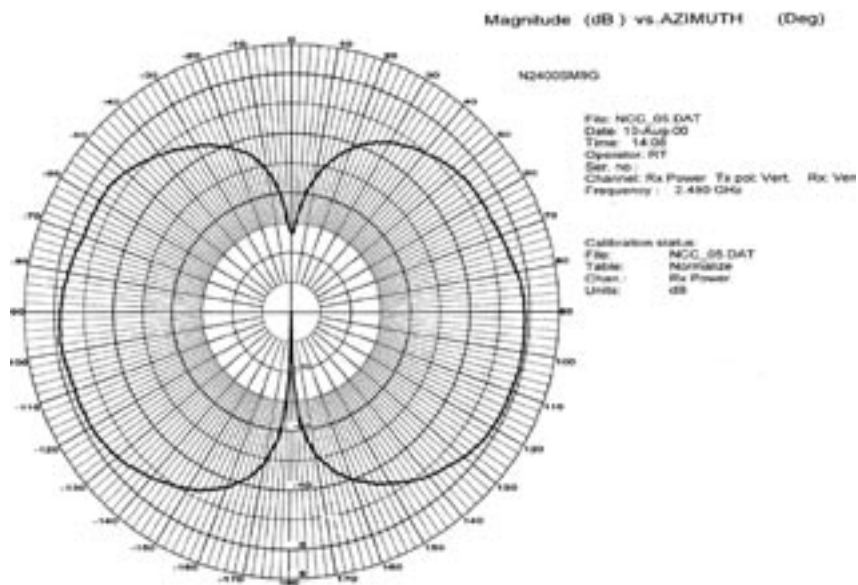
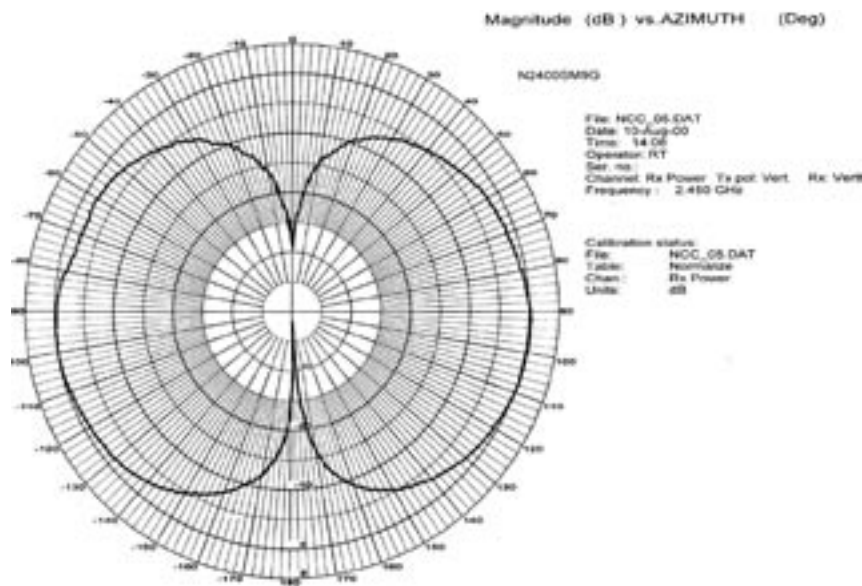
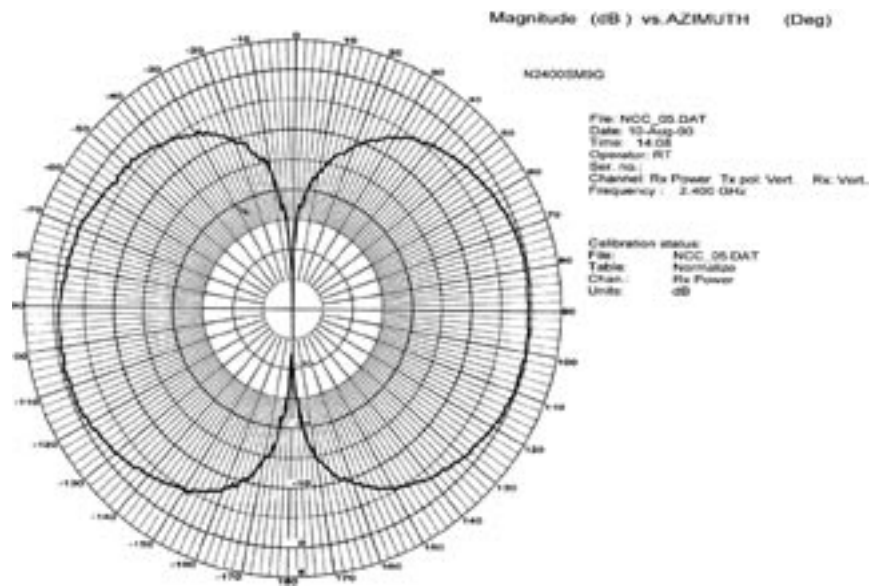
4. Use caution when installing or modifying telephone lines.

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.

The following are Radiation Patterns for the included N2400SMA1G Antenna. The Antenna Under Test was measured against a 1/2 Wave Dipole, therefore; The Gain is measured in dBd (0 dBd = 2.14 dBi).



Hornet™



802.11b WLAN MONITORING SYSTEM

The Hornet™ is a self-contained 802.11b WLAN Monitoring System that detects and responds to unauthorized access attempts and sources of channel interference on any local DSSS network. By continually running through a checklist of valid MAC addresses, Hornet™ is able to instantly identify unauthorized "hackers" and distinguish them from valid AP traffic on the

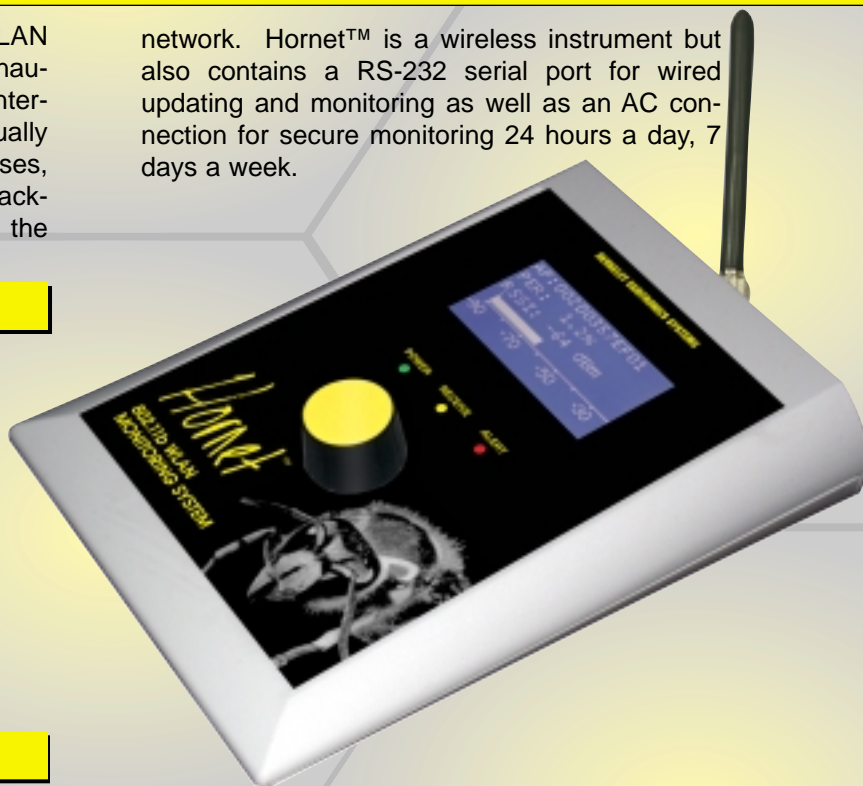
network. Hornet™ is a wireless instrument but also contains a RS-232 serial port for wired updating and monitoring as well as an AC connection for secure monitoring 24 hours a day, 7 days a week.

KEY APPLICATIONS:

- Wireless monitoring of WLAN traffic
- Guard & Secure any DSSS WLAN
- Identify unauthorized MACs (Aps & STAs)
- Channel interference detection
- AP signal strength analysis
- Channel allocation post-processing analysis

FEATURES:

- Fast channel scan for immediate detection and identification of all local APs, STAs and MACs
- RS-232 connection for remote monitoring, download/upload MAC lists and data collection to any PC
- Audible and visible ALERT status warns of unauthorized users in the area
- Real-time clock built in for time and date stamp of all logs
- Built-in graphic backlit LCD and simple rotary knob menu navigation and selection
- Customizable MAC filters set by user including alert upon specific MAC detection



SECURE YOUR WLAN NOW

Hornet is just one of many exceptional design solutions from Berkeley Varitronics Systems. Call us today for more information:

(732) 548-3737 / Fax: (732) 548-3404

Internet: www.bvsystems.com

Email: info@bvsystems.com





SPECIFICATIONS

BANDS SUPPORTED	ISM: 2.400-2.495 GHz
RF SENSITIVITY (Wide Band)	-20 to -90 dBm
RSSI MEASUREMENT (Narrow Band)	-30 to -90 dBm @ 343.75 kHz resolution bandwidth
TUNING INCREMENTS	Tunes 11 USA channels & 3 international channels

PACKET PREAMBLE DEMODULATOR and ANALYZER:

Multipath Measurement and Graphical Display

CORRELATED POWER MEASUREMENTS:

Correlated Power (dBm)

Correlated Power to Total Power Ec/Io (dB)

Total Channel Power Measurement

RATIO

-30 dBm : -100 dBm

0 dB : -10 dB

-20 dBm : -90 dBm

GENERAL SPECIFICATIONS

RF Sensitivity:	>-95 dBm
Frequency Range:	2.400-2.485 GHz (all 14 channels)
IF Bandwidth:	Wideband 22 MHz @ -3dB
Stability:	± 2.5 PPM Temp range 32° to 120 F°
Antenna:	SMA Female, 50 ohms impedance
Controls:	Rotary, push button knob
Warm Up Time:	< 3 minutes
Power:	110 VAC @ 0.5 Amps
Weight:	3 lbs.
Dimensions:	2" H x 4" W x 9" L (water resistant, high impact ABS plastic case)

NETWORK SECURITY:

Enter valid APs manually
Generate valid AP list automatically
Upload AP list from PC
Flag invalid APs as "suspect"

UNAUTHORIZED

