

Mantis

manual version 1.4





Contents

GETTING STARTED.....	2
MAIN SCREEN.....	2
PRODUCT INFORMATION.....	3
SEARCHING.....	3
ACQUIRING NAMES.....	3
AVAILABLE DEVICES.....	3
SELECTED DEVICE.....	4
SERVICE.....	4
MEASUREMENT SELECTION.....	4
SIGNAL STRENGTH.....	5
PER.....	5
OPTIONS.....	5
USING A DIRECTION FINDING ANTENNA.....	6
BATTERY TIPS.....	7
NETWORKING BASICS.....	8
GLOSSARY OF ACRONYMS.....	10
BLUETOOTH GLOSSARY.....	11
GENERAL SAFETY.....	24
ANTENNA RADIATION PATTERNS	
MANTIS DATA SHEET	

Mantis™ is a handheld, wireless transceiver designed specifically for installing, sweeping and verifying Bluetooth devices and parameters. The instrument identifies all nearby Bluetooth devices and their status in dBm.

Mantis uses common AA battery cells found in any convenience store. Ni-Cad, Alkalines, Ni-MH and Li-Ion cells may all be used. **Mantis** does require 4 AA cells with at least 1500 mAh per cell. BVS supplies 8 Ni-MH battery cells and a Ni-MH charger to get users working right out of the box. Ni-MH cells are recommended for best performance from your **Mantis**. See the charger's instructions and battery tips in this manual.

Mantis 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 **Mantis** rest the power switch and antenna connector. The power switch is a simple two way toggle switch. 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 **Mantis**.



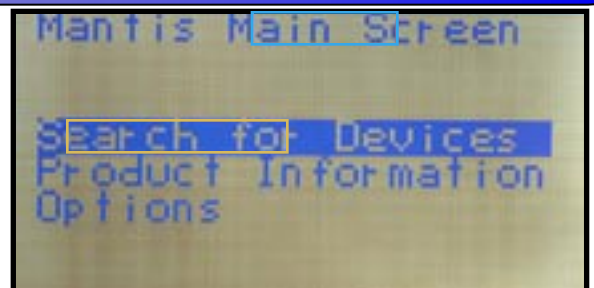
GETTING STARTED

Operation of the **Mantis** is straightforward. Insert 4 fresh battery cells into removable pack. Close back up and power on the **Mantis**. The **Mantis** will display the startup screen followed by the Main Screen.



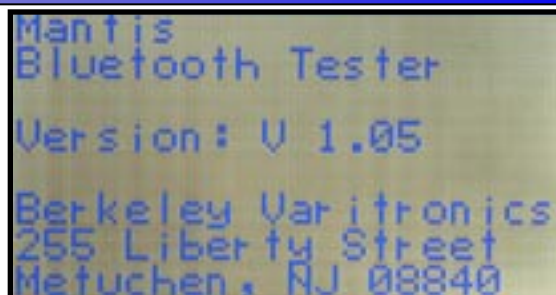
Mantis Main Screen

Use the UP/DOWN arrows to scroll through menu selections. Push the RIGHT arrow button to make a selection and push the LEFT button to move back one previous screen.



Product Information

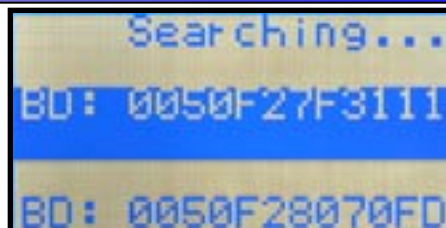
This screen displays the current version of Mantis that you are using. Visit www.bvsystems.com to find out if you have the latest Mantis version.



Mantis
Bluetooth Tester
Version: V 1.05
Berkeley Varitronics
255 Liberty Street
Metuchen, NJ 08840

Searching...

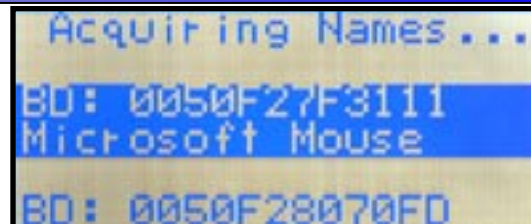
From the Main Screen, select Search for Devices and press the RIGHT arrow key. This screen will appear. Mantis takes approximately 10 seconds for a complete scan of nearby Bluetooth devices. The devices found will be listed by their ID numbers first.



Searching...
BD: 0050F27F3111
BD: 0050F28070FD

Acquiring Names...

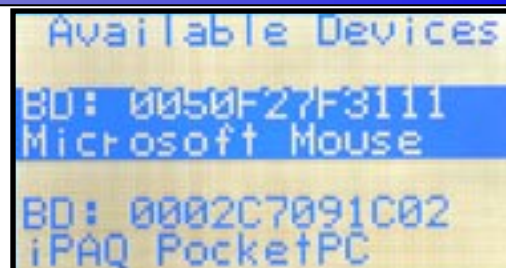
After acquiring the ID of each device, Mantis will go back and list the name given to each device (up to 20 characters).



Acquiring Names...
BD: 0050F27F3111
Microsoft Mouse
BD: 0050F28070FD

Available Devices

After the 10 second scan, Mantis will list all Bluetooth devices found that are currently powered and operational. Use the UP and DOWN arrow keys to scroll through the list of devices. Mantis creates a list of up to 16 devices at once. Once you have selected the device you wish to verify, press the RIGHT arrow key to select that device. Press the LEFT arrow key at anytime to return to the previous menu.



Available Devices ↑
BD: 0050F27F3111
Microsoft Mouse
BD: 0002C7091C02
iPAQ PocketPC

Selected Device

This screen provides basic information about the device including the ID number, the name and the class. Class is an attribute assigned by the Bluetooth standard. Here are some common classes:

Class: Computer
Desktop

Class: Computer
Handheld

Class: Peripheral
Keyboard

BD: 0050F27F3111
Microsoft Mouse
↓
Class: Peripheral
Pointing

Use the DOWN arrow key to see Service information for the selected Bluetooth device.

Service

This screen provides basic Service information regarding the nature and capabilities of the selected Bluetooth device. An x to the left of any category identifies it as a known Service. Use the DOWN arrow key to see more Service information for the selected Bluetooth device.

BD: 0050F27F3111
Microsoft Mouse
Service: ⬆
x Lfd Discovery
- Positioning
- Networking
- Rendering
- Capturing

Service (continued)

You may use the UP arrow key to scroll back up to the top of the Service list. Use the LEFT arrow key to return back to the Main Screen. Use the RIGHT arrow key to see the Signal Strength of the selected Bluetooth device.

BD: 0050F27F3111
Microsoft Mouse
Service: ⬆
- Object Transfer
- Audio
- Telephony
- Information

Measurement Selection

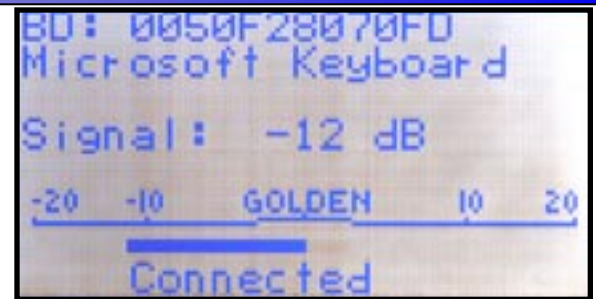
Select the type of measurement you wish to make using the UP or DOWN arrow key. After you select either RSSI or PER, use the RIGHT arrow key to continue to the desired measurement screen.

Measurement Selection

RSSI Test
PER Test

Signal Strength

This screen indicates the current received signal strength of the selected Bluetooth device in dB on a scale from -20 to 20 dB. The orange receive LED on the front of the Mantis will blink whenever any data is received. Use the arrow keys to return to the Main Screen or perform another Search.



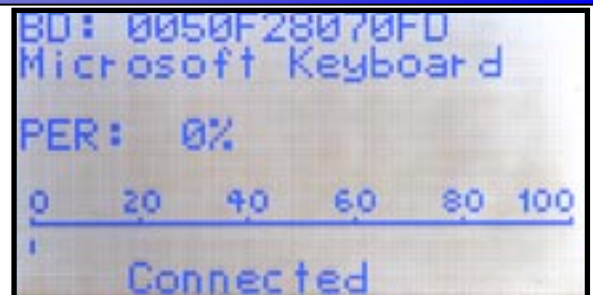
Note: A transceiver that wishes to support power-controlled links must be able to measure the strength of the received signal and determine if the transmitter on the other side of the link should increase or decrease its output power level. A Receiver Signal Strength Indicator (RSSI) makes this possible.

The RSSI measurement compares the received signal power with two threshold levels, which define the Golden Receive Power Range. The lower threshold level corresponds to a received power between -56 dBm and 6 dB above the actual sensitivity of the receiver. The upper threshold level is 20 dB above the lower threshold level to an accuracy of ± 6 dB.

(BLUETOOTH SPECIFICATION Version 1.1)

PER

This screen indicates the PER (Packet Error Rate) of the selected Bluetooth device from 0 to 100 percent. A PER of 0% indicates optimal transmission of Bluetooth data packets.

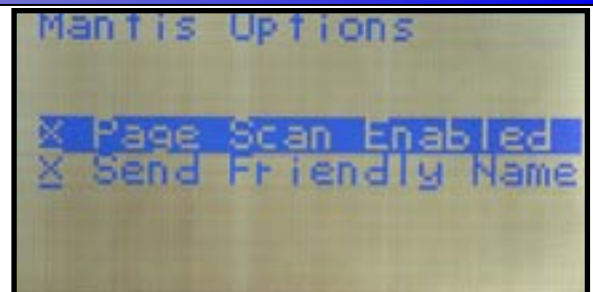


OPTIONS

Mantis provides two privacy options. To enable or disable an option, use the UP or DOWN arrow keys to select the option and the RIGHT arrow key to toggle the enabled "X" on or off. The LEFT arrow key returns to Main screen.

Page Scan Enabled

When enabled, Mantis answers page scans from other Bluetooth devices. Page scans provide the Bluetooth



MAC address and information about features the device has. Disabling this option prevents the Mantis from being seen by other Bluetooth devices. The default is enabled.

Send Friendly Name

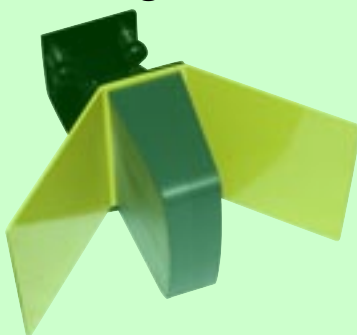
When enabled, Mantis responds to requests for a user friendly name with “BVS Mantis Bluetooth Tester”. When disabled, it responds with a blank string.



USING A DIRECTION FINDING ANTENNA

Mantis ships with an optional Direction Finding Antenna for locating and pinpointing local Bluetooth devices. This antenna may be removed at anytime and replaced with the standard omni-directional antenna. See antenna specifications and guidelines below.

2.4 GHz Direction Finding Corner Reflector

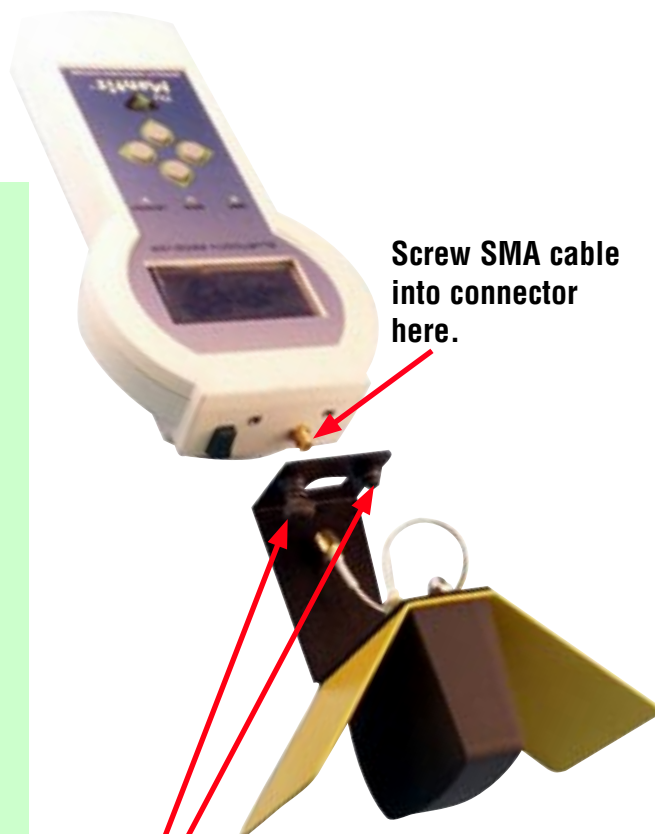
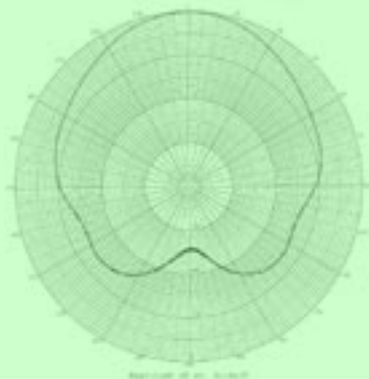
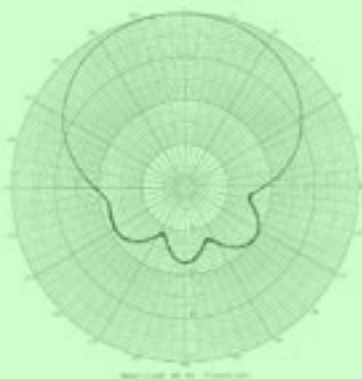


1. 2.4 GHz 2.4 GHz Direction Finding Corner Reflector

BVS P/N DFA-001 & DFA-000

1. 2.4 GHz 2.4 GHz Direction Finding Corner Reflector

BVS P/N DFA-001 & DFA-000



Screw SMA cable into connector here.

Secure these screws to the top of Mantis case.

BATTERY TIPS

The Mantis™, Grasshopper™, Locust™, Yellow Jacket™ and Yellow Jacket Plus (formally called Scorpion), Beetle™, Cricket™, and Cicada W-LAN receivers use 4 or 5 Ni-MH long-lasting “AA Cells”.

1. Ni-MH batteries do not charge to full capacity the first time they are charged.
2. Ni-MH batteries do not charge to full capacity the first time they are charged after a long period of inactivity, or after a long period of non-use.

Cause:

When charging Ni-MH batteries for the first time after long-term storage, deactivation of reactants may lead to increased battery voltage and decreased capacity, (which causes premature termination of charging). Because batteries are chemical products involving internal chemical reactions, performance deteriorates with prolonged storage. This is normal in Ni-MH batteries.

Resolution:

Ni-MH batteries may not charge to full capacity the first time they are charged, or after a long period of inactivity.

The first-time charge of the Ni-MH Rechargeable Battery Pack should take approximately 2 hours. If the Receiver Dock light turns green, indicating a full charge, in less than 2 hours, repeat the charge cycle as follows:

First-time Charge:

1. To begin charging, place the instrument on the Charge Dock. Refer to your instrument's User Guide for details.
2. When the charge light turns green, remove the W-LAN Receiver from the dock and place back on the dock after several seconds.
3. Repeat steps 1 and 2 three or four times or until the combined charge time is 2 hours.

Subsequent charges of the W-LAN Ni-MH Battery Pack will not require multiple charging cycles unless left uncharged for a long period of time (greater than 2 months).

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.

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

Bluetooth Glossary

ACK

Acknowledge.

ACL

Bluetooth Asynchronous Connectionless Link. An Asynchronous packet-switched connection between two devices created on the LMP level. ACL link is primarily used for data transmission. Bluetooth links are either of the ACL type or SCO type. See also SCO.

Active Mode

The operational status of a slave Bluetooth unit within a Piconet. In the active mode, the Bluetooth unit actively participates on the channel. The master schedules the transmission based on traffic demands to and from the different slaves. In addition, it supports regular transmissions to keep slaves synchronized to the channel. Active slaves listen in the master-to-slave slots for packets. If an active slave is not addressed, it may sleep until the next new master transmission. Bluetooth supports up to seven active slaves within a Piconet.

AG

Audio Gateway. See also HS profile.

AM_ADDR

Bluetooth Active Member Address. A temporary address assigned to an active member of a Piconet. The AM-ADDR may be assigned 1 through 7 where zero denoted the Piconet broadcast address. See also BD_ADDR, which refers to the fixed MAC address of a Bluetooth device.

AP

Access Point. A hardware / software entity which provides the Bluetooth unit access to some external network. See also LAP and NAP.

API

Application Programming Interface.

Application Layer

The group of protocols at the user level. The application layer in the Bluetooth protocol layers will contain those protocols involved with the user interface (UI).

AR_ADDR

Bluetooth Access Request Address. AR_ADDR is assigned to a parking slave by the master. The ARADDR is used by parked slaves when initiating a request for unparking.

ARQ

Automatic Repeat reQuest. An error control scheme in which packets are either acknowledged or retransmitted. An ARQ scheme provides a reliable communication link and is implemented in the Bluetooth base-band layer.

AT Command Handler

A module that handles the AT commands which control a phone or modem (between a DTE and a DCE). authentication The process of verifying the identity of the device on the other end of the link. Bluetooth authentication procedure is based on the stored link key or by entering a passkey (PIN) (also referred to

as pairing).

authenticated device

A device whose identity has been verified during the lifetime of the current link based on the authentication procedure.

authenticate using a passkey

The procedure where a user is requested to enter a passkey during the link establishment procedure, where the devices did not share a common link key beforehand. This differs from the bonding procedure where the user enters the passkey without it being requested.

authorization

The process of deciding if a certain device is allowed to have access to a specific service. This is where the concept of trust exists. Trusted devices (the device is authenticated and indicated as “trusted”), are allowed access services. Un-trusted or unknown devices may require authorization based on user interaction before it is allowed access to the services. Authorization always includes authentication.

BAP

Bluetooth Access Point

BB, BaseBand

A Bluetooth layer. The baseband describes the specifications of the digital signal processing part of the hardware -- the Bluetooth link controller, which carries out the baseband protocols and other low-level link routines.

BD_ADDR

Bluetooth Device Address. A unique 48-bit address, distinguishing between different Bluetooth transceivers.

Bluetooth

An open specification for wireless communication of data and voice. It is based on a low-cost short-range radio link facilitating protected ad hoc connections for stationary and mobile communication environments.

Bluetooth clock

The master timing mechanism defined by the master of the piconet. Every Bluetooth unit has an internal system clock, which determines the timing and hopping of the transceiver.

Bluetooth device class

A parameter that indicates the type of device and which types of services that are supported. The class is received during the discovery procedure.

Bluetooth passkey

The name of the Bluetooth PIN code . The term “Bluetooth passkey” is used in the UI. See Bonding.

BNEP

Bluetooth Network Encapsulation Protocol. The protocol to be used by the Bluetooth PAN profiles. This layer encapsulates packets from various networking protocols, which are transported directly over the L2CAP Layer.

bonding

Bonding is the creation of a relationship between two devices. The bond is a link key. The relationship is created when the link key is exchanged between two devices. The devices are known to each other prior to the bonding procedure. A user initiates the bonding procedure and enters a passkey with the explicit purpose of creating a bond between two devices. This differs from the authentication using a passkey procedure where the user is requested to enter a passkey during the establishment of the link.

Browser

An application that allows interaction with Internet web pages.

BT

Bluetooth.

channel

In Bluetooth, a logical connection on L2CAP layer between two devices serving a single application or higher layer protocol.

Circuit Switched

The application of a network where a dedicated resources are used to transmit information. Only one user may employ the line resources at a time.

Circuit Switched Bluetooth

The application of a Bluetooth network where dedicated time slots are used to transmit Bluetooth data. See also SCO.

CL

Connectionless.

class of device , CoD

See Bluetooth device class. Also abbreviated as CoD.

CO

Connection-oriented.

CODEC

Coder/Decoder. A device that converts analog to digital, and digital to analog for transmission over a digital communications system. The Codec sometimes also applies additional digital processing.

connect to service

The establishment of a connection to a service. If not already done, this includes establishment of a physical link, link and channel connection as well.

connectable device

Any Bluetooth device within range that will respond to paging and set-up connection.

CP

Capability Provider. A Capability Provider is a module within the local device that provides a service to other modules. Protocol stack modules (RFCOMM, L2CAP) are Capability Providers. So are “application interface modules” such as OBEX and CTS-AT. In fact, any module that registers a port that other modules can connect to is a Capability Provider.

CT profile

Cordless Telephony Profile. Defines the protocols and procedures that shall be used by devices implementing the '3-in-1 phone' use case. The entities defined in this profile are gateway (GW) and terminal (TL).

CVSD

Continuous Variable Slope Delta Modulation. A robust voice modulation method.

DAC

Device Access Code. It is used during page, page scan and page response sub-states. It is a code derived from the unit's BD_ADDR.

DCE

Data Circuit-Terminating Equipment. In serial communications, DCE refers to a device in-between the communication endpoints. The task of the DCE is to facilitate the communications process within the communication network; typically a modem. See also DTE.

Device Discovery

The mechanism to request and receive the Bluetooth address, clock, and class of device, used page scan mode, and names of devices.

device security level

Access to a device can be denied based on the required device security level. There are two levels of device security: trusted device and un-trusted device. See also service security level.

DH

Data-High Rate. Data packet type used with ACL link for high rate data. See also DM.

discoverable device

A Bluetooth device in range that will respond to an inquiry message.

DM

Data - Medium Rate. Data packet type used with ACL link for medium rate data. See also DH.

DTE

Data Terminal Equipment. In serial communications, DTE refers to a device at the endpoint of the communications path; typically a computer or terminal.

DTMF

Dual Tone Multiple Frequency.

DUN profile

Dial Up Network profile. Defines the protocols and procedures that shall be used by devices implementing the usage model called 'Internet Bridge' (typically modems and cellular phones). The entities defined in this profile are gateway (GW) and data terminal (DT).

DV

Data Voice. Data packet type use with SCO link for data and voice.

E1/T1

The most common standard distribution interface. European E1 provides 2.048 Mbps in 30 64-kbps voice channels + 2 64kbps signaling channels, while American T1 provides 1.544 Mbps in 24 64-kbps voice channels + a single 8kbps framing channel.

FEC

Forward Error Correction.

FH

Frequency Hopping.

GA profile

Generic Access profile. Describes requirements related to modes and access procedures that are to be used by transport and application profiles. Most important, this profile defines discovery, link establishment and security procedures. The entities defined in this profile are two Bluetooth devices.

GFSK

Gaussian Frequency Shift Keying. This is the modulation used in the radio layer of the Bluetooth system.

GOE profile

Generic Object Exchange Profile. The most basic Bluetooth profile. Defines modes and access procedures that are to be used by transport and application profiles. The entities defined in this profile are client and server.

HA

Host Application. A software program that uses Bluetooth.

HCI

Host Controller Interface. A protocol Stack Layer that provides a command interface to the LMP and Baseband layers.

Hold mode

Devices synchronized to a piconet can enter power -saving modes in which device activity is lowered. The master unit can put slave units into HOLD mode, where only an internal timer is running. Slave units can also demand to be put into HOLD mode. Data transfer restarts instantly when units transition out of Hold mode. It has an intermediate duty cycle (medium power efficient) of the 3 power saving modes: sniff, hold and park.

host

A software and hardware platform in which the Bluetooth package runs.

HS profile

Headset Profile. Defines the protocols and procedures that shall be used by devices implementing the usage model called 'Ultimate Headset'. The entities defined in this profile are headset (HS) and audio gateway (AG, typically a cellular phone).

HSM

Host-specific Mechanism.

HV

High quality Voice. An SCO link voice packet. HV packets do not have a CRC and are never retransmitted.

Idle mode

A device is in idle mode when it has no established links to other devices. In this mode, the device may discover other devices. In general, a device sends inquiry codes to other devices. Any device that allows inquiries will respond with information. The device might then decide to establish a link.

initiator

The Bluetooth device initiating an action to another Bluetooth device. The device receiving the action is called the acceptor. The initiator is typically part of an established link.

Inquiry Procedure

The inquiry procedure enables a device to discover which devices are in range, and determine the addresses and clocks for the devices. After the inquiry procedure has completed, a connection can be established using the paging procedure. Note: a device should be in Inquiry scan mode to be discovered.

intelligent peripheral

A peripheral that is capable of exchanging information with the handset. Information may include battery status, charging status, data storage status, or other high-level functionality. Also referred to as a smart peripheral.

Internet Bridge

Method of using a wireless modem for connecting to Internet access.

IP

Internet Protocol. The protocol by which data is sent from one computer to another on the Internet.

ISM

Industrial, Scientific, Medical - the unlicensed frequency band in which Bluetooth operates (2.4 –2.483 GHz).

Key Management

The handling and control of encryption keys.

known device

A device for which at least the BD_ADDR is stored.

L2CAP

Logical Link Controller and Adaptation Protocol. The data link layer of the Bluetooth protocol stack. This layer of the Bluetooth protocol stack supports higher-level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

L_CH

Logical Channel. A channel that is used to transmit data over a physical Bluetooth link.

LA profile

LAN access profile. Defines LAN Access using PPP over RFCOMM. The entities defined in this profile are LAN Access point (LAP) and Data terminal (DT).

LAN

Local Area Network. A group of computers and associated devices that share a common communications

line and typically share the resources of a single server within a local geographic area (for example, within an office building).

LAP

LAN Access Point. One of the entities defined in the LA profile. The LAP is an AP, which acts like a router between a Bluetooth Piconet and an external Network.

link

Shorthand for an ACL link.

LC

Link Controller. The Link Controller manages the link to the other Bluetooth devices. It is the low-level baseband protocol handler.

LCP

Link Control Protocol.

link key

The authentication key used to establish a link between devices. See also bonding.

LM

Link Manager. The Link Manager software entity carries out link setup, authentication, link configuration, and other aspects of managing the Bluetooth physical link. Resides within the Bluetooth hardware.

LMP

Link Manager Protocol. Defines communication procedures between link managers.

LMP-authentication

An LMP level procedure for verifying the identity of a remote device. The procedure is based on a challenge-response mechanism using a random number, a secret key and the BD_ADDR of the noninitiating device. The secret key used can be a previously exchanged link key or an initialization key created by using a PIN (as used when pairing).

Imp-pairing

A LMP procedure that authenticates two devices based on a PIN and subsequently creates a common link key that can be used as a basis for a trusted relationship or a (single) secure connection. The procedure consists of the steps: (1) creation of an initialization key (based on a random number and a PIN), (2) Imp-authentication based on the initialization key, and (3) creation of a common link key.

LocDev

Local Device. A Bluetooth device which initiates a SDP procedure. A Local Device is typically a master device on the piconet. However, a Local Device may not always have a master connection relationship to other devices. See also RemDev.

MAC

Media Access Control.

MAC Address

3-bit address to distinguish between units participating in the piconet.

Management Entity

Management Entity. The portion of the Bluetooth implementation that mediates the internal functions of the Bluetooth stack.

master device

A device that initiates an action or requests a service on a piconet. See also LocDev. The Master's BD_ADDR and clock are used to generate the frequency hopping sequence of all Bluetooth devices in the piconet.

MTU

Maximum Transmission Unit. The largest size packet or frame, specified in bytes, that can be sent in a packet or frame-based network.

NAK

Negative Acknowledge.

Name Discovery

The mechanism to request and receive a device name.

NAP

Network Access Point. One of the entities defined in the PAN profile. The NAP is an AP, which acts like a bridge or a router between a Bluetooth Piconet and an external Network.

non-connectable mode

A device that does not respond to paging (an attempt to establish a communication link) is said to be in non-connectable mode. See also connectable mode.

non-discoverable , non-discoverable mode

A device that cannot respond to an inquiry is said to be in non-discoverable mode.

non-pairable mode

A device that does not accept pairing is said to be in non-pairable mode. The opposite of non-pairing mode is pairable mode.

OBEX

Object EXchange Protocol - protocol defining a way to exchange data objects between devices. Adapted to Bluetooth from the IrDA standard.

Packet Switched

A network that routes data packets based on an address contained in the data packet is said to be a packet switched network. Multiple data packets can share the same network resources.

Packet Switched Bluetooth

The application of routing Bluetooth data packets on a network using addresses contained in the Bluetooth data packets. A baseband state where a device transmits page messages and processes any eventual responses.

Page Scan state

A mode where a device listens for page messages containing its own device access code (DAC).

Page state

A mode that a device enters when searching for services. The LocDev sends out a page to notify other devices that it wants to know about the other devices and/or their services.

paged device

A paged device is typically contacted by a paging device to establish a communication link.

paging

A procedure of attempting to establish a communication link.

paging device

A paging device is typically attempting to establish a communication link with other devices. See initiator.

Paging Procedure

With the paging procedure, an actual connection can be established. The paging procedure typically follows the inquiry procedure. Only the Bluetooth device address is required to set up a connection. Knowledge about the clock will accelerate the setup procedure. A unit that establishes a connection will carry out a page procedure and will automatically be the master of the connection.

pairable mode

A device that accepts pairing. is said to be in pairable mode. The opposite of pairing mode is nonpairable mode.

paired device

A device with which a link key has been exchanged (either before connection establishment was requested or during connecting phase). See also pre-paired device and un-paired device.

pairing

The creation and exchange of a link key between two devices. The devices (LocDev and RemDev) use the link key for future authentication when exchanging information. Pairing procedure is based on a common link key. The link key is also referred to as a bond. Pairing can also establish a link by the user entering a PIN, which is authenticated by the device providing the service.

PAN

Personal Area Network. A group of mobile communication and computing devices that share a small geographic space (for example, a room) , within which they have non-wired communication channel (typically based on radio waves or infrared).

PAN profile

Personal area network profile. A Bluetooth profile that describes how two or more Bluetooth enabled devices can form an ad-hoc network and how the same mechanism can be used to access a remote network through a network access point. The entities defined in this profile are PAN user (PANU), network access point (NAP) and group ad-hoc network (GAN).

Park mode

In the PARK mode, a device is still synchronized to the piconet but does not participate in the traffic. Parked devices have given up their MAC address and occasional listen to the traffic of the master to resynchronize and check on broadcast messages. It has the lowest duty cycle and best power efficiency of all 3 power saving modes: Sniff, Hold and Park.

PCMCIA

Personal Computer Memory Card International Association.

PDA

Personal Digital Assistant.

Phone Services Database

The portion of the Bluetooth implementation that stores information about device services, both local services and remote services.

Physical channel

A synchronized Bluetooth RF hopping sequence in a piconet.

Piconet

A collection of devices connected via Bluetooth wireless technology in an ad hoc fashion. A piconet starts with two connected devices, such as a portable PC and an Access Point, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a master and the other(s) as slave(s) for the duration of the piconet connection. All devices have the same physical channel utilizing the same Frequency-hopping sequence, defined by the master device clock and BD_ADDR.

PIM

Personal Information Manager.

PIN

Personal Identification Number. The Bluetooth PIN is used to authenticate two devices that have not previously exchanged link key. By exchanging a PIN, the devices create a trusted relationship. The PIN is used in the pairing procedure to generate the initial link that is used for further identification.

PIN(BB)

The PIN used on the baseband level. The PIN(BB) is used by the baseband mechanism for calculating the initialization key during the pairing procedure. (128 bits)

PIN(UI)

The PIN used on the user interface level. The PIN(UI) is the character representation of the PIN that is entered on the UI level.

POTS

Plain Old Telephone system. A landline telephone connection system.

PPP

Point-to-Point Protocol. A way of implementing the IP and other networking protocols over a dial-up or other serial link.

pre-paired device

A device with which a link key was exchanged, and, before link establishment. See also paired device and un-paired device.

PRNG

Pseudo Random Noise Generation.

Profile

A description of the operation of a device or application. Defines a selection of messages and procedures (generally termed capabilities) from the Bluetooth specifications and describes the air interface for specified service(s) and use case(s). Profiles are broadly classified as either basic profiles (referring to access and transport), or application profiles (referring to specific use cases). Some of the main profiles are referred to in this glossary.

PSM

Protocol/Service Multiplexer.

PSTN

Public Switched Telephone Network. The general Telephony network.

QoS

Quality of Service - the idea that communication characteristics (data rates, error rates, and other s) can be measured, improved, and, to some extent, guaranteed to an application in advance, in spite of the fact that the network has limited resources.

RemDev

Remote Device. A Bluetooth device that participates in the SDP process. A Remote Device must contain a SDP server along with a service record database. A Remote Device is typically a slave device, however, a Remote Device may not always have a slave connection with a LocDev.

requestor

An entity that requests information from another entity via the Bluetooth API.

RFCOMM

Serial Cable Emulation Protocol based on ETSI TS 07.10.

RSSI

Received Signal Strength Indication. Usually used for power management procedures.

Scatternet

Multiple independent and non-synchronized piconets form a scatternet.

SAR

Segmentation and reassembly. One of the main functions of the L2CAP layer

SCO

Synchronous Connection Oriented link. A synchronous circuit-switched connection for reserved bandwidth communications. It is created on the LMP level by reserving slots periodically on a physical channel. SCO link is used primarily to transport SCO packets (voice data). It supports time-bounded information like voice. See also ACL.

SD

Service Discovery.

SDP

Service Discovery protocol.

SDA

Service Discovery Application. Also sometimes called the **Service Discovery User Application.**

SDA profile

Service Discovery Application Profile. Defines the protocols and procedures that shall be used by a service discovery application on a device to locate services in other Bluetooth-enabled devices using the Bluetooth Service Discovery Protocol (SDP). The entities defined in this profile are a local device (LocDev) and a remote device (RemDev).

SDDB

Service Discovery Database.

SDP

Service Discovery Protocol. This Bluetooth defined protocol provides a means for applications to discover which services are available and to determine the characteristics of those available services.

SDP client

The SDP in a Local Device (LocDev). The SDP client requests service information from SDP servers.

SDP server

The SDP in a Remote Device (RemDev). The SDP server responds to requests made by SDP clients.

SDP Session

The exchange of information between an SDP client and an SDP server. The exchange of information is referred to as an SDP transaction.

SDP Transaction

The exchange of an SDP request from an SDP client to an SDP server, and the corresponding SDP response from an SDP server back to the SDP client.

Security Manager

The module in a Bluetooth device that controls security aspects of communications to other Bluetooth devices.

Security Mode 1

A device will not initiate any security. This is a non-secure mode.

Security Mode 2

A device does not initiate security procedures before channel establishment on L2CAP level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel. A service level enforced security mode.

Security Mode 3

A device initiates security procedures before the link setup on LMP level is completed. A link level enforced security mode.

Serial Interface

An interface to provide serial communications.

SP profile

Serial Port profile. Defines the protocols and procedures that shall be used by devices using Bluetooth for RS232 (or similar) serial cable emulation (typically , in cable replacement scenarios).

Service Discovery

A procedure for querying and browsing for services offered by or through another Bluetooth device.

Service Layer

The group of protocols that provides services to the application layer and the driver layer in a Bluetooth device.

Service Record Database

A database that contains the service discovery-related information.

service security level

Access to services can be denied based on the required service security level. There are three levels of service security: authorization and authentication; authentication only, and no security (open to all). Encryption can be another security requirement for service use in addition to the requirements listed above. Encryption is typically applied at the physical level (baseband). See also device security level.

SIG

Special Interest Group. For information about the Bluetooth SIG refer to www.bluetooth.com.

Slave device

All devices in a piconet that are not the master.

Sniff mode

Devices synchronized to a piconet can enter power-saving modes in which device activity is lowered. In the SNIFF mode, a slave device listens to the piconet at reduced rate, thus reducing its duty cycle. The SNIFF interval is programmable and depends on the application. It has the highest duty cycle (least power efficient) of all 3 power saving modes: Sniff, Hold, and Park.

TBAN

Tadlys Bluetooth Access Network. First generation Bluetooth network by provided by Tadlys Ltd.

TCI

Test Control Interface. In the context of Bluetooth testing procedure, the interface and protocol used by the tester to send and receive commands and messages to and from the upper interface of the system under test (SUT) or the implementation under test (IUT).

TCP

Transport Control Protocol. a reliable connection oriented protocol that runs on top of IP networks .

TCS

Telephone Control protocol Specification. A bit-oriented protocol that defines the call control signaling for the establishment of audio and data transmission

TCS-AT

A set of AT-commands by which a mobile phone and modem can be controlled in the multiple usage models. In Bluetooth, AT-commands are based on ITU-T recommendation v.250 and ETS 300 916(GSM 07.07).

In addition, the commands used for fax services are specified by the implementation. TCS -AT will also be used for dial-up networking and headset profiles.

TCS Binary , TCS-BIN

Bluetooth Telephony Control protocol Specification using bit-Oriented protocol. TCS-BIN is being used for cordless telephony profiles.

TGAP

Timer used in the General Access Profile (GAP).

3-in-1 phone

One of Bluetooth use cases. Provides an extra mode of operation to cellular phones, using Bluetooth as a short-range bearer for accessing fixed network telephony services via a base station.

Trusted device

A device that has been authenticated.

UART

Universal Asynchronous Receiver Transmitter. A device that converts parallel data into serial data for transmission, or it converts serial data into parallel data for receiving data.

UDP

User Datagram Protocol - a connectionless protocol that, like TCP, runs on top of IP networks (and unlike TCP, provides very few error recovery services).

UI

User Interface. The area on a device that contains interface mechanisms such as displays, dialog boxes, manuals, packaging, advertising, etc., where the user is likely to encounter Bluetooth terminology and parameters.

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.

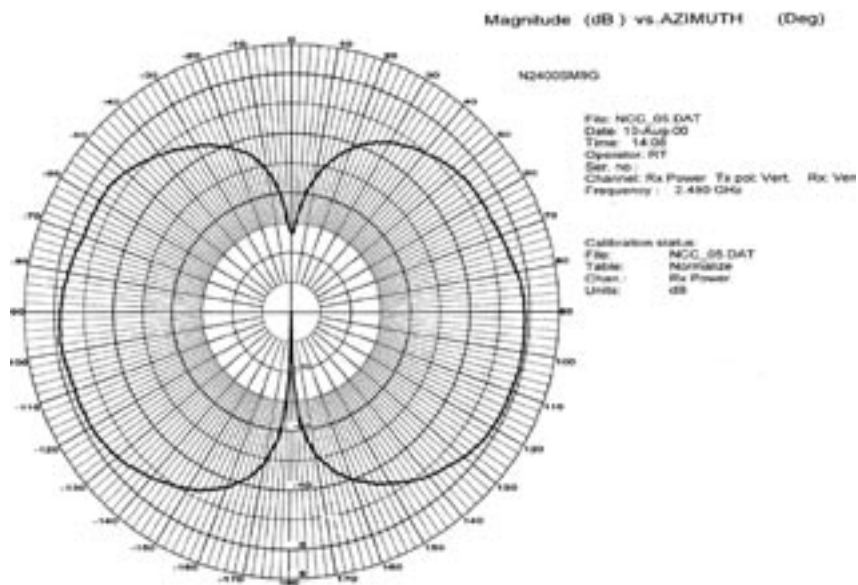
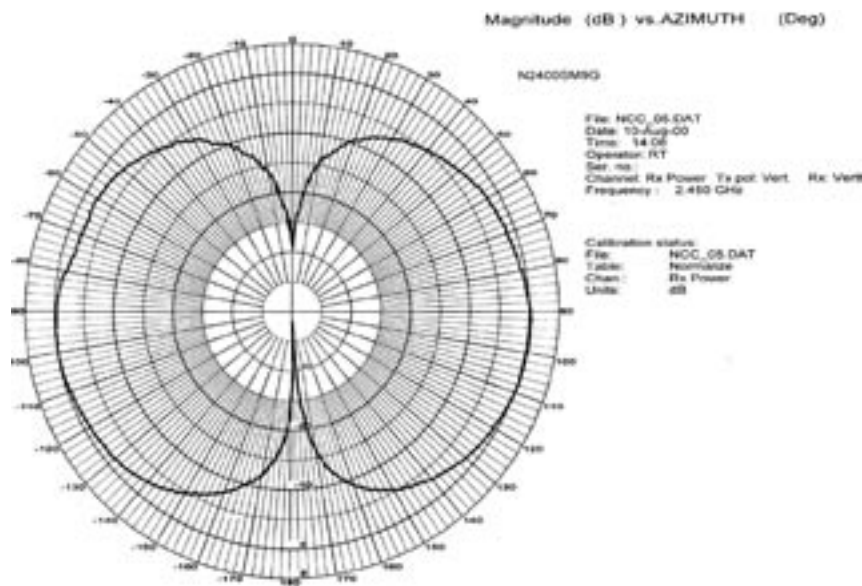
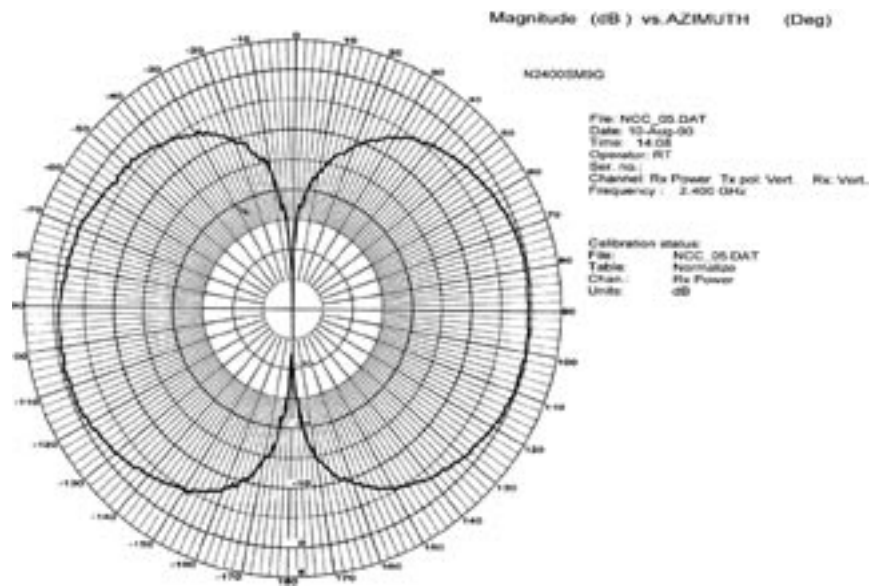
2. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
3. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
4. Use caution when installing or modifying telephone lines.

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).



Mantis™ BLUETOOTH TRANSCEIVER

INSTALL, TEST, VERIFY

Mantis™ is a handheld, wireless transceiver designed specifically for sweeping, installing and verifying **BLUETOOTH** wireless devices and connections. The instrument locates all nearby Bluetooth devices, identifies them and “follows” their frequency-hopping signature allowing for RSSI measurement, Packet Error Rate breakdowns as well as other device parameters and identification. Privacy/Stealth mode renders **Mantis™** invisible to all network devices for secure verification scanning. Other features include a built-in backlit display, simple, keypad menu navigation and removable, rechargeable Ni-MH batteries for true portability.

BLUETOOTH



Mantis is ideal for installing and optimizing Bluetooth networks and device placement.

- Detects and displays all available Bluetooth devices
- Measures Packet Error Rate
- Measures RSSI and device parameters
- Low-cost instrument that any field technician can afford
- Privacy mode keeps Mantis invisible to all Bluetooth devices
- Instantly locks on to any Bluetooth hopping pattern for continuous analysis
- Light-weight, portable and rugged design ideal for realtime network analysis
- Removable battery power (4 AA Ni-MH cells with 4 extra batteries & charger included)
- Built-in 128 x 64 Graphic backlit LCD with simple menu interface and navigation

NEW Privacy/Stealth mode keeps Mantis invisible to any Bluetooth network

The Mantis 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



Mantis™

BLUETOOTH TRANSCEIVER

INSTALL, TEST, VERIFY



BANDS SUPPORTED

RF SENSITIVITY (Wide Band)

RSSI MEASUREMENT (Narrow Band)

TUNING INCREMENTS

ISM: 2.400-2.485 GHz

-20 to -90 dBm

-30 to -90 dBm @ 687.5 kHz resolution bandwidth

FHSS

PACKET PREAMBLE DEMODULATOR and ANALYZER:

Multipath Measurement and Graphical Display

POWER MEASUREMENTS:

AP Power Measurement

RATIO

-20 dBm : -90 dBm

GENERAL SPECIFICATIONS

IF Bandwidth:

Stability:

Antenna:

Controls:

Warm Up Time:

Power:

Weight:

Dimensions:

Wideband 22 MHz

± 2.5 PPM Temp range 32° to 120 F°

SMA Female 50 ohm

4 button keypad

< 3 minutes

Internal batteries (4 AA Ni-MH)

Under 2 lbs.

2" H x 4" W x 9" L (water resistant, high impact ABS plastic case)



Mantis includes 8 AA Ni-MH batteries, fast-charger, low profile 3dBi 2.4 GHz antenna (SMA Female 50 ohm) and belt holster.