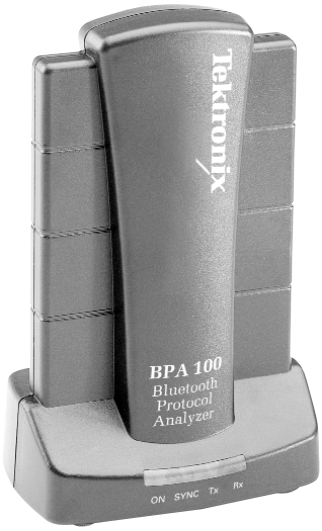
BPA100 Bluetooth Protocol Analyzer

▶ BPA100



▶ ***Figure 1.*** *The Tektronix BPA100 (based on proven Digianswer™ technology). Bluetooth Protocol Analyzer consists of the Protocol Analyzer Version 2.2 Software and an Air Probe which houses the Bluetooth approved baseband controller and radio. The Air Probe connects to a Windows-based PC through the included USB interface cable.*

Superior Solutions for Bluetooth Protocol Analysis and Debug

Developers of Bluetooth enabled devices are faced with unique challenges when integrating hardware and application software. The end device must be thoroughly tested for correct operation within a wide range of piconet/scatternet configurations and interoperability with other devices is critical. Since Bluetooth is a wireless interface between devices, it is necessary to have a test tool that can non-intrusively and independently intercept the baseband traffic and log, decode and analyze the packet data being transmitted and received.

Developers also require a protocol debug tool that can participate in a piconet as either a master or slave in order to initiate various modes of operation, introduce intentional errors and act as a known reference device.

Developers will appreciate the highly intuitive user interface and powerful triggering and filtering tools that allow them to capture and log faults in real time, without sorting through large amounts of non-relevant data.

The BPA100 can be easily upgraded by the user through software to accommodate changes in the core Bluetooth specification or to add increased functionality when it becomes available.

▶ Features & Benefits

Operation in Either Independent (Sniffer) or Piconet (Master/Slave) Modes Allows the Developer Maximum Test and Debug Flexibility

Data Packet Error Generation Enables the User to Introduce Errors into Packets and Stress Test the Design

Direct Control of BPA100 with the HCI Terminal Application using HCI Commands Directly or through Scripting

Advanced Triggering and Filtering Allows User to Capture, Log and Display Only Events or Transactions of Interest

Free Run Analyzer Display Allows User to Continuously Monitor Latest Session Transactions with Real-time Screen Updates

Direct Logging to PC Hard Drive Provides Maximum Log History File Size, Allowing for Long-term Monitoring of Packet Traffic

▶ Applications

Debug of Problems Related to New Application Software Integration

Acts as a Known Reference and Debug/Test Device When Bringing Up New Baseband/Radio Module

Interoperability Testing

Consistency in Testing Using the HCI Terminal Application with Scripting Capability

Tektronix
Enabling Innovation

▶ Characteristics

Modes of Operation

Independent Mode – As an independent (sniffer) unit, the Protocol Analyzer does not participate directly in the piconet. Instead, after synchronizing to the piconet it passively listens in and logs all baseband packets transmitted between the master and slaves of the piconet. Through the use of advanced triggering and filters, selected data of interest to the developer can be logged and analyzed.

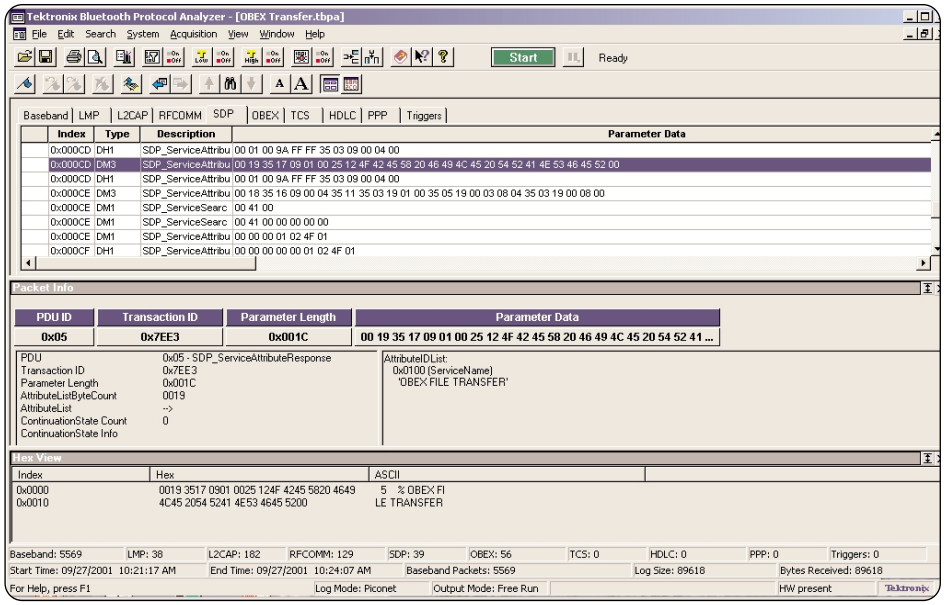
Piconet Mode – In Piconet Mode, the Protocol Analyzer uses its fully Bluetooth qualified protocol stack and participates as the master or a slave in a piconet. As a master, the Protocol Analyzer logs all baseband packets between itself and the slaves. When setup as a slave, it logs all packets between itself and the piconet master device. Piconet mode is useful when the developer requires a known reference device in the piconet or needs to generate user-defined errors and packets for stress testing. Another useful feature in Piconet Mode is the ability to log FHS packets before connection is established.

Protocol Analyzer Software Version 2.2

The Tektronix Bluetooth Protocol Analyzer software is an integrated application that performs baseband traffic data acquisition and display. The user can also display transactions and packet data at higher levels in the Bluetooth protocol stack such as LMP, L2CAP, RFCOMM, OBEX, HDLC, PPP, TCS and SDP including service attributes. By using powerful triggering and filtering features, the user can selectively choose what data to acquire, log to disk, or display onscreen. In the Free Run display mode, packet data is viewed as it is acquired.

Protocol Analyzer supports testing of proper security setup and authentication between devices using data decryption. Data decryption is supported in both piconet mode and independent mode, independent mode will require the input of the link-key, pin code or KC code information.

The HCI Terminal Application allows direct access to the BPA100 hardware via the Host Controller Interface layer. The HCI Terminal makes it easy to send commands to a BPA100 and to receive responses from a Bluetooth device. Data statistics are available showing transfer rates and number of packets sent and received. HCI traffic can be viewed displaying the sequence of packet traffic between the BPA100 and another device. Details of an individual packet are available in an easy to read format by selecting the desired packet in the traffic window. Scripting with control flow capabilities allow for consistent and repetitive testing to be done on devices.



The Digianswer™ Bluetooth Neighborhood bundled with the protocol analyzer software provides developers with a robust application that can be used in conjunction with the piconet mode of operation. If piconet mode is selected, then the Bluetooth Neighborhood is used for controlling the communication between the Protocol Analyzer as either a master or slave and the other devices in the piconet. In this mode, the protocol analyzer can be used to generate traffic, introduce errors, and help test for proper overall operation. The Bluetooth Neighborhood is an intuitive application that allows the user to quickly discover other devices within range, make connections by simply dragging and dropping device icons and perform other tasks such as transferring data between devices. In independent mode, the protocol analyzer synchronizes to the master and logs the packet traffic without actually becoming part of the piconet.

Single Interface for Control

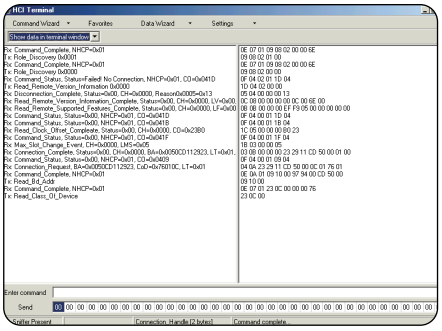
Acquisition Setup Display

The BPA application software v2.2 integrates the data collector and packet analyzer applications. This provides the user with a single interface for controlling the BPA100 and analyzing packets.

- Ability to capture all baseband packets within a Bluetooth piconet including re-transmitted packets
- Logging of data directly to the hard drive file on the host PC
- Capable of transmitting and receiving on a single user defined frequency
- Ability to turn data whitening on and off

Packet Analysis

- Provides packet status – access error, packet header error, estimated clock and hop frequency
- Analyzes baseband packets and displays ID, IQ, NULL, POLL, FHS, DMx, DHx, AUX1, HVx and DV packets
- Isolates, decodes and displays baseband, LMP, L2CAP, RFCOMM, OBEX, HDLC, PPP, TCS and SDP commands including services attributes, events and data packets
- View wide range of filters to display data of interest
- Export of post filtered data for the total logged session into a comma separated (.CSV) file for documentation



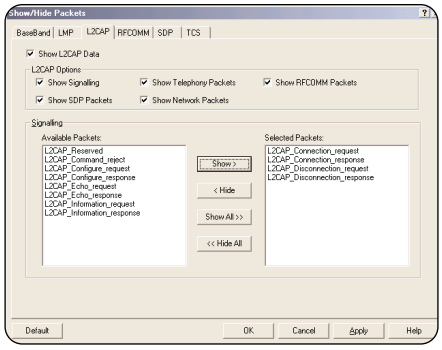
HCI Terminal Application

- ▶ Command line interface allows low-level control of HW
- ▶ Enter HCI commands to bypass middleware for direct access to transport layer
- ▶ Use the HCI scripting capability for repetitive tests
- ▶ Create HCI Scripts to insure consistency in testing

Trigger Functionality

Triggering enables the user to selectively acquire data based on occurrence of specific events, errors, sequences or patterns, thereby getting to the source of the problem more quickly.

- ▶ Trigger on user defined sequences or patterns
- ▶ Trigger on errors
- ▶ Control Field – SABM, DM, UIH, UA, DISC
- ▶ Information Field – DATA, PN, Test, FCon, FCoff, MSC, NSC, RPN, RLS
- ▶ Payload Data – 1 to 8 bytes of payload data
- ▶ Available in free running mode
- ▶ PDU upcode 1 to 7
- ▶ 1 to 8 bytes of payload data
- ▶ Available in free running mode
- ▶ Pre-trigger: 0 – 100,000 packets
- ▶ Post-trigger: 0 – unlimited packets (manual stop)



Filtering

Filtering can be enabled pre-acquisition for selective logging to disk or post-acquisition for selective display of acquired data from the log file.

- ▶ Options for viewing combinations of Error, ID, NULL, POLL, FHS, DXX, HVX, AUX, DV, etc., packets, including LMP and L2CAP at baseband
- ▶ Filters at each protocol level; Baseband, LMP, L2CAP, RFCOMM or SDP
- ▶ Extensive post-acquisition filtering, combined with large disk based record size ensures that customers can see all the data and yet filter it for optimal analysis
- ▶ Pre-acquisition filtering on baseband Access Error, ID, NULL and POLL packets greatly minimizes disk usage

Synchronization

- ▶ Sync to piconet using master inquiry
- ▶ Sync to piconet using fake connection response
- ▶ Sync to piconet using slave inquiry

Independent Mode Packet Capture and Tracking

When used in independent mode the BPA100 captures the normal traffic of the piconet that is being monitored. There are specific sequences of events of interest between two devices under test, which the BPA100 can capture while it is monitoring them in independent mode.

- ▶ Track the test mode 5 frequency hopping sequence between two devices while monitoring them in Independent Mode
- ▶ Ability to follow the Master/Slave switch between two devices while monitoring them in Independent Mode
- ▶ Capture the paging sequence (ID, ID, FHS, ID) between two devices in Independent Mode

Error Data Generator

When in piconet mode, the protocol analyzer can introduce the following errors into baseband packets. This is very useful when bringing up the baseboard/radio portion of the design or when stress testing network operation.

- ▶ Header FEC 1/3 error
- ▶ Header HEC error
- ▶ Payload FEC 1/3 and 2/3 recoverable error
- ▶ Payload FEC 2/3 non-recoverable error
- ▶ Payload CRC error

The above errors may also be introduced based on user defined sequence criteria (errors only generated if criteria met). Some of the criteria parameters that can be used are:

- ▶ Estimated clock
- ▶ Hop frequency
- ▶ Header type
- ▶ Header AM_ADDR
- ▶ Header flow
- ▶ ARQN, SEQN, L_CH
- ▶ Payload flow, Payload length

Free Run Display

In Free Run Display, the protocol analyzer updates the data list box continuously with the latest packets received. The user can halt the real-time updating at any time and scroll through the received data. This is particularly useful when debugging traffic flow at higher levels in the protocol stack.

Baseband Parameter Controls

- Inquiry timeout, user selectable in the interval of 1-41 sec
- Correlation value between 40 and 64 to indicate the value for accepting a received packet

Data Decryption

- Dialog for entering the key in hexadecimal

System Requirements

- Microsoft Windows 98, ME or 2000
- Intel Pentium III, 800 MHz or above

  Lower Processor speeds are acceptable if Decryption and Free Run mode are not used
- 256 MB of RAM
- Minimum of 200 MB of free space on hard drive

Hardware Specifications

- Compliant with the USB specification version 1.1
- Power is supplied to Bluetooth Air Interface Probe through USB cable and host PC
- Standby power consumption: <20 mA
- Active power consumption: <350 mA

Bluetooth Radio Specifications

- Bluetooth V1.1 qualified device
- Transmit Power: +20 dBm
- Receiver Sensitivity: <-80 dBm
- Frequency Range: 2.402 – 2.480 GHz
- Compliant with FCC 47CFR part 15.19 USA
- Compliant with RSS-210/RSS-139 Industry Canada
- Compliant with R&TTE directive European Union (EU) and EFTA
- See web site for complete list of regulatory compliance

Physical Characteristics

Dimensions	**mm**	**in.**
Bluetooth Air Interface Probe		
Height	110	4.25
Width (base)	70	2.75
Depth (base)	42	1.625
Complete Bluetooth Protocol Analyzer Package (software, probe, manuals)		
Length	342.90	13.50
Width	234.95	9.25
Depth	133.35	5.25
Weight	**kg**	**lb.**
	1.41	3.10

Environmental – Bluetooth Air Interface Probe

Temperature –
Operating: +5°C to +50°C.
Nonoperating: –20°C to +60°C.

Humidity – 20% to 80%.

Altitude –
Operating: –1000 ft. to 10,000 ft. (–305 meters to 3,050 meters).

▶ Ordering Information

BPA100

Tektronix Bluetooth Protocol Analyzer.

Includes: Bluetooth Protocol Analyzer Software CD, Bluetooth Air Interface Probe, USB interface cable and User Manual.

Contact Tektronix

ASEAN Countries (65) 356-3900

Austria, Central Eastern Europe, Greece, Turkey, Malta & Cyprus +43 2236 8092 0

Belgium +32 (2) 715 89 70

Brazil & South America 55 (11) 3741-8360

Canada 1 (800) 661-5625

Denmark +45 44 850 700

Finland +358 (9) 4783 400

France & North Africa +33 1 69 86 81 81

Germany +49 (221) 94 77 400

Hong Kong (852) 2585-6688

India (91) 80-2275577

Italy +39 (02) 25086 501

Japan (Sony/Tektronix Corporation) 81 (3) 3448-3111

Mexico, Central America & Caribbean 52 (5) 666-6333

The Netherlands +31 23 56 95555

Norway +47 22 07 07 00

People's Republic of China 86 (10) 6235 1230

Poland (48) 22 521 5340

Republic of Korea 82 (2) 528-5299

South Africa +27 11 254-8360

Spain & Portugal +34 91 372 6000

Sweden +46 8 477 65 00

Taiwan 886 (2) 2722-9622

United Kingdom & Eire +44 (0)1344 392000

USA 1 (800) 426-2200

For other areas contact Tektronix, Inc. at: 1 (503) 627-7111

Updated October 1, 2001

For the most up-to-date product information visit our web site at www.tektronix.com

10/01 HB/XBS 5AW-14408-2

Tektronix
Enabling Innovation