BPA105 Bluetooth Protocol Analyzer

▶ BPA105

▶ *The Tektronix BPA105 Bluetooth Protocol Analyzer consists of version 2.4 Analysis Software and the air probe which houses the Bluetooth V1.1 compliant baseband controller and radio.*

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.

The Tektronix Bluetooth Protocol Analyzer BPA100 was designed to meet these demanding and critical needs. It is capable of logging, decoding and displaying all baseband packets that are transmitted within a Bluetooth piconet.

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 user can easily upgrade the BPA105 with free software updates available via the Internet. Tektronix provides frequent software enhancements that address changes to the Bluetooth specification and continually add increased functionality to the protocol analyzer.

▶ Features & Benefits

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

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

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

Powerful API Provides Custom Test Capabilities – Automated Tests and Remote Control of Analyzers over Network

Sync Wizard Simplifies Synchronization and Monitoring Process for All Types of Piconet Configurations

Profile View Displays Only the Applicable Protocols Associated with a Profile for Analysis and Debug

▶ Applications

Identify and Isolate Problems Encountered in All Aspects of Bluetooth Testing from Silicon or Stack Development to Module Integration and Application Software Analysis

Operate As a Known Reference Device in Piconet Mode with Emulation of Common Bluetooth Profiles

Facilitate the Interoperability Testing Process with Complete "Over the Air" Analysis of Bluetooth Transactions and by Sharing Commented Log Files with Other Developers

Automate Testing and Analysis Tasks with HCI Scripting Capabilities and Fully-featured Application Programming Interface (API)

BPA Application Software Can Be Loaded onto any PC and Used as a Viewer for Data Analysis

Tektronix

Enabling Innovation

BPA105 Bluetooth Protocol Analyzer

▶ BPA105

▶ 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.
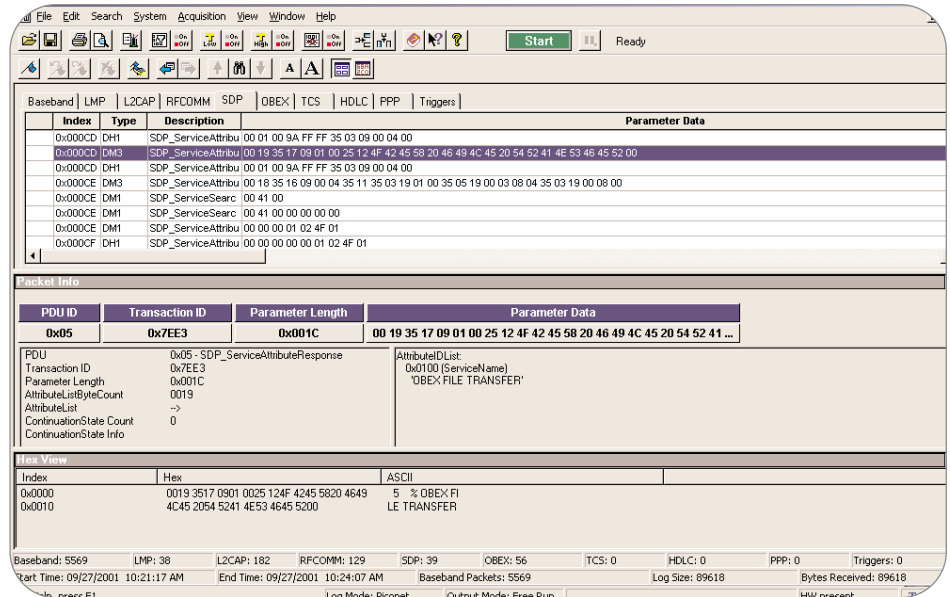
Piconet Mode – In Piconet Mode, the protocol analyzer uses its fully Bluetooth qualified protocol stack and participates as the master or a slave in a piconet. As a master, the protocol analyzer logs all baseband packets between itself and the slaves. When setup as a slave, it logs all packets between 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 2.4

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, BNEP, HID, AT, HCRP, AVCTP, AVDTP 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.

The BPA105 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 BPA105 hardware via the Host Controller Interface layer. The HCI Terminal makes it easy to send commands to a BPA105 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 BPA105 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.

Acquisition Setup Display

▶ 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, BNEP, HID, AT, HCRP, AVCTP, AVDTP 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

Profile View

Profile View allows the user to focus on the analysis of transactions associated with a particular profile. Profile View supports the Advanced Audio Distribution, Audio Visual Remote Control, Basic Printing, Cordless Telephony, Dial-up Networking (DUN), FAX, File Transfer, Generic Object Exchange, Hands-free, Hardcopy Cable Replacement, Headset, Human Interface Device (HID), Imaging, Intercom, LAN Access, Object Push, Personal Area Networking (PAN), Serial Port, Synchronization and Video Distribution Profiles.
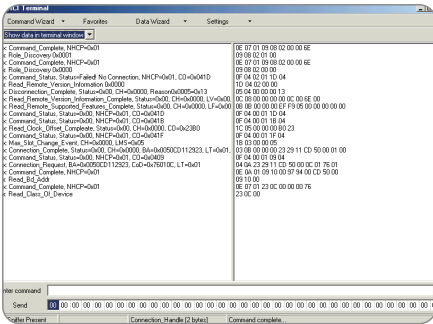
HCI Terminal Application

▶ 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 ensure consistency in testing

Trigger Functionality

Triggering enables the user to selectively acquire data based on occurrence of specific events, error sequences or patterns as defined in trigger machine. Trigger machine supports up to 4 independent sequences with up to 4 events/patterns in each sequence. The BPA trigger machine can generate a trigger out to cross trigger other instrumentation such as a logic analyzer, spectrum analyzer or microprocessor emulation probe. Similar equipment can also be used to drive the trigger to function in order to force the trigger of the BPA based on an external event not visible to the protocol analyzer.

▶ Trigger on baseband packets

▶ Trigger on errors

▶ Trigger on LMP and L2CAP packets

▶ Trigger on RFCOMM packets

▶ Trigger on SDP packets

▶ Trigger on In/Out

▶ Trigger positioning

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
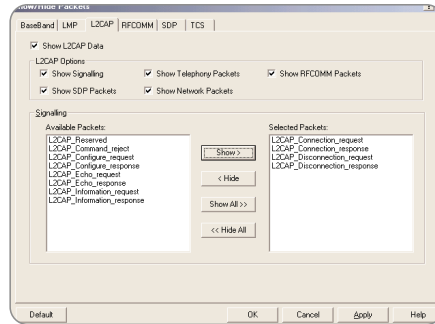
▶ Extensive post-acquisition filtering, combined with large disk-based record size ensures that customers can see all the data and yet filter it for optimal analysis

▶ Pre-acquisition filtering on baseband Access Error, ID, NULL and POLL packets greatly minimizes disk usage

Synchronization

Synchronizing to a Piconet is one of the more difficult tasks encountered when using any protocol analyzer. To ensure success when synchronizing to a Piconet, the BPA provides a Sync Wizard to guide the user through the critical steps of this process.

The User Can Select from the Following Modes to Synchronize to a Piconet:

▶ Sync to a Piconet using master inquiry

▶ Sync to a Piconet using fake connection response

▶ Sync to a Piconet using slave inquiry

Independent Mode Packet Capture and Tracking

When used in Independent Mode the BPA105 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 BPA105 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 to 41 sec

▶ Correlation value between 40 and 64 to indicate the value for accepting a received packet

Data Decryption

▶ Decryption in Independent Mode and Piconet Mode with support for authentication or pairing

▶ Support for both single-session and multi-session operations

BPA105 Bluetooth Protocol Analyzer

▶ BPA105

Application Programming Interface

The API to the BPA Application Software provides access through standard Microsoft COM and DCOM technology. The API provides inter-program operability between the BPA application and other user applications. Over 50 function calls are supported to provide a robust and flexible programmable interface. The API is a standard part of the BPA application software.

System Requirements

▶ Microsoft Windows 98SE, Me, 2000, XP Home or XP Professional

▶ Intel Pentium III, 600 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

▶ BPA105 Air Probe connections: USB, Trigger In/Out, Clock Out

Bluetooth Radio Specifications

▶ Bluetooth V1.1 qualified device

▶ Transmit Power: +20 dBm

▶ Receiver Sensitivity: <−80 dBm

▶ Frequency Range: 2.402 to 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

Bluetooth Air Interface Probe

Dimensions	mm	in.
Height	110	4.25
Width (base)	70	2.75
Depth (base)	42	1.625

Complete Bluetooth Protocol Analyzer Package (software, probe, manuals)

Dimensions	mm	in.
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

BPA105

Tektronix Bluetooth Protocol Analyzer.

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

Our most up-to-date product information is available at: **www.tektronix.com**

CE

09/02   HB/XBS   5AW-14408-4

Tektronix

Enabling Innovation