User Manual

Tektronix

BPA105
Bluetooth Protocol Analyzer

071-XXXX-00

This document applies to firmware version 2.3 and above.

Check for regular BPA Series software updates at www.tektronix.com/bpa_software

www.tektronix.com

Tektronix, Inc., P.O. Box 500, Beaverton, OR 97077

WARRANTY

Tektronix warrants that the products that it manufactures and sells will be free from defects in materials and workmanship for a period of three (3) years from the date of shipment. If a product proves defective during this warranty period, Tektronix, at its option, either will repair the defective product without charge for parts and labor, or will provide a replacement in exchange for the defective product.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period and make suitable arrangements for the performance of service. Customer shall be responsible for packaging and shipping the defective product to the service center designated by Tektronix, with shipping charges prepaid. Tektronix shall pay for the return of the product to Customer if the shipment is to a location within the country in which the Tektronix service center is located. Customer shall be responsible for paying all shipping charges, duties, taxes, and any other charges for products returned to any other locations.

This warranty shall not apply to any defect, failure or damage caused by improper use or improper or inadequate maintenance and care. Tektronix shall not be obligated to furnish service under this warranty a) to repair damage resulting from attempts by personnel other than Tektronix representatives to install, repair or service the product; b) to repair damage resulting from improper use or connection to incompatible equipment; c) to repair any damage or malfunction caused by the use of non-Tektronix supplies; or d) to service a product that has been modified or integrated with other products when the effect of such modification or integration increases the time or difficulty of servicing the product.

THIS WARRANTY IS GIVEN BY TEKTRONIX IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPAIR OR REPLACE DEFECTIVE PRODUCTS IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

WARRANTY

Tektronix warrants that the media on which this software product is furnished and the encoding of the programs on the media will be free from defects in materials and workmanship for a period of three (3) months from the date of shipment. If a medium or encoding proves defective during the warranty period, Tektronix will provide a replacement in exchange for the defective medium. Except as to the media on which this software product is furnished, this software product is provided “as is” without warranty of any kind, either express or implied. Tektronix does not warrant that the functions contained in this software product will meet Customer’s requirements or that the operation of the programs will be uninterrupted or error-free.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period. If Tektronix is unable to provide a replacement that is free from defects in materials and workmanship within a reasonable time thereafter, Customer may terminate the license for this software product and return this software product and any associated materials for credit or refund.

THIS WARRANTY IS GIVEN BY TEKTRONIX IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX’ RESPONSIBILITY TO REPLACE DEFECTIVE MEDIA OR REFUND CUSTOMER’S PAYMENT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

List of Figures

List of Tables

General Safety Summary

Review the following safety precautions to avoid injury and prevent damage to this product or any products connected to it. To avoid potential hazards, use this product only as specified.

Only qualified personnel should perform service procedures.

To Avoid Fire or Personal Injury

Observe All Terminal Ratings. Connect the ground lead of the probe to earth ground only.

Do Not Operate With Suspected Failures. If you suspect there is damage to this product, have it inspected by qualified service personnel.

Do Not Operate in Wet/Damp Conditions.

Do Not Operate in an Explosive Atmosphere.

Keep Product Surfaces Clean and Dry.

Symbols and Terms

Terms in this Manual. These terms may appear in this manual:

WARNING. *Warning statements identify conditions or practices that could result in injury or loss of life.*

CAUTION. *Caution statements identify conditions or practices that could result in damage to this product or other property.*

Symbols on the Product. The following symbols may appear on the product:

CAUTION
Refer to Manual

Preface

This manual provides operating information for the Tektronix BPA105 Bluetooth Protocol Analyzer and is organized into the following sections:

- *Operating Basics p*rovides basic instructions for operating the Tektronix Bluetooth Protocol Analyzer.
- *Reference* provides detailed information on acquiring and analyzing piconet packet data.
- *Appendix A: Specifications* provides hardware specifications and regulatory statements.
- *Appendix B: Accessories* lists the standard accessories.
- *Appendix C: Sample Scripts* provides sample HCI scripts.
- *Glossary* explains the terms used in this manual.

Reference Documents

The following third-party reference documents provide additional information:

- *HCI Terminal Guide* (Digianswer #00-11-03) provides information about using a HCI terminal as an interface with Bluetooth hardware.
- *Bluetooth Revealed* (Prentice Hall, Inc., ISBN 0-13-090294-2) provides background on several areas including the basic technology, the Bluetooth specification with information about the protocol stack, Bluetooth profiles, and the future of the technology.
- *Bluetooth: Connect without Cables* (Prentice Hall, Inc., ISBN 0-13-089840-6) provides less background about the technology and more in-depth information about the protocol stack and other areas. This book provides many diagrams.

***NOTE**. Check for regular BPA Series software updates at www.tektronix.com/bpa_software.*

Contacting Tektronix

Phone	1-800-833-9200*
Address	Tektronix, Inc. Department or name (if known) 14200 SW Karl Braun Drive P.O. Box 500 Beaverton, OR 97077 USA
Web site	www.tektronix.com
Sales support	1-800-833-9200, select option 1*
Service support	1-800-833-9200, select option 2*
Technical support	Email: techsupport@tektronix.com 1-800-833-9200, select option 3* 6:00 a.m. – 5:00 p.m. Pacific time

*** This phone number is toll free in North America. After office hours, please leave a voice mail message.**

Outside North America, contact a Tektronix sales office or distributor; see the Tektronix web site for a list of offices.

Operating Basics

Acquiring Piconet Packet Data

This section introduces you to the basic operation of the Bluetooth Protocol Analyzer. This section contains information on the following topics:

- Monitoring a piconet
- Piconet operating modes
- Understanding the data collection process
- Understanding the application window
- Using the menu and toolbars
- Setting up an acquisition
- Setting up the data filter
- Setting up triggers
- Starting and ending a logging session
- Saving a log session
- Using the HCI Terminal application

Overview

Using the Bluetooth Protocol Analyzer you can connect to and monitor the activity of a Bluetooth piconet and log data containing all of the baseband packets transmitted between the participating Bluetooth devices.

Following data collection, you can display the contents of the files you saved during acquisition and use the analysis features of the Bluetooth Protocol Analyzer to further interpret the data. Detailed information on data analysis is provided in the *Analyzing Piconet Packet Data* section, beginning on page 1–27.

Additionally, the Bluetooth Protocol Analyzer has features that allow you to generate baseband packets containing known errors for testing purposes. Information on error packet generation can be found on page 2–3.

Operating Mode

You can operate the Bluetooth Protocol Analyzer in either Independent or Piconet mode.

Independent Mode. Configured as an independent unit, the Bluetooth Protocol Analyzer does not interact directly in the piconet. Instead, after synchronizing to the net, it passively monitors and logs all baseband packets transmitted between the master and the slaves comprising the piconet. By using the advanced triggering and filter features, you can identify the data you want to log and then analyze it following the session.

Piconet Mode. Configured as a participant in the piconet, the Bluetooth Protocol Analyzer uses a full-protocol stack and participates as the master or a slave in the piconet.

As a master, the Bluetooth Protocol Analyzer logs all baseband packets between itself and the piconet slave device(s). When set up as a slave, it logs all packets between itself and the piconet master as well as between the master and all other slave devices.

For information on how to configure the analyzer for independent or piconet mode operation, see *Logging Mode* on page 1-9.

Collecting Data

With the Bluetooth Protocol Analyzer you can connect to and create a log containing all the baseband packets transmitted between Bluetooth devices in a piconet. Using the analyzer features you can do the following:

- Operate as a member of a piconet, as a stand-alone (independent) unit, or independent with data decryption.
- Select the master or slave to which the Bluetooth Protocol Analyzer is synchronized.
- Set the duration over which the Protocol Analyzer tries to synchronize to a piconet master.
- Capture all baseband packets transmitted within a Bluetooth piconet, including packets that are normally not visible to the host such as retransmitted packets. View the status of each packet and estimated the clock and hop frequency.
- Select specified hopping patterns: Europe/USA, Japan, France, or Spain.
- Transmit and receive on a single user-defined frequency.
- Set a correlation value.

- Turn data whitening on and off.
- Output data to a log file or view as a real-time display.
- Start or stop a logging session manually.
- Enable data decryption in Independent mode.
- Display the paging sequence in Independent mode.
- Filter packets during data acquisition (prior to logging), such as ID, NULL, POLL, and Access Error packets.
- Generate known errors for testing and debugging.

***NOTE**. When you use the Bluetooth Protocol Analyzer with Bluetooth Neighborhood, you must use the Piconet mode (working as a participant in a piconet). When you use the Bluetooth Protocol Analyzer in the Independent mode (working as a passive listener), you cannot use it with Bluetooth Neighborhood.*

Understanding the Data Acquisition Window

Figure 1-1 shows the data acquisition window of the Bluetooth Protocol Analyzer. and identifies each of the functional areas. This is the window that is displayed during data acquisition. Note that when the data acquisition window is the active window, many of the toolbar buttons are disabled.

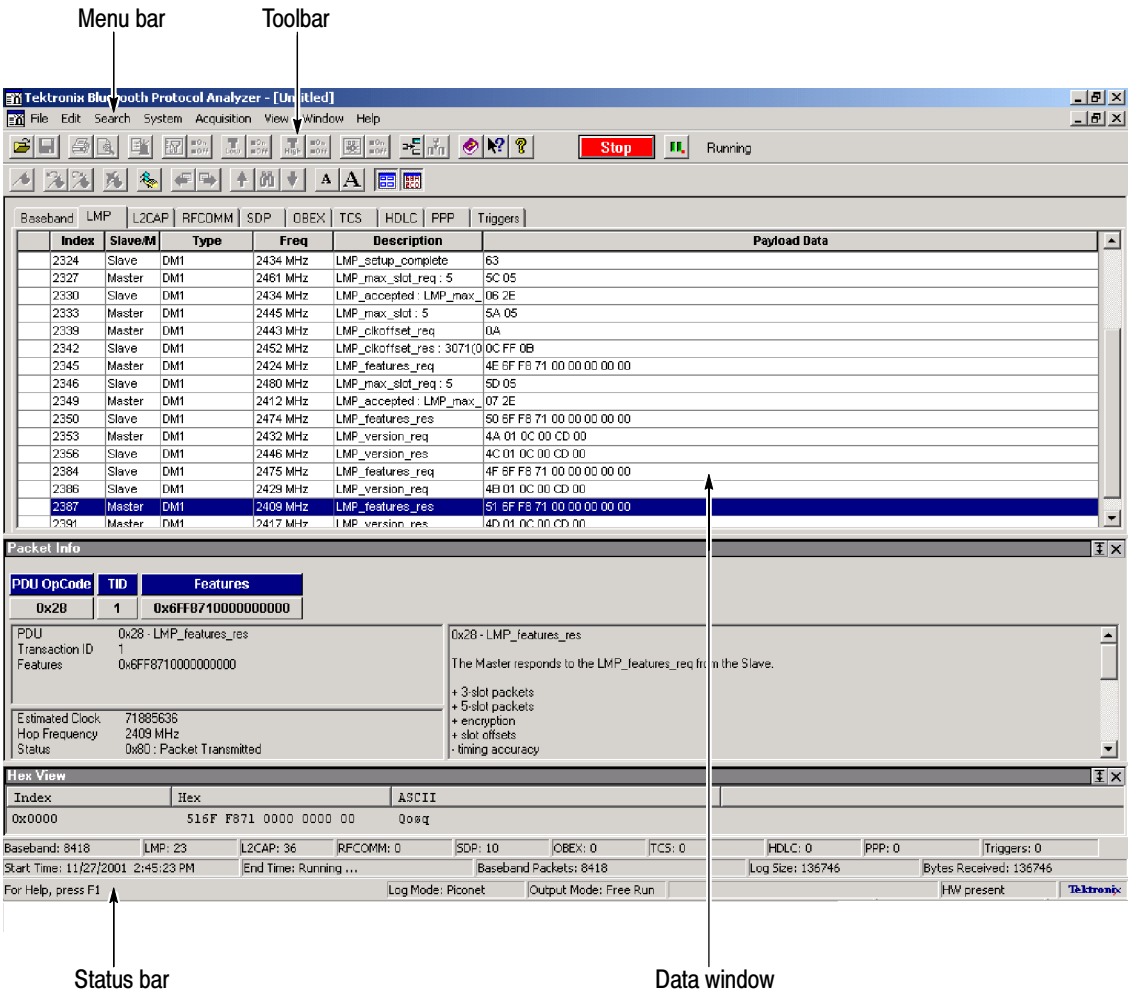


Figure 1-1: The Bluetooth Protocol Analyzer data acquisition window

Menu Bar The Menu Bar hosts the data acquisition and analysis functional menus. The menus and menu selections vary depending on the current analyzer function. Table 1–1 lists the menus that are available during data acquisition.

Toolbars The toolbar contains shortcut buttons for the major analyzer functions. Most toolbar buttons have corresponding menu selections in the Menu Bar. The number and function of the available buttons varies, depending on the type of window you have open. Table 1–1 identifies the acquisition toolbar buttons and their functions.

Status Bar The Status Bar provides useful information on the status of the Bluetooth Protocol Analyzer. View this area for information on the current log session.

Table 1-1: Acquisition window menus and toolbar buttons

Menu	Selection	Function	Toolbar button	Additional information
File >	Open	Use Windows Explorer to browse and open a previously saved log session.		See page 1-27.
	Close	Close a file.		
	Save	Save a file.		
	Save As	Open the Save As dialog box to save a file to a specified location.		See page 1-24.
	Search Files	Search for a file.		
	Export	Export data to a comma separated file (.csv)		
	Properties	Display properties of the active data file.		
	Acquisition Summary	Display acquisition details of the active data file.		
	Send To	Send the active file as email to the mail profile you specify.		
	Print	Print entire or partial contents of the active data file.		
	Print Preview	Display a sample view of the the data file selected for printing.		
	Print Setup	Define the margins and other printer properties for printing data files.		
	Print Window	Print the active window using the Page Setup dialog box.		

Table 1-1: Acquisition window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	1, 2, 3...	Reopen a recently opened file.		
	Exit	Quit the Bluetooth Protocol Analyzer application		
System >	Start Session	Begin an acquisition session using the criteria defined in the Acquisition Setup dialog box.		
	Stop Session	End the current acquisition session.		
	Pause	Click to suspend the current acquisition session. Click again to resume the session.		
	System Properties	Display BPA105 version and copyright information.		
	Tools >	Access executable files set up with the Tools tab of the System Options dialog box.		
	Options	Define packet type display colors; define disk location for storing acquisition log files; identify executable files to be run from the System > Tools menu.		
	Default	Return the factory default settings for the following: acquisition setup, data files, pre- post-trigger, error packet generation.		
Acquisition >	Setup	Define parameters for the next acquisition session.		See page 1-9.
	Data Filter	Specify the packets you do not want to acquire during the next acquisition session in the Data Filter dialog box. These settings become the default settings.		See page 1-14.
	Enable Data Filter	Activate/deactivate the Data Filter dialog box settings.		
	Pre-Post Trigger Buffer	Set the number of packets collected before and after a trigger event in the Pre-Post Trigger Buffer dialog box.		Unless enabled, the post-trigger buffer size is limited only by the disk space available on your PC. See page 1-23 for additional information.

Table 1-1: Acquisition window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	Low Level Trigger	Define trigger events for the next acquisition based on low-level trigger characteristics, such as FLOW, ARQN, hop frequency, payload headers, etc.		See page 1-15.
	Enable Low Level Trigger	Enable/disable settings defined in the Low Level Trigger Setup dialog box.		
	High Level Trigger	Define the trigger events for the next acquisition base on high-level trigger characteristics, such as RFCOMM and SDP protocols.		See page 1-22.
	Enable High Level Trigger	Enable/disable settings defined in the High Level Trigger Setup dialog box.		
	Error Packet Generation	Set error packet generation sequences for testing and debugging, such as FLOW, ARQN, hopping frequency, payload headers, etc.		See page 2-3.
	Enable Error Packet Generation	Enable/disable settings defined in the Error Packet Generator dialog box.		
View >	Toolbar	Enable/disable the toolbar.		See Figure 1-1 on page 1-4.
	Status bar	Enable/disable the status bar.		
	Sync Bar	Enable/disable the synchronization information bar.		Contains status LEDs.
	Session Info Bar	Enable/disable the session information bar.		Displays time stamps.
	Show/Hide Packets	Define which packets you want to display in the List views.		
	Show/Hide Columns	Define which columns you want to display in the List views.		
	Format Columns	Define the data format of the displayed columns: decimal, hex, binary, ASCII.		
Help >	Topics	Display online help contents main menu.		
	Help on window	Display the help topic for the active window.		

Table 1-1: Acquisition window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	What's This?	Point to an element in the display window and obtain a help topic.		
	Technical Support	Access the Tektronix Bluetooth Protocol Analyzer technical support Web site.		Download drivers and software updates. Obtain product-related technical information.
	Customer Feedback	Obtain a request for feedback, thank you, and the product support Web site.		
	About Tektronix Bluetooth Protocol Analyzer	Display Bluetooth Protocol Analyzer software version and copyright.		

Data Window

The data window displays information on the traffic you are currently logging (acquiring). Data windows are either acquisition windows (during data collection) or analysis windows (when you are displaying the contents of a saved acquisition file). See *Analyzing Piconet Packet Data* beginning on page 1–27 for more information on analysis windows.

At the bottom of the data windows the Session Info toolbar displays the following information:

- Start and end times of the last acquisition session
- Number of baseband packets logged
- Log size
- Date

Setting Up an Acquisition

Select **Acquisition > Setup** or click the  shortcut button to display the Acquisition Setup dialog box. (See Figure 1-2.) Use this dialog box to configure the settings for a new logging session.

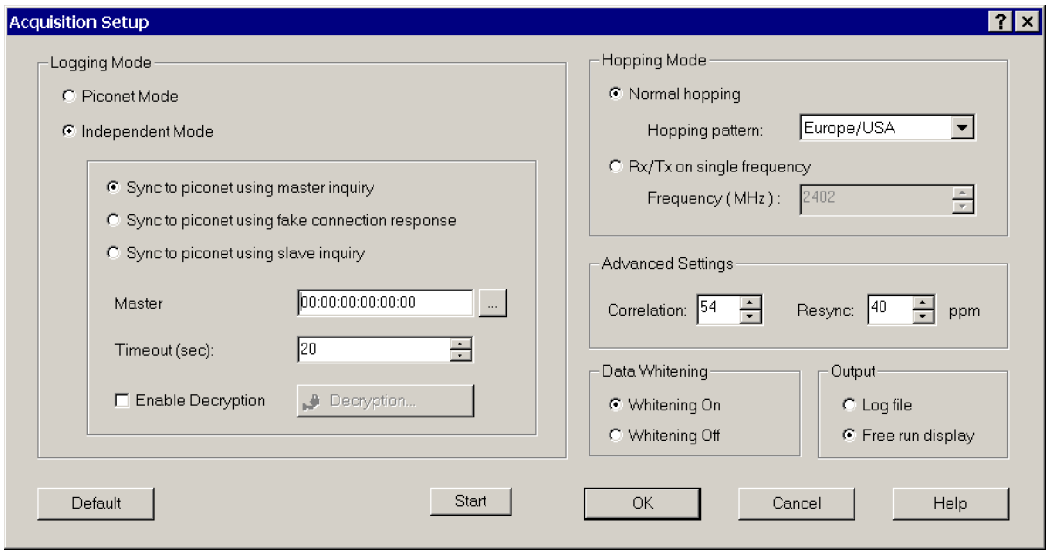


Figure 1-2: Acquisition Set up dialog box

Logging Mode

Before you can start a new logging session, decide whether you will operate the Bluetooth Protocol Analyzer as an active member of a piconet (either as a master or as a slave) or as a stand-alone unit that nonintrusively monitors data flowing across the piconet.

Piconet Mode. Use this mode with the Bluetooth Neighborhood or HCI Terminal to set up the Bluetooth Protocol Analyzer as an active participant in the piconet. When you start a logging session, the analyzer logs all baseband packets sent from and received by your computer, whether the Bluetooth Protocol Analyzer is acting as a slave or a master.

Independent Mode. Use this mode to set up the Bluetooth Protocol Analyzer as a stand-alone unit. When you select this mode, the analyzer displays the Sync bar shown in Figure 1–4 near the bottom of the acquisition window.

Select a synchronization mode:

- Sync to piconet using master inquiry. In this mode, synchronization is obtained by performing an inquiry and using the clock information returned by the master to set the clock of the Bluetooth Protocol Analyzer. You must identify a master in the Select Master dialog box. See *Select Master or Slave* on page 1–11.

  In some Bluetooth devices, the clock drifts away when the device is not in connect mode; this synchronization mode can be troublesome if you want to monitor negotiations during the connect phase. The problem occurs because there are often several seconds of delay from the time when the protocol analyzer obtains the master clock information until the master actually connects to the slave. Likewise, if the inquiry scan mode on the Bluetooth device is not implemented or disabled during the connection, this mode cannot be used for synchronization. See *Resync* on page 1–13.

- Sync to piconet using a fake connection response. This mode can only be used during the connect phase, when the piconet master connects to a new slave. The protocol analyzer operates as if it were the slave unit selected in the Select Slave dialog box (see Figure 1–3 on page 1–11) and obtains the master clock information by initiating a new connection as if it were that slave. Immediately after the clock information is retrieved, the protocol analyzer stops transmitting, and the piconet master continues the connection attempt with the true slave. You must identify a slave in the Select Slaver dialog box. See *Select Master or Slave* on page 1–11.

***NOTE**. The HCI Terminal application provides user control of the Bluetooth Protocol Analyzer in piconet member mode. See the* HCI Terminal *topic on page 1–24.*

- Sync to piconet using slave inquiry. This mode can only be used during the connect phase and is based on the same principle as the method mentioned above in *Sync to piconet using fake connection response*. Instead of pretending to be the slave unit chosen in the Select Slave dialog box (see Figure 1–3), the protocol analyzer listens for the clock information sent in the connect phase to the new piconet slave, and does not interfere with the piconet in any way. To catch the clock information on the right frequency, it is necessary to obtain the slave clock. This is done by performing an inquiry to the slave. You must identify a slave in the Select Slave dialog box. See *Select Master or Slave* on page 1–11.

Select Master or Slave. Click the  shortcut button in the Acquisition dialog box (see Figure 1-2 on page 1-9) to open a Master or Slave dialog box and set up the options to discover and connect to a Bluetooth device within range. See Figure 1-3.

- Inquiry Timeout. Select how long the Bluetooth Protocol Analyzer performs the inquiry process. The default time is 12 seconds. However, you can set the time from 2 seconds to 60 seconds.
- Inquiry Access Code: Enter an inquiry access code (IAC); there are 64 IACs. The default is the General IAC (GIAC), which is 0x9E8B33. The remaining 63 access codes are Dedicated IACs (DIACs). You can set any of the 64 IACs. Although the GIAC is normally used, you can use a DIAC in certain instances.

For example, a group of users might agree to set their devices to a specific DIAC to make their devices easier to discover in an environment with many Bluetooth devices.

- Discover: Click this button to carry out device discovery and display a list of all active Bluetooth devices within range.
- Select: Click on the device name you want to synchronize too; then click **Select** and close the Select Master or Select Slave dialog box.

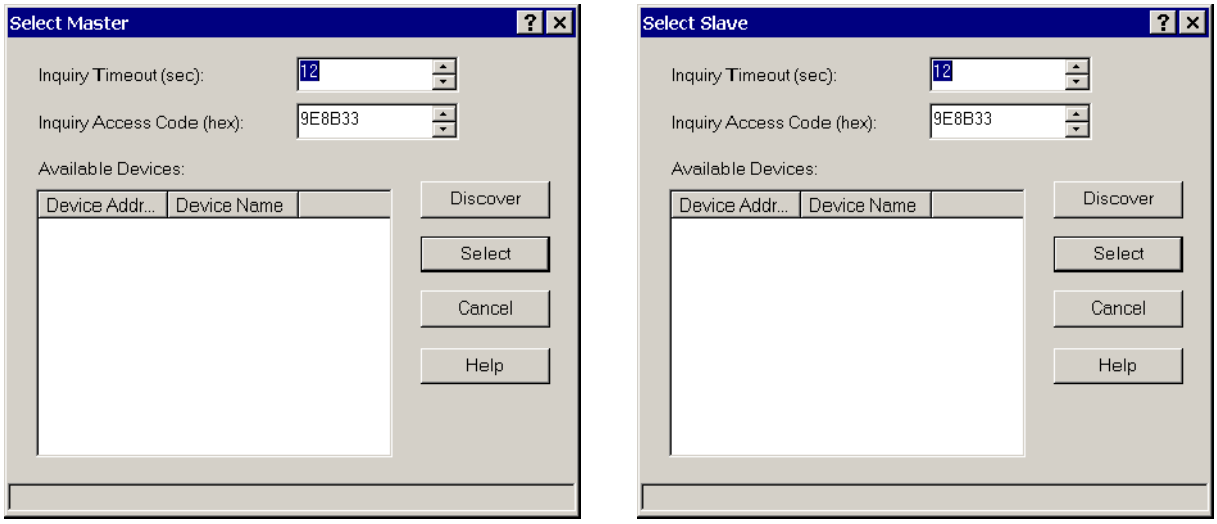


Figure 1-3: Select Master and Select Slave dialog boxes

Acquisition Timeout. In the Acquisition Setup dialog box (see Figure 1–2 on page 1–2), use the Timeout (sec) field to set the number of seconds following synchronization before the Bluetooth Protocol Analyzer loses synchronization if there is no activity on the piconet. In such an event, the Bluetooth Protocol Analyzer will display the message *Out of sync with piconet!*.

NOTE. *When you operate the Bluetooth Protocol Analyzer and Bluetooth Neighborhood together to participant in a piconet, you must use Piconet mode.*

When you operate the Bluetooth Protocol Analyzer in Independent Mode working as a passive listener, you cannot use Bluetooth Neighborhood.

Sync Indication Bar. When you select Independent mode as the logging mode, the acquisition window displays a Sync Bar. See Figure 2–4.

The Sync Bar contains the following indicators:

- Inquiry. This indicator is green when the Bluetooth Protocol Analyzer starts the inquiry procedure during master inquiry or slave inquiry. The indicator changes to red if the target device does not answer within a 60-second timeout.
- PageScan. This indicator is green when the Bluetooth Protocol Analyzer enters the Page scan portion of the synchronization procedure. It is present only if the slave inquiry or fake connection is selected. A timeout is not included as part of this synchronization procedure, consequently, the user can only stop the synchronization by clicking the toolbar Stop button.
- Connect. This indicator is green when the Bluetooth Protocol Analyzer enters the channel hopping sequence (the analyzer searches for first traffic on the piconet). If no traffic is recorded, the indicator changes to red, indicating that synchronization has failed.
- In sync. This indicator turns green when the first packet of the channel hopping sequence is received. If synchronization to the piconet is lost (41-second timeout) the indicator changes to red, indicating that synchronization to the piconet is lost.

Figure 1-4: Acquisition window Sync Bar

Hopping Mode

Specify the piconet search criteria:

- Normal Hopping. Specify the hopping pattern for the geographical area you want (Europe/USA, France, Spain or Japan).
- Rx/Tx on single-frequency. Specify the desired frequency (from 2402 MHz to 2480 MHz). This mode is useful for testing and debugging.

***NOTE**. To meet FCC regulations, the transmit power is reduced from 20 dBm to 0 dBm when operating in the single-frequency mode.*

Advanced Settings

Specify the piconet synchronization parameters:

- Correlation. This value sets the number of bits in the synchronization word of each received packet that must be matched for the packet to be valid. Normally, the radio uses 54 to 64 bits correlation. The default value is 54. The value can range from 40 to 64.
- Resync. This value sets the drift in parts per million. If synchronization is lost during connection, for example when the link enters Park, Sniff or Hold mode, you can enter the drift in PPM. Instead of the normal limit of 250 PPM that a device may drift in Park, Sniff or Hold mode, the user can force the Bluetooth Protocol Analyzer not to use “window search” by setting the resync drift to 40 PPM (default). This is useful if you know that the device has negligible drift and helps ensure that no packets are lost because of the window search.

Data Whitening

You can turn data whitening on or off. By default, this function is on, which is normal operation for Bluetooth devices. Data whitening encrypts all data packets that are sent between Bluetooth devices on a piconet to remove DC bias in the transmitted data. However, for test purposes, you can turn off data whitening. In this test situation all devices must have whitening turned off, or you will get scrambled data.

Output

Specify where to send the data output from your logging session:

- Log file. Send the output to a log file on the PC hard disk. You can open the file and analyze the data later. See *Understanding the Data Analysis Window* on page 1–28 for additional information.
- Free run display. Send the data directly to the List view field in the Acquisition Window to continuously monitor the latest session transactions with real-time screen updates.

In both cases, stop the acquisition and save the data to a file for later analysis.

Setting Up the Data Filter

Select **Acquisition > Data Filter** or click the  shortcut button to display the Data Filter set up dialog box. See Figure 1-5.

The data filter allows you to reduce the amount of data captured during a logging session. This function can greatly reduce the size of the log file, making it easier to work with the data.

You can set up the filter to ignore the following baseband packets: ID, NULL, POLL, and Access Error packets.

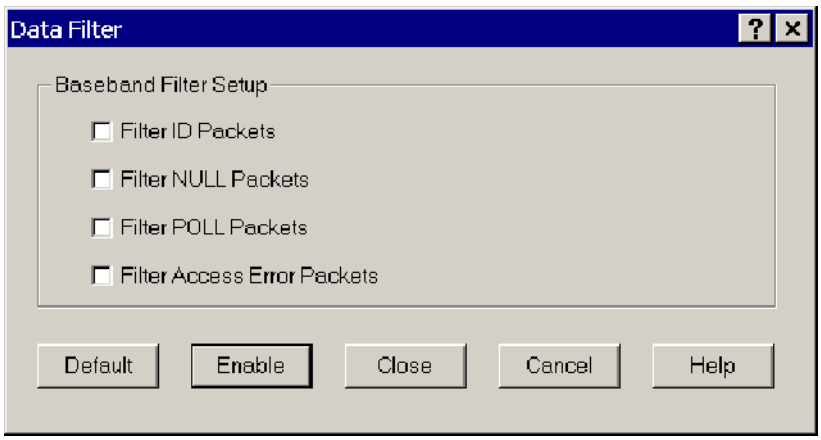


Figure 1-5: Data Filter set up dialog box

Setting Up Triggers

Use the following information to learn more about triggers:

- CIDs (Channel Identifiers) are logical endpoints used in the L2CAP layer to connect with other devices and are vendor-specific. From 0x0040-0xffff, a vendor can implement as needed.
- If you use a Bluetooth device other than Digianswer, the vendor might have used a different CID in the L2CAP layer.
- For Digianswer devices, the SDP layer uses 0x0040 and the RFCOMM layer uses 0x0041. This information is available in the Comments portion of the Customize pattern dialog in LLT. You can also recover this information when performing service discovery for SDP and business card exchange for RFCOMM.

- If a Bluetooth device has a different CID for SDP and RFCOMM, you need to find the CID values and change them in the Customize Pattern dialog box in order to trigger on that pattern. For example, if the Ericsson™ SDP CID is 0x0FFF then you have to change the value in Customize Pattern Data field. You do not need to change the mask value.
- For Digianswer devices:

  DATA: 00 00 41 00 01 73
  MASK: 00 00 FF FF 01 FF
- For other vendors if CID is 0x0FFF

  DATA: 00 00 FF 0F 01 73
  MASK: 00 00 FF FF 01 FF
- For HLT, the application can find the CID value of the other device. This occurs when both devices exchange the CID value before establishing a L2CAP connection between the two devices. It is important for the HLT to have a high pretrigger buffer value set so that the triggers are marked when the log file is loaded. This is the reason HLT sometimes fails to indicate or mark, although it actually triggers at the specified pattern.

Low Level Trigger

Select **Acquisition > Low Level Trigger** or click the 

shortcut button to open the Low Level Trigger Setup dialog box. See Figure 1-6 on page 1-16. Use this dialog box to set up low level triggers.

***NOTE**. Due to hardware limitations, you are allowed only 10 hardware patterns (slots 0 through 9) for low level triggers. See* Hardware Slot Info *on page 1-21.*

Sequences. This field displays the sequences you have created. You can create a maximum of four sequences, each containing a maximum of four patterns. The default sequence is named Trigger. As you create additional sequences, they will automatically be named Trigger1, Trigger2, and Trigger3.

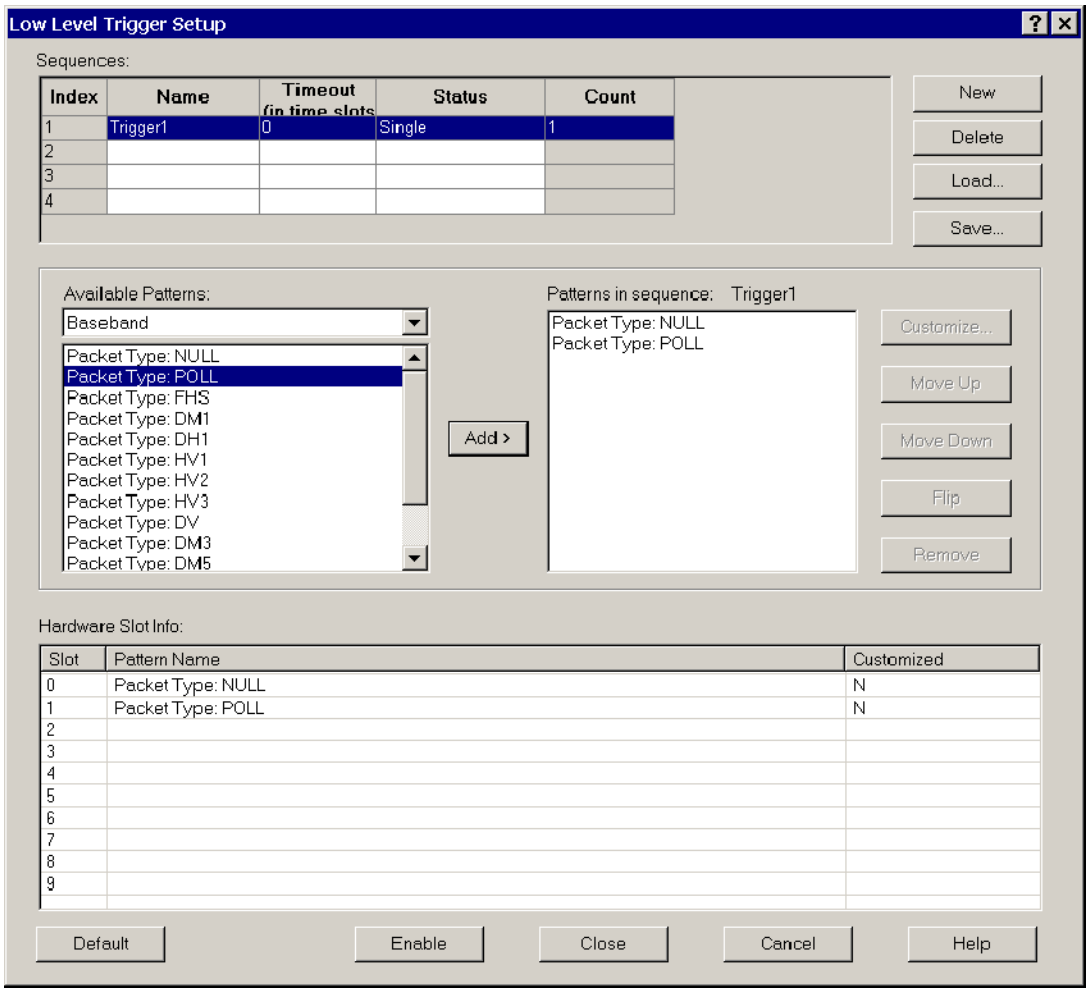


Figure 1-6: Low Level Trigger Setup dialog box

Each sequence is a potential trigger and the sequence that is detected first causes the Bluetooth Protocol Analyzer to begin logging. Occurrences of the remaining sequences are indicated in color and function as markers in the analyzer display.

The color codes are as follows:

- Yellow indicates a pattern in an active sequence.
- Green indicates the final pattern (low and high-level trigger packets).
- Red indicates a time-out.

For example, the following two sequences are set up:

Sequence1 (Status set to Single)
LMP_detach
NULL

Sequence2 (Status set to Single)
LMP_host_connection_request
LMP_accepted

If you monitor a connection establishment followed by a connection detachment, Sequence2 will be found first and will be the trigger. Sequence1 will function as a marker.

The following list describes the elements in the Sequence group at the top of the dialog box:

- Name: This field displays the name of the sequence. Use this field to change the default name of a sequence that you have created.
- Timeout: Use this field to control how long the application looks for the next pattern in a sequence. Enter the value as the number of Bluetooth time units. A Bluetooth time unit is 625 μs. The range for this field is 0 to 65535 time units. If you enter 0, you disable the time-out. If a time-out precludes a sequence from completing, a red marker is indicated in the Bluetooth Packet Analyzer List view and the sequence is reset.
- Status: Use this field to control the status of each of the sequences that you have created and how packets are marked in List views. The following four status selections are available:
  - Off. When selected, the highlighted sequence is disabled and will not be recognized by the Bluetooth Protocol Analyzer.
  - Single. When single is selected, only the first occurring sequence whose patterns occur in their listed order will be marked in the Bluetooth Packet Analyzer display.
  - Repeat. When you select repeat as the status, each time the patterns in the sequence occur in order, they will be marked in the Bluetooth Protocol Analyzer display.
  - Number. When you select number as the status, an additional field called Count is displayed. The value in this field determines the number of times the sequence is marked. You can enter a value from 2 through 200. In all cases, the first sequence to be completed triggers the Bluetooth Protocol Analyzer, and the following sequences are marked in the display.

- Load: Click this button to display the Open dialog box that allows you to browse and open a trigger setup file (*.llt).
- Save: Click this button to display the Save As dialog box that allows you to browse and save a trigger setup file (*.llt).

Available Patterns. This field displays the available patterns for the selected tab. You can add a pattern to a sequence in the following ways:

- Double-click the pattern you want to add.
- Highlight the pattern you want to add, and then click **Add**.
- Drag the pattern you want to add to the Patterns in sequence field.

Patterns in Sequence. This field shows the patterns that are contained in the sequence that is highlighted in the Sequence field. You can add four patterns to a sequence.

Customize Pattern. To activate the Customize button, you must do the following in the Low Level Trigger Setup dialog box (see Figure 1–6 on page 1–16):

1. Set up one or more sequences containing one or more patterns.
2. Select the sequence containing the pattern that you want to modify.
3. Select the pattern that you want to modify.

Once activated, click the **Customize** button to access the Customize Pattern dialog box and set up advanced triggering parameters. See Figure 1–7.

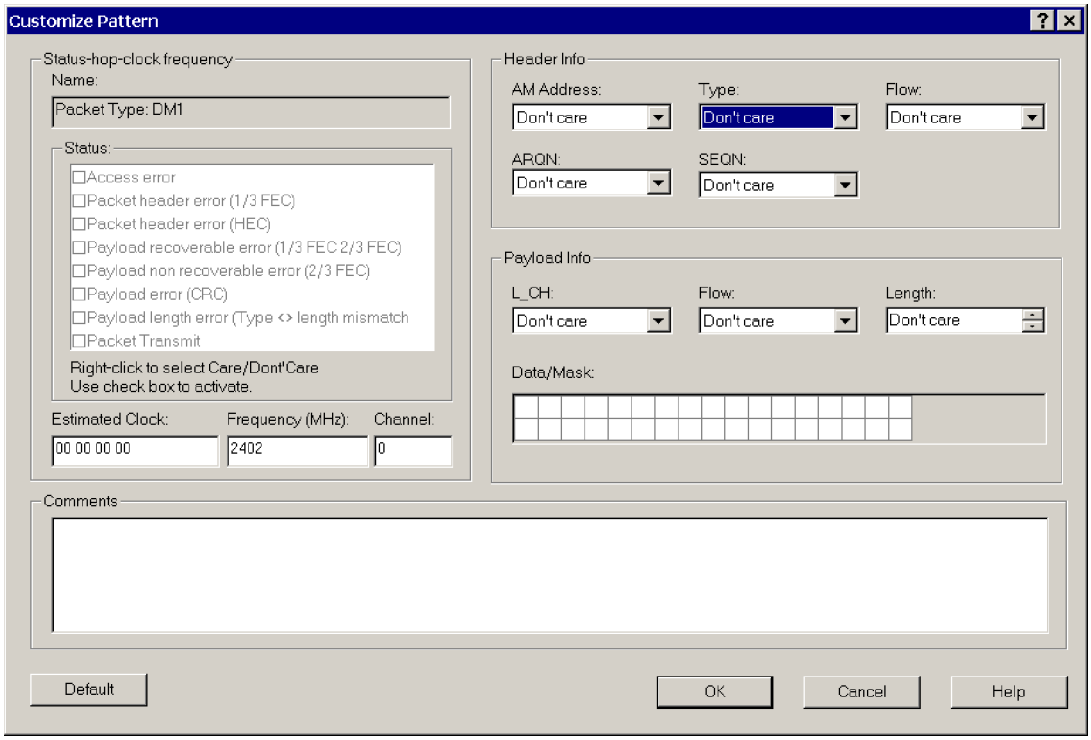


Figure 1-7: Customize Pattern dialog box

NOTE. *You can also access the Customize Pattern dialog box by double-clicking a pattern in the Patterns in sequence field in the Low Level Trigger Setup dialog box (see Figure 1-6 on page 1-16).*

The fields in the Customize Pattern dialog box are described below:

- Name: This field displays the name of the pattern that you selected to customize in the Low Level Trigger-Setup dialog box (see Figure 1-6 on page 1-16).
- Status Option Boxes: This field contains information about the status of the packet. This is a different field from Status in the Low Level Trigger-Setup dialog box. Here Status indicates whether the packet is an Rx or Tx packet. For a receive packet, this field also may contain information about errors that were in the packet (for example, Header Errors and Payload Errors). There are no restrictions in what can be specified, so it is possible to specify a trigger on a Tx packet with access error, although this is not a combination that can occur. You can also specify the bits to be “don’t care”.

  All the fields in Customize pattern dialog box are used to set conditions for triggers to occur. In the Status field you can set some conditions like trigger

only if an error occurs. The following options are available in the Status field:

- Access error
- Packet header error (1/3 FEC)
- Packet header error (HEC)
- Payload recoverable error
- Payload non-recoverable error
- Payload error
- Payload length error
- Packet transmit

By right-clicking you can enable and set the condition or make the condition "don't care." For example, if you select the the third option, then trigger on that pattern occurs only if there is an HEC error in that pattern. If you select the eighth option, trigger occurs only if that pattern is transmitted.

- Estimated Clock: This is the Bluetooth clock for the master used in the piconet. X specifies that four bits are "don't care". For example, XXXXXXXX causes the entire estimated clock is to be ignored in the triggering.
- Frequency: In this two-part field, you can enter a specific frequency. In addition to the frequency, the channel is displayed (on the right). The mapping from frequency to channel is (Freq = 2402 + Channel), and the mapping goes both ways. For example, if you specified channel 10, the frequency field automatically displays 2412. You can also select "don't care" for these bits.
- AM Address: This field sets the Active Member (AM) address. This address is used to access different members in the piconet. Three bits are used for this address, that is, eight different AM addresses are available. AM_ADDR = 0 is used for broadcast. You can also select "don't care" for these bits.
- Type: This field specifies the packet type. Four bits are used for the packet type, that is, 16 different Packet types are available. You can specify only the packets that are not reserved. You can also select "don't care" for these bits.
- Flow: One bit is used for flow control in the header. Flow = 0 means STOP; Flow = 1 means GO. You can also select "don't care" for this bit.
- ARQN: One bit is used for acknowledgement of the last transmission. If a packet is received correctly, the ARQN bit is set to 1 in the return packet. You can also select "don't care" for this bit.

- SEQN. The SEQN is a sequential numbering used to detect retransmission. You can also select “don’t care” for this bit.
- L_CH: This field specifies the Logical Channel. This field is two bits and is used to indicate if the packet is an LMP message or an L2CAP fragment.
- Flow: This flow bit is used to control flow on the L2CAP level. One bit is used for flow control in the payload. Flow = 0 means STOP; Flow = 1 means GO. You can also select “don’t care” for this bit.
- Length: This field allows you to select a specific length to trigger on. The length can be from 0–339, and you can also select “don’t care”.
- Data/Mask: This field specifies the payload data (the first row) and the mask that is used with the data (the second row). A mask of FF will mask in the whole byte and a mask of 00 will mask out the whole byte. The position of the mask and Data is linked together so that the value in data index 1 links to the mask at mask index 1 and so on.
- Comments: You can use this field to enter additional information (notes) about the specified pattern.

Hardware Slot Info. This field shows information about the patterns you have loaded into hardware. There are ten hardware slots into which you can load patterns.

***NOTE**. Due to hardware limitations, you are only allowed 10 hardware patterns (slots 0 through 9) for low level triggers.*

High Level Trigger

Select **Acquisition > High Level Trigger** or click the 

shortcut button to open the High Level Trigger Setup dialog box. See Figure 1–8. Use this dialog box to set up high level triggers for the RFCOMM protocol and the Service Discovery Protocol (SDP).

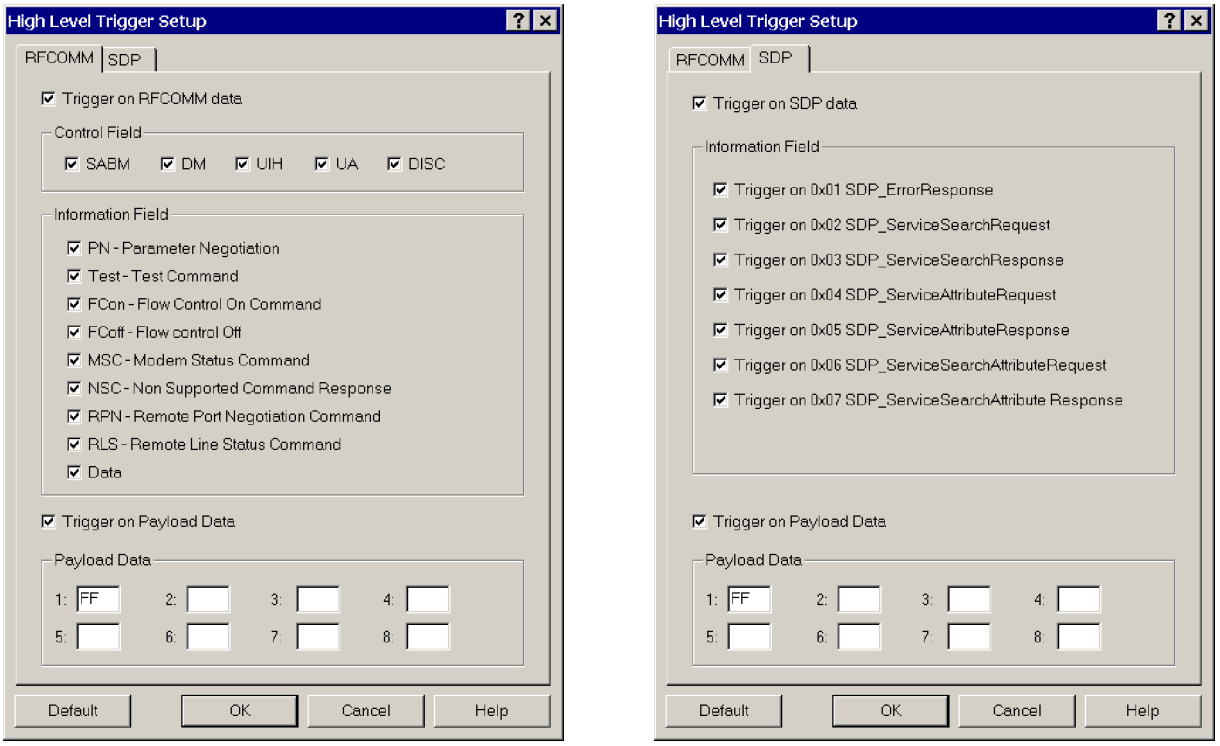


Figure 1-8: High Level Trigger Setup dialog box

To set up and/or trigger on RFCOMM or SDP protocols, you must check the Trigger on RFCOMM data or Trigger on SDP data option box.

RFCOMM Tab. When you click the RFCOMM tab and select the Trigger on RFCOMM Data option box, you can select from among the following control fields: SABM, DM, UIH, UA, and DISC. If you check UIH, additional information fields become active.

You can also select Trigger on Payload Data to set up a trigger on the first 8 bytes of payload data. (Values for each byte are 0 through FF.) Empty fields mean Don't Care. For RFCOMM, the Payload data starts at the second byte of the RFCOMM information field; for SDP, the Payload data starts from the first byte of the SDP parameter data part.

SPD Tab. When you click the SDP tab in the High Level Trigger Setup dialog box and select the Trigger on SDP Data box, you can do the following:

- Select from among various SDP information fields.
- Select Trig on Payload Data to set up a trigger on the first 8 bytes of payload data. (Values for each byte are 0 through FF.)

Pre- Post-Trigger Buffer

Select **Acquisition > Pre-Post Trigger Buffer** to display the Pre-Post Trigger Buffer dialog box for setting pre-trigger and post-trigger buffer sizes. See Figure 1–9.

Use this dialog box to set how many packets are saved prior to the trigger event (0 to 100,000) and how many packets are saved after the trigger event (up to 3,200,000).

***NOTE**. If you do not check the* Enable Post Trigger *box, post-trigger data is saved until you manually stop the logging or the hard disk becomes full.*

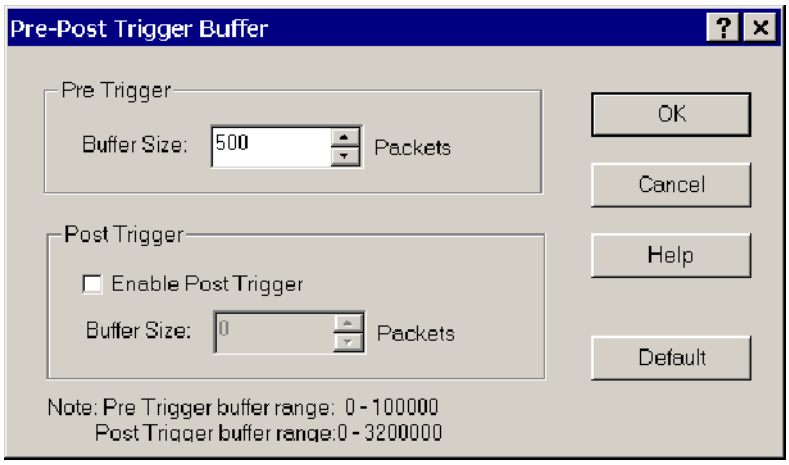


Figure 1-9: Pre-Post Trigger Buffer set up dialog box

Starting a Logging Session

Select **System > Start Session** or click the Start button to begin logging. A secondary window will open within the application window to display the session views. A description of the List, Packet, and Hex session views begins on page 1-35.

If you configured the Acquisition Setup dialog box Output option button for *Free run display*, you can use one of the following methods to pause the automatic screen updates during a session:

- Select **System > Pause** in the menu bar.
- Click the  shortcut button in the tool bar.
- Press the ESC key on your computer keyboard.

Ending a Logging Session

Select **System > Stop Session** or click the Stop button to discontinue the current logging session. When the sessions ends, you will find the following information displayed at the bottom of the application window:

- Start and end times of the logging session
- Number of baseband packets logged
- Log size

Saving the Current Logging Session

Stop the current log session, and then select **File > Save As** or click the  shortcut button. Save the current logging session (.tba file) to a specified location using the displayed Save As dialog box.

Using the HCI Terminal Application

The HCI Terminal application (included on the BPA105 Bluetooth Protocol Analyzer product software disk) provides a hardware interface similar to the interface provided by an AT terminal application when communicating with a modem. The HCI Terminal application provides control of the BPA105 Bluetooth Protocol Analyzer in piconet member mode. This is similar to using the Bluetooth Neighborhood from the Software Suite. For further information on this product, refer to the documentation available on disk.

How to Create HCI Scripts. The *HCI Terminal Guide* (also available on the BPA105 Bluetooth Protocol Analyzer product software disk) describes the functionality of the script language. The sample scripts provided in *Appendix C: Sample Scripts* on page C–1 of this manual, will help you to understand HCI scripting.

NOTE*. The HCI Terminal application and Bluetooth Neighborhood cannot be simultaneously. For error generation, you are advised to use the HCI terminal instead of Bluetooth Neighborhood.*

Analyzing Piconet Packet Data

This section includes information on the following topics:

- Opening a log file
- Understanding the analysis window
- Using the menus and toolbars
- Interpreting data in the List, Packet Information, and Hex views

You can perform the following operations on the data files you logged and saved during acquisition:

- Search for files
- Export data to comma separated value (.CSV) files that you can read with other applications, such as Microsoft Excel
- Add or remove bookmarks
- Display a summary that includes session information and packet count
- Analyze and decode packet information at Baseband, LMP, L2CAP, RFCOMM, SDP, OBEX, TCS, HDLC, and PPP protocol levels
- Display error packets and access errors
- Identify trigger packets and defined sequences

Opening a Data File

To open a data file for analysis, do the following:

- Select **File > Open** or click the  shortcut button to display the Open dialog box.
- Browse to the folder containing your saved acquisition files with the .data extension.
- Select the file you want to open.
- Click **OK**.

Understanding the Data Analysis Window

The Bluetooth Protocol Analyzer opens each data file separately within the application window. Figure 1–10 identifies the functional areas available for data analysis.

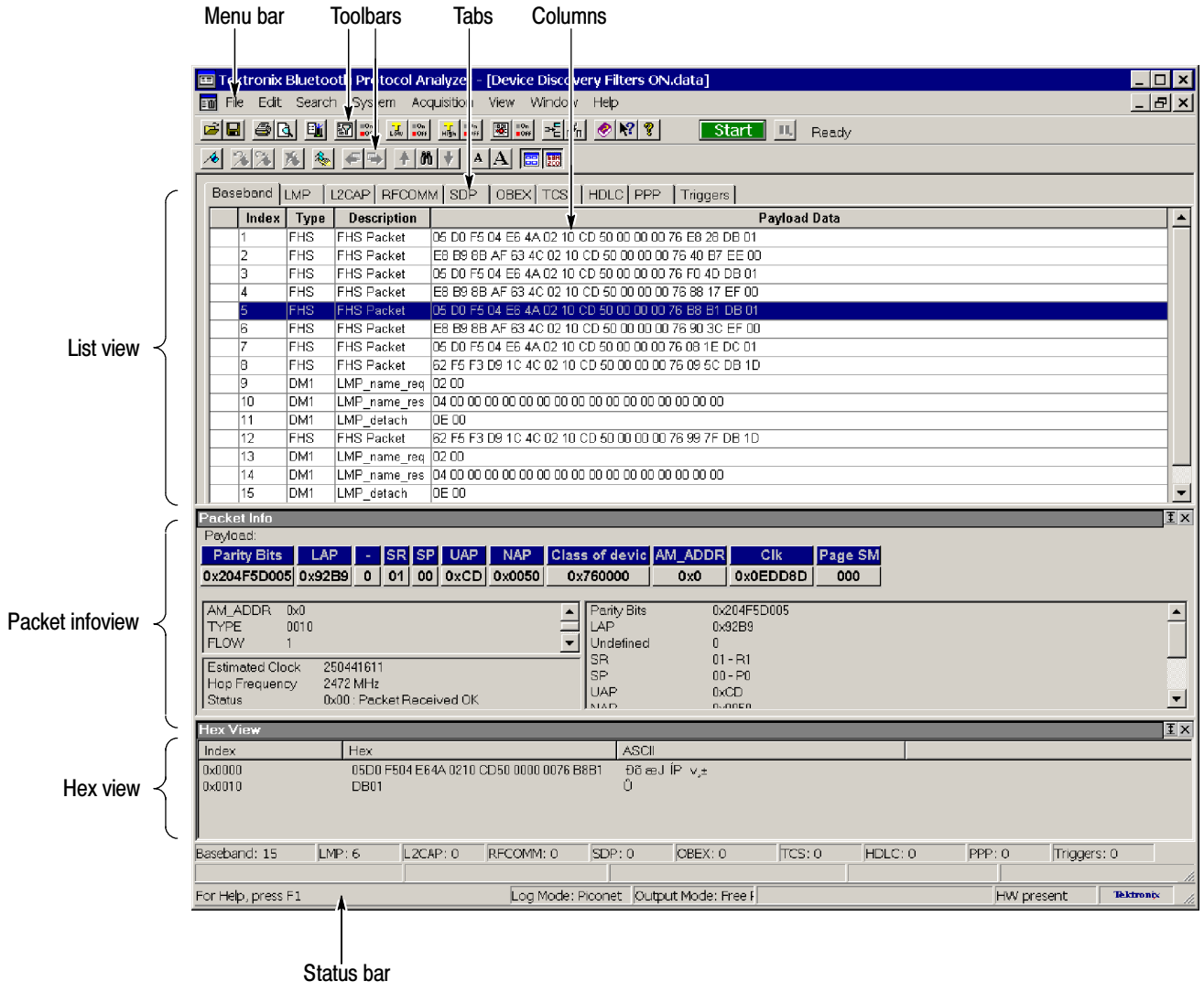


Figure 1-10: The Bluetooth Protocol Analyzer data analysis window

Menu Bar Table 1-2 lists the menus that are available when a file is open.

Toolbars The toolbars contain shortcut buttons. Table 1-2 identifies the analysis toolbar buttons and explains their functions. Most toolbar buttons have a corresponding menu selection in the menu bar.

Table 1-2: Analysis window menus and toolbar buttons

Menu	Selection	Function	Toolbar button	Additional information
File >	Open	Use Windows Explorer to browse and open a previously saved log session.		See page 1-27.
	Close	Close a file.		
	Save	Save a file.		
	Save As	Open the Save As dialog box to save a file to a specified location.		See page 1-24.
	Search Files	Search for a file.		
	Export	Export data to a comma separated file (.csv)		
	Properties	Display properties of the active data file.		
	Acquisition Summary	Display acquisition details of the active data file.		
	Send To	Send the active file as email to the mail profile you specify.		
	Print	Print entire or partial contents of the active data file.		
	Print Preview	Display a sample view of the the data file selected for printing.		
	Print Setup	Define the margins and other printer properties for printing data files.		
	Print Window	Print the active window using the Page Setup dialog box.		
	1, 2, 3...	Reopen a recently opened file.		
	Exit	Quit the Bluetooth Protocol Analyzer application		
Edit >	Add/Remove Bookmark	Toggle a bookmark on or off for the packet that you have highlighted in the List view.		See page 2-1.

Table 1-2: Analysis window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	Add Comment	Add a comment to the selected packet in the List view. Comments are displayed in the Navigate Bookmarks dialog box.		
	Goto Prev Bookmark	Select the previous packet in the List view with a bookmark.		
	Goto Next Bookmark	Select the next packet in the List view with a bookmark.		
	Clear All Bookmark	Remove all bookmarks from the List view.		
	Navigates Bookmarks	Open the Bookmarks dialog box so you can: ■ Jump to a specified bookmark in the List view. ■ Display a bookmarked comment. ■ Display the time difference between two bookmarked packets.		
	Go One Level Back	Move to the previous protocol level List view that the selected packet appears in. The currently selected packet is also selected in the new view.		You can also press the Backspace key.
	Go To Next Level	Move to the next higher protocol level List view that the selected packet appears in. The currently selected packet is also selected in the new view.		You can also press the Enter key.
	L2CAP Connection Properties	Set the L2CAP packet type for packets that cannot be decoded from previous acquisitions.		
	Highlight L2CAP Connection	Highlight all packets with the same L2CAP connection properties as the selected packet.		You can set the highlight color in the Color tab of the System Options dialog box.
	Highlight AM_ADDR	Highlight all packets with the same AM_ADDR value as the selected packet.		You can set the highlight color in the Color tab of the System Options dialog box.
	Highlight Fragmentation	Hghlight the packets associated with the selected fragment.		Fragmentation occurs when payload data is too large and must be segmented and transmitted in more than one packet.

Table 1-2: Analysis window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	Clear Highlights	Clear all highlighting in all of the List views.		
	Toggle Hex/ASCII in Payload	Toggle payload display of the selected packet between hexadecimal and ASCII format in the List view.		
	Clear Toggled Fields	Return all toggled fields to their original format.		Does not affect bookmarks.
Search >	Find	Search for specific data in the active List view using the various parameters.		
	Find Prev	Select the previous packet in the List view that contains data that matches the search criteria last entered in the Find dialog box.		
	Find Next	Select the next packet in the List view that contains data that matches the search criteria last entered in the Find dialog box.		
System >	Start Session	Begin an acquisition session using the criteria defined in the Acquisition Setup dialog box.		
	Stop Session	End the current acquisition session.		
	Pause	Click to suspend the current acquisition session. Click again to resume the session.		
	System Properties	Display BPA105 version and copyright information.		
	Tools >	Access executable files set up with the Tools tab of the System Options dialog box.		
	Options	Define packet type display colors; define disk location for storing acquisition log files; identify executable files to be run from the System > Tools menu.		
	Default	Return the factory default settings for the following: acquisition setup, data files, pre- post-trigger, error packet generation.		

Table 1-2: Analysis window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
Acquisition >	Setup	Define parameters for the next acquisition session.		See page 1-9.
	Data Filter	Specify the packets you do not want to acquire during the next acquisition session in the Data Filter dialog box. These settings become the default settings.		See page 1-14.
	Enable Data Filter	Activate/deactivate the Data Filter dialog box settings.		
	Pre-Post Trigger Buffer	Set the number of packets collected before and after a trigger event in the Pre-Post Trigger Buffer dialog box.		Unless enabled, the post-trigger buffer size is limited only by the disk space available on your PC. See page 1-23 for additional information.
	Low Level Trigger	Define trigger events for the next acquisition based on low-level trigger characteristics, such as FLOW, ARQN, hop frequency, payload headers, etc.		See page 1-15.
	Enable Low Level Trigger	Enable/disable settings defined in the Low Level Trigger Setup dialog box.		
	High Level Trigger	Define the trigger events for the next acquisition base on high-level trigger characteristics, such as RFCOMM and SDP protocols.		See page 1-22.
	Enable High Level Trigger	Enable/disable settings defined in the High Level Trigger Setup dialog box.		
	Error Packet Generation	Set up error packet generation sequences for testing and debugging, such as FLOW, ARQN, hopping frequency, payload headers, etc.		See page 2-3.
	Enable Error Packet Generation	Enable/disable settings defined in the Error Packet Generator dialog box.		
View >	Toolbar	Enable/disable the toolbar.		See Figure 1-1 on page 1-4.
	Status bar	Enable/disable the status bar.		
	Log Toolbar	Enable/disable the log toolbar.		Contains navigation buttons.
	Log Statusbar	Enable/disable the log statusbar.		Displays packet information.

Table 1-2: Analysis window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	Sync Bar	Enable/disable the synchronization information bar.		Contains status LEDs.
	Session Info Bar	Enable/disable the session information bar.		Displays time stamps.
	Show/Hide Packets	Define which packets you want to display in the List views.		
	Show/Hide Columns	Define which columns you want to display in the List views.		
	Format Columns	Define the data format of the displayed columns: decimal, hex, binary, ASCII.		
	Smaller Font	Decrease the font size of the text in the active window.		
	Larger Font	Increase the font size of the text in the active window.		
	Default Font	Return the text in the active window to the default font size.		
	Hex View	Show/hide Hexadecimal view window		
	Packet Info	Show/hide Packet Information view window		
	Vertical Lines	Toggles the vertical lines that define the columns of the List view on or off.		
	Horizontal Lines	Toggle the horizontal lines that define the rows of the List view on or off.		
	Wrap Payload Data	Wrap/unwrap the data within the selected payload cell.		
Window >	New Window	Open a duplicate window showing the current view.		
	Cascade	Overlap all windows within the Application window from upper-left to lower-right.		
	Tile Horizontally	Adjust window size horizontally within the Application window and position them side-by-side.		

Table 1-2: Analysis window menus and toolbar buttons (Cont.)

Menu	Selection	Function	Toolbar button	Additional information
	Tile Vertically	Adjust window size vertically within the Application window and position them side-by-side.		
	Minimize All	Minimize all windows to icons at the bottom of the Application window. Click an icon to return a window to its original size.		
	Split	Specify the bottom edge of List views in the active window.		
	1, 2, 3...	Display a list of the open windows.		The window you select from the list becomes the active window.
Help >	Topics	Display online help contents main menu.		
	Help on window	Display the help topic for the active window.		
	What's This?	Point to an element in the display window and obtain a help topic.		
	Technical Support	Access the Tektronix Bluetooth Protocol Analyzer technical support Web site.		Download drivers and software updates. Obtain product-related technical information.
	Customer Feedback	Obtain a request for feedback, thank you, and the product support Web site.		
	About Tektronix Bluetooth Protocol Analyzer	Display Bluetooth Protocol Analyzer software version and copyright.		

Tabs

Table 1-3 lists the tabs available in the Analysis window. Click on the tabs to select which packet types you want to display in the List view. For example, you can click on the Triggers tab to view the triggers that you have set up.

Table 1-3: Packet tabs

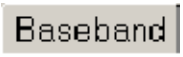
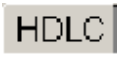
Tab	Tab Icon	Function	Additional information
Baseband		View all baseband packets.	See page 1-27.
LMP		View all LMP packets.	

Table 1-3: (Cont.)Packet tabs

Tab	Tab Icon	Function	Additional information
L2CAP			
RFCOMM			
SDP			
OBEX		View file transfer and business card data.	
TCS		View the protocol discriminator, message type, and other data (depending upon the message type).	
HDLC			
PPP			
Triggers		View defined triggers and trigger arming events.	

Status Bar

The Status Bar displays the number of packets logged of the type: Baseband, LMP, L2CAP, RFCOMM, SDP, OBEX, TCS, HDLC, and PPP. It also displays the number of trigger packets and indicates whether a filter is selected for the packet type being displayed (see *Setting Up the Data Filter* on page 1–14).

List View

The List view displays the contents of the active file as a list of the packets that the file contains. During an acquisition, if the system is configured for free run mode, the List view will display packet data as it is received and logged. You can start and stop the automatic screen updates during an acquisition by pressing the Esc key on your keyboard.

NOTE*. If the Acquisition Setup is set to* Free run display *mode, clicking the tabs will change the protocol levels but it will not maintain highlighting or necessarily display the same packet.*

Columns. These columns reflect the elements that you configured in the View Setup, where you can decide which elements you want the List view to show. For additional information, see *Setting Up an Acquisition* on page 1–9.

Bookmarks. Bookmarks allow you to quickly display packets that you have highlighted (marked) in the List view. You can also measure the time between any two bookmarks. For additional information on bookmarks, see page 2-1.

Context Menu. You can right-click in the List view area of the analysis window to display the context-sensitive menu shown in Figure 1-11. See page 1-29 for additional information on these Edit menu selections.

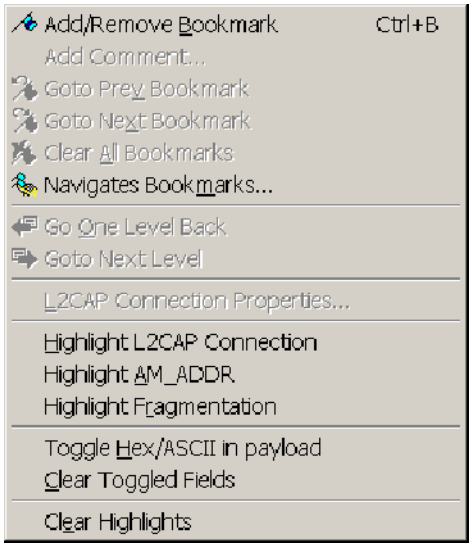


Figure 1-11: List view context-sensitive menu

Packet Info View

This area displays information on the packet currently highlighted in the List view. The type of information that is displayed depends on the type and contents of the packet. Various elements (columns) of packet data can be switched off or on in the View Setup dialog box. For additional information, see *Setting Up an Acquisition* on page 1-9.

Hex View

The List view only displays the first several bytes of the entire payload (unless Wrap Payload Data is selected from the View menu). If you want to view the entire contents of a packet of any length, open a Hex view (**View > Hex View**)

Reference

Reference

In this section you will find information on the following topics:

- Using bookmarks
- Exporting data
- Generating error packet data
- Enabling decryption

Using Bookmarks

In the menu bar, select **Edit > Add/Remove Bookmark** or click the  shortcut button to toggle a bookmark on or off for the packet you have highlighted (clicked on) in the List view. When a bookmark is assigned to a packet, a blue arrow is placed at the left side of the Index field for the highlighted packet. See Figure 2-1.

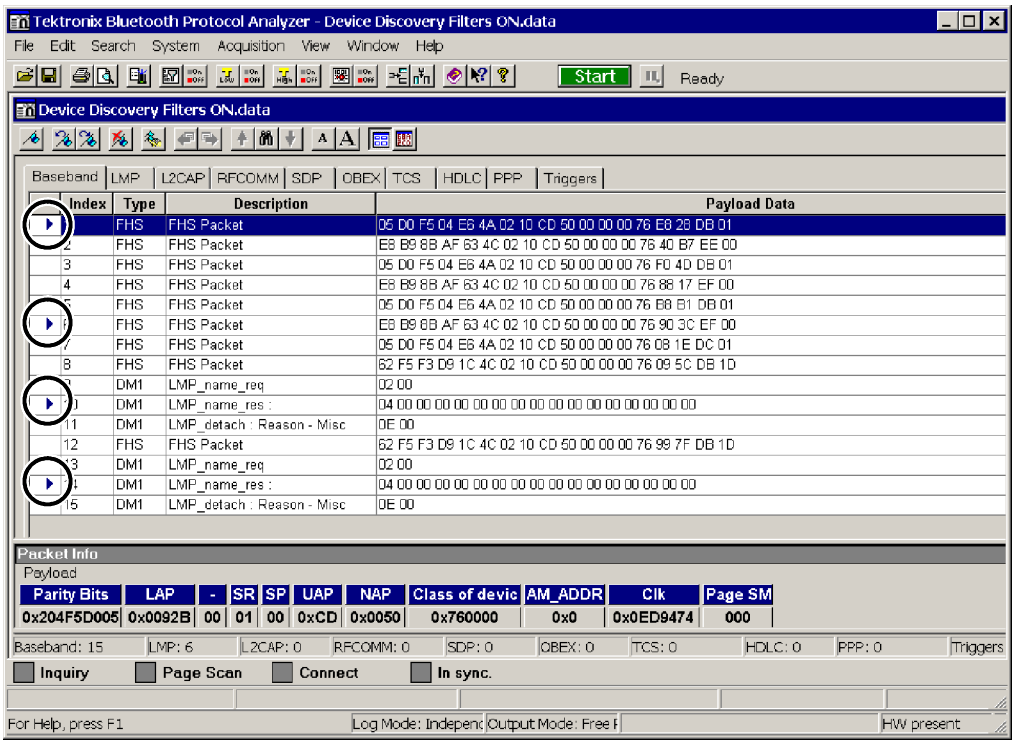


Figure 2-1: Analysis window showing bookmarked packets

Bookmarks allow you to quickly display packets you are interested in. To move between bookmarked packets, select **Edit > Goto Prev Bookmark** or **Edit > Goto Next Bookmark**.

You can also click the  or  shortcut buttons.

Measure the Time Between Bookmarks

To measure the time between any two bookmarks, select **Edit > Navigate Bookmarks** to open the Bookmarks dialog box (see Figure 2–2). First click one of the bookmarks to select it; then control-click the other bookmark to highlight it. Read the time between the bookmarks at the bottom of the Bookmarks dialog box. The timespan is displayed in hours, minutes, seconds, or microseconds. Also, time is shown in timeticks (625 µs per timetick).

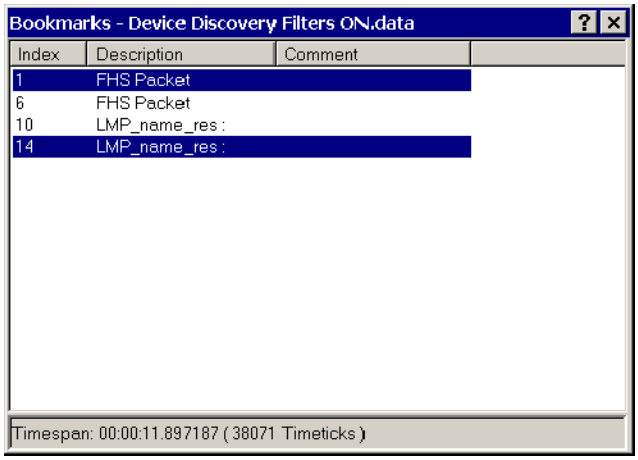


Figure 2-2: Bookmarks dialog box

To remove all bookmarks from the active List view, click the  shortcut button.

Exporting Data

To export acquisition data from a log file, do the following:

1. Select **File > Export**.
2. In the Export Data dialog box, select the destination path and folder.
3. Name the file.
4. Select a file type from the drop-down list box.
5. Add comment text if desired.
6. Click **Save**.

Generating Error Packet Data

To successfully generate errors you must meet the following requirements:

- Participate in a piconet using Piconet mode. See S*etting Up an Acquisition* on page 1-9.
- Define one or more sequences with bit errors (see *Defining Bit Errors* on page 2-5), and a pattern for each sequence (see *Defining Error Patterns* on page 2-6) in the Error Packet Generator dialog box.
- Disable Low Level Trigger in the Bluetooth Protocol Analyzer toolbar.
- Enabled Error Packet Generation in the Bluetooth Protocol Analyzer toolbar.

Error Packet Generator Dialog Box

Select **Acquisition > Error Packet Generation** or click the  shortcut button to open the Error Packet Generator dialog box. See Figure 2-3.

The Error Packet Generator dialog box allows you to generate error packets for testing the handling of errors and possible retransmissions. You can use error generation to cross-check error-correcting algorithms, such as FEC, HEC, and CRC. You can also generate error packets for any baseband packet, such as DM1, DM3, POLL, etc. Errors can be introduced as individual bits in the header, payload, or custom-defined bit positions of the packet.

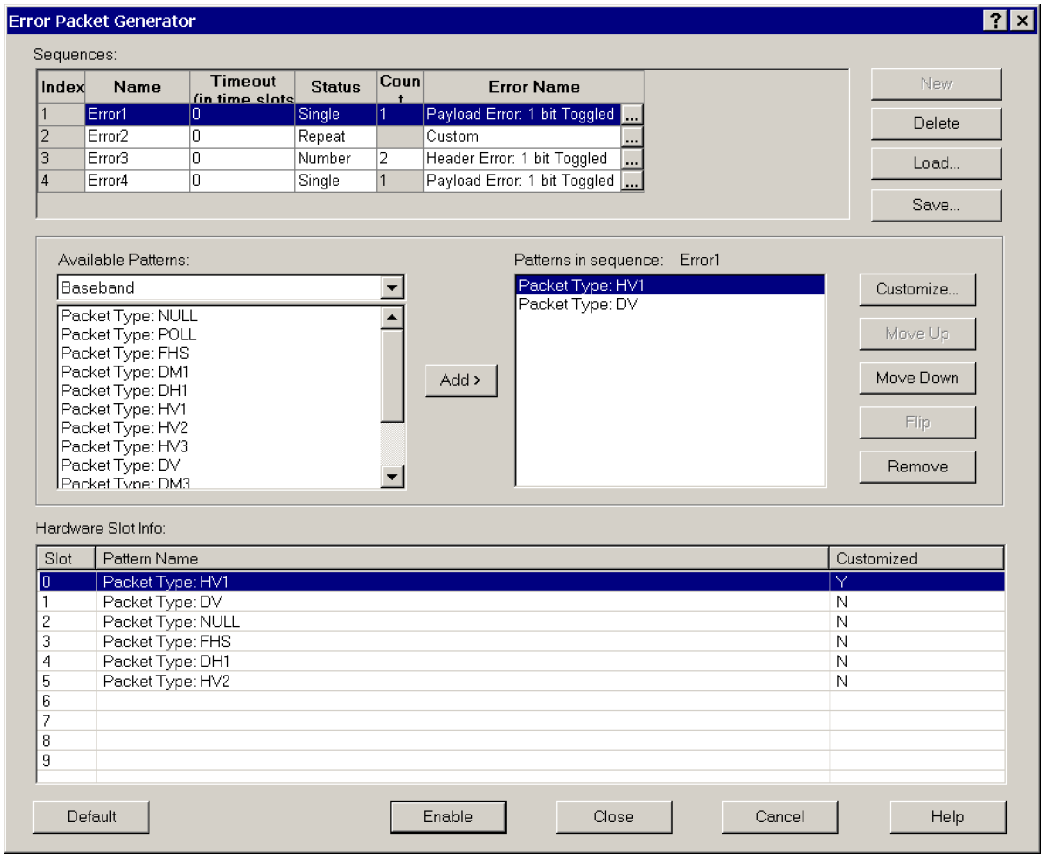


Figure 2-3: Error Packet Generator dialog box

With the exception of the the Error Name field, the Error Packet Generator window is identical to the Low Level Trigger Setup window. See *Low Level Trigger* on page 1–15 for information about the various fields in this dialog box.

***NOTE**. If you want to generate an error using a setup that you previously created and saved, click **Load**. In the Open dialog box browse to the location and open your error packet generation file (*epg).*

Defining Bit Errors. Perform the following steps to define bit errors.

1. In the Sequences Name column, type in a name for the error sequence you are defining. You can define up to four sequences.
2. Enter a Timeout value between 0 and 100. The Timeout value determines how long the application looks for the next pattern in a sequence. Enter the value as the number of Bluetooth time units. A Bluetooth time unit is 625 µs.
3. Click in the Status column and select an entry from the drop-down list box:
   - Off: Disables the highlighted sequence so it will not be recognized by the Bluetooth Protocol Analyzer.
   - Single: Only the first sequence whose patterns occur in the listed order will be marked in the Bluetooth Protocol Analyzer display.
   - Repeat: Whenever the patterns in the specified sequence occur in order, they will be marked in the Bluetooth Protocol Analyzer display.
   - Number: Enter a value between 2 and 200 in the Count column. This value determines the number of times the sequence will be marked. In all cases, the first sequence that reaches completion triggers acquisition and the Bluetooth Protocol Analyzer will mark the following sequences in the display.
4. Click in the Error Name column and select a predefined bit position error from the drop-down list box. See Figure 2–4.

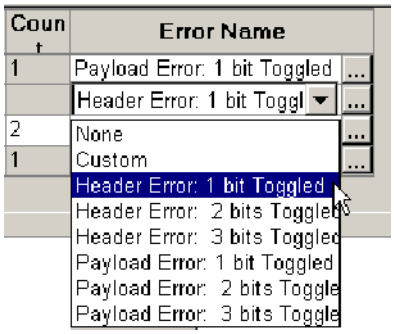


Figure 2-4: Error Name drop-down list box

5. Click the  shortcut button adjacent to the Error Names to display the custom error selection dialogs. See the examples in Figure 2–5.

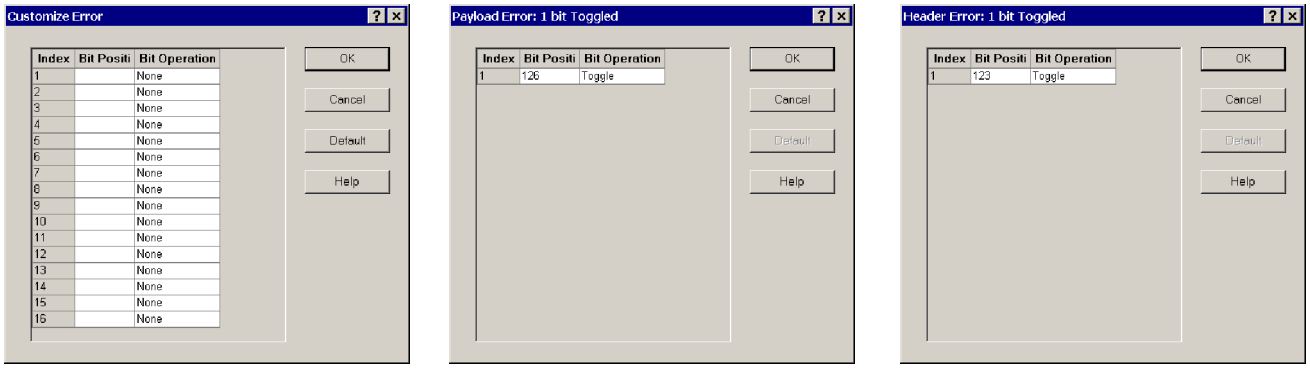


Figure 2-5: Custom error dialog boxes

NOTE. *If you have more than one pattern in the sequence for which you are generating an error, the error is sent with the last pattern in the sequence.*

Defining Error Patterns. Perform the following steps to define the patterns that will be used to generate an error in a sequence that you have created.

1. Click the down arrow at the right side of the Available Patterns list box.
2. Select an entry for the pattern type in which you want to insert the error. See Figure 2-6.

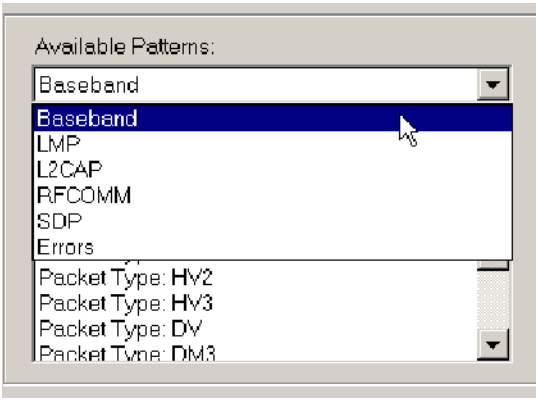


Figure 2-6: Available Patterns drop-down list box

3. Double-click on a packet type in the list box (or click **Add**) to incorporate a pattern into the sequence. You can select up to four patterns per defined sequence.

4. Click **Customize** to display the Customize Pattern dialog box that allows you to create a custom pattern. (See *Customize Pattern* beginning on page 1–18 for more information about this dialog box.)
5. Click **Move Up**, **Move Down**, **Flip**, or **Remove** to reorder the bit patterns.
6. Click **Save** to display the Save As dialog box that allows you to browse and save your Error packet generation setup file (*epg).
7. Click **Enable** to generate error packets.

***NOTE**. Error generation on packets that contain payload data may not have errors introduced into the access code or into the first few bytes of the header. This is because the first few bytes of the packet will already have been transmitted by the time the error packet generator recognizes this packet as one in which to introduce errors.*

Defining Hardware Slots. The Hardware Slot Info field shows the locations used for the defined pattern sequences. You can use up to ten hardware slots. The pattern name and custom information is listed next to the slot number. Slots are filled as patterns are added. Customized packets use additional slots.

Header Error

A header with a 1-bit error should be recoverable by devices receiving the error packet. A 2- or 3-bit error results in an unrecoverable error in the receiving device. Packets with recovered errors are indicated in green text in the list window of the; unrecovered errors are displayed in red text.

Payload Error

CRC is used for error checking the payload. Similar to header errors, a 1-bit error is recoverable; 2- and 3-bit errors are not recoverable. Bit positions 126 and 127 correspond to the L_CH of the payload header format. See Figure 2–7.

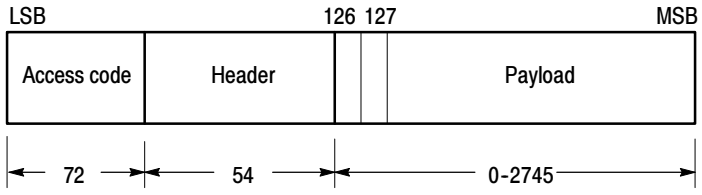


Figure 2-7: Standard packet format

When generating a 2- or 3-bit error, it is recommended that you do not use the Repeat status (in the Error Packet Generator set up window), since this will result in a continuous, unrecoverable error. Instead, use the Number status and set the count to a desired value (for example, set the count to 5).

Custom Error

To enter the bit operation for a custom error, click the Bit operation field to activate a pull down menu from which you can choose Forced 1, Forced 0, or Toggle as the bit operation. It is recommended that you use Toggle instead of Forced 1 or Forced 0. (Refer to the first example in Figure 2–5 on page 2–6.)

Example of Generated Error

In Figure 2–3 on page 2–4, the Error Packet Generator set up window was used to create a sequence named Error Seq1 that contained an LMP_host_connection_req pattern. A Payload error with 3 bits toggled was set to be transmitted with this pattern. The status was set to Single, which resulted in the error being transmitted one time. Figure 2–8 shows the Bluetooth Protocol Analyzer display resulting from transmitting the error.

In the Index column, 697 is highlighted (in blue in the application). This indicates an error was transmitted. Following this error, Index 699 shows that the LMP_host_connection_req pattern was transmitted again but without the error.

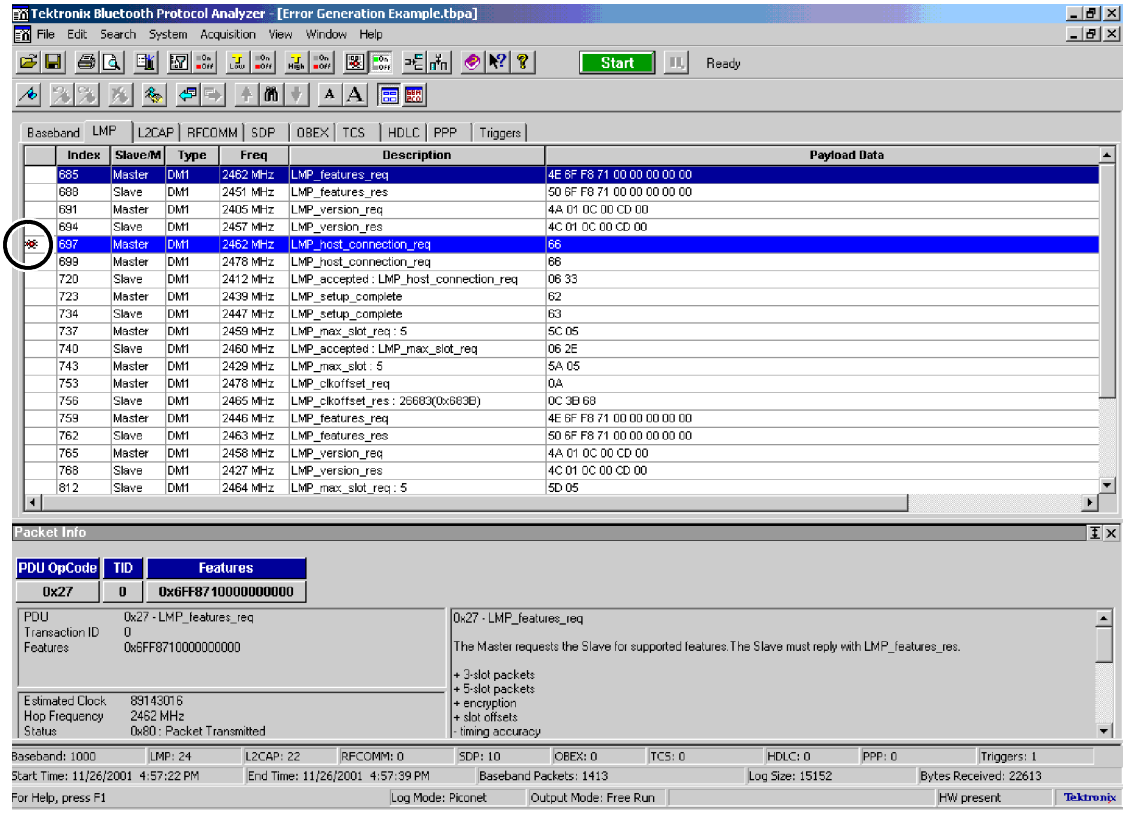


Figure 2–8: Analyzer display of generated error

Enabling Decryption

To enable decryption and enter settings, do the following:

1. Select **Acquisition > Setup**.
2. In the Acquisition Setup dialog box, click the **Independent Mode** option button.
3. Click the **Enable Decryption** option button.
4. Click the **Decryption** button to open the Decryption dialog box. See Figure 2-9.

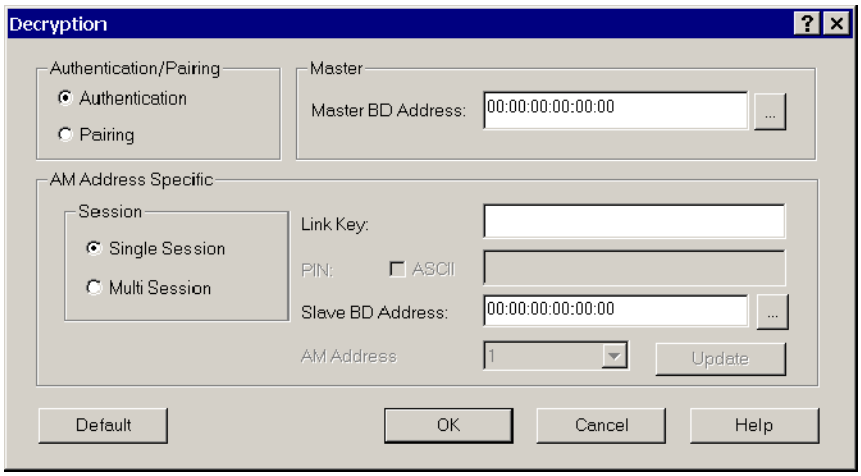


Figure 2-9: Decryption dialog box

The Bluetooth Protocol Analyzer is responsible for detection of Kc' (see Bluetooth Specification 1.0B or 1.1).

When a log session is started, data is logged for both encrypted and decrypted packets. The log file also includes LinkKey or PIN information.

The Bluetooth Protocol Analyzer displays decrypted data in real-time mode if performance is critical, or it can open a log file and display either decrypted or encrypted packets. In the case of encrypted packets, it is possible to decrypt using the LinkKey or PIN used during acquisition, or enter a LinkKey or PIN using the Decryption dialog box. This is explained in the *Enable Decryption Procedure* on page 2-11.

Decryption in Independent Mode

Bluetooth security supports authentication (unidirectional or mutual) and encryption, which are based on a secret LinkKey that is shared by a pair of devices. This secret key is derived during initialization and is not disclosed.

Authentication

The size of the LinkKey is always 128 bits. In encryption it may vary from 8–128 bits (the authentication key is used in generating the encryption key).

Pairing

This is an authentication process. You do not have to calculate the LinkKey using a complex algorithm. Enter the PIN code (optional ASCII entry) used between master and slave for authentication. In pairing, the K_{init} value is calculated and used for decrypting the data transaction between master and slave (see note).

***NOTE**. When using decryption in Independent mode with the Pairing option, some of the following keys are generated and displayed in the application window: Random number, Kc, Kc prime, and LinkKey.*

Encryption Set Up

To enable encryption, you must perform the following set up in the Bluetooth Neighborhood application.

1. In the Bluetooth menu bar, select **Bluetooth > Bluetooth Neighborhood Properties**.
2. Open the Security tab and select **Link level security** for the Security Mode.
3. Select **Enable** for the Encryption Mode.
4. Once bonding is established between master and slave, you need to expire bonding to use decryption in Independent mode. Right-click the device bonded in Bluetooth Neighborhood and select expire bonding.

Enable Decryption Procedure

Use the following procedure to enable decryption on the Bluetooth Protocol Analyzer:

1. Select **Acquisition > Setup** in the Bluetooth Protocol Analyzer menu bar.
2. Select **Enable Decryption** in the Acquisition Setup dialog box; then click the **Decryption** button.
3. In the Decryption dialog box (Figure 2–9 on page 2–9), make your other selections from the following:
   - Authentication/Pairing. Choose either Authentication (default) or Pairing and follow these guidelines:
     - If using Authentication, enter the LinkKey.
     - If using Pairing, enter the PIN. The BPA100 Protocol Analyzer derives the LinkKey from the PIN. If entering the PIN in ASCII, click the ASCII check box.
   - Master: Enter the Master BD Address.
   - AM Address specific: Select Single session (default) or Multi session.
   - LinkKey/PIN: See Authentication/Pairing above.
   - Slave BD Address: Enter the address.
   - AM Address: Make a selection.
4. Click **OK**.

Appendices

Appendix A: Specifications

This section lists the electrical, environmental, and physical characteristics of the BPA105 Bluetooth Protocol Analyzer.

Specifications listed in this section are guaranteed unless labeled “typical.” Typical specifications are provided for your convenience and are not guaranteed.

The electrical characteristics listed in Table A–1 are valid when the BPA105 Bluetooth Protocol Analyzer operates within the environmental conditions listed in Table A–2.

Table A-1: Air probe characteristics

Characteristic	Description
Device compatibility	Communicates with USB Specification V1.1 devices.
Operating range	0 to 250 m (820 ft)
Frequency range	2.402 to 2.480 GHz
Transmitter	
Power output	Active mode: +20 dBm (100 mW) Single frequency mode: 0 dBm (1 mW)
Receiver	
Sensitivity	> -80 dBm
Power	
Requirements	Powered through USB cable connection between the host PC and the Bluetooth Air Probe interface.
Consumption	Active mode: < 350 mA. Inquiry scan mode: 81 mA Hibernation/standby mode: 400 μA

Table A-2: Environmental characteristics

Characteristic	Description
Temperature Range	
Operating	+5° C to +55° C (+41° F to +131° F)
Nonoperating	0° C to +55° C (+32° F to +131° F)
Humidity	
Operating	20 to 90% RH, noncondensing
Nonoperating	20 to 95% RH, noncondensing

Table A-2: Environmental characteristics (Cont.)

Characteristic	Description
Altitude	
Operating	3,050 m (10,000 ft)
Nonoperating	10,058 m (33,000 ft)

Table A-3: Certifications and compliances

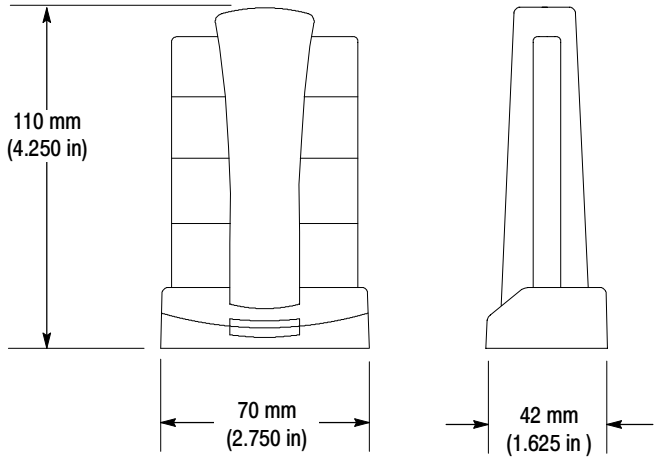
Category	Standards or description
EC Declaration of Conformity - EMC	Meets intent of Directive 999/S/EG for Radio and Telecommunications Terminal Equipment. Compliance was demonstrated to the following specifications as listed in the Official Journal of the European Union: ETS 300-328 11/1996 and A1 07/1997, Spread Spectrum data transmission equipment in the 2.4 GHz ISM band. ETS 300-826 11/1997 EMC and Radio Spectrum Matters, 2.4 GHz wideband transmission systems. IEC 61000-4-2 Electrostatic discharge immunity (Performance criterion C). IEC 61000-4-3 RF electromagnetic field immunity (Performance criterion A).
United States and Canada	Emissions comply with FCC Code of Federal Regulations 47, Part 15, Subpart C, Section 247, Class A Limits. Complies with RSS-210/RSS-139 of the Industry Canada.
Australia/New Zealand Declaration of Conformity - EMC	Complies with EMC provision of Radiocommunications Act: AS/NZS 2064.1/2 Industrial, Scientific, and Medical Equipment:1992.

Table A-4: Physical characteristics

Characteristic	Description
Weight	3 lbs (1.36 kg)[1]
Dimensions[2]	Height: 110 mm (4.250 in) Width: 70 mm (2.750 in) Depth: 42 mm (1.625 in)

1 **Includes accessories and shipping container.**

2 **Dimensions of Bluetooth air probe:**



Appendix B: Accessories

This section lists the Bluetooth Protocol Analyzer standard and optional accessories.

Standard Accessories

Your Bluetooth Protocol Analyzer includes the following accessories:

- *BPA100 Bluetooth Protocol Analyzer Product Software CD-ROM*, Tektronix part number 063-3469-xx. Includes *BPA100 Bluetooth Protocol Analyzer User Manual (.pdf file).*
- Custom USB cable, Tektronix part number 174-4580-xx.
- *BPA100 Bluetooth Protocol Analyzer Installation Manual,* Tektronix part number 071-0115-xx.

Appendix C: Sample Scripts

This section contains technical information you may need to write your own scripts.

HCI Terminal Scripts

Use the following HCI Terminal scripts as a guide when creating your own scripts.

Sniffer Test Script for Master Packet Types

```
Report(Sniffer test script for packet types [Master])
report( )

RESET(All)
SETDEBUGLEVEL(81)
SETMAXLOOPCOUNT(5000)
WAITCOMPLETE_ENABLED
//TIMESTAMPS_ENABLED

// Write Scan enable
// Set Event Filter
// Change connection packet type

TXCMD 1A 0C 01 00
WAITEVENT($0E,5000,[TestError])
TXCMD 05 0C 03 02 00 02
WAITEVENT($0E,5000,[TestError])

// Establish ACL connection

report( )
report(Establishing ACL connection)

label: Establish_one_connection
label: create_connection_retry#1

// NOTE:
// change the Bluetooth address in this command
// if your BD_Addr is 00 50 CD 00 93 38 then it should be reversed as 38 93 00
CD 50 00
// Its starts |              | it is reversed
TXCMD 05 04 0C 38 93 00 CD 50 00 18 CC 00 00 00 00
WAITEVENT($03,20000,[TestError])
```

```
if byte[2] = $04 jump(create_connection_retry#1)
if byte[2] = $10 jump(create_connection_retry#1)

report(ACL connection established!)
report( )

delay(1000)
//WAITEVENT($1B,5000,[TestError])
WAITEVENT($1C,5000,[TestError])
WAITEVENT($0B,5000,[TestError])
WAITEVENT($0C,5000,[TestError])

//TXCMD 0F 04 04 00 00 18 CC
//WAITEVENT($1D,5000,[TestError])

report(Connection packet type changed)
report( )

// switch from master to slave

TXCMD 0B 08 07 38 93 00 CD 50 00 00
WAITEVENT($12,1000,[TestError])

// Disconnect ACL connection
// This Device is Slave now so wait for Disconnect from master

label: Disconnect

//TXCMD 06 04 03 00 00 13
WAITEVENT($05,60000,[TestError])
report(ACL connection disconnected)
report( )

label: TestSuccess
report(Test passed!)
report( )
jump(end)

label: TestError

report()
report(**********Test failed!**********)
report()

label: end
REPORT(DONE!)
```

Sniffer Test Script for Slave Packet Types

```
Report(Sniffer test script for packet types [Slave])
report( )

RESET(All)
SETDEBUGLEVEL(81)
SETMAXLOOPCOUNT(5000)
WAITCOMPLETE_ENABLED
//TIMESTAMPS_ENABLED

// Write Scan enable
// Set Event Filter
// Wait for max slots changed event

TXCMD 1A 0C 01 03
//WAITEVENT($0E,5000,[TestError])
TXCMD 05 0C 03 02 00 02
WAITEVENT($0E,5000,[TestError])

// Establish ACL connection

report( )
report(Establishing ACL connection)

WAITEVENT($03,60000,[TestError])

report(ACL connection established from master!)
report( )

delay(1000)

WAITEVENT($1B,60000,[TestError])
WAITEVENT($1C,60000,[TestError])
WAITEVENT($0B,60000,[TestError])
WAITEVENT($0C,60000,[TestError])


//WAITEVENT($1B,5000,[TestError])
//report(Connection packet type changed from master)
report( )

// ROLE Switch this device becomes master

//WAITEVENT($12,10000,[TestError])
delay(6000)

// Wait for master to disconnect ACL connection
// This device is master now so disconnect the connection
```

```
label: Disconnect

TXCMD 06 04 03 00 00 13
WAITEVENT($05,10000,[TestError])
report(ACL connection disconnected from master)
report( )

label: TestSuccess
report(Test passed!)
jump(end)

label: TestError
report()
report(****************Test failed!***************)
report()

label: end
REPORT(DONE!)
```

Sniffer Test Script for Slave Connection Packet Types

```
Report(BPA100 connection test script for packet types [Slave])
report( )

RESET(All)
SETDEBUGLEVEL(81)
SETMAXLOOPCOUNT(5000)
WAITCOMPLETE_ENABLED
//TIMESTAMPS_ENABLED

// Write Scan enable
// Set Event Filter
// Wait for max slots changed event

TXCMD 1A 0C 01 03
WAITEVENT($0E,5000,[TestError])
TXCMD 05 0C 03 02 00 02
WAITEVENT($0E,5000,[TestError])

REPORT(The following tests are from the test specification)

// Wait for events from master
// When master is done add 1 SCO HV1 connection and disconnect it 5.5.18.1.4
& 5.5.18.1.10

// Establish ACL connection

report( )
```

```
report(Establishing ACL connection)

WAITEVENT($03,60000,[TestError])
report(ACL connection established from master!)
report( )

WAITEVENT($1B,5000,[TestError])
report(Connection packet type changed from master)
report( )

// Set some payload
SETPAYLOAD(49 66 20 79 6F 75 20 63 61 6E 20 72 65 61 64 20 74 68 69 73
20 74 68 65 6E 20 79 6F 75 20 68 61 76 65 20 73 65 74 20 74 68 65 20 66 6F
72 6D 61 74 20 6F 66 20 74 68 65 20 70 61 79 6C 6F 61 64 20 74 6F 20 62 65
20 64 69 73 70 6C 61 79 65 64 20 69 6E 20 41 53 43 49 49 2E 20 53 6F 6D 65
74 69 6D 65 73 20 74 68 65 20 50 43 20 67 75 79 73 20 66 6F 72 67 65 74 73
20 74 6F 20 77 72 61 70 20 74 68 65 20 70 61 79 6C 6F 61 64 20 73 6F 20 79
6F 75 20 63 61 6E 20 6E 6F 74 20 73 65 65 20 69 74 20 61 6C 6C 20 61 74 20
6F 6E 65 20 74 69 6D 65 20 74 68 65 6E 20 79 6F 75 20 77 69 6C 6C 20 68 61
76 65 20 74 6F 20 63 68 6F 73 65 20 48 45 58 20 76 69 65 77 20 74 6F 20 73
65 65 20 69 74 20 61 6C 6C 2E 20 49 20 74 68 69 6E 6B 20 74 68 69 73 20 73
68 6F 75 6C 64 20 62 65 20 63 68 61 6E 67 65 64 20 61 73 20 73 6F 6F 6E 20
61 73 20 70 6F 73 73 69 62 6C 65 2C 20 68 6F 77 65 76 65 72 20 69 66 20 79
6F 75 20 63 61 6E 20 72 65 61 64 20 74 68 69 73 20 6C 69 6E 65 20 74 68 65
20 70 72 6F 62 6C 65 6D 20 69 73 20 66 69 78 65 64 20 21)

// Test DM1, DH1, DM3, DH3, DM5, DH5 packets

label: NoSCO

REPORT(Testing for DM1, DH1, DM3, DH3, DM5, DH5 packets)
report( )

TXDATA(hCon:0,bc:0,pb:2,Len:1,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:2,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:3,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:4,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:5,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:6,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:7,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:8,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:9,cnt:500,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:10,cnt:500,Random:0)

report()
report(Packets size = 1..10 ”passed”)
report()
```

```
// Wait for master to disconnect ACL connection

WAITEVENT($05,60000,[TestError])
report(ACL connection disconnected from master)
report( )

label: TestSuccess
report(Test passed!)
jump(end)

label: TestError
report(Test failed!)
label: end
REPORT(DONE!)
```

Sniffer Test Script for Master Connection Packet Types

```
Report(BPA100 Connection test script [Master])
report( )

RESET(All)
SETDEBUGLEVEL(81)
SETMAXLOOPCOUNT(5000)
WAITCOMPLETE_ENABLED
//TIMESTAMPS_ENABLED

// Write Scan enable
// Set Event Filter
// Change connection packet type

TXCMD 1A 0C 01 00
WAITEVENT($0E,5000,[TestError])
TXCMD 05 0C 03 02 00 02
WAITEVENT($0E,5000,[TestError])

// Establish ACL connection

report( )
report(Establishing ACL connection)

label: Establish_one_connection
label: create_connection_retry#1

// NOTE:
// change the Bluetooth address in this command
// if you BD_Addr is 00 50 CD 00 93 11 then it should be reversed as 11 93 00
CD 50 00
// Its starts |              | it is reversed
```

```
TXCMD 05 04 0C 11 93 00 CD 50 00 18 CC 00 00 00 00
WAITEVENT($03,20000,[TestError])
if byte[2] = $04 jump(create_connection_retry#1)
if byte[2] = $10 jump(create_connection_retry#1)

report(ACL connection established!)
report( )

//TXCMD 0F 04 04 00 00 18 CC
//WAITEVENT($1D,5000,[TestError])

report(Connection packet type changed)
report( )

// Set some payload
SETPAYLOAD(49 66 20 79 6F 75 20 63 61 6E 20 72 65 61 64 20 74 68 69 73
20 74 68 65 6E 20 79 6F 75 20 68 61 76 65 20 73 65 74 20 74 68 65 20 66 6F
72 6D 61 74 20 6F 66 20 74 68 65 20 70 61 79 6C 6F 61 64 20 74 6F 20 62 65
20 64 69 73 70 6C 61 79 65 64 20 69 6E 20 41 53 43 49 49 2E 20 53 6F 6D 65
74 69 6D 65 73 20 74 68 65 20 50 43 20 67 75 79 73 20 66 6F 72 67 65 74 73
20 74 6F 20 77 72 61 70 20 74 68 65 20 70 61 79 6C 6F 61 64 20 73 6F 20 79
6F 75 20 63 61 6E 20 6E 6F 74 20 73 65 65 20 69 74 20 61 6C 6C 20 61 74 20
6F 6E 65 20 74 69 6D 65 20 74 68 65 6E 20 79 6F 75 20 77 69 6C 6C 20 68 61
76 65 20 74 6F 20 63 68 6F 73 65 20 48 45 58 20 76 69 65 77 20 74 6F 20 73
65 65 20 69 74 20 61 6C 6C 2E 20 49 20 74 68 69 6E 6B 20 74 68 69 73 20 73
68 6F 75 6C 64 20 62 65 20 63 68 61 6E 67 65 64 20 61 73 20 73 6F 6F 6E 20
61 73 20 70 6F 73 73 69 62 6C 65 2C 20 68 6F 77 65 76 65 72 20 69 66 20 79
6F 75 20 63 61 6E 20 72 65 61 64 20 74 68 69 73 20 6C 69 6E 65 20 74 68 65
20 70 72 6F 62 6C 65 6D 20 69 73 20 66 69 78 65 64 20 21)

REPORT(Testing for DM1, DH1, DM3, DH3, DM5, DH5 packets)
report( )

TXDATA(hCon:0,bc:0,pb:2,Len:1,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:2,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:3,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:4,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:5,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:6,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:7,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:8,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:9,cnt:10,Random:0)
TXDATA(hCon:0,bc:0,pb:2,Len:10,cnt:10,Random:0)

report()
report(Packets size = 1..10 ”passed”)
report()
```

```
// Disconnect ACL connection

TXCMD 06 04 03 00 00 13
WAITEVENT($05,10000,[TestError])
report(ACL connection disconnected)
report( )

label: TestSuccess
report(Test passed!)
report( )
jump(end)

label: TestError
report(Test failed!)
label: end
REPORT(DONE!)
```

Glossary

Glossary

ACL
An acronym for Asynchronous Connection-Less Link, this provides a packet-switched connection (master to any slave).

Active Member Address (AM_ADDR)
The Active Member Address is a 3-bit number. This address is allocated by the master to each active slave in the piconet. The address is used to identify the specific slave for which a packet is intended.

Authentication
Security mechanism that prevents access to critical data and makes it impossible to falsify the origin of a message. Authentication is performed for devices. In Bluetooth, this is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN).

AUX
An ACL (asynchronous connectionless) link packet type for data. An AUX1 packet resembles a DH1 packet except it has no CRC code. As a result it can carry up to 30 information bytes.

Baseband
The baseband describes the specifications of the Bluetooth link controller, which carries out the baseband protocols and other low-level link routines.

BD_ADDR
The Bluetooth Device Address is a unique, 48-bit number used to identify a Bluetooth device. The Bluetooth device address is also used in encryption and in generation of frequency hop sequences. It is similar to an Ethernet MAC address.

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
Every Bluetooth unit has an internal system clock that determines the timing and hopping of the transceiver. It can be implemented as a 28-bit counter, with the LSB ticking in units of 312.5us, giving a clock rate of 3.2kHz.

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

Bluetooth Host
This is a computing device, peripheral, cellular telephone, access point to PSTN (public switched telephone network), etc. A host attached to a Bluetooth unit may communicate with other Bluetooth hosts attached to their Bluetooth units.

Bluetooth Neighborhood
A Bluetooth application created by Digianswer that provides an interface for you to interact with Bluetooth systems. Its basic functions are to perform device and service discovery and to enable you to make service-oriented connections to other Bluetooth devices.

Bluetooth Service Type
One or more services a device can provide to other devices. The service information is defined in the service class field of the Bluetooth device class parameter.

Bluetooth Unit
A voice/data circuit equipment for a short-range, wireless communication link. It allows voice and data communications between Bluetooth units.

Channel
A logical connection at the L2CAP level between two devices serving a single application or higher layer protocol.

Channel (Hopping) Sequence
A pseudo-random sequence of 79 frequencies (23 for the 23MHz system). The frequency is calculated using the BD_ADDR of the master of the piconet. The phase in the sequence is derived from an estimate of the master clock. The channel hopping sequence has a very long period that does not show repetitive patterns over a short time interval, but which distributes the hop frequencies equally over the 79 MHz (23 MHz for the 23 MHz system) during a short time interval. See also Frequency sequence.

CID (Channel Identifier)
An abbreviation for Channel Identifier. Used to identify L2CAP connections.

CLK
An acronym for Clock, this is the master clock that defines the timing used on a Bluetooth piconet.

CLKE
An estimate of the clock of another device.

CLKN
The native clock of a Bluetooth device. A slave device must add an offset to its own CLKN to synchronize with the master clock (CLK).

Coverage Area
The area where two Bluetooth units can exchange messages with acceptable quality and performance.

Destination
The Bluetooth device receiving an action from another Bluetooth device. The device sending the action is called the source. The destination is typically part of an established link, though not always (such as in inquiry/ page procedures).

Device Discovery
Before a link can be established, a Bluetooth device needs to discover the other Bluetooth devices that are active within the range. The mechanism to request and receive the Bluetooth address, clock, class of device, used page scan, and names of devices is referred to as device discovery.

Device Name
The name that a Bluetooth device presents when supplying identity information to another device.

DH (Data-High Rate)
An ACL link data packet type for high-rate data. DH1 packets are similar to DM1 packets, except that the information in the payload is not FEC encoded. This means the DH1 packet can carry up to 28 information bytes and covers a single time slot. The DH3 is the same, except it can cover up to 3 time slots and contain up to 185 information bytes. The DH5 packet is the same again except it can cover up to 5 time slots and contains up to 341 information bytes.

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

DM (Data-Medium Rate)
An ACL link data packet type for medium rate data. DM1 packets carry information data only, containing a 16-bit CRC code and up to 18 info bytes. They are encoded using 2/3 FEC and the packet can cover up to a single time slot. DM3 packets are the same except they can cover up to 3 time slots, and can carry up to 123 information bytes. DM5 packets are the same again except they can cover up to 5 time slots and can hold up to 226 information bytes.

DV (Data Voice)
A SCO (synchronous connection oriented) link data packet type for data and voice. It is divided into a voice field of 80 bits and a data field of 150 bits. The voice field is not covered by FEC, but the data field is covered by 2/3 FEC. The voice and data fields are treated completely separate. The voice field is handled like normal SCO data and is never retransmitted; that is, the voice field is always new. The data field is checked for errors and is retransmitted, if necessary.

Encryption
Security mechanism that prevents eavesdropping and maintains link privacy.

FEC (Forward Error Correction)
The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. Within Bluetooth, there are 2 versions of FEC: 1/3 FEC and 2/3 FEC. 1/3 FEC is a simple, 3-times repetition of each information bit. 2/3 FEC is a (15,10) shortened Hamming code.

Frequency Hopping (Selection)
Bluetooth is characterized by its system of fast frequency hops. Ten different types of hopping sequences are defined, five of the 79 MHz range/79 hop system and five for the 23 MHz range/23 hop system. The two range system hopping sequences differ only in frequency range (79 MHz or 23 MHz) and segment length: 32 hops (79 MHz system) or 16 hops (23 MHz system).

The individual hopping sequences include the page sequence and the page response sequence. These are used in the page procedure. Used in the inquiry procedure are the inquiry sequence and the inquiry response sequence. Finally the main hopping sequence used in the Bluetooth system is the channel-hopping sequence.

Frequency Hopping Synchronization (FHS) Packet
This a special control packet revealing, among other things, the BD_ADDR and the clock of the source device. It contains 144 information bits and a 16-bit CRC code. The payload is coded with 2/3 FEC, which brings the total payload length to 240 bits. The FHS packet covers a single time slot.

Gateway
A Bluetooth enabled device that is connected to an external network.

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) for the 3 power-saving modes (sniff, hold, and park).

Host Controller Interface (HCI)
Allows higher layers of the stack, including applications, to access the baseband, link manager, and other hardware registers through a single, standard interface.

HV (High Quality Voice)
A SCO link voice packet. HV1 packets carry 10 information bytes, which are protected by 1/3 FEC. HV2 packets carry 20 information bytes and are protected by 2/3 FEC. HV3 packets carry 30 information bytes and are not protected by FEC. HV packets do not have a CRC or payload header.

Inquiry
A Bluetooth unit transmits inquiry messages to discover the other Bluetooth units active within the coverage area. Units that capture inquiry messages may send a response to the inquiring Bluetooth unit. The response contains information about the Bluetooth unit and its inquiring host.

Isochronous User Channel
A channel used for time-bounded information such as compressed audio (ACL link).

L2CAP
Acronym for Logical Link Controller and Adaptation Protocol.

LAN
Acronym for Local Area Network.

LMP
Acronym for Link Manager Protocol. The LMP is used for link setup and control. The LMP PDU signals are interpreted and filtered out by the Link Manager on the receiving side and are not propagated to higher layers.

Logical Channel
The different types of channels on a physical link.

Master Device
The device that initiates a connection and, during this connection, controls all traffic in a piconet. The clock and hopping sequence of the master are used to synchronize all other devices in the piconet.

Name Discovery
The mechanism to request and receive a device name.

OBEX
An abbreviation for OBject EXchange protocol. The OBEX tab displays file-transfer and business card data.

NULL packet
A 126-bit packet consisting of the CAC (channel access code) and packet header only. It is used to return link information to the source. The NULL packet does not have to be acknowledged.

Packet
Format of aggregated bits that can be transmitted in 1, 3, or 5 time slots.

Paging
A Bluetooth unit transmits paging messages to set up a communication link to another Bluetooth unit that is active within the coverage area.

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

(AM_ADDR) address and occasionally listen to the traffic of the master to resynchronize and check on broadcast messages. This mode has the lowest duty cycle (power efficiency) of the three power-saving modes (sniff, hold, and park).

PDU
Acronym for Protocol Data Unit (that is, a message).

Physical Channel
Synchronized RF hopping in a piconet.

Physical Link
Connection between devices.

Piconet
A wireless network formed by two or more Bluetooth devices.

POLL Packet
Similar to the NULL packet, except it requires a confirmation from the destination. Upon reception of a POLL packet, the slave must respond with a packet.

Profile
Application that a Bluetooth device facilitates. For one device to communicate with another, the two devices must have a shared profile. For example, to transfer files from one computer to another, both computers must feature the file transfer profile.

Protocol Stack
Allows devices to locate, connect to, and exchange data with each other and to execute interoperable, interactive applications against each other. The stack is logically partitioned into three groups: transport protocol, middleware protocol, and application group.

RFCOMM
Serial Cable Emulation Protocol based on ETSI TS 07.10. (European Telecommunications Standards Institute).

RX
Abbreviation for receive.

Scatternet
Multiple independent and nonsynchronized piconets form a scatternet.

SDP (Service Discovery Protocol)
SDP is a Bluetooth-defined protocol provided for or available through a Bluetooth device. This protocol essentially is a means for applications to discover which services are available and to determine the characteristics of those available services.

Slave
A device in a piconet controlled by another device (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 the 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).

Source
The Bluetooth device initiating an action to another Bluetooth device. The device receiving the action is called the destination. The source is typically part of an established link, although not always (such as in inquiry/page procedures).

Time Slot
A time slot is the time it takes to send one packet from one Bluetooth device to another. A single time slot in a Bluetooth system lasts 625 us.

TCS
Acronym for Telephony Control (protocol) Specification. The TCS tab displays protocol discriminator, message type, and other data (depending upon the message type).

TX
Abbreviation for transmit.

Index

Index

A

B

C

D

M

N

O

P

R

S

T

U

V

W