BLUETOOTH PBAP PROFILE

iWRAP APPLICATION NOTE

Saturday, 09 June 2012

Version 2.0

VERSION HISTORY

Version	Comment
1.0	First version
1.5	Revision
1.8	Further Revision
1.9	More Addition and Revision
2.0	Made changes to formatting, modified UCD

TABLE OF CONTENTS

iWRAP firmware overview

iWRAP is an embedded firmware running entirely on the RISC processor of WT12, WT12 and WT32 modules. It implements the full *Bluetooth* protocol stack and many *Bluetooth* profiles as well. All software layers, including application software, run on the internal RISC processor in a protected user software execution environment known as a Virtual Machine (VM).

The host system can interface to iWRAP firmware through one or more physical interfaces, which are also shown in the figure below. The most common interfacing is done through the UART interface by using the ASCII commands that iWRAP firmware supports. With these ASCII commands, the host can access *Bluetooth* functionality without paying any attention to the complexity, which lies in the *Bluetooth* protocol stack. GPIO interface can be used for event monitoring and command execution. PCM, SPDIF, I2S or analog interfaces are available for audio. The available interfaces depend on the used hardware.

The user can write application code to the host processor to control iWRAP firmware using ASCII commands or GPIO events. In this way, it is easy to develop *Bluetooth* enabled applications.

On WT32 there is an extra DSP processor available for data/audio processing.

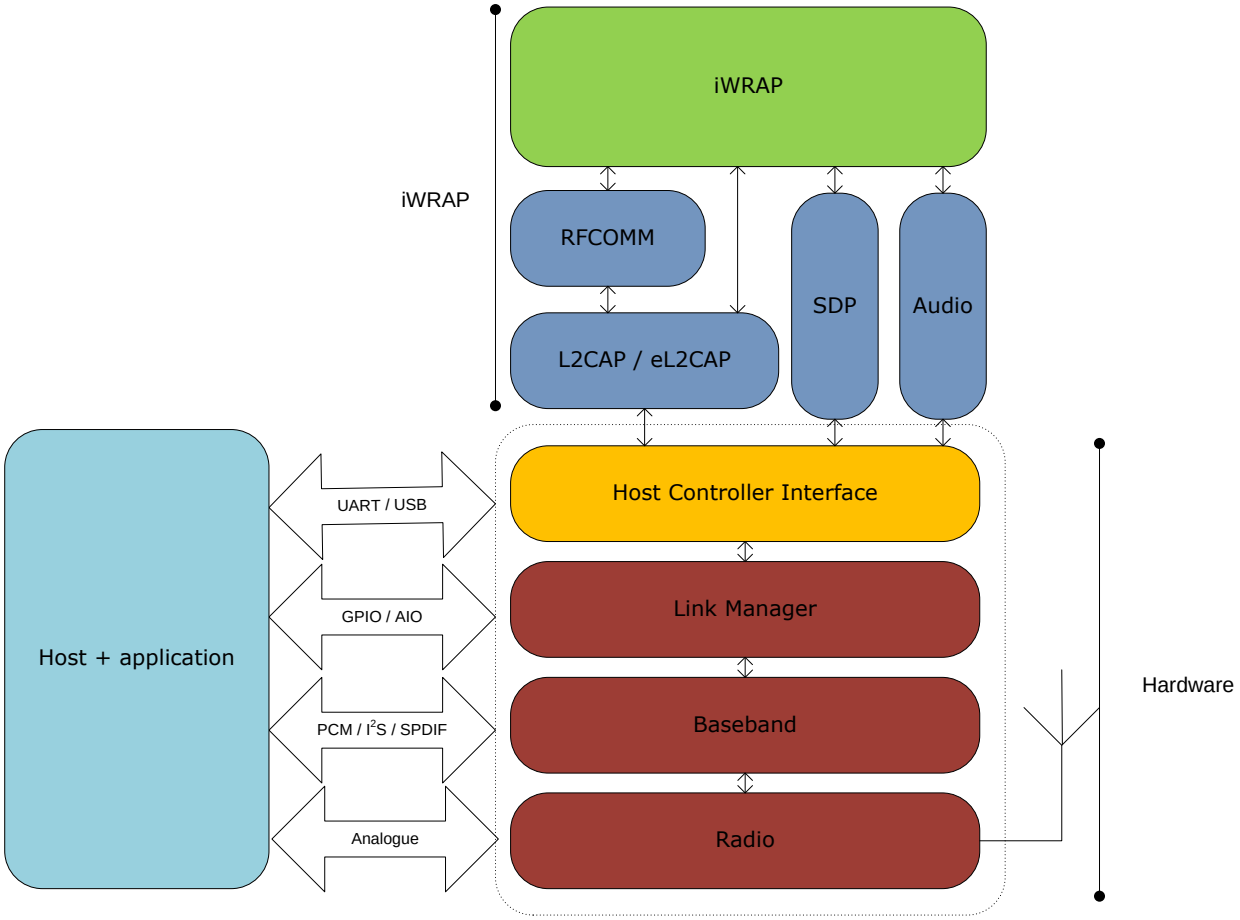

Figure 1: iWRAP Bluetooth stack In the figure above, a Bluegiga *Bluetooth* module with iWRAP firmware could be connected to a host system for example through the UART interface. The options are:

- If the host system has a processor, software can be used to control iWRAP by using ASCII based commands or GPIO events.
- If there is no need to control iWRAP, or the host system does not need a processor, iWRAP can be configured to be totally transparent and autonomous, in which case it only accepts connections or automatically opens them.
- GPIO lines that WRAP THOR modules offer can also be used together with iWRAP to achieve additional functionality, such as Carrier Detect or DTR signaling.

1 Introduction

This application note discusses Phone Book Access Profile (PBAP), its advantages and how this profile can be utilized. Also practical examples are given how the PBAP is used with the iWRAP firmware.

1.1 Phone Book Access Profile

The Phone Book Access Profile (PBAP) specification defines the procedures and protocols to exchange Phone Book objects between devices. It is especially tailored for the automotive Hands-Free use case where an onboard terminal device (typically a Car-Kit installed in the car) retrieves Phone Book objects from a mobile device (typically a mobile phone or an embedded phone). This profile may also be used by any client device that requires access to Phone Book object is stored in a server device.

Figure 2: Typical PBAP Use Case

The PBAP is based on a Client-Server interaction model where the Client device pulls phone book objects from the Server device. In Figure 1 for example, the client is the Handsfree Unit in the car and the server is the mobile phone. In many of today's automobiles, this PBAP functionality is enabled and intergrated within the factory car audio system.

Please note however that this profile only allows for the consultation of phone book objects (read-only). It is not possible to alter the content of the original phone book object (read/write). Phone Book Access Profile is dependent upon the Generic Object Exchange Profile, the Serial Port Profile and the Generic Access Profile

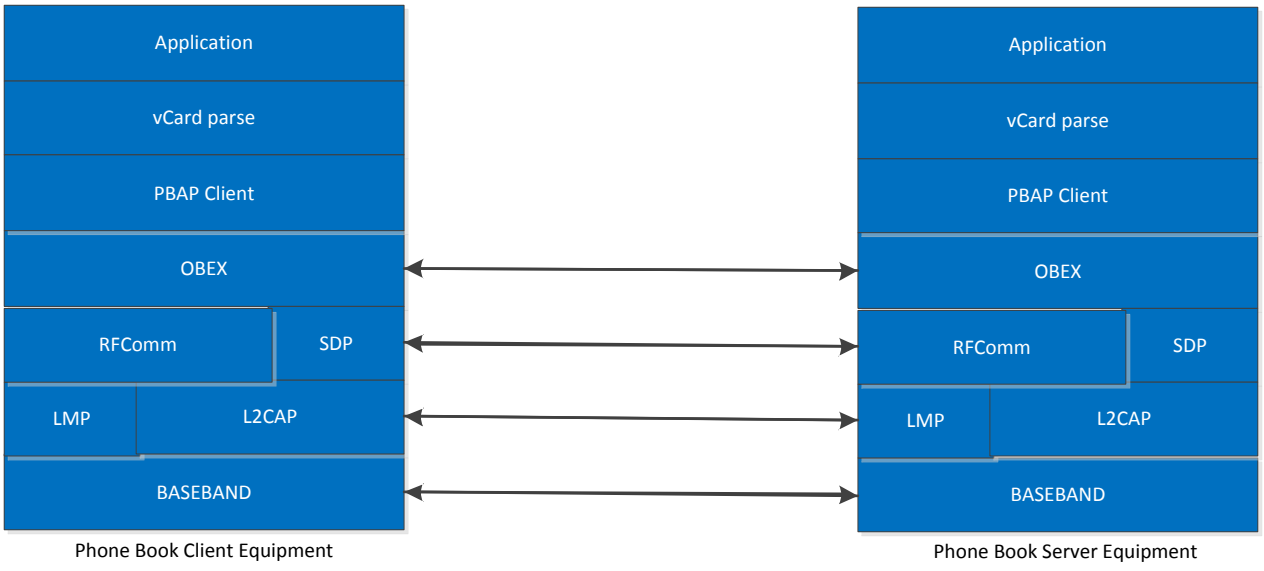

Figure 3: PBAP Profile Stack

2 Using PBAP with iWRAP

This chapter instructs the PBAP usage and configuration with the iWRAP firmware.

2.1 Profile configuration

The PBAP profile must be turned on along with the HFP profile. In iWRAP the HFP profile is needed as it works hand in hand with the PBAP profile to retrieve phone book objects from the Phone Server Equipment (PSE). For more info on the HFP profile, please refer to the HFP/HSP Application note. The PBAP is turned on by issuing "**SET PROFILE PBAP ON**"

```
SET PROFILE PBAP ON
SET PROFILE HFP ON
SET BT CLASS 200408
SET BT NAME {Module Friendly Name}
SET BT AUTH * {0-16 DIGIT PIN}
RESET
```

As can be seen in the box above, a reset command is issued to make the profile(s) and configurations active.

N.B. The PIN code can be set from 0-16 characters. Also, with iWRAP 5 Secure Simple Pairing (SSP) is enabled by default to fulfil Bluetooth 2.1 specification requirements. It is not possible to disable SSP in iWRAP 5 and if the remote device does not support SSP, iWRAP will automatically fall back to legacy pairing through PIN code. For more info on SSP, please refer to the extensive documentation in iWRAP5 User Guide.

2.2 Service discovery

Bluetooth technology enables wireless service discovery, so you can find out the capabilities the remote device supports. Wireless service discovery uses the Bluetooth Service Discovery Profile (SDP).

With iWRAP the service discovery is performed with command: "**SDP {*bd_addr*} {*uuid*}**".

bd_addr	Bluetooth device address of the remote device.
uuid	Universally unique identifier. Refers to the Bluetooth profile to be discovered. For PBAP the ***uuid*** is 1130. Please refer to the iWRAP user guide for ***uuid*** of PBAP PCE and PSE.

Below is an example how to perform a service discovery for PBAP device.

```
SDP 00:07:80:aa:bb:cc 112F
SDP 00:07:80:aa:bb:cc < I SERVICENAME S "OBEX Phonebook Access Server" > < I PROTOCOLDESCRIPTORLIST < < U L2CAP > < U RFCOMM I 13 > < U OBEX > > >
SDP
```

OBEX Phonebook Access Server = Service name

13 = L2CAP PSM for PBAP profile

2.3 Connection establishment

Usually the PBAP connection is opened by the PCE right after pairing. This can be seen by an incoming **CALL** event generated by iWRAP.

"**CALL {*bd_addr*} 112F PBAP**"

bd_addr Bluetooth device address of the remote device.

Below is an example how to set up a PBAP from iWRAP to a PSE device.

CALL 00:07:80:aa:bb:cc 112F PBAP
CALL 0
CONNECT 0 PBAP 5
OBEX 0 READY

2.4 PBAP Command

PBAP command is used to retrieve phone book entries or call history from a PBAP PSE device.

2.4.1 Syntax

Synopsis
PBAP {*path*} {*count*} [*offset*] [*filter*] [*format*]

Description		
path	**Left HEX** Store to retrieve data from. **0** Phone **1** SIM card	**Right HEX** Phone book or call history to read. **0** Phonebook **1** Incoming call history **2** Outgoing call history **3** Missed call history **4** Combined call history
count	Number of entries to be retrieved. **0** Returns phone book size **FFFF**	

	Retrieves all entries
offset	Offsets from which to start the retrieve from.
filter	This is a bit mask to filter the response. If this is left to 0 all fields will be returned. Mandatory attributes for vCard 2.1 are VERSION ,N and TEL and they are returned always. Mandatory attributes for vCard 3.0 are VERSION, N, FN and TEL and they are also returned always. **bit 0** VERSION vCard Version **Bit 1** FN Formatted pbap Name **bit 2** N Structured Presentation of Name **bit 3** PHOTO Associated Image or Photo **bit 4** BDAY Birthday **bit 5** ADR Delivery Address **bit 6** LABEL Delivery **bit 7** TEL Telephone Number **bit 8** EMAIL Electronic Mail Address **bit 9** MAILER Electronic Mail **bit 10** TZ Time Zone **bit 11** GEO Geographic Position **bit 12**

		TITLE Job
	bit 13	
		ROLE Role within the Organization
	bit 14	
		LOGO Organization Logo
	bit 15	
		AGENT vCard of Person Representing
	bit 16	
		ORG Name of Organization
	bit 17	
		NOTE Comments
	bit 18	
		REV Revision
	bit 19	
		SOUND Pronunciation of Name
	bit 20	
		URL Uniform Resource Locator
	bit 21	
		UID Unique ID
	bit 22	
		KEY Public Encryption Key
	bit 23	
		NICKNAME Nickname
	bit 24	
		CATEGORIES Categories
	bit 25	
		PROID Product ID
	bit 26	
		CLASS Class information
	bit 27	
		SORT-STRING String used for sorting operations
	bit 28	

	X-IRMC-CALL-DATETIME Time stamp
format	**1** Return vcard 3.0 **0** Return vcard 2.1

2.4.2 Examples

PBAP 00 1

BEGIN:VCARD

VERSION:2.1

FN:My name

N:My name

TEL;CELL:1234567890

END:VCARD

Following the syntax structure, the above command returns the “first” entry in the “Phone’s PhoneBook”. The example below is another example which shows the Phone’s incoming call history of the last two calls

PBAP 01 2

BEGIN:VCARD

VERSION:2.1

FN:701-921-5750

N:701-921-5750

TEL;X-0: 701-921-5750

X-IRMC-CALL-DATETIME;RECEIVED:20120529T123716

END:VCARD

BEGIN:VCARD

VERSION:2.1

FN:678-318-3100

N:678-318-3100

TEL;X-0:678-318-3100

X-IRMC-CALL-DATETIME;RECEIVED:20120524T085933

END:VCARD

The responses from iWRAP are basically OBEX Frames. This is because the PBAP profile is based on top of OPBEX OPP profile to transfer phone book content. The OBEX frame header format is shown in the table in the following page.

Response	
{OBEX header} {vCARD}	
OBEX header	OBEX header. See the header descriptions below.
vCARD	vCARD data

Length	Name	Description	Value
8 bits	Begin	Start of OBEX frame.	0xFC (last frame) or 0xFB (more frames to follow)
8 bits	Length	Length of full frame	0x00 – 0xFF
8 bits	Length	Length of full frame	0x00 – 0xFF
8 bits	Body	Body or end-of-body.	0x49 (last frame) 0x48 (more frames to follow)
8 bits	Length of data	Length of data field	0x00 – 0xFF
8 bits	Length of data	Length of data field	0x00 – 0xFF

Table 1: OBEX header

Events	
OBEX AUTH	This event occurs if the server requires authentication

2.5 Connection termination

The PBAP connection should be terminated on iWRAP using the "**DISCONNECT**" or "**CLOSE {link_id}**" command.

If the Virtual Cable Unplug procedure needs to be done, the command "**UNPLUG**" can be issued. It instructs the Host to delete all pairing information of the Device. iWRAP will delete its corresponding pairing information automatically.

PABP connection termination:

CLOSE 0

NO CARRIER 0 ERROR 0

Example connection diagram

An example of PBAP configuration and a simple PBAP connection setup is illustrated below.

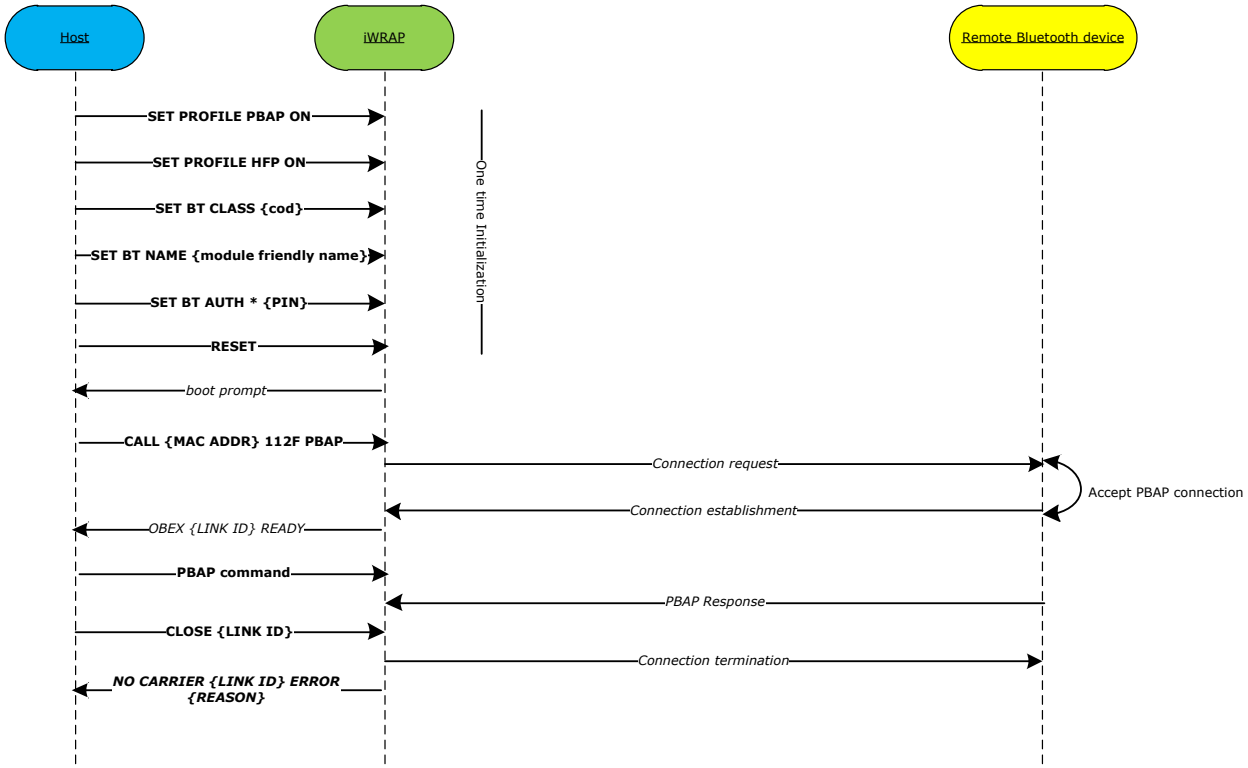

Figure 4: PBAP connection example

In the above example the **AUTH** event is only seen if a legacy pairing with pin code and interactive paring is made. If the legacy pairing does not take place and SSP pairing is used instead then **AUTH** event is not seen and there is no need to reply to it with the **AUTH** command. With SSP pairing, depending on the SSP mode, however SPP events may be displayed and then need to be responded with correct SSP pairing commands.

Please refer to iWRAP user guide for more information about the iWRAP command and events.

3 References

[1]The Bluetooth SIG, Human Interface Device Profile overview, URL:
http://www.bluetooth.com/Bluetooth/Technology/Works/PBAP.htm

[2]VCARD File Format, URL: http://en.wikipedia.org/wiki/VCard

5 Contact Information

Sales: sales@bluegiga.com

Technical support: support@bluegiga.com
http://www.bluegiga.com/techforum/

Orders: orders@bluegiga.com

Head Office / Finland:

Phone: +358-9-4355 060
Fax: +358-9-4355 0660

Street Address:

Sinikalliontie 5A
02630 ESPOO
FINLAND

Postal address:

P.O. BOX 120
02631 ESPOO
FINLAND

Sales Office / USA:

Phone: (770) 291 2181
Bluegiga Technologies, Inc.
3235 Satellite Blvd, Building 400, Suite 300
Atlanta, GA 30096