Bluetooth

Part 12: The Personal Area Networking Profile

Kjell Jørgen Hole
UiB

Last updated 18.03.06
Mail: Kjell.Hole@ii.uib.no
URL: www.kjhole.com

Outline

- Definition of Bluetooth profiles
- **Personal Area Networking** (PAN) profile
- Bluetooth Network Encapsulation Protocol (BNEP)
- How to publish MIDlets for mobile phones

Profile

Profile A set of rules to use the Bluetooth protocol stack in a device. Different profiles are defined for different types of services. The aim of the profiles is to ensure that different device types will be able to interoperate. Each profile defines

- what features of the Bluetooth stack are required and how they are used
- a minimum set of user and behaviour characteristics that enable common end-user functionality
- how a programmer should use an API for a Bluetooth protocol

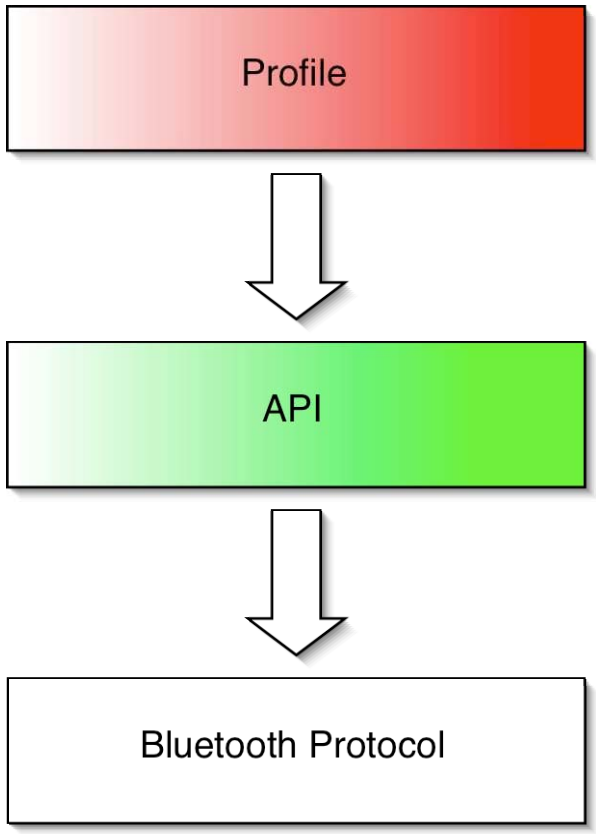

Figure 12-1 Connection between a profile and an API for a Bluetooth protocol

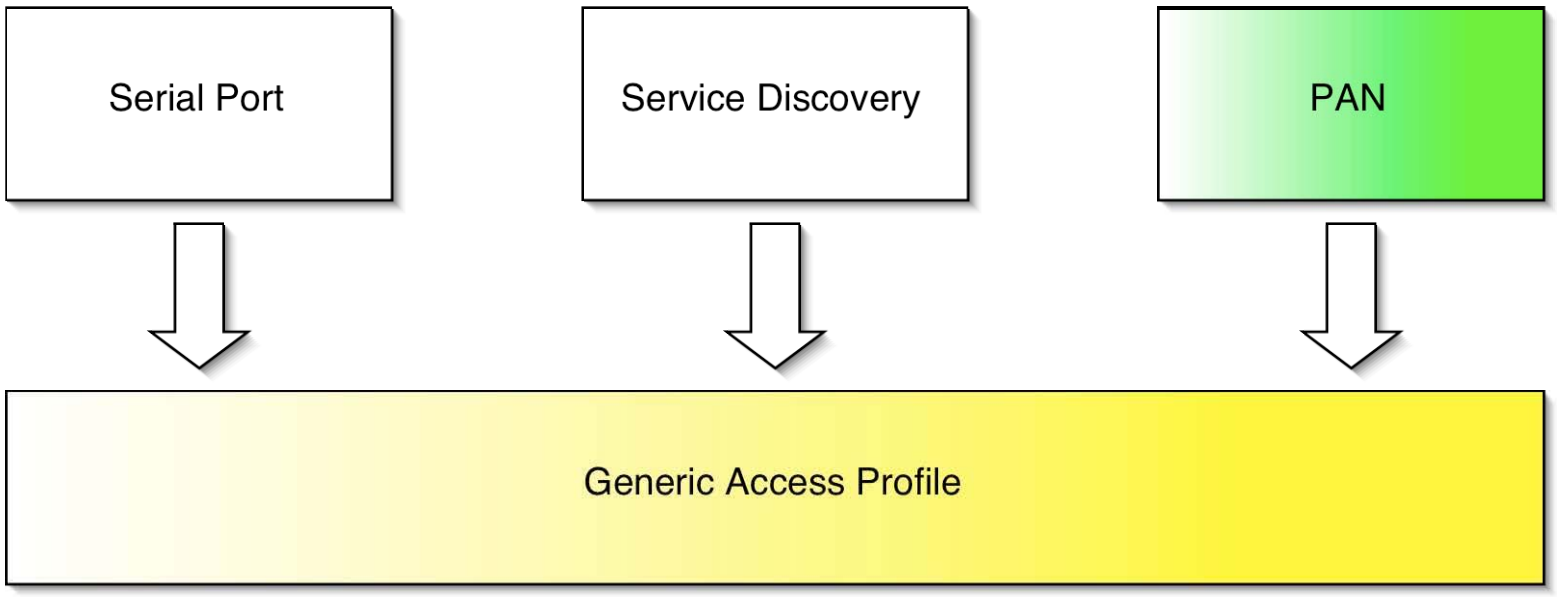

Figure 12-2 Hierarchal organisation of important profiles

PAN Overview

- The PAN profile lays out the rules for carrying Internet Protocol (IP) traffic across Bluetooth connections
  - Ethernet packets are encapsulated in L2CAP packet payloads using BNEP
- The PAN profile relies upon the Generic Access Profile, but does not make use of any other profiles

Topics Not Covered by PAN Profile

- Automatic network formation
- General ad-hoc networking where more than one piconet are involved
- Quality of Service (QoS)

These topics may be covered in future versions of the PAN profile

NAP and GN Scenarios

There are two general PAN scenarios, denoted the **Network Access Point** (NAP) and **Group ad-hoc Network** (GN) scenarios

NAP A Bluetooth device acting as a bridge to connect a piconet to an IP network. It forwards packets to and from the network and amongst PAN users

GN A Bluetooth device which connects to one ore more PAN users, forwarding packets between PAN users when more than one is connected

PAN User

Each of the PAN scenarios has unique network architecture and unique network requirements. The term **PAN User** (PANU) used in the scenario descriptions is defined by

PANU A client device which uses the Group ad-hoc Network or Network Access Point service

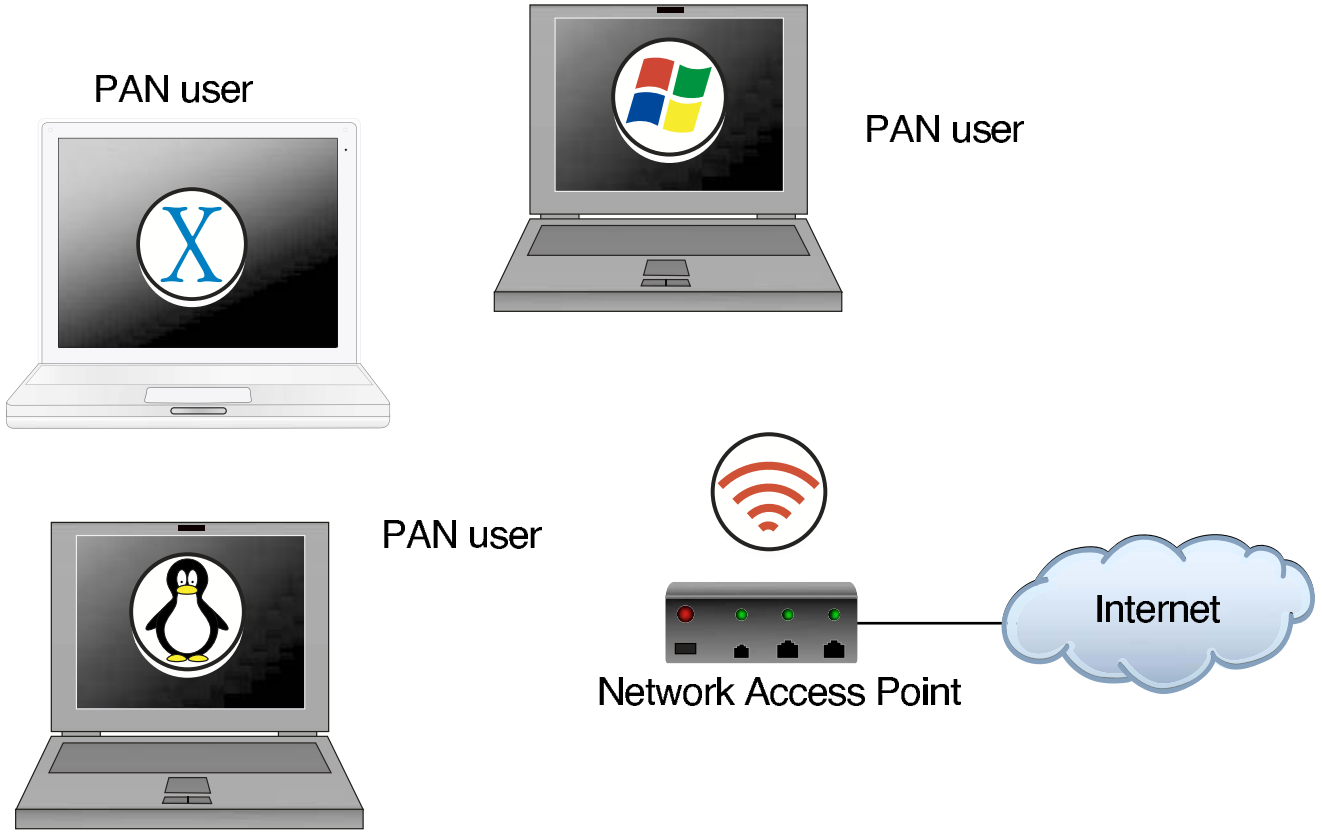

Figure 12-3 Network Access Point (NAP) scenario

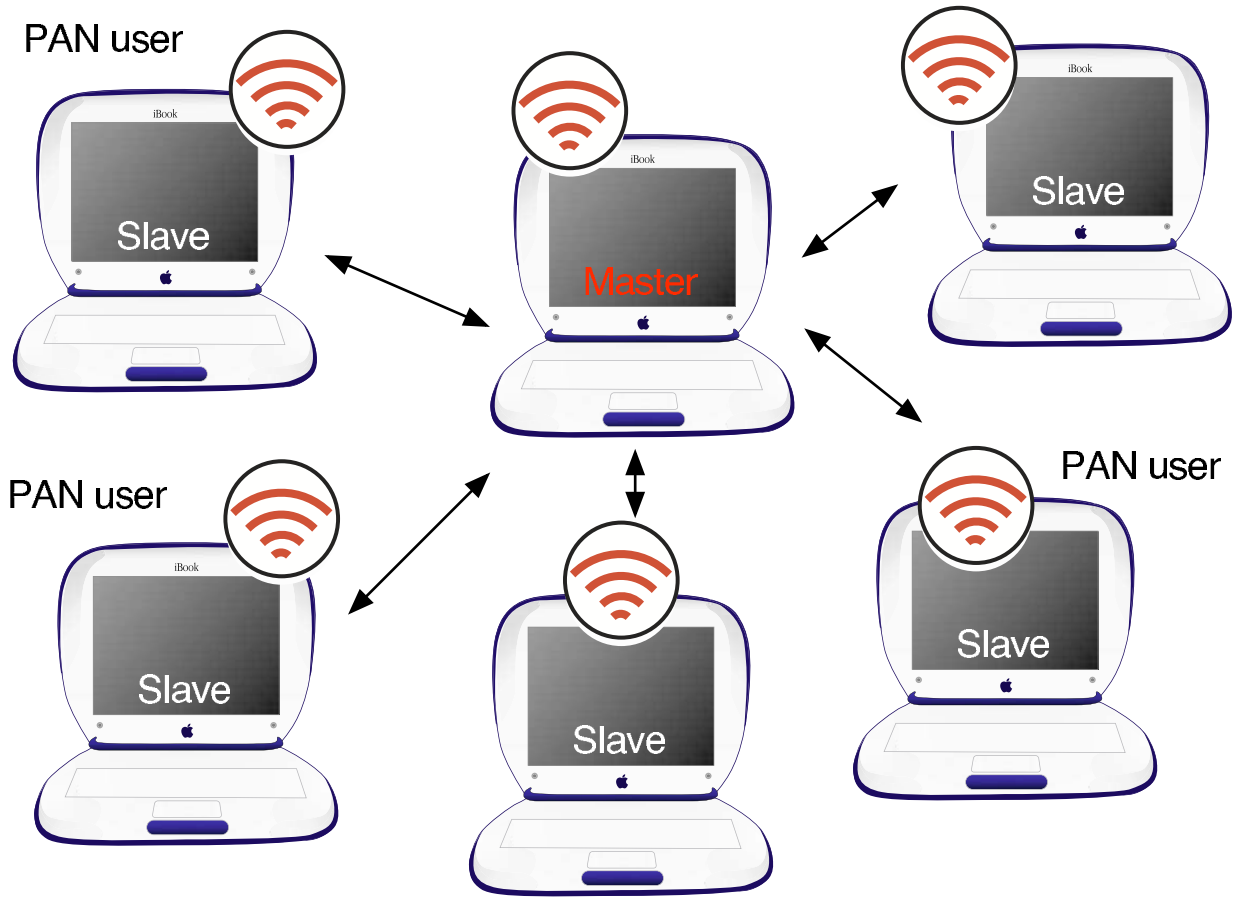

Figure 12-4 Group ad-hoc Networking (GN) scenario

Group Ad-Hoc Networking

- In general, Group ad-hoc networking is a collection of mobile hosts that cooperatively create an ad-hoc wireless network without the use of additional networking hardware or infrastructure

- the PAN profile focuses on a simple networking scenario consisting of a single Bluetooth piconet with connections between two or more Bluetooth devices

GN Example with PANU Initiating Connection

A PANU connects to a GN to create an ad-hoc network with other Bluetooth devices. This example provides a brief summary of the typical interactions of a GN and a PANU:

1. The PANU tries to find another Bluetooth device that is within radio range and is providing the GN service by using baseband inquiries and SDP searches

2. If there is no existing Bluetooth connection, then the PANU requests a Bluetooth connection with the selected device providing the GN service

GN Example (cont.)

3. Once the connection is made, the PANU can create an L2CAP channel for BNEP and use the BNEP control commands to initialize the BNEP connection and setup filtering of different network packet types

4. Ethernet traffic can now flow across the link. GNs will not provide networking services and therefore each of the PANUs will perform various tasks to operate without these services. The GN will forward all Ethernet packets to each of the connected PANUs

5. At any time the PANU or the GN may terminate the connection

GN Usage Model

- When a GN is created the PANUs have access to shared resources
  - each PANU may define an area that can be shared safely
  - a PANU may place documents and other items in this area
- This model may be used for networked games, where the Master hosts the game and PANUs may choose to join in

NAP Example (1)

A PANU will connect to a NAP in order to access a remote network. This example provides a brief summary of the typical interactions of a NAP and a PANU:

1. PANU tries to find a NAP that is within radio range and is providing the NAP service. For example, the PANU could use an application to inquire for nearby devices and then use SDP (Service Discovery Protocol) to retrieve records that support the NAP service

2. If there is no existing Bluetooth connection, then the PANU requests a Bluetooth connection with the selected NAP

NAP Example (2)

3. Once the connection is made, the PANU shall create an L2CAP channel for BNEP and may use the BNEP control commands to initialize the BNEP connection and setup filtering of different network packet types

4. Ethernet traffic can now flow across the link. The PANU uses the services provided by the remote network, such as obtaining an IP address by using DHCP (Dynamic Host Configuration Protocol)

5. At any time the PANU or the NAP may terminate the connection

PAN Usage Model

- The PAN usage model is very similar to the GN usage model
  - A PANU gets access to shared resources and services
  - many of the services are offered by the wired network

Initializing PAN Services

- NAPs and GNs rely on SDP to advertise their services to PANUs
- NAPS and GNs must register their services in a service discovery database before they can be used
- When a NAP or GN service is initialized, the device must initialize its packet filtering database. This database defines which packet types will be forwarded across the Bluetooth link
- The security database must also be initialized if security is used

More on Initializing PAN Services

- NAPs may have Management Information Bases (MIBs). The PAN profile suggests that the following items should be included:
  - maximum number of users
  - discoverable/non-discoverable mode
  - packet filter database
  - security modes
  - networking, device, and security parameters

Discovering PAN Services (1)

A connection between a PANU and a NAP (or GN) is started as follows:

1. ACL link is set up between PANU and NAP
2. PANU sends *LMP_host_connection_req*
3. NAP sends *LMP_accepted*
4. NAP sends *LMP_switch_req* to achieve a Master/Slave switch
5. PANU returns *LMP_accepted*

Discovering PAN Services (2)

6. Security is set up
7. NAP sends *LMP_setup_complete*
8. PANU sends *LMP_setup_complete*
9. Service discovery
10. PANU sends *LMP_detach* (or start using PAN services)

Establishing PAN Service Connection

PANU creates an ACL connection to selected device. PAN profile defines different modes which govern the security procedures:

Authorization mode Controls if and when authentication and access rights checks are used. Mode 1 is no authorization, mode 2 the PANU is authenticated, mode 3 the PANU is authenticated and its access rights are verified

PAN Service Connection (cont.)

Security mode Controls if and when link keys are required, and when other security procedures are used. Mode 1 is nonsecure, mode 2 is service level enforced security (when L2CAP channel is established), mode 3 is link-level enforced security (when ACL link is established)

Secrecy mode Controls if and when encryption is switched on. Clear mode means no encryption, encrypted mode means all PAN communications are encrypted. Encryption could be done by the Bluetooth baseband or at BNEP/IP level

Security

- The security procedures are applied individually to each link

- A GN and NAP can have simultaneously active connections with different security modes

  – data sent by a PANU over a secure link may be repeated unencrypted over another link

  – must require that all links are encrypted to eliminate this problem

Packet Forwarding

- The NAP or GN acts as a bridge and forwards packets between PAN users. It performs a subset of the operations specified by the IEEE 802.1D standard for MAC bridges

- Each PANU is treated as if it was a bridge port. For NAPs the Ethernet connection is also treated as a bridge port

- It is possible to filter out packet types

Bluetooth Network Encapsulation Protocol

- BNEP allows IP packets to be carried in the payload of L2CAP packets

- The BNEP layer sits directly above the L2CAP layer, supporting IP transport (see Figure 12-5)

- Above the IP layer, there is a session management layer, i.e., the Transport Control Protocol (TCP) or User Datagram Protocol (UDP)

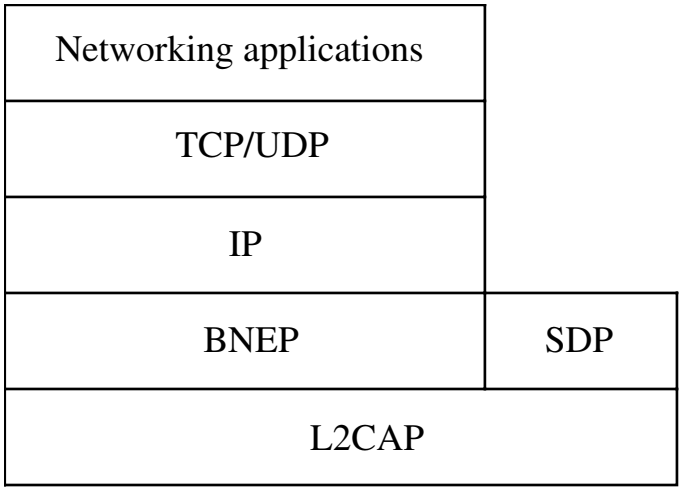

Figure 12-5 The BNEP protocol stack

BNEP

- BNEP attaches a header to the information to identify the packet type

Java

How to Publish MIDlets for Smartphones

- WAP pages may be used to publish a JAD and JAR files for MIDlets
- Eclipse generates the needed JAD and JAR files for a given project
- The following example is taken from `http://wap.klings.org/`

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>
<card title="wap.klings.org">
<p>Welcome to the wap section of klings.org</p>

<p>There are three Java programs available for download at this time.
Check out the links for details.</p>
```

```
<p>
<a href="btbrowser.wml">BTBrowser</a><br />
<a href="btbenchmark.wml">BTBenchmark</a><br />
<a href="phoneinfo.wml">Phoneinfo</a>
</p>
</card>
</wml>
```

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<card title="BTBrowser">
<p>The Bluetooth Browser can show you nearby discoverable Bluetooth
devices, their services and information about each service.  It has been
tested on a Nokia 6600, a Nokia 6230, and a Sony Ericsson P900.</p>
<p>
<a href="http://wap.klings.org/java/btbrowser.jad">Download BTBrowser</a>
</p>
</card>
</wml>
```

http://wap.klings.org/java/btbrowser.jad

```
MIDlet-Jar-Size:  16082
MIDlet-1:  BTBrowser,,org.klings.j2me.BTBrowser.BTBrowserMIDlet
MIDlet-Jar-URL: http://wap.klings.org/java/btbrowser.jar
MicroEdition-Configuration:  CLDC-1.0
MIDlet-Version:  1.4.0
MIDlet-Vendor:  Klings, NoWires
MIDlet-Name:  BTBrowser
MIDlet-Description:  Bluetooth Browser
MIDlet-Info-URL: http://wap.klings.org/btbrowser.wml
MicroEdition-Profile:  MIDP-2.0
```

Summary

- The PAN profile uses BNEP to enable *ad hoc* IP networks
  - BNEP provides a way for IP packets to be routed to and from Bluetooth devices
- A series of PANUs can connect to a NAP acting as a bridge forwarding packets to and from an ethernet
- PANUs can also connect to a GN with no outside network connection