Abstract
This article proposes the Simple Internet Access Procedure (SINAP), which enables IP communication in a Bluetooth piconet where one or more devices may have Internet access. Alternatives for allocation of IP addresses are also discussed. The Piconet consists of Bluetooth enabled computing devices, such as laptops, which may have Internet connections over Ethernet, WLAN, or GSM/UMTS. It is formed according to an automatic Piconet formation procedure. The procedure provides topology information, which makes it is possible to deploy IP directly on the L2CAP protocol without the need for any adaptation layer.

Keywords
Bluetooth, Piconet, Ad-Hoc network, L2CAP, PAN, BNEP, IP address allocation, DHCP, Personal Area Network.

Motivation
Bluetooth SIG has defined a PAN profile that can provide an ad-hoc network of Bluetooth devices (i.e. Piconet) with access to a remote network through a network access point. However, this profile uses the BNEP protocol to emulate Ethernet. BNEP is an adaptation layer, which introduces overhead and limits the PAN’s dynamics where devices can appear and disappear at any time.

The intention of the proposed Simple Internet Access Procedure (SINAP) is to enable Internet access in a Bluetooth Ad-hoc network (Piconet) without any adaptation layer. The devices may have Internet connections over Ethernet, WLAN or GSM/UMTS (Figure 1).

It is assumed that the Piconet is formed by the automatic Piconet formation procedure, SAPIFO [4]. Since the procedure provides all devices with topology information, it is possible to enable IP communication in the Piconet directly on the L2CAP protocol and make the BNEP protocol superfluous.

1 Background

1.1 L2CAP Logical Link Control and Adaptation Protocol

The Logical Link Control and Adaptation Layer Protocol (L2CAP) [1] is layered over the Baseband Protocol and resides in the data link layer (Figure 3). L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.
L2CAP is based on logical channels. Channel identifiers (CIDs) are local names representing logical channel end-points on devices.

A connection-oriented data channel represents a connection between two devices (Figure 2), where a CID identifies each endpoint of the channel. A connectionless channel restricts data flow to a single direction. It is used to support a channel 'group' where the CID on the source represents one or more remote devices. There are also a number of CIDs reserved for special purposes. The signaling channel is one example of a reserved channel. This channel is used to create and establish connection-oriented data channels and to negotiate changes in the characteristics of these channels. L2CAP transfer data between higher layer protocols and the lower layer protocol.

### Table 1 CID definitions

<table>
<thead>
<tr>
<th>CID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>Null identifier</td>
</tr>
<tr>
<td>0x0001</td>
<td>Signalling channel</td>
</tr>
<tr>
<td>0x0002</td>
<td>Connectionless reception channel</td>
</tr>
<tr>
<td>0x0003-0x003F</td>
<td>Reserved</td>
</tr>
<tr>
<td>0x0040-0xFFFF</td>
<td>Dynamically allocated</td>
</tr>
</tbody>
</table>

A Protocol Service Multiplexer (PSM) distinguishes the different protocols. Table 2 shows some PSM values. Values < 0x1000 are reserved.

### Table 2 Protocol and service multiplexor (PSM)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>PSM Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP</td>
<td>0x0001</td>
</tr>
<tr>
<td>RFCOMM</td>
<td>0x0003</td>
</tr>
<tr>
<td>TCS-BIN</td>
<td>0x0005</td>
</tr>
<tr>
<td>TCS-BIN-CORDLESS</td>
<td>0x0007</td>
</tr>
<tr>
<td>BNEP</td>
<td>0x000F</td>
</tr>
<tr>
<td>HID_Control</td>
<td>0x0011</td>
</tr>
<tr>
<td>HID_Interrupt</td>
<td>0x0013</td>
</tr>
<tr>
<td>AVDTP</td>
<td>0x0019</td>
</tr>
</tbody>
</table>

Various signalling commands can be passed between two L2CAP entities on remote devices. All signalling commands are sent with CID = 0x0001.

### 1.2 PAN profile

The PAN Profile [2] is running on the Bluetooth Protocol Stack shown in Figure 3 and identifies two configurations of a Bluetooth PAN: The Network Access Point (NAP) configuration is used when the master is connected to an external network, and the Group Ad-hoc Node (GN) configuration is used when no devices have a network connection. In both cases, the Bluetooth device that uses the NAP service or GN service is a PAN User (PANU). NAP and GN forward BNEP packets between PANUs according to the BNEP protocol, which implements parts of the IEEE 802.1D standard [8].

### 1.3 BNEP

The Bluetooth Network Encapsulation Protocol, BNEP [3], emulates an Ethernet on a broadcast network segment, hiding the underlying master-slave based piconet topology. BNEP runs over L2CAP and reuses the Ethernet packet format commonly used for local area networking technology. The 48 bits Bluetooth addresses are used as IEEE source and destination addresses. The BNEP header (Figure 1) may be extended with one or more extension headers that allows for additional capabilities. BNEP also defines connection control messages.

Before completion of the BNEP connection setup, the initiator has to indicate the roles of both end-points. For bandwidth saving purposes, protocol and multicast filter
commands have been defined to indicate which protocol
types and multicast addresses a device wants to receive.
All these control messages have to be confirmed before the
new configuration applies. BNEP accommodates IP com-
mutation by transporting IP packets between two
Ethernet-based link-layer end-points on an IP segment. It
encapsulates the IP packets in BNEP headers, letting the
source and destination addresses reflect the Bluetooth end-
points and setting the 6-bit Networking Protocol Type field
to code for an IP packet in the payload. BNEP finally en-
capsulates the BNEP packet in an L2CAP header and
sends it over the L2CAP connection.

To illustrate the SAPIFO procedure, we consider a
Bluetooth topology shown in Figure 2. The figure illus-
trates six Bluetooth devices with BD-Address BD-1 to BD-
6 in an ascending order.

Figure 5: Piconet Example

The lines in Figure 5 indicate connections of devices
within radio range. Thus, after awhile each device will
have detected neighboring devices according the connec-
tion Table 3 below.

Table 3: Connection table

<table>
<thead>
<tr>
<th></th>
<th>BD-1</th>
<th>BD-2</th>
<th>BD-3</th>
<th>BD-4</th>
<th>BD-5</th>
<th>BD-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD-1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>BD-2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-4</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-5</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each device sends information of its neighboring de-
vices to its neighbors. To do this, the devices will both go
in a sequence of Page and Page Scan according to Table 2.
A device will page another device with higher BD-Address
and go into Page Scan for a device with lower BD-ADDR.

Table 4: Page and Page Scan table

<table>
<thead>
<tr>
<th></th>
<th>BD-1</th>
<th>BD-2</th>
<th>BD-3</th>
<th>BD-4</th>
<th>BD-5</th>
<th>BD-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD-1</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-2</td>
<td>PS</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-3</td>
<td>PS</td>
<td>PS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-4</td>
<td>PS</td>
<td>PS</td>
<td>PS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-5</td>
<td>PS</td>
<td>PS</td>
<td>PS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BD-6</td>
<td></td>
<td>PS</td>
<td>PS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When every device has exchanged information about
their neighbors, every device will have one copy of the
connection table that was shown in Table 3.
In our example, the connection table determines that there are two master candidates for the piconet, namely BD-3 and BD-4. Since BD-4 has the highest Bluetooth address, it will become the master while BD-3 will serve as a backup master.

2 SINAP

SINAP exploits the information derived from the SAPIFO procedure. The connection table of the SAPIFO procedure contains information about the Piconet topology, Bluetooth MAC addresses devices within radio range, as well as master and backup master information. This information might form a basis for an neighbour table (or ARP table) with Bluetooth IEEE addresses (BD-ADDR) and IP addresses. By combining the connection table with knowledge of capabilities of different Bluetooth devices (such as processing capacities, network access parameters etc.) one also has information that connects the Bluetooth link layer and the IP layer.

For this special case of Piconet, we suggest to run the IP protocol directly on L2CAP. By omitting the BNEP layer, we will get a simpler protocol hierarchy than in the more general concept specified in the PAN profile.

2.1 IP communication without external IP connections

![Figure 6. The link layer topology of a sample Piconet](image)

Figure 6 illustrates the Layer 2 topology of a Piconet without any network connections. The topology consists of a master and four slaves. The router resides on the master, since only the master is on-link with every node, while the slaves are hosts and use the master as default router.

The Router assigns private IP addresses [5] to Bluetooth slaves from a private IP prefix (e.g. 10/8) and in an ascending order based on the size of the BD-ADDR. Thus, every node can derive its own IP address from the connection table, and every slave can derive the IP address of the master, which is used as the default gateway IP address. Hence, neither ARP [7] nor DHCP [6] is required for private IP addresses and local communication.

The router uses the information from the connection table to build a neighbour table (or ARP table), which maps the assigned private IP addresses to their BD-ADDR.

L2CAP has the necessary capabilities to run a point-to-point protocol that carries a Payload of an IP packet. By specifying a PSM value for SINAP, we can use this L2CAP channel to carry IP packets in both directions between master and slave. To do this, the master must set up a connection-oriented channel with the selected PSM value. When the Piconet is formed, L2CAP connections are is set up between the master and each slaves. The master will perform the signalling to set up a SINAP channel to all the slaves.

2.2 IP communication with external IP connections

Some devices in the Piconet might be able to connect to the Internet over different access technologies including WLAN, GSM GPRS or GSM HSCD. IP is a technology that allows such inter-technology communication, and the ubiquitous IPv4 protocol is therefore assumed [12]. We therefore require that a router process run on each access device in addition to the router on the master.

The most limiting factor for IPv4 is the scarcity of IP addresses. ISPs are often reluctant to allocate global IP addresses to roaming nodes, which often have limited access privileges. This means that an access point is likely to receive one external IP-address at most - probably a private IP-address (i.e. the ISP is implementing a NAT solution) or a global IP address at best.

Hence, different nodes in the Bluetooth Piconet might have to share the external IP-address that the access point acquires. The easiest way to accommodate this is to allow devices to use private IP addresses for both local and external communication, and implement a Network Address and Port Translation (NAPT) on access nodes for Internet Access [10]. A NAPT is a router that replaces a private or link-local IP source address and port number for outgoing IP packets with a global IP address and a unique port number before forwarding them towards the Internet. It performs the reverse translation with the destination addresses of incoming packets before forwarding them into the internal network.

One problem with using NAPTs and multiple access points is that all outgoing packet of a stateful session (e.g. a TCP session) must pass through the same address translator where the state information about the address translation is stored. Otherwise, the IP-packet will be assigned a new global source IP-address and the session will break. Furthermore, since Internet Service Providers (ISPs) are probable to implement ingress filtering, the packet should
be sent over the access point corresponding to the IP-address that the private IP-address is translated into.

SINAP therefore mandates that the master assigns an access point to each communicating host, and that this information is stored as a host-specific default route on the master. When the master-router receives an IP-packet bound for an external network, it checks the routing table to find which access point represent the default router of the source device, and forwards the packet to that access device. If the master has a connection to an external network, it may naturally serve as an access point for some of the slaves.

In some cases the access device may acquire a number of IP addresses from the external network, and devices in the Piconet might not have to share IP addresses. The access device should then implement a DHCP server, the master should implement a DHCP relay, and the Bluetooth hosts should implement a DHCP client. The Bluetooth host may issue a DHCP request, which is relayed by the master to the right access node. The access node returns a global IP address to the DHCP client. However, the router on the master should still be the default gateway of the host.

**Conclusion**

We proposed a simple procedure to accommodate local and external IP communication in a Bluetooth Piconet. The proposal is based on an automatic formation procedure, SAPIFO, and it allows IP to run directly on the L2CAP protocol. The external network connection can be located in any of the Piconet devices. Allocation of IP addresses was also discussed.

**References**


[2] Personal Area Networking Profile
http://www.bluetooth.com/pdf/PAN_Profile_0_95a.pdf


[5] Address Allocation for Private Internets
http://www.ietf.org/rfc/rfc1918.txt

http://www.ietf.org/rfc/rfc2131.txt

http://www.ietf.org/rfc/rfc826.txt


[12] Internet Protocol (IPv4),
http://www.ietf.org/rfc/rfc0791.txt