Personal Area Networking Profile

Abstract:
The Personal Area Networking (PAN) Profile describe how two or more Bluetooth enabled devices can form an ad-hoc network and how the same mechanism can be used to access a remote network through a network access point. The profile roles contained in this document are the Network Access Point, Group Ad-hoc Network, and Personal Area Network User. Network access points can be a traditional LAN data access point while Group Ad-hoc Networks represent a set of devices that are only attached to one another.

Disclaimer and Intellectual Property Notice

The copyright in these specifications is owned by the Promoter Members of Bluetooth SIG Inc. ("Bluetooth SIG"). Use of these specifications and any related intellectual property (collectively, the "Specification") is governed by the Promoters Membership Agreement among the Promoter Members and Bluetooth SIG (the "Promoters Agreement"), certain membership agreements between Bluetooth SIG and its Adopter and Associate Members (the "Membership Agreements"), and the Bluetooth Specification Early Adopters Agreements (1.2 Early Adopters Agreements) among Early Adopter members of the unincorporated Bluetooth special interest group and the Promoter Members (the "Early Adopters Agreement"). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to Bluetooth SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of Bluetooth SIG or a party to an Early Adopters Agreement (each such person or party, a "Member") is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement, or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement, or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by applicable law to Bluetooth SIG or any of its members for patent, copyright, and/or trademark infringement.

THE SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION, OR SAMPLE.

Each Member hereby acknowledges that products equipped with the Bluetooth™ technology ("Bluetooth™ Products") may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation, and distribution of Bluetooth™ Products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls, and health and safety regulations. Each Member is solely responsible for the compliance by their Bluetooth™ Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their Bluetooth™ Products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations, or licenses. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NON-COMPLIANCE WITH LAWS RELATING TO USE OF THE SPECIFICATION, IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST BLUETOOTH SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserves the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate and to adopt a process for adding new Bluetooth™ profiles after the release of the Specification.

BLUETOOTH is a trademark owned by Bluetooth SIG, Inc.

Contents

Revision History

Revision	Date	Comments
0.0	April 4, 2000	Original Document Started
0.1	May 11, 2000	Added various sections and added useful part of the Ethernet bridge profile proposal
0.2	July 10, 2000	Added Monte Carlo F2F feedback
0.3	July 17, 2000	Fixed formatting errors
0.4	July 24, 2000	Added Addressing
0.5	September 26, 2000	Various structure and editorial changes Released to Adopters
0.6	October 12, 2000	Editorial changes Clarify Required Security PAN User Service Record Moved Testing Section to Appendix
0.7	November 27, 2000	Editorial changes Added Test Cases
0.9	February 6, 2001	Removed Test Cases to a separate document Updated IP Address Assignment, Name Resolution Updated Security section
0.95	June 12, 2001	Editorial changes and changes based on BARB, BTI, BQRB, BTAB feedback.
0.95a	June 26, 2001	Editorial changes and changes based on BARB & BTI adoption review.
0.96	September 9, 2001	Minor editorial and correction changes.
0.96a	September 20, 2001	Editorial and correction changes.
0.96b	October 16, 2001	Editorial and correction changes.
0.96d	November 19, 2001	Editorial and correction changes.
0.96e	January 2, 2002	Updated version number and clarifying text to mDNS section
1.0	July 23, 2002	Errata and feedback incorporated. Interoperability testing completed
1.0RC	December 2, 2002	BTI and BQRB Comments
1.0RC2	December 6, 2002	PAN WG Comments

1.0RC3	December 17 2002	PAN WG Meeting editorial fixes
1.0	February 14, 2003	Profile Adopted

Contributors

Name	Company
David Moore	3COM Corporation
Tom Scribner	3COM Corporation
Barry Corlett	Agere Systems
Willy Sagefalk	Axis Communications
Dan Willey	Certicom Corporation
Horia Balog	Classwave Wireless Inc.
Conrad Maxwell	Conexant Systems
Mark Rison	CSR
Allan Bogeskov	Telefonaktiebolaget LM Ericsson
Theo Borst	Telefonaktiebolaget LM Ericsson
Per Johansson	Telefonaktiebolaget LM Ericsson
Tero Kauppinen	Telefonaktiebolaget LM Ericsson
Martin Kitchen	Telefonaktiebolaget LM Ericsson
Jesper Krogh	Telefonaktiebolaget LM Ericsson
Tony Larsson	Telefonaktiebolaget LM Ericsson
Johan Sorensen	Telefonaktiebolaget LM Ericsson
Dave Suvak	Extended Systems Inc.
Jean Tourrilhes	Hewlett Packard Corporation
Toru Aihara	International Business Machines Corporation
Chatschik Bisdikian	International Business Machines Corporation
Kris Fleming (Editor)	Intel Corporation
Robert Hunter	Intel Corporation
Jon Inouye	Intel Corporation
Diego Melpignano	Philips Inc.
Eiji Kato	Matsushita Electric Industrial
Mike Foley	Microsoft Corporation

Billy Brackenridge	Microsoft Corporation
Dale Farnsworth	Motorola Inc.
Brian Redding	Motorola Inc.
Carmen Kuhl	Nokia Corporation
Jaakko Lipasti	Nokia Corporation
James Scales	Nokia Corporation
Markus Schetelig	Nokia Corporation
Sander van Valkenburg	Nokia Corporation
Steven Kenny	Norwood Systems
Rebecca Ostergaard	Norwood Systems
Graeme Reid	Norwood Systems
Darrell Goff	Rappore
Daniel Shaw	Red-M Communications Ltd
Simon Harrison	Red-M Communications Ltd
Pravin Bhagwat	ReefEdge, Inc.
Daryl Hlasny	Sharp Laboratories of America Inc.
Leonard Ott	Socket Communications Inc.
Johannes Loebbert	Sony Corporation
Wilhelm Hagg	Sony Corporation
Takashi Sasai	Sony Corporation
Mike Blackstock	Synchropoint Wireless, Inc.
Yosuke Tajika	Toshiba Corporation
Tatuya Jinmei	Toshiba Corporation
Kazuo Nogami	Toshiba Corporation
Jim Hobza	Widcomm Inc.
Ravindranath Singamneni	Widcomm Inc.

1 Introduction

Bluetooth is a short-range wireless technology operating in the 2.4 GHz ISM band. Many devices such as notebook computers, phones, PDAs, Home Electric Appliances, and other computing devices will incorporate Bluetooth wireless technology. Using Bluetooth wireless technology, devices will have the ability to form networks and exchange information. For these devices to interoperate and exchange information, a common packet format has been defined to encapsulate layer 3 network protocols.

The document describes how to use the Bluetooth Network Encapsulation Protocol (BNEP) Specification [1] to provide networking capabilities for Bluetooth devices. The document describes the first version of the Bluetooth PAN profile. Phase I addresses the following:

- Ethernet Encapsulation
- Single-Piconet IP PAN
- Master Forwarding
- Network Access Point

Future versions of the profile will be developed to address additional PAN profile requirements.

1.1 Bluetooth Networking Functional Requirements

The functional requirements for the PAN profile include the following:

- Define/reference dynamic ad-hoc IP-based personal networking
- Must be OS, language and device independent
- Provide support for common networking protocols such as IPv4 and IPv6. For other existing networking protocols support may or may not be provided.
- Provide support for network access points where the network could be a corporate LAN, GSM, and other data networks.
- Accommodate the reduced resources available to small devices with respect to memory, processing power, and user interfaces.

1.2 Assumptions

- IPv4 and IPv6 SHALL be supported by the PAN profile. Other standard protocols may or may not be enabled.
- In a generalized network, traffic can originate from any network-connected device and may be destined to any other network-connected device. Any suitable transport media may be involved in the traffic's path, for example Bluetooth, Ethernet, Token Ring, PSTN, ISDN, ATM, GSM, etc.

1.3 Scope

This document covers the following topics:

- Network Discovery
- Manual Network Formation
- IP Address Allocation
- Address Resolution
- Hostname Resolution
- Link Layer Bridging/IP Routing
- Networking Security

The PAN profile defines a means of enabling Bluetooth devices to participate in a personal area network. Completely un-modified Ethernet payloads can be transmitted using the Bluetooth Network Encapsulation Protocol (BNEP) to exchange packets between Bluetooth devices.

The profile defines how PAN is supported in the following situations.

(a) Ad-hoc IP networking by two or more Bluetooth devices in a single piconet.

(b) Network access for one or more Bluetooth devices.

This document does not cover the following topics:

- Automatic Network Formation.
- General ad-hoc networking where more than one piconet (i.e. multiple piconets) are involved.
- Indirect access to a Network Access Point via one or more intermediate Bluetooth devices.

- Group Ad-hoc Networks connecting to Network Access Points.
- Quality of Service (QoS)

The Bluetooth Network Encapsulation Protocol [1] specifies the transmission of Ethernet payloads over Bluetooth.

1.4 Byte Order and Numeric Values

All values contained in the document are represented in hexadecimal notation. Multiple-byte fields are drawn with the more significant bytes toward the left and the less significant bytes toward the right. The multiple-byte fields in the Bluetooth Networking encapsulation header are in standard network byte order (big endian), with more significant (byte 0 is the most significant byte) bytes being transferred before less-significant (low-order) bytes. Multiple-bit fields are drawn with the more significant bits toward the right and the less significant bits toward the left.

1.5 Profile Dependencies

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile does have direct dependencies on the profile(s) within which it is contained, as illustrated in the figure. In particular, the PAN profile is dependent on the Generic Access profile [4].

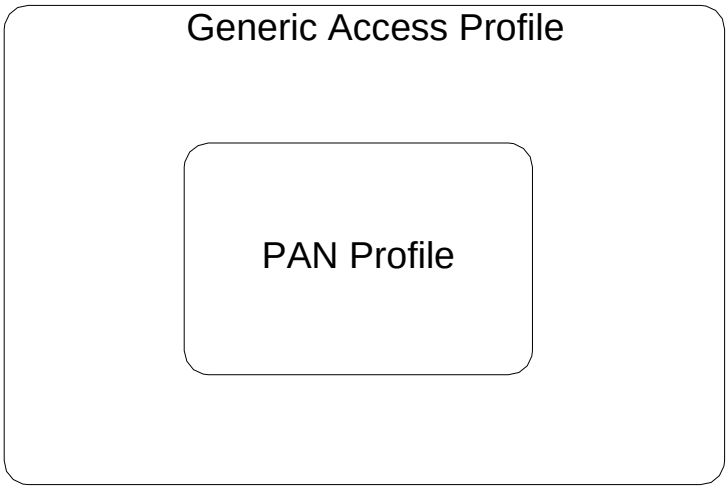

Figure 1: Bluetooth Profile Hierarchy

1.6 Symbols And Conventions

1.6.1 Requirement status symbols

In this document (especially in the profile's requirements tables), the following symbols are used:

- 'M' for mandatory to support (used for capabilities that SHALL be used in the profile);
- 'O' for optional to support (used for capabilities that can be used in the profile);
- 'C' for conditional support (used for capabilities that SHALL be used in case a certain other capability is supported);
- 'X' for excluded (used for capabilities that MAY be supported by the unit but SHALL NOT be used in the profile);
- 'N/A' for not applicable for this profile (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile

In this specification, the word 'SHALL' is used for mandatory requirements, the word 'MAY' is used for optional features.

2 Profile overview

2.1 Scenarios

For this profile, three general scenarios are discussed: (1) Network access points, (2) Group Ad-hoc Networks, (3) PANU-PANU. Each of the scenarios has unique network architecture and unique network requirements, but all are various combinations of a PAN.

2.1.1 Network Access Points

A network access point is a unit that contains one or more Bluetooth radio devices and acts as a bridge, proxy, or router between a Bluetooth network and some other network technology (10BASE-T, GSM, etc). To a computing device connected to an access point, the access point's radio and host controller appear to be a direct bus connection to a network interface device with network access. Each network access point can allow one or more computing devices to gain access to its service which MAY include access to all of a LAN's shared resources. Network access points SHALL provide access to other networks via technologies such as Ethenet, ISDN, Home PNA, Cable Modem and cellular.

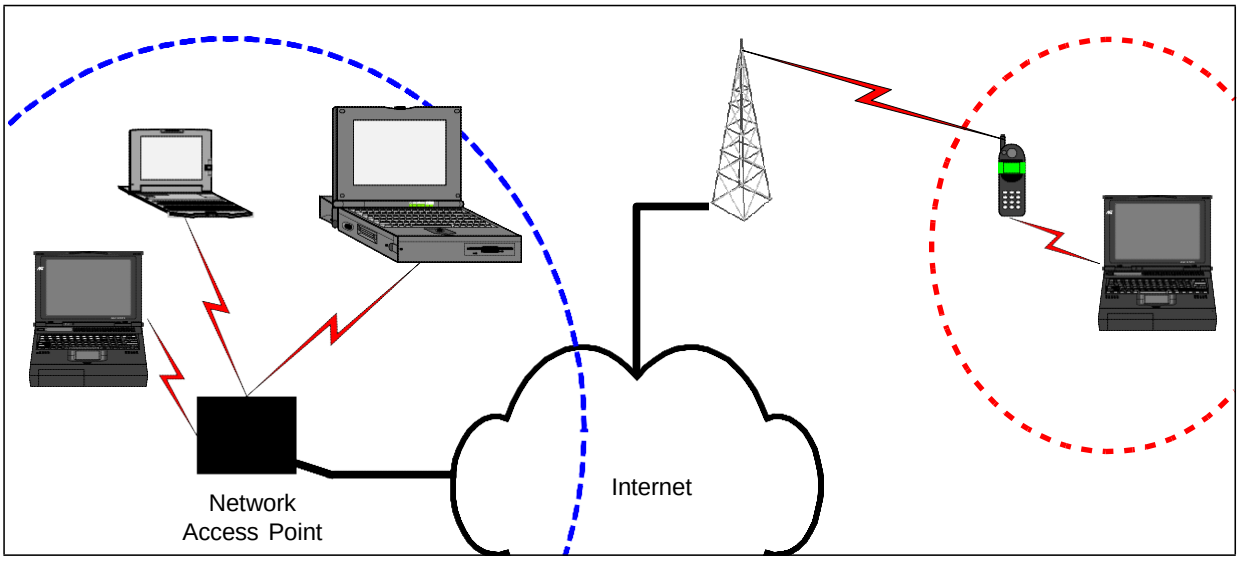

Figure 2: Example of two types of Network Access Points

2.1.2 Group Ad-hoc Networks

Group ad-hoc networking allows mobile hosts to cooperatively create ad-hoc wireless networks without the use of additional networking hardware or

infrastructure. Version 1.0 of the PAN profile focuses on the following simple personal ad-hoc networking scenario consisting of a single Bluetooth piconet with connections between two or more Bluetooth devices.

A piconet consists of one Bluetooth device operating as a piconet master communicating with between 1 and 7 active Bluetooth devices operating as slaves. Communications in a piconet are between the master and the slaves and under the control of the master either in a point-to-point or point-to-multi-point fashion. In addition, there MAY be further non-active piconet members that are in park mode. The limitation of 7 active slaves in a piconet is enforced by the Bluetooth active member-addressing scheme [2]. A group ad-hoc network is a set of computing devices which interact with each other to form a self-contained network, the network being formed without the need for additional external networking hardware. A typical group ad-hoc network consisting of eight active computing devices connected in one piconet is illustrated in Figure 3 on page 16.

2.1.3 PANU-PANU

In this scenario, a point to point connection between two PANUs allows direct communication between these two nodes only.

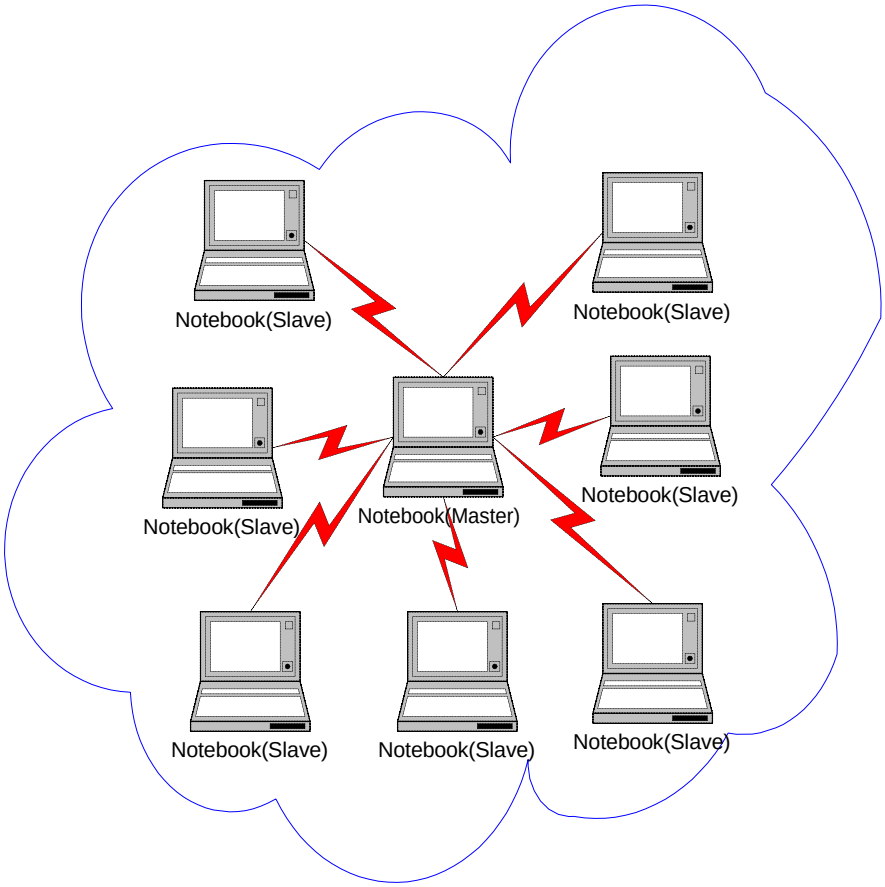

Figure 3: Single Piconet Personal Ad-hoc Network

2.2 PAN Profile Scenarios summary

The services offered by the Network Access Point role and the Group Ad-hoc Network role provide for different networking requirements. The NAP role provides network services to each of the Bluetooth devices connected, while the GN role allows two or more Bluetooth devices to become part of an ad-hoc network. Connecting to a Network Access Point or the formation of a Group Ad-hoc Network provide the facility for applications to use IP and other networking protocols.

Connections between two PANUs are used to simulate a cross-over cable between two nodes only.

2.3 Profile stack

The figures below show the protocols and entities used in each of the three roles defined by the PAN profile.

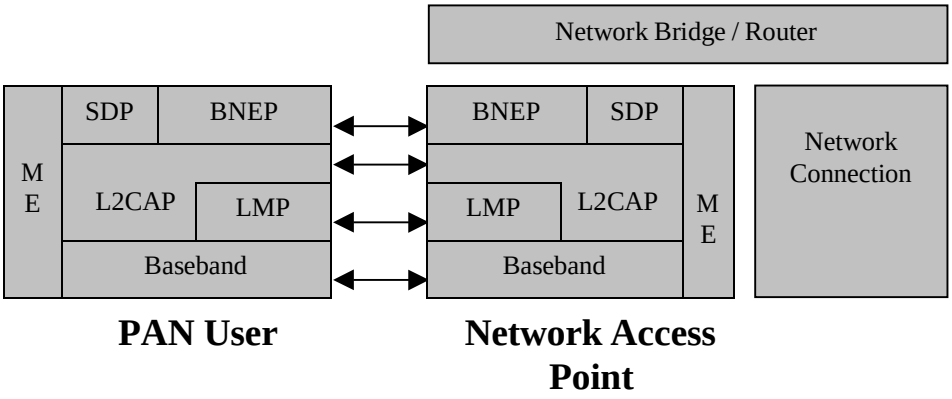

Figure 4 Network Access Point Profile Stack for Phase I

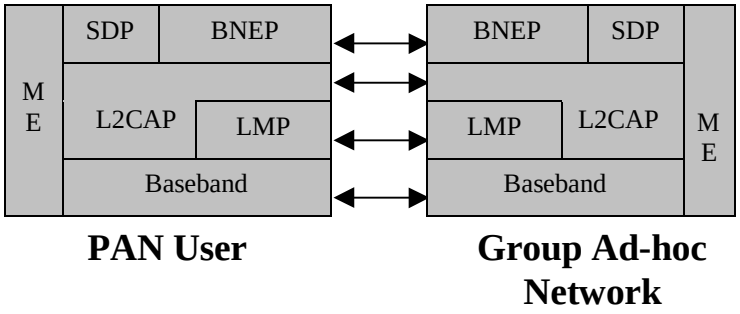

Figure 5 Group Ad-hoc Network Profile Stack for Phase I

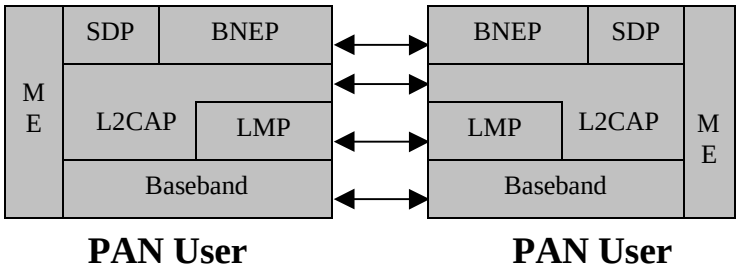

Figure 6 PANU to PANU Profile Stack for Phase I

Ethernet is specified by the IEEE 802.3 standards. Ethernet Bridging is specified in the IEEE 802.1D standards [3]. The 802.1D standard defines a means of moving Ethernet packets between various media and ports. Only a small part of the 802.1D standard is required by the PAN profile as defined in section 5.4.

The Baseband [2, part B], LMP [2, part C] and L2CAP [2, part D] are the part of the Bluetooth protocols that reside in the OSI layers 1 and 2. SDP is the Bluetooth Service Discovery Protocol [2, part E].

ME is the Management Entity which co-ordinates procedures during initialization, configuration and connection management.

2.4 Configurations and roles

The following roles are defined within the PAN profile.

Network Access Point (NAP) and NAP service: A Bluetooth device that supports the NAP service is a Bluetooth device that provides some of the features of an Ethernet bridge to support network services. The device with the NAP service forwards Ethernet packets between each of the connected Bluetooth devices, referred to as PAN users, see below. A device with the NAP service is simply referred to as a NAP. The NAP and the PAN User exchange data using the Bluetooth Network Encapsulation Protocol (BNEP) [1]. The device with the NAP service has an additional network connection to a different network media in which the Ethernet packets are either exchanged via Layer 2 bridging or Layer 3 routing mechanism. These devices may require additional functionality when bridging to additional networks, for example GPRS.

Group Ad-hoc Network (GN) and GN service: A Bluetooth device that supports the GN service is able to forward Ethernet packets to each of the connected Bluetooth devices, the PAN users, as needed. The Group Ad-hoc Network and the PAN User exchange data using the Bluetooth Network Encapsulation Protocol (BNEP) [1]. Group Ad-hoc Networks do not provide access to any additional networks. Instead, Group Ad-hoc Networks are intended to allow a group of devices to form temporary network and exchange information.

PAN User (PANU) and PANU service – This is the Bluetooth device that uses either the NAP or the GN service. PANU supports the client role for both the NAP and GN roles, and direct PANU to PANU communication.

The presentation of the PAN profile will continue with the simplifying assumption that each device involved has a single Bluetooth radio.[1] Table 1 on page 19, explains the valid interactions between the three roles. Behavior of multiple active roles with connections on one radio is not defined, but traffic for each role SHALL NOT be forwarded between roles.

[1] Products with multiple radios can still be conformant to this profile. The NAP, GN, and PANU roles can be adopted independently by each radio.

Role of the acceptor	Role of the initiator			
		NAP	GN	PANU
	NAP	NO	NO	YES
	GN	NO	NO	YES
	PANU	YES	YES	YES

Table 1: Valid interactions between the three PAN profile roles

2.5 Profile fundamentals

The following examples illustrate how the NAP, GN and PANU roles interact in all the combinations permitted by version 1.0 of the PAN profile. The first example describes how a PANU discovers, connects, and uses a NAP and its network services. The second example describes how a PANU discovers, connects, and uses a GN service. The third example describes how a NAP/GN finds, connects, and then offers NAP/GN services access to a PANU. The fourth example shows a direct PANU to PANU connection. Subsequent sections in the PAN profile provide more detail for each of the following steps. All examples are for informative purposes only.

2.5.1 NAP example

A PANU connects to a NAP in order to gain access to an advertised network service. This example provides a brief summary of the typical interactions between a NAP and a PANU.

1. The first step is for the PANU to discover a suitable NAP that is within radio range and advertising the particular NAP service that the user or application wishes to connect to. To do this the PANU could perform an inquiry for nearby devices and then use SDP to retrieve the NAP record from those devices that support the NAP role. The list of devices returned from the inquiry MAY be filtered by Class of Device to remove any which don't have the Networking bit set in the service class field.

2. The choice of which NAP to establish a connection with MAY be based on, among other things, the service names extracted from the NAP's SDP records. Where more than one NAP provides the desired service the user or an

application will have to choose one. When no Bluetooth connection[2] exists to the selected device the PANU SHALL create one. If the NAP is in multi-user mode, a M/S switch SHALL be required to complete the connection.

3. Once an ACL connection has been created the PANU SHALL initiate the establishment of an L2CAP channel for BNEP. The BNEP connection setup procedure including the required BNEP control commands and optionally setting of packet filters is described in [1]. If the NAP supports filtering, it SHALL store all accepted network packet type filters for each connection..

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) for example. (See section 6.3 on page 36). If the PANU already has an IP address for the connection, such as the case from moving from on NAP to another NAP, the PANU SHALL verify that the current IP address is still valid for the this new connection. Other network services of interest can also be used by the PANU. The NAP SHALL forward Ethernet packets appropriately to the connected PANUs and/or over the NAP network connection. This is similar behavior as a network bridge.

5. Either the PANU or the NAP MAY terminate the connection at any time.

2.5.2 PANU initiates a connection to a GN

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 first step is 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. A master-slave switch SHALL be required to complete the connection if the GN is in multi-user mode.

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. If the GN supports filtering, it SHALL store all accepted network packet type filters for each connection.

[2] A Bluetooth connection is an established Bluetooth ACL connection. Creating this includes all of the intermediate steps involved with ACL connection establishment. During the connection establishment, the devices may perform mutual authentication. Either device may insist that encryption is used on the link. Authenticated and encrypted baseband connections are not required for the connection. Also during the ACL connection establishment, a master/slave switch may occur.

4. Ethernet traffic can now flow across the link. GNs might not provide networking services and therefore each of the PANUs SHALL perform various tasks to operate without these services, for example Autonet [7]. The GN SHALL forward Ethernet packets appropriately to the connected PANUs.

5. At any time the PANU or the GN MAY terminate the connection(s).

2.5.3 NAP/GN initiates a connection to a PANU

A NAP/GN connects to a PANU to create an ad-hoc network with other Bluetooth devices. This might only be possible if the PANU advertises a PANU service record as specified in section 8.1.3 on page 47. This example provides a brief summary of the typical interactions of a NAP/GN and a PANU.

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

2. If there is no existing Bluetooth connection, then the NAP/GN requests a Bluetooth connection with the selected device with the PANU service. No master-slave switch SHALL be required.

3. Once the connection is made, the NAP/GN can create an L2CAP channel for BNEP. The NAP/GN uses the BNEP control commands to initialize the BNEP connection and the PANU MAY set up filtering of different network packet types. If the NAP/GN supports filtering, it SHALL store all accepted network packet type filters for each connection.

4. Ethernet traffic can now flow across the link. The PANUs SHALL perform various tasks to obtain an IP address and other network services, for example Autonet [7]. The NAP/GN SHALL forward all Ethernet packets to each of the connected PANUs.

5. At any time the PANU or the NAP/GN MAY terminate the connection(s).

2.5.4 PANU initiates a connection to PANU

A PANU connects to a PANU to simulate a cross-over cable network connection. If SDP is used before the connection setup, the target PANU has to advertise a PANU service record as specified in section 8.1.3 on page 47. This example provides a brief summary of the typical interactions of two PANUs.

1. The first step is to find another Bluetooth device that is within radio range and is providing the PANU 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 with the PANU service. No master-slave switch SHALL be required.

3. Once the connection is made, the PANU can create an L2CAP channel for BNEP. The PANU uses the BNEP control commands to initialize the BNEP connection.

4. Ethernet traffic can now flow across the link. Both PANUs SHALL perform various tasks to obtain an IP address and other network services, for example Autonet [7].

2.6 Conformance

A device MAY claim conformance to one or more of the roles of the PAN profile. If conformance to the PAN profile is claimed, all capabilities indicated as mandatory for the applicable role(s) SHALL be supported in the specified manner. Any devices that provide the NAP or GN service, and also any devices which use the NAP or the GN service, SHALL support the mandatory capabilities indicated in this document for that service. This also applies for all optional and conditional capabilities for which support is indicated. All mandatory, optional, and conditional capabilities, for which support is indicated, are subject to qualification as part of the Bluetooth certification program. In addition, passing all PAN profile mandatory tests for each support role is a requirement to claim compliance to the PAN profile.

3 User interface aspects

The PAN profile is built upon the Generic Access Profile [4, part K].

- When reading Generic Access Profile [4, part K], DevA and DevB can be a NAP, GN, or PANU as defined in Table 1 on page 19.

- All the mandatory requirements of the Generic Access Profile [4, part K] are mandatory for the PAN profile.

- Unless otherwise stated below, all the optional requirements of the Generic Access Profile [4, part K] are optional for the PAN profile.

3.1 Authentication & Encryption

It is recognized that the security provided by fixed cables in wired networks has to be replaced by some other security means in the wireless environment. In [2] security mechanisms are specified to provide authentication and encryption in the baseband at the link layer. All devices MAY support Bluetooth security mechanisms. To provide link layer security a method for establishing secure link keys between the communicating devices SHALL be used. In Bluetooth [2] one such method is specified using a shared secret in the form of a PIN.

3.2 Generic Modes

The following modes are defined in Section 4 of the Generic Access Profile [4]. The PAN profile requires the following operational modes.

Modes	**Support in NAP**	**Support in GN**	**Support in PANU**
Discoverability modes			
Non-discoverable mode	O	O	O
Limited discoverable mode	O	O	O
General discoverable mode	M	M	O
Connectability modes			
Non-connectable mode	O	O	O
Connectable mode	M	M	O
Pairing modes			

Non-pairable mode	O	O	O
Pairable mode	C1	C1	C1

Table 2 Generic Mode requirements table

Notes

1. A typical use for the Non-discoverable mode is where the NAP/GN is intended for personal use only. The PANU MAY remember the identity of the NAP/GN and MAY choose not to use the Bluetooth inquiry mechanism.

2. A typical use for the General discoverable mode is where the NAP/GN is intended for public use. The PANU SHALL NOT be expected to remember, and may not have prior knowledge of, the identity of all the NAPs/GNs it uses. The PANU is expected to use the Bluetooth inquiry mechanism to discover the NAPs/GNs in range.

3. Pairable mode MAY be supported, but is not required to be supported or to be used. Device owners MAY be able to configure this setting to improve security.

4. Table 2, describes the operational modes for devices conforming to each of the roles defined by the PAN profile.

C1: If the bonding procedure is supported, support for pairable mode is mandatory, otherwise it is optional.

4 Application layer

Section	Feature	Support in NAP	Support in GN	Support in PANU
4.1	Initialization of NAP/GN service	M	M	X
4.2	Shutdown of NAP/GN service	M	M	X
4.3	Establish NAP/GN service Connection	O	O	M
4.4	Lost NAP/GN Service Connection	O	O	M
4.5	Disconnect NAP/GN Service Connection	M	M	M
4.6	Management Information Base (MIB)	O	O	X

Table 3 Application layer requirements table.

4.1 Initialization of NAP/GN service

This procedure initiates the configuration of the device as a NAP/GN. This operation involves setting the following parameters.

- All the configurable parameters defined in sections 3.2 and 4.6 for example maximum number of users, Discoverable/Non-Discoverable mode, NAP/GN name, etc.
- If required, any Bluetooth PINs and/or link keys.
- The NAP/GN service is initialized – as defined in section 5.1

When initialization is completed, the device SHALL be able to accept NAP/GN service connections.

4.2 Shutdown of NAP/GN service

This procedure stops the device from acting as a NAP/GN.

- The NAP/GN service is shut down – as defined in section 5.6.

4.3 Establish NAP/GN service Connection

This procedure is performed by a PANU connecting to a NAP/GN. The following is an example of the connection establishment steps and is for informative purposes only.

1. The first step is to select a NAP/GN and a suitable NAP/GN service that it provides. This selection MAY be done in one of the following ways.

- The PANU is presented with a list of NAPs/GNs that are within radio range and the services that they provide. The user can then select a NAP/GN service from the list provided.
- The PANU is presented with a list of services that are being provided by the NAPs/GNs that are within radio range. Where the same service is provided by multiple NAPs/GNs (i.e. identical ServiceClass-IDs), the application MAY choose to show the service only once. The user can then select a service from the list provided and in that case the PANU MAY automatically select a suitable NAP/GN that provides the selected service.
- The PANU enters the name of the service that is required, e.g. “network”, or “Meeting #1” (see section 8.1 for more information on service names). The PANU SHALL automatically select a suitable NAP/GN that provides the required service, for example support anonymous network.
- Some application on the PANU automatically searches for and selects a suitable NAP/GN service. The Bluetooth Service Discovery mechanisms are used to retrieve service information.

2. When the PANU has selected a NAP/GN, the PANU SHALL attempt to establish a connection to the selected NAP/GN service using the LM/baseband procedures and service connection procedures in section 5.2 on page 30.

3. Optionally if requested by either the PANU or NAP/GN and supported by both devices, a Bluetooth link key can be established between PANU and NAP/GN. The link key can be supplied directly by the PANU user (human intervention) or the application, or it can be created in the connection setup from a PIN value supplied by the PANU user or an application in both devices. If the link key is derived from PIN using the method specified in [2], a sufficiently long PIN value SHALL be used to provide adequate security especially in public places. Alternatively, a link layer security/access control scheme such as IEEE 802.1x can be used at BNEP level.

The procedure above describes how a PANU seeks out and joins a network. However, this is not the only possible network formation technique. For example, the GN establishing connections to PANUs MAY also form a group ad-hoc network. Automatic network formation is out of the scope of this document.

4.4 Lost NAP/GN Service Connection

When the NAP/GN service connection is lost, the actions taken by the device are dependent on the role of the device. The next sections describe the actions taken by the PANU and NAP/GN when the service connection is lost.

4.4.1 Lost NAP/GN Service Connection for PANU

If the NAP/GN Service connection is lost for any reason, then the PANU device response to the lost connection is dependent on that device. The PANU device MAY try to re-establish the connection to the NAP/GN. The PANU device could remember the previous NAP/GN, service, PIN, link key, username and password and use them to allow speedy or automatic re-establishment of the NAP/GN service connection. The procedures described in section 4.3 SHALL be used. After the PANU device has determined that the connection cannot be re-established or is not to be reestablished then the PANU device notifies the user or application.

4.4.2 Lost NAP/GN Service Connection for NAP/GN

If the NAP/GN Service connection is lost (i.e. the connection becomes disconnected, due to link loss, supervision timeout, etc.) for any reason, then the NAP/GN device actions in response to the connection loss are also dependent on that device. The NAP/GN device MAY hold the resources to allow that device to reconnect or it MAY free those resources and allow other PANU devices to use those resources. The NAP/GN device MAY also try to reconnect the connection.

4.4.3 Lost PANU/PANU connection

If the connection is lost for any reason, the source PANU MAY try to reconnect.

4.5 Disconnect NAP/GN Service Connection

Either the NAP/GN or the PANU MAY terminate the connection at any time using the procedures in section 5.5.

4.6 Management Information Base (MIB)

Devices that support the NAP service MAY have MIBs. If the NAP/GN has multiple Bluetooth radios, then the MIB MAY allow each radio to be separately configured. If the NAP service provides the administrator or user the ability to configure the service, the following features are recommendation for possible parameters to be configurable:

- Maximum number of users. – Determines the number of PANUs that MAY have simultaneous connections to the NAP.
    - 0 = Device is disabled
    - 1 = Single-user mode – a single PANU has exclusive access to a NAP/GN service.
    - >1 = Multi-user mode – multiple PANUs have access to the NAP/GN service.

- Discoverable/Non-Discoverable Modes – determines if the device will be discovered during Inquiry performed by other devices.
- Packet Filter Database– a list of filters used to determine which network packets are filtered out, and are not forwarded to a connected Bluetooth device. Note: Packet Filters are optional.
- Security modes - determines what security procedures are initialized at what point during the connection establishment. See also Section 7
- Configurable parameters of the Service Record.
- Other various networking and device parameters, security parameters, such as access lists and device link keys.

The following optional features MAY be configured if supported:

- Management Information Base (MIB) Objects – allows administrator to manage the NAP. Note: MIBs are optional.

5 NAP/GN/PANU Service

For the NAP/GN/PANU service, the NAP/GN and the PANU exchange data using the Bluetooth Network Encapsulation Protocol [1]. The NAP/GN performs Ethernet Bridge functions to forward Ethernet packets from one PANU to another PANU or from a PANU to another network. The Ethernet Bridge functions required for NAP/GN in role for this profile are a subset of the IEEE 802.1D MAC Bridge standard [3].

The following table together with the associated sub-clauses defines the mandatory requirements with regard to the PAN profile.

Section	Procedure	Support in NAP	Support in GN	Support in PANU
5.1	Initialize NAP, GN, PANU Service	M	M	M
5.2	Establish NAP, GN, and PANU Service Connection	O	O	M
5.3	NAP, GN, and PANU Service Packet Transfer	M	M	M
5.4	NAP/GN Service Packet Forwarding Operation	M	M	X
5.5	Disconnect NAP, GN, or PANU Service Connection	M	M	M
5.6	Shutdown NAP, GN, or PANU Service	M	M	M
5.7	Broadcasts and Multicasts	M	M	N/A

Table 4 NAP/GN/PANU Service

5.1 Initialize NAP, GN, PANU Service

A NAP/GN SHALL register the existence of the NAP/GN Service it provides in its Service Discovery Database. If a PANU wishes to advertise its PANU capabilities it MAY also register a PANU service record in its Service Discovery Database. The service attributes for each of the three records are defined in 8.1.

It is possible for a device to be a NAP and/or a GN and/or a PANU therefore, devices MAY register multiple service records, each one being for a different PAN profile role.

During the initialization of a NAP/GN service the NAP/GN SHALL initialize its Packet Filter Database (PFD) if filtering is supported. To do this a NAP/GN can either create an empty PFD, void of any packet filter definitions, in which case all network packet types and multicast addresses SHALL be forwarded, or it MAY configure some default PFD settings which define the greatest set of packet types and multicast addresses allowed to be forwarded to any devices which connect.

Optionally, to support PAN profile security, the NAP/GN initializes its secure database and stores all necessary security related information, such as information about which authorization mode, encryption mode and security mechanisms to be used, as well as all PANU related security information, such as access rights and secret keys.

5.2 Establish NAP, GN, and PANU Service Connection

The NAP, GN, or PANU MAY obtain the appropriate L2CAP PSM value to use from the service information it discovered earlier, if service discovery is used before connection setup. It then requests the creation of an L2CAP channel with the NAP, GN, or PANU.

Part of the L2CAP channel creation is the negotiation of the Maximum Transmission Unit (MTU) to be used for the BNEP [3]. Both devices SHALL agree to use a MTU of at least the minimum MTU. They MAY negotiate a higher MTU than specified by the minimum MTU for BNEP [3].

There can be only one BNEP connection between two devices, therefore a device SHALL reject an L2CAP connection request for BNEP if a BNEP connection exists between those Bluetooth devices.

PANU MAY optionally setup filters for network protocol types and multicast addresses after the BNEP channel is established.

If NAP/GN operates in PAN Profile Authorization Mode 2, see section 7.2.1, on page 40, it authenticates the PANU. In Mode 3 it authenticates the PANU and verifies the access right of the PANU.

5.3 NAP, GN, and PANU Service Packet Transfer

Each Ethernet packet is transmitted as a single L2CAP packet. Ethernet packets are transmitted as the L2CAP payload between Bluetooth devices using the Bluetooth Network Encapsulation Protocol [1].

If NAP/GN operates in PAN Profile Secrecy Mode 2, see section 7.2.2 on 41, then the packets are encrypted. The encryption can be at Ethernet encapsulation level or at Baseband level, where entire Bluetooth payloads are encrypted using the encryption method defined in [2].

5.4 NAP/GN Service Packet Forwarding Operation

The Bluetooth Network Encapsulation Protocol is used to exchange data between the NAP/GN and each PANU. The operation of a NAP/GN executing the NAP/GN

service follows a small subset of the IEEE 802.1D standard [3]. In summary, the NAP/GN SHALL perform the following.

- Regard each established Bluetooth Network Encapsulation Protocol (BNEP) connection as a valid Bridge Port. Thereby the NAP/GN SHALL perform bridging between all of the BNEP connections.
- Regard the optional physical Ethernet port as a valid Bridge Port. (Note: This only applies to the NAP, if the NAP is acting as a bridge and not as a router.)
- Forward and filter Ethernet frames as described in [3] section 7.1 and specified in [3] sections 7.5, 7.6, and 7.7 for support of Basic Filtering Services.
- Automatically learn and maintain the information required to make frame-filtering decisions as described in [3] section 7.1 and specified in [3] sections 7.8 and 7.9, for the support of Basic Filtering Services.[3]

The NAP/GN is not required to perform any of the following aspects of the 802.1D standard.[4]

- Static configuration of the PFD
- Permanent entries in the PFD
- Bridge Management.
- Spanning Tree Protocol.
- Group Multicast Filtering and GARP.
- Traffic classification and user priority processing.
- Processing of 802.1Q tags.

In addition a NAP/GN could implement additional filters and other techniques to reduce wasted bandwidth over the BNEP connection, provided that these optimizations do not cause adverse effects to the connected Bluetooth enabled devices or other devices on the network. For example, a NAP/GN MAY strip padding from received packets before forwarding them. A PANU, which supports being present in more than one piconet on a timesharing basis, is outside the scope of this profile. However, this topology is to be addressed in a future PAN profile.

A PANU connected to a NAP/GN could be operating in low-power mode. It is left to manufacturers to develop suitable means for providing efficient support for these low-power modes, such as buffering packets until the next park beacon for nodes in park mode.

PANUs SHALL NOT forward packets.

[3] Notice that the addresses for devices that are not connected directly to the local device are learned from the contents of the Ethernet header, not from the Bluetooth address associated with the L2CAP connections.
[4] Sophisticated Bluetooth NAP devices may choose to implement some or all of the 802.1D features.

5.5 Disconnect NAP, GN, or PANU Service Connection

The following reasons SHALL cause the connection to be terminated.

1. User intervention (i.e. the user or an application determines that the connection SHALL be disconnected).

2. Failure of the Bluetooth Network Encapsulation Protocol [1] connection. The Bluetooth Network Encapsulation Protocol [1] connection may fail for several reasons. For example, when the radio link has failed or the device has been out of range of an excessive amount of time, see [2, part D].

3. Termination by the NAP, GN, or PANU if the device can no longer provide the appropriate service. The reasons that can cause this are very dependent on the implementation of the NAP, GN, or PANU, but they could include (a) loss of connection to the external network, or (b) loss of the NAP, GN, or PANU service.

4. Security failure. This may be caused by a failure in the authentication procedure, or a change of security level that is not accepted or supported by the other device.

5. Some implementation specific policy decision made by an application that is running on the NAP/GN or the PANU.

The NAP, GN, or PANU service handles each of the above situations in the same way. In all cases the L2CAP channel is terminated – as defined in [2, part D].

5.6 Shutdown NAP, GN, or PANU Service

A NAP, GN, or PANU MAY stop advertising an active NAP, GN, or PANU service and all existing connections to the NAP, GN, or PANU service SHALL be terminated.

5.7 Broadcasts and Multicasts

The 802.1D standard states that Ethernet broadcast and multicast frames SHALL be transmitted to all operational bridge ports. This means that a NAP/GN SHALL transmit the frame separately to each connected PANU. It is recognized that this is wasteful of the piconet's bandwidth when there is more than one PANU. It is left to the product manufacturers to develop suitable means for reducing the amount of un-necessary traffic sent to each PANU. A PANU connected to a NAP/GN could be operating in low-power mode. It is left to manufacturers to develop suitable means for providing efficient support for broadcast and multicast packets destined

to these PANUs. An example of such support MAY be a proxy reply on behalf of a PANU by a NAP/GN to control broadcast information such as ARP requests.

6 Internet Protocol (IP) Support

Support for the Internet Protocol (IP) is the major focus on the PAN profile. This protocol is defined and maintained by the Internet Engineering Task Force (IETF). IP is described by a set of RFC documents defining its usage. This section specifies the required RFCs, address assignment, and name resolution techniques required to enable IP over Bluetooth wireless communications. All of the RFCs are available from http://www.ietf.org/rfc.html.

6.1 Required RFC

The mandatory set of IETF RFCs required for communication is listed in the following tables. Inclusion of additional IETF RFCs are optional in the PAN profile scenario.

6.1.1 IPv4

RFC Number(s)	Description
0791	Internet Protocol
0792	Internet Control Message Protocol
0826	An Ethernet Address Resolution Protocol
0894	A Standard for the Transmission of IP Datagrams over Ethernet Networks
0919	Broadcasting Internet Datagrams
0922	Broadcasting Internet Datagrams In The Presence Of Subnets
0950	Internet Standard Subnetting Procedure
1112	Host Extensions for IP Multicasting
1122	Requirements for Internet Hosts -- Communication Layers
1123	Requirements for Internet Hosts -- Application and Support

Table 5 Required IPv4 RFCs

6.1.2 IPv6

RFC Number(s)	Description
1981	Path MTU Discovery for IP version 6
2373	IP Version 6 Addressing

	Architecture
2374	An IPv6 Aggregatable Global Unicast Address Format
2460	Internet Protocol, Version 6 (IPv6) Specification
2461	Neighbor Discovery for IP Version 6 (IPv6)
2462	IPv6 Stateless Address Autoconfiguration
2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
2464	Transmission of IPv6 Packets over Ethernet Networks
2526	Reserved IPv6 Subnet Anycast Addresses

Table 6 Required IPv6 RFCs

6.2 Recommended RFCs

The set of IETF RFCs listed in the following tables are recommended for communication, in particular for communication across subnet boundaries.

6.2.1 IPv4

RFC Number(s)	Description
1034	Domain Names - Concepts And Facilities
1035	Domain Names - Implementation And Specification
1256	ICMP Router Discovery Messages
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions

Table 7 Recommended IPv4 RFCs

It is recognized that some devices do not make use of name-to-address resolution and the Domain Name System themselves. Examples of such devices are devices that do not provide any user network applications, or devices that only support applications that invoke remote name-to-address resolution (e.g. a WAP client). Such devices MAY choose not to implement any of the name-to-address resolution functionality as described in RFC 1034 and RFC 1035

It is also recognized that some devices MAY, for various reasons, only communicate with devices on the same IP subnet. For example, a device which serves the printer in a home network (also described in [7]). Such devices MAY choose not to implement the functionality for stateful address auto-configuration as described in RFC 2131 and RFC 2132, and/or active discovery of networking infrastructure as described in RFC 1256. Such a device SHALL NOT configure a default router.

6.2.2 IPv6

RFC Number(s)	Description
1034	Domain Names - Concepts And Facilities
1035	Domain Names - Implementation And Specification
1886	DNS Extensions to support IP version 6

Table 8 Recommended IPv6 RFCs

It is recognized that some devices do not make use of name-to-address resolution and the Domain Name System themselves. Examples of such devices are devices that do not provide any user network applications, or devices that only support applications that invoke remote name-to-address resolution (e.g. a WAP client). Such devices MAY choose not to implement any of the name-to-address resolution functionality as described in RFC 1034, RFC 1035 and RFC 1886.

6.3 Address Assignment

The IP address length, as well as the technique used by a node to obtain an IP address is dependent on the version of IP the node is executing. The following sections specify this process for IPv4 and IPv6.

6.3.1 IPv4

For IPv4 Address assignment, Bluetooth PAN Profile devices SHALL comply with the Dynamic Configuration of IPv4 link-local addresses [7]. This draft SHALL be used until Dynamic Configuration of IPv4 link-local addresses becomes a standard draft RFC, at which time all devices supporting the Bluetooth PAN profile SHALL comply with that RFC.

6.3.2 IPv6

IPv6 supports the ability to perform address assignment as defined in RFC 2462 IPv6 Auto-Configuration.

6.4 Name Resolution

For Name Resolution, Bluetooth PAN profile devices SHALL comply with the Linklocal Multicast Name Resolution (LLMNR) [9]. This draft will be used until Linklocal Mulicast Name Resoultion (LLMNR) becomes a standard draft RFC, at which time all devices supporting the Bluetooth PAN profile SHALL comply with that RFC.

7 Security

The Bluetooth specifications [2] provide a set of security features that enable Bluetooth equipped devices to authenticate other Bluetooth equipped devices upon connection to a particular device or service, as well as protect transmitted data using encryption. This section of the profile contains optional security mechanisms for the Bluetooth PAN profile and the Bluetooth PAN profile does not require any security modes. Even though these options are not tested in the PAN profile test cases, it is strongly recommend that the recommended security mechanisms be used. The two mechanisms for this, authentication and encryption, operate at Baseband level. Authentication relies on a link key, from which the encryption key is derived. The link key between two Bluetooth equipped devices can be based on supply of a PIN in both devices. Alternatively, it can be provided directly by an application. On top of the Bluetooth Baseband security mechanisms, other security mechanisms MAY be applied, such as provided by 802.1x, IPSEC, TLS/WTLS, application level security, etc.

7.1 Bluetooth security modes

As the PAN profile is dependent on the Generic Access Profile [4, part K], the specifications concerning security from the Generic Access Profile (GAP) are also relevant for the PAN profile. GAP specifies three security modes, here identified as the ***Bluetooth Security Modes*:**

1 **Non-secure:** a device SHALL NOT initiate any security procedure.

2 **Service-level enforced security:** a device does not initiate security procedures before channel establishment at L2CAP level.

3 **Link-level enforced security:** a device initiates security procedures before the link set-up at LMP level is completed.

The operation of devices relating to these security modes within the PAN profile is described below in more detail.

7.1.1 Security mode 1: non-secure

When a Bluetooth device is operating in security mode 1 it SHALL NOT initiate any security procedure (i.e., it SHALL NOT send LMP_au_rand, LMP_in_rand or LMP_encryption_mode_req). Security mode 1 can be considered as a special case of security mode 2 where no service demands any security.

For a NAP/GN this means that the NAP/GN service is accessible to all devices, no Bluetooth security procedures are initiated by the NAP/GN/PANU device. This does not prevent a NAP/GN to enforce higher layer security mechanisms.

7.1.2 Security mode 2: service-level enforced security

When a Bluetooth device is in security mode 2 it SHALL NOT initiate any security procedure before a channel establishment request (L2CAP_ConnectReq) has been received or a channel establishment procedure has been initiated by itself. The behavior of a Bluetooth device in security mode 2 is further described in [10]. Whether a security procedure is initiated or not depends on the security requirements of the requested channel or service.

For the PAN profile, this security mode is expanded to the more general PAN profile service-level enforced security mode where the security procedures (Bluetooth Baseband security and/or higher layer security) are initiated upon accessing a PAN profile service through NAP or GN . This security mode is further described in Section 7.2.

7.1.3 Security mode 3: link-level enforced security

When a Bluetooth device is in security mode 3 it SHALL initiate security procedures before it sends LMP_ setup_complete. The behavior of a Bluetooth device in security mode 3 is as described in [2, part C].

A NAP/GN operating in this mode can either request authentication only or both authentication and encryption. On top of Bluetooth security, higher layer security mechanisms MAY be applied.

7.2 NAP/GN service-level security

The NAP/GN operates in one of the Bluetooth security modes (see Section 7.1). Within the PAN profile, Bluetooth security mode 2 (service-level enforced security) is expanded to the PAN profile service-level enforced security mode, including both Bluetooth and higher layer (802.1x, IPSEC) security mechanisms. This mode is composed of the PAN Profile Authorization Modes and the PAN Profile Secrecy Modes, both further described below.

PAN Profile service-level enforced security mode can use security mechanisms at Bluetooth Baseband level, at a higher link level (IEEE 802.1x) or at another layer (IPSEC).

For example, assume that a NAP/GN is configured in PAN profile service-level enforced security mode and has established a Baseband connection with a PANU. Assume now that the PANU wants to connect to the NAP/GN service, i.e., it sends

an L2CAP_ConnectReq for a BNEP channel. Then the NAP/GN SHALL initiate connection security according to the Bluetooth security procedures. Higher layer security is initiated after the establishment of an L2CAP channel for BNEP. Security mechanisms at different levels can be applied at the same time.

Additionally, security of services accessed through a NAP/GN MAY be supported in the PAN profile service-level enforced security mode by initiating Bluetooth and/or higher layer security procedures upon connection to the particular service. This is outside of the scope of the PAN profile.

7.2.1 PAN Profile Authorization Modes

The PAN Profile Authorization modes specify the level of authorization required to get access to a PAN. The PAN Profile Authorization Mode is set by the NAP/GN, and indicated in the respective Service Record. Authentication and authorization mechanisms are invoked by the NAP/GN upon the reception of an L2CAP_ConnectReq for a BNEP channel. The NAP/GN operates in one of the following three modes:

1. **Open PAN** meaning that no authorization and authentication is required for joining a PAN.

2. **Authentication required** by the NAP/GN before the PANU is registered as a member of the group ad-hoc network PAN. If Bluetooth authentication is used, an L2CAP_ConnectRsp with result Connection pending and status Authentication pending is returned. Also BNEP (802.1x) or IP layer authentication can be used.

3. **Authorization and authentication required** before the connection establishment with the PAN is completed. This can be done at Bluetooth level, or at Ethernet (802.1x) or IP level. At Bluetooth level, authorization of the establishment of a new L2CAP channel is performed by the NAP/GN[5][6]. An L2CAP_ConnectRsp with result Connection pending and status Authorization pending is returned. At BNEP or IP level, authentication and authorization of that level is used. This is initiated after an L2CAP channel for BNEP is established.

If a PANU fails to comply with a request for authentication, or if a PANU is not authorized by the NAP/GN, its L2CAP channel for BNEP SHALL be terminated by the NAP/GN. In case Bluetooth authentication is used, an L2CAP message with result Connection refused – security block is used. If a PANU is successfully

[5] An example procedure of authorization by a NAP/GN is to consult a Device Database as defined in [10].

[6] Optionally, a NAP/GN could export the authorization functionality to another node with special access rights, in the same way as with configurable settings of a NAP/GN.

authenticated at Bluetooth level and it is authorized by the NAP/GN to join the PAN, an L2CAP message with result Connection successful is returned.

7.2.2 PAN Profile Secrecy Modes

The PAN Profile Secrecy Modes specify the level of protection of traffic within the PAN. The level of secrecy for a PAN is set by the NAP/GN. The PAN operates in one of the following two modes:

1 **Clear mode** meaning that no encryption is applied.

2 **Encrypted mode** meaning that encryption is enforced on all communication within the PAN. This can be either at Baseband level or at BNEP/IP level. If Baseband encryption is enforced, it SHALL be preceded by Baseband authentication. Then the Profile authorization mode SHALL be either mode 2 or 3 enforcing Baseband authentication.

If a PANU fails to comply with a request for encryption, its connection with the PAN SHALL be terminated at L2CAP level by the NAP/GN. In case Bluetooth encryption is used, an L2CAP message with result Connection refused – security block is used. If encryption is enforced at Bluetooth level, and an encryption key is successfully derived, an L2CAP message with result Connection successful is returned.

At any point, the NAP/GN MAY decide to change the level of security to a more secure mode, i.e., from clear mode to encrypted mode. A PANU that fails to comply with the change of mode SHALL be excluded from the PAN.

7.3 PANU security modes

A PANU also operates in one of the Bluetooth security modes as defined in Section 7.1 above. Any PANU participating in a Bluetooth PAN MAY demand a certain level of security and subsequently reject a lower level of security if these demands are not met. This results in termination of the communication channel at the relevant level, i.e., relevant to the applied security mechanism. E.g. if the request for Bluetooth authentication is not met and the PANU is configured in security mode 3, the PANU SHALL terminate the Bluetooth connection with the NAP/GN or the other PANU. Similarly, if 802.1x authentication fails, the L2CAP channel for BNEP SHALL be terminated.

When the NAP/GN initiates connection establishment with the PANU, the procedures specified above for NAP/GN also apply for this case, with the roles of NAP/GN and PANU reversed. Security mode 2 (service-level security) applies when the PANU has configured specific security requirements for the L2CAP channel for BNEP (in this case the NAP/GN connects to the "PANU service"). If the PANU operates in Bluetooth security mode 2 or 3, the PANU SHALL realize that

the security procedures are only applied between that particular PANU and the NAP/GN, and that security might not be applied to other connections. An example of this situation is if the PANU and NAP are configured to always encrypt Baseband traffic between each other.

7.4 BNEP and higher layer security

Bluetooth Baseband security can be used to provide security at link layer where it operates. Similar to other link layer communication protocols, such as IEEE 802.1x, it does not provide end-to-end security.

Security mechanisms at levels above the Bluetooth communication layers, such as VPN, IPSEC, TLS/WTLS, application level security, etc, can be used to provide adequate level of security for the specific PAN network. These additional security mechanisms are optional and are not required for the PAN profile. The usage of mechanisms generally applicable to PAN profile (802.1x, IPSEC) is outlined for service-level enforced security in Section 7.2.

For the PAN profile, the security mechanisms provide protection of the participants in a PAN against unauthorized participants and eavesdropping of link layer Bluetooth communication. However, the security mechanisms do not protect the participants of malicious behaviour of other participants in the same PAN, nor from malicious behaviour through an external connected network. If desired, security mechanisms to protect communication of an individual participant of a PAN MAY be applied to protect against such attacks. Examples of such mechanisms are IPSEC, TLS/WTLS, and application level security.

Further, at levels above PAN profile specific protocol layers appropriate security mechanisms MAY be applied. Examples of such mechanisms are IPSEC, TLS/WTLS, application level security, etc.

8 Service Discovery

A device supporting the PAN profile could be capable of providing each of the PAN profile services. For example, a device could support the NAP, GN and PANU service. If multiple services are advertised by a device, the PAN profile user or an application SHALL be able to choose which of the PAN profile services it intends to use.

8.1 SDP service records

Each PAN profile capable device support either the NAP, GN, or both roles SHALL provide one or more Service Class for its PAN profile services. A device MAY contain one instance of each of these Service Classes, e.g. one NAP, one GN, and one PANU service. The service selection is based on service attributes. These services are made public via the SDP.

8.1.1 NAP service records

The NAP service record SHALL have the following attributes. The syntax and usage of these attributes is defined in [2, part E].

Item	Definition	M/O	Type/Size	Value	Default Value
ServiceRecordHandle		M			
ServiceClassIDList		M			
ServiceClass0	UUID for NAP	M	UUID	See [5]	See [5]
ProtocolDescriptorList		M			
Protocol0	UUID for L2CAP	M	UUID	See [5]	See [5]
SpecificParameter0	PSM	M	UInt16	See [5]	See [5]
Protocol1	UUID for BNEP	M	UUID	See [5]	See [5]
SpecificParameter0	Version	M	UInt16	0x0100	0x0100
SpecificParameter1	Supported Network Packet Type List	M	Data Element Sequence of Uint16	See [6] for Network Packet Type values	
LanguageBaseAttributeIDList	Language used for the Stings in the Record	M	Data Element Sequence	See [2]	See [2]
Service Availability	Load Factor	O	Uint8	As defined in SDP section of [1]	Dynamic
BluetoothProfileDescriptorList		M			
Profile#0	UUID for NAP	M	UUID	See [5]	See [5]
Parameter#0	Version “1.00”	M	Uint16	0x0100	0x0100
Service Name	Displayable Name	M	String	Configurable	“Network Access Point Service”
Service Description	Displayable	M	String	Configurable	“Personal Ad-hoc

	Name				Network Service which provides access to a network"
Security Description	Security Information	M	Uint16	0x0000 = None 0x0001 = Service - level enforced Security 0x0002 = 802.1x Security	0x0000
NetAccessType	Type of Network Access Available	M	Uint16	0x0000 = PSTN 0x0001 = ISDN 0x0002 = DSL 0x0003 = Cable Modem 0x0004 = 10Mb Ethernet 0x0005= 100Mb Ethernet 0x0006 = 4 Mb Token Ring 0x0007 = 16 Mb Token Ring 0x0008 = 100 Mb Token Ring 0x0009 = FDDI 0x000A = GSM 0x000B = CDMA 0x000C = GPRS 0x000D = 3G Cellular 0xFFFE = other	Values for the type of Network access supported by this device
MaxNetAccessRate	Maximum possible Network Access Data Rate	M	Uint32	Based on NetAccessType Speed	
IPv4Subnet	Displayable only in format described below	O	String	Configurable	Configurable
IPv6Subnet	Displayable only in format described below	O	String	Configurable	Configurable

The actual values of universal attribute IDs that SHALL be used are defined in the Assigned Numbers specification [5].

- The SpecificParameter1 for BNEP is a data element sequence of Unit16 identifying the list of supported network packet types. This list is used to identify the various networking protocols are supported by the device, which is advertising the service. The supported network packet types SHALL be ordered in ascending order.

- The ServiceName attribute is a short friendly name for the service, e.g. “Corporate Network”, “Conference#1”, etc.

- The ServiceDescription attribute is a longer description for the service. For example. “This network is provided for our guests. It provides free Internet Access and printing services. No username or password is required.“

- The ServiceAvailability attribute MAY be used in conjunction with the LoadFactor field of the CoD defined for NAP – see Assigned Number Specification [5].

- The MaxNetAccessRate attribute is used to advertise the data rate of the connection the NAP has to the network which it is providing access. The attribute is measure in octets per second.

- IP4vSubnet and IPv6Subnet attributeID is a displayable string containing subnet definition of the network, e.g. “10.0.0.0/8” for IPv4 and “fe80::/48” for IPv6. For IPv4 the first 4 numbers define the IP subnet in dotted-decimal notation. The fifth number, after the “/” character, is the number of subnet bits to use in the subnet mask; e.g. 8 means a subnet mask of 255.0.0.0. IPv6 subnet strings SHALL use IPv6 address notation as specified by the IETF. These strings are given in the standard IETF format with the absolute attribute IDs, and thus without multilingual support.

8.1.2 GN service records

The GN service record SHALL have the following attributes. The syntax and usage of these attributes is defined in [2, part E].

Item	Definition	M/O	Type/Size	Value	Default Value
ServiceRecordHandle		M			
ServiceClassIDList		M			
ServiceClass0	UUID for GN	M	UUID	See [5]	See [5]
ProtocolDescriptorList		M			
Protocol0	UUID for L2CAP	M	UUID	See [5]	See [5]
SpecificParameter0	PSM	M	UInt16	See [5]	See [5]
Protocol1	UUID for BNEP	M	UUID	See [5]	See [5]
SpecificParameter0	Version	M	UInt16	0x0100	0x0100
SpecificParameter1	Supported Network Packet Type List	M	Data Element Sequence of Uint16	See [6] for Network Packet Type values	
LanguageBaseAttributeIDList	Language used for the Stings in the Record	M	Data Element Sequence	See [2]	See [2]
Service Availability	Load Factor	O	Uint8	As defined in SDP section of [1]	Dynamic

BluetoothProfileDescriptorList		M.			
Profile#0	UUID for GN	M	UUID	See [5]	See [5]
Parameter#0	Version "1.00"	M	Uint16	0x0100	0x0100
Service Name	Displayable Name	M	String	Configurable	"Group Ad-hoc Network Service"
Service Description	Displayable Name	M	String	Configurable	"Personal Group Ad-hoc Network Service"
Security Description	Security Information	M	Uint16	0x0000 = None 0x0001 = Service - level enforced Security 0x0002 = 802.1x Security	0x0000
IPv4Subnet	Displayable only in format described below	O	String	Configurable	Configurable
IPv6Subnet	Displayable only in format described below	O	String	Configurable	Configurable

The actual values of universal attribute IDs that SHALL be used are defined in the Assigned Numbers specification [5].

- The SpecificParameter1 for BNEP is a data element sequence of Unit16 identifying the list of supported network packet types. This list is used to identify the various networking protocols are supported by the device, which is advertising the service. The supported network packet types SHALL be ordered in ascending order.

- The ServiceName attribute is a short friendly name for the service, e.g. "Corporate Network", "Conference#1", etc.

- The ServiceDescription attribute is a longer description for the service. For example. "This network is provided for our visitors of this meeting room. It provides projector display and printing services. No username or password is required."

- The ServiceAvailability attribute MAY be used in conjunction with the LoadFactor field of the CoD defined for NAP – see Assigned Numbers Specification [5]

- IPv4Subnet and IPv6Subnet attributeID is a displayable string containing subnet definition of the network, e.g. "10.0.0.0/8" for IPv4 and "fe80::/48" for IPv6. For IPv4, the first 4 numbers define the IP subnet in dotted-decimal notation. The fifth number, after the "/" character, is the number of subnet bits to

use in the subnet mask; e.g. 8 means a subnet mask of 255.0.0.0. IPv6 subnet strings SHALL use IPv6 address notation as specified by the IETF. These strings are given in the standard IETF format with the absolute attribute IDs, and thus without multilingual support.

8.1.3 PANU service records

The PANU MAY advertise a service record but is not required to do so. If a device does not advertise a PANU service record, then the device might not be able to support other NAP, GN or other PANU devices initiating the connection if SDP is used to identify the available services. This may prevent support of "PUSH" usage models from a network access point and may prevent these devices to participate in automatic network formation, which is to be defined in the future. If supported, the PANU service record SHALL have the following attributes. The syntax and usage of these attributes is defined in [2, part E].

Item	Definition	M/O	Type/Size	Value	Default Value
ServiceRecordHandle		M			
ServiceClassIDList		M			
ServiceClass0	UUID for PANU	M	UUID	See [5]	See [5]
ProtocolDescriptorList		M			
Protocol0	UUID for L2CAP	M	UUID	See [5]	See [5]
SpecificParameter0	PSM	M	UInt16	See [5]	See [5]
Protocol1	UUID for BNEP	M	UUID	See [5]	See [5]
SpecificParameter0	Version	M	UInt16	0x0100	0x0100
SpecificParameter1	Supported Network Packet Type List	M	Data Element Sequence of Uint16	See [6] for Network Packet Type values	
LanguageBaseAttributeIDList	Language used for the Stings in the Record	M	Data Element Sequence	See [2]	See [2]
Service Availability	Load Factor	O	Uint8	As defined in SDP section of [1]	Dynamic
BluetoothProfileDescriptorList		M.			
Profile#0	UUID for PANU	M	UUID	See [5]	See [5]
Parameter#0	Version "1.00"	M	Uint16	0x0100	0x0100
Service Name	Displayable Name	M	String	Configurable	"Personal Ad-hoc User Service"
Service Description	Displayable Name	M	String	Configurable	"Personal Ad-hoc User Service"
Security Description	Security Information	M	Uint16	0x0000 = None 0x0001 = Service - level enforced Security 0x0002 = 802.1x Security	0x0000

The actual values of universal attribute IDs that SHALL be used are defined in the Assigned Numbers specification [5].

- The SpecificParameter1 for BNEP is a data element sequence of Unit16 identifying the list of supported network packet types. This list is used to identify the various networking protocols are supported by the device, which is advertising the service. The supported network packet types SHALL be ordered in ascending order.

- The ServiceName attribute is a short friendly name for the service, e.g. “Corporate Network”, “Conference#1”, etc.

- The ServiceDescription attribute is a longer description for the service. For example. “This is a PANU service.“

- The ServiceAvailability attribute MAY be used in conjunction with the LoadFactor field of the CoD defined for NAP – see Assigned Numbers Specification [5].

9 L2CAP Interoperability Requirements

The following text together with the associated subclauses defines the mandatory requirements with regard to the PAN profile.

	Procedure	Support in NAP/GN	Support in PANU
1.	**Channel types**		
	Connection-oriented channel	M	M
	Connectionless channel	X1	X1
2.	**Signaling**		
	Connection Establishment	M	M
	Configuration	M	M
	Connection Termination	M	M
	Echo	M	M
	Command Rejection	M	M
	Information	O	O
3.	**Configuration Parameter Options**		
	Maximum Transmission Unit	M	M
	Flush Timeout	O	O
	Quality of Service	O	O

Table 9 L2CAP procedures

X1: Connectionless channel is not used within the execution of the PAN profile, but concurrent use by other profiles/applications is not excluded.

9.1 Channel types

In the PAN profile, only connection-oriented channels SHALL be used.

In the PSM field of the Connection Request packet, the value defined for BNEP in the Assigned Numbers specification [5] SHALL be used.

9.2 Signaling

Typically, the PANU MAY issue an L2CAP Connection Request within the execution of the PAN profile. However, there MAY be situations when the NAP/GN makes the connection request. One example is an error recovery situation where the NAP/GN temporarily malfunctions and attempts to restore the NAP/GN after it is operational.

9.3 Configuration options

This section describes the usage of configuration options in the PAN profile.

9.3.1 Maximum Transmission unit

The PAN profile requires a minimum MTU as required by the BNEP specification [1]

9.3.2 Flush Time-out

Bluetooth networking encapsulation protocol is recommended to be used over a reliable L2CAP channel. For some networking protocols, such as many real-time protocols, guaranteed delivery is undesirable. The flush time-out value SHALL be set to its default value 0xffff for a reliable L2CAP channel, and MAY be set to other values if guaranteed delivery is not desired.

9.3.3 Quality of Service

Negotiation of Quality of Service is optional in the PAN profile.

9.4 Broadcast

L2CAP connectionless broadcasts are not used in the PAN profile.

10 Link Manager (LM) Interoperability Requirements

10.1 Capability overview

In addition to the requirements on supported procedures stated in the Link Manager specification itself (see Section 3 in the Link Manager Protocol), the PAN profile also supports the following features.

Procedure	Support in NAP/GN	Support in PANU
Authentication	O	O
Pairing	C1	C1
Encryption	O	O
Request master/slave switch	C2	X
Perform master/slave switch	C3	C3

Table 10 LMP Procedures

1. Authentication may be required by the NAP/GN or PANU to complete a connection.
2. Encryption may be required by the NAP/GN or PANU to complete a connection.

C1: Pairing SHALL be supported if the bonding procedure is supported.
C2: The master/slave switch is mandatory if the NAP/GN supports multi-user mode.
C3: The PANU SHALL support the master/slave switch if it wishes to connect to a NAP/GN that is in multi-user mode.

- For bandwidth reasons, it is advisable but not mandatory for both devices to use multi-slot packets.

- During baseband connection establishment, if either the PANU or the NAP/GN is operating in security mode 3 (see Section 7.1 above), it SHALL initiate the Bluetooth security procedures. If this is not supported then the device SHALL terminate the Baseband connection. Optionally, a one byte length PIN containing all zeros MAY be used.

- When the NAP/GN is configured in single-user mode (i.e. maximum number of users is 1), then the NAP/GN MAY be either the master or the slave of the piconet.

- When the NAP/GN is configured in multi-user mode (i.e. maximum number of users is more than 1), then the NAP/GN SHALL become the master of the piconet.

10.2 Unexpected Behavior

If a unit tries to use a mandatory feature, and the other unit replies that it is not supported, then the NAP/GN service SHALL be denied.

A unit SHALL always be able to handle the rejection of the request for an optional feature.

10.3 Profile Errors

A node SHALL deny access to the service, if the other side fails to comply with the mandatory requirements for its role. The following are additional conditions where a device SHALL deny access to the PAN profile service, using the appropriate error codes for the failure; see [2, part C], section 5.1.2 for the appropriate LMP rejection reasons:

- Failure to complete the pairing process, if pairing is required.
- Failure to complete the authentication process, if authentication is required.
- Failure to comply with a request to enable encryption on the baseband connection, if encryption is required and supported.
- Failure by the PANU to comply with a request to perform a master/slave switch when the NAP/GN is in multi-user mode, thereby changing the PANU from master to slave. The NAP/GN SHALL request a master/slave switch when it is configured in multi-user mode. It is therefore recommended that PANUs always be prepared to accept a master/slave switch requested by a NAP/GN.
- Failure by the PANU to support Hold, Sniff, or Park when request by the NAP/GN MAY result in a termination of the connection. .

The NAP/GN SHALL reject all attempts by the PANU to perform the following operations. If the NAP/GN is connecting to the PANU then the responses to errors are the same for the conditions; see [2, part C], section 5.1.2 for the appropriate LMP rejection reasons.

1. The connection SHALL be rejected by the NAP/GN if the PANU is requesting that the NAP/GN SHALL switch to be a slave when the NAP/GN is configured to be in multi-user mode. The error code “LMP PDU not allowed” is used.

2. The connection SHALL be rejected by the NAP/GN if the PANU is requesting that a new connection be made when the NAP/GN already has its configured maximum number of users. The error code “Other End Terminated Connection: Low Resources” is used.

3. The connection SHALL be rejected by the NAP/GN if the NAP/GN device is configured in security mode 2 or 3 (see Section 7.1 above), and encryption is applied on the Baseband connection, a request to disable Baseband encryption. The error code "Encryption mode not acceptable" is used.

11 Link Control (LC) Interoperability Requirements

11.1 Capability overview

The following table lists all capabilities on the LC level.

	Capabilities	Support in NAP	Support in GN	Support in PANU
	Inquiry using GIAC	O	O	O
	Inquiry scan using GIAC	M	M	O
	Paging	O	O	M
	Page scan	M	M	O
	Type R0	M	M	O
	Type R1	M	M	O
	Type R2	M	M	O
	Master/Slave Role Switch	C2	C2	C3
	Hold Mode	O	O	C1
	Sniff Mode	O	O	C1
	Park	O	O	C1
	Packet types	M	M	M
	ID packet	M	M	M
	NULL packet	M	M	M
	POLL packet	M	M	M
	FHS packet	M	M	M
	DM1 packet	M	M	M
	DH1 packet	O	O	O
	DM3 packet	O	O	O
	DH3 packet	O	O	O
	DM5 packet	O	O	O
	DH5 packet	O	O	O
	AUX packet	X1	X1	X1

	Capabilities	Support in NAP	Support in GN	Support in PANU
	HV1 packet	X1	X1	X1
	HV2 packet	X1	X1	X1
	HV3 packet	X1	X1	X1
	DV packet	X1	X1	X1
	Inter-piconet capabilities	X1	X1	X1
	Voice codec	X1	X1	X1
	A-law	X1	X1	X1
	μ-law	X1	X1	X1
	CVSD	X1	X1	X1

Table 11 Baseband/LC capabilities

C1: Failure by the PANU to support Hold, Sniff, or Park when request by the NAP/GN MAY result in a termination of the connection.

C2: A NAP or a GN SHALL support Master/Slave role switch if it supports multiple users.

C3: A PANU SHALL support Master/Slave role switch if it wishes to connect to a NAP/GN which supports multiple users.

X1: These capabilities are not used within the execution of the PAN profile, but concurrent use by other profiles/applications is not excluded.

11.2 Inquiry

When inquiry is invoked in NAP/GN or PANU, it SHALL use the General Inquiry, see GAP [4], Section 6.1. NAP/GN or PANU MAY inquire within the execution of the PAN profile.

11.3 Inquiry scan

For inquiry scan, (at least) the GIAC SHALL be used, according to one of the discoverable modes defines in GAP [4], Section 4.1.2 and Section 4.1.3.

11.4 Paging

Depending on the paging class indicated by a device, the other device SHALL page accordingly. NAP/GN or PANU MAY page within the execution of the PAN

profile. The paging step SHALL be skipped in the PANU or NAP/GN when execution of the PAN profile begins when there already is a baseband connection between the PANU and the NAP/GN.

11.5 Unexpected behavior

Since most features on the LC level have to be activated by LMP procedures, errors MAY be caught at that layer. However, there are some LC procedures that are independent of the LMP layer, e.g. inquiry or paging. Misuse of such features is difficult or sometimes impossible to detect. There is no mechanism defined to detect or prevent such improper use.

11.6 Class of Device

Devices that support the PAN profile SHALL set the Networking bit in the service class field on the CoD.

12 Management Entity Procedures

The following table list all capabilities required by the Management Entity.

Section	Procedure	Support in NAP/GN	Support in PANU
12.1	Link Establishment	M	M
12.2	Single/Multi-user mode	M	N/A
12.3	Encryption	O	O

Table 12 Management Entity Procedures

12.1 Link Establishment

The Management Entity controls initialization of the connection with NAP/GN service.

The initialization procedure is started as a direct consequence of the user operations described in section 4.3 above.

Initialization is required for communication between a NAP/GN/PANU and a PANU. Before having been initialized, a NAP/GN/PANU and a PANU cannot perform any other procedure together. This is an example when the PANU establishes a link with a NAP/GN device, after performing an optional inquiry.

1. The PANU first performs an Inquiry to discover what networking devices are within radio range, see [2, part B]. Having performed inquiry, the PANU may have gathered a list of inquiry responses from nearby devices which may support the PAN profile.

2. The PANU sorts the list according to some product specific criteria. For some PAN profile enabled devices, their CoD contains a field called “Load Factor”, see [5], section 1.2.6. It is recommended (but not mandated) that this field be used to sort the list.

3. The PANU SHALL start with the first at the top of the list (order by some product specific criteria) and try to form a connection with it. Any error or failure to form a connection SHALL cause the PANU to skip this PAN profile enabled device. The PANU MAY attempt to form a connection the next PAN profile enabled device in the list.

4. If there are no more PAN profile enabled devices in the list, the PANU SHALL NOT proceed with further initialization procedures. Initialization has to be re-initiated.

Figure 6 below shows the signaling flow, for a typical initialization. In this case; (a) the NAP/GN is configured to be in 'public' mode (i.e. it SHALL respond to inquiries), and (b) the NAP/GN is configured to be in multi-user mode (i.e. it SHALL become the piconet master). In this example authentication and encryption were requested and supported.

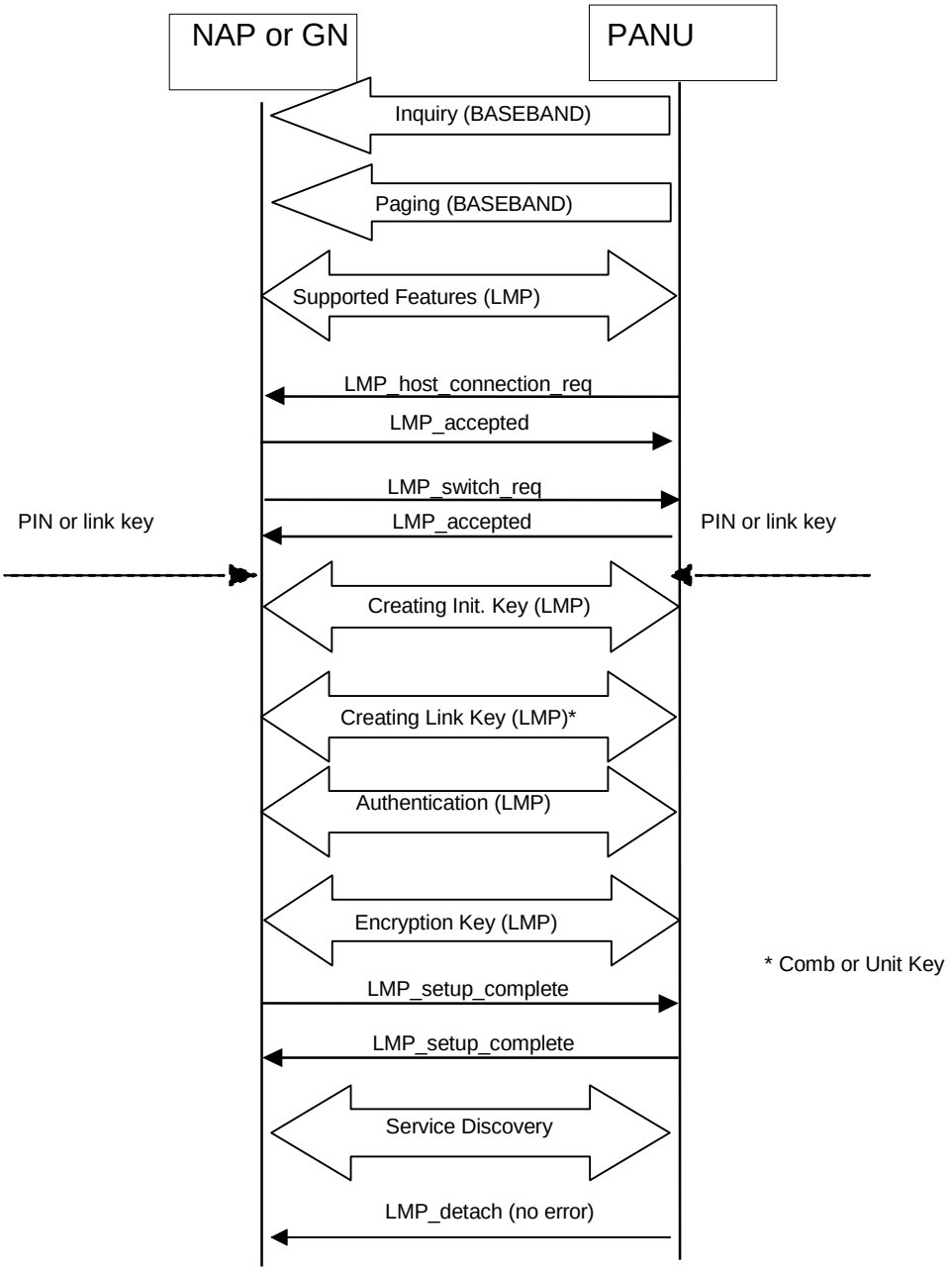

Figure 6 Initialization

The following subsections apply.

12.1.1 No responses to inquiry

If the PANU performed an inquiry and did not get any responses, the PANU SHALL NOT proceed with further initialization procedures.

12.1.2 No response to paging

If a NAP/GN does not respond to paging attempts, the PANU SHALL NOT connect to this NAP/GN.

12.1.3 Pairing

During initialization, the NAP/GN and PANU MAY be paired, which means that the PANU and NAP/GN build a security wall towards other devices. If, at any time, authentication is requested and a common link key is not available (i.e. the devices are not paired), a PIN MAY be supplied by the user or through an application.

12.1.4 Errors

If any LM procedure or Service Discovery procedure fails, or if link is lost at any time during initialization, then the PANU SHALL skip this NAP/GN.

12.2 Single/Multi-user mode

When the NAP/GN is configured to allow multiple users, then the NAP/GN SHALL be the master of the piconet. In this mode, the Management Entity on the NAP/GN SHALL ensure that the NAP/GN remains the master of the Bluetooth piconet.

While in multi-user mode, the NAP/GN SHALL request that it become the master of any new baseband connection. If, for any reason, the NAP/GN cannot remain the master of a Baseband connection, then that Baseband connection SHALL fail. The LMP [2, part C], allows a device to (a) request a master/slave switch and also (b) to refuse to comply with a request to perform a master/slave switch, see [2, part B], section 10.9.3.

The NAP/GN is not required to support multi-user mode.

12.3 Encryption

The Management Entity on the NAP/GN MAY ensure that the baseband connection is always encrypted. If, for any reason, the link cannot be encrypted, while required so, then the PANU SHALL NOT be allowed access to the PAN profile service.

The Management Entity in the NAP/GN or PANU MAY request that encryption be used on the link.

The Management Entity in the NAP/GN SHALL refuse any request to disable encryption, if authentication and encryption is required.

13 References

[1] Bluetooth Special Interest Group, “Bluetooth Network Encapsulation Protocol (BNEP) Specification”, Specification of the Bluetooth System, Version 1.0, February 14, 2003

[2] Bluetooth Special Interest Group, “Bluetooth Core”, Specification of the Bluetooth System, Version 1.1, February 22, 2001

[3] ISO/IEC 10038:1998 [ANSI/IEEE Std 802.1D-1998], Information technology—Telecommunications and information exchange between systems—Local area networks—Media Access Control (MAC) bridges.

[4] Bluetooth Special Interest Group, “Bluetooth Profile”, Specification of the Bluetooth System, Version 1.1, February 22, 2001

[5] Bluetooth Special Interest Group, “Bluetooth Assigned Number”, http://www.Bluetooth.org/assigned-numbers.htm

[6] Ethernet Protocol Numbers http://www.iana.org/assignments/ethernet-numbers

[7] Dynamic Configuration of IPv4 link-local Addresses (Autonet) http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-07.txt

[8] Bluetooth Special Interest Group, “Bluetooth Personal Area Networking (PAN) Marketing Requirement Document

[9] Linklocal Multicast Name Resolution, http://www.ietf.org/internet-drafts/draft-ietf-dnsext-mdns-12.txt

[10] Bluetooth SIG, Bluetooth Security Architecture, Version 1.0 15 July1999, at http://www.bluetooth.com.

14 Acronyms and Abbreviations

List of abbreviations necessary for the understanding the PAN profile.

Abbreviation or Acronym	Meaning
BB	Baseband
BNEP	Bluetooth Network Encapsulation Protocol
CL	Connectionless
CoD	Class of Device
DHCP	Dynamic Host Configuration Protocol
GN	Group Ad-hoc Network
MIB	Management Information Block
NAP	Network Access Point
GIAC	General Inquiry Access Code
IP	Internet Protocol
LAN	Local Area Network
LC	Link Controller
LIAC	Limited Inquiry Access Code
LM	Link Manager
LMP	Link Manager Protocol
ME	Management Entity
MTU	Maximum Transmission Unit
OSI	Open Systems Interconnect (model)
PAN	Personal Area Network
PANU	Personal Area Network User
PFD	Packet Filter Database
QoS	Quality of Service
RFC	Request For Comment

15 Appendix B (Normative): Timers and counters

No specific timers are required by the PAN profile

Timer name	Recommended value	Description	Comment
T_{crt}	10 Secs	Timer used to determine when a BNEP Setup Connection Control packet has be lost and SHALL be retransmitted.	Range: 1 – 30 seconds
T_{frt}	10 Secs	Timer used to determine when a BNEP Filter Control packet has be lost and SHALL be retransmitted.	Range: 1 – 30 seconds

Table 13 Defined timers

No specific counters are required by the PAN profile.

Counter name	Proposed value	Description	Comment

Table 14 Defined Counters

The following parameters are required by the PAN profile.

Parameter	Description
Maximum users	The maximum the number of simultaneous users/connections.

Table 15 Defined parameters

16 List of Figures

17 List of Tables