ECMA TR/102

1st Edition / December 2010

Personal Networks – Overview and Standardization Needs

Contents

Introduction

This Ecma Technical Report explores Personal Networks (PNs) and their extensions. PNs provide secure and ubiquitous communication between (personal) devices over multiple network technologies. PNs provide automatic configuration of networking, security, and offers users access to their Services across their PNs.

This Technical Report introduces the PN architecture and identifies various communication scenarios as well as standardization needs of PNs.

This work is based on - and Ecma acknowledges - the valuable results from EU FP6-IST projects Magnet and Magnet Beyond (see [33] and Dutch Freeband PNP2008 (see [32]).

A comprehensive PN overview may be found in [34].

This Ecma Technical Report has been adopted by the General Assembly of December 2010.

Personal Networks – Overview and Standardization Needs

1 Scope

This Technical Report introduces and defines architectural concepts, and standardization needs concerning personal networks (PN) and PNs that are extended with Services using various scenarios.

This report does not specify the standards or the technologies to be used.

2 References

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1]   ECMA TR/92, Corporate Telecommunication Networks - Mobility for Enterprise Communications

[2]   ECMA TR/96, Next Generation Corporate Networks (NGCN) - Identification and Routing

[3]   ECMA TR/101, Next Generation Corporate Networks (NGCN) - Emergency Calls

[4]   ISO/IEC 29341-1:2008, Information technology -- UPnP Device Architecture -- Part 1: UPnP Device Architecture Version 1.0

[5]   ISO/IEC 7498-1:1994, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model

[6]   ITU-T Rec. X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

[7]   ITU-T Rec X.200, Information technology - Open Systems Interconnection - Basic Reference Model: The basic model

[8]   ITU-T Rec. Y.1542, Framework for achieving end-to-end IP performance objectives

[9]   ITU-T Rec. Y.1542 Amd1, Framework for achieving end-to-end IP performance objectives

[10]   ITU, Performance, QoS and QoE, ITU-T Study Group 12 (Study Period 2009-2012)

[11]   IETF RFC 3261, SIP: Session Initiation Protocol

[12]   IETF RFC 4306, Internet Key Exchange (IKEv2) Protocol

[13]   IETF RFC 2205, Resource ReSerVation Protocol (RSVP)

[14]   IETF, The Optimized Link State Routing Protocol, V2, draft-ietf-manet-olsrv2-11

[15]   IETF, Dynamic MANET On-demand (DYMO) Routing, draft-ietf-manet-dymo-19

[16]   IETF, Simplified Multicast Forwarding (SMF), draft-ietf-manet-smf-10

[17]   IETF, Network Mobility Work Group, online: http://tools.ietf.org/wg/nemo

[18]   IETF, Mobile Ad Hoc Network (MANET) Neighbourhood Discovery Protocol (NHDP), draft-ietf-manet-nhdp-12

[19]   IETF RFC 5201 Host Identity Protocol

[20]   IETF, Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), draft-ietf-behave-turn-16

[21]   IETF, Service Location Protocol (SLP, srvloc), Version 2, RFC2608

[22]   IETF, Link-Local Multicast Name Resolution (LLMNR), RFC4795

[23]   IETF RFC 2407 defined The Internet IP Security Domain of Interpretation for ISAKMP

[24]   IETF RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

[25]   IETF RFC 2409 defined The Internet Key Exchange (IKE)

[26]   IETF, REsource LOcation And Discovery (RELOAD), draft-ietf-p2psip-reload-00

[27]   OMA-TP-CPNS-2008-0002-INP_CPNS: "Personal network concepts: Standardization needs in Personal Networks"

[28]   Digital Living Network Alliance (DLNA), online: http://www.dlna.org/

[29]   Peer to Peer Universal Computing Consortium, online; http://www.pucc.jp/

[30]   Apache River, Jini, online: http://www.jini.org/

[31]   Universal Plug and Play (UPnP), online: http://www.upnp.org/

[32]   Freeband PNP2008, http://pnp2008.freeband.nl/

[33]   IST MAGNET Project, http://magnet.aau.dk

[34]   Martin Jacobsson, Ignas Niemegeers, Sonia Heemstra de Groot, "Personal Networks: Wireless Networking for Personal Devices", ISBN 978-0-470-68173-2, John Wiley & Sons, Chichester, May 2010

[35]   Ramjee Prasad (editor), "My personal Adaptive Global NET (MAGNET)", Springer Series on Signals and Communication Technology, ISBN 978-90-481-3436-6, 2010

[36]   IBBT TranseCare project, https://projects.ibbt.be/transecare/

[37]   F. Stajano, "Security for ubiquitous computing, John Wiley & Sons, Chichester, 2002

3   Terms and definitions

For the purposes of this Technical Report, the following definitions apply, abbreviations are indicated between brackets. The relationships among the concepts introduced in this clause are depicted in the UML class diagram in Figure 1.

3.1
Relay, Layer 2 (L2), Layer 3 (L3)
As defined in [5]

3.2
Device
Entity able to host one or more Nodes

3.3
Node
Logical PN element

3.4
Imprinting
Creating a Node on a Device by giving it authentication data for a certain PN

3.5
Foreign Node
Node of a another PN

3.6
Cluster
Non-empty Node subset of a PN having a distinctive property

3.7
EPN
Extended PN
PN extended with Services via Proxies

NOTE   Extension implies authorisation and connectivity

3.8
Gateway
Communication service between a Node and a Foreign Node or non-PN device

3.9
Gateway Node
Node that provides the Gateway

3.10
Network Cluster
Cluster with Nodes that can reach each other over L2 connections, possibly using L3 relaying

NOTE   A PN can contain one or more Network Clusters

3.11
OPN
Offering PN
PN that allows other PNs to use one or more of its Services

3.12
PN
Personal Network
The set of all Nodes that have common (PN) credentials

3.13
Proxy
Service that provides the possibility to use non-PN and Offered Services

NOTE   A Node may provide both Gateways and Proxies

3.14
Interconnecting Structure
Network for Network Clusters, registries and Non-PN Services

3.15
Owner
Individual or organization exclusively controlling the use of Devices, PNs, Nodes or Services

3.16
PoA
Point of Attachment

3.17
Service
Set of functionalities provided by a Node

3.18
Non-PN Service
Service not hosted on a Node

3.19
Offered Service
Service offered by an OPN
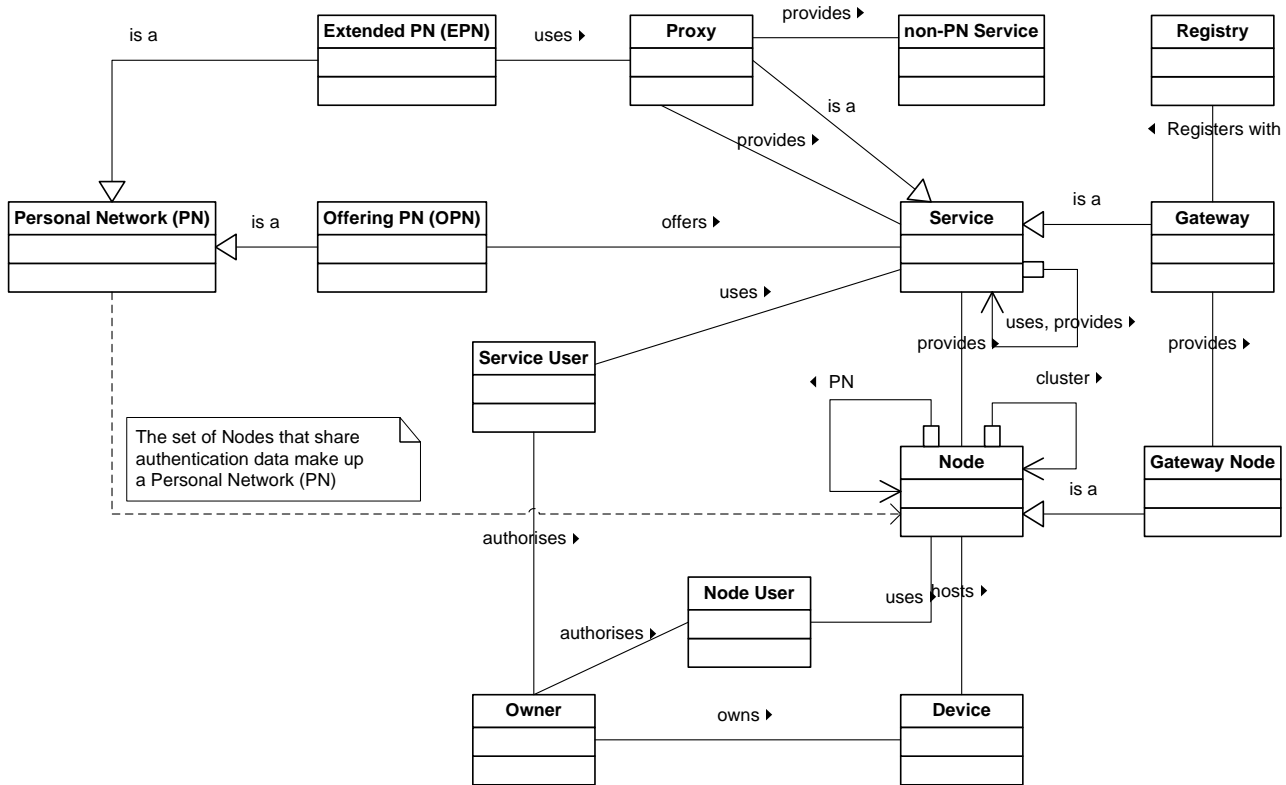
Figure 1 — PN terms and their main relationships

4   Background and General Concepts

Nowadays, people have at their disposal a wide range of devices that can assist them in their daily life, both personal and professional. Devices such as personal computers, laptops, smart phones, digital cameras, networked hard disks should enable them to carry out tasks quicker, smarter and while on the move. Since multiple devices are being used, information gets increasingly spread over several devices. This leads to the problem of interconnecting those devices in a secure way in order to have the omnipresent availability to all data independent of where the information stored and wherever the user is as depicted in Figure 2. Today, few dedicated solutions exist to achieve this, often based on central servers that act as a broker. Another alternative is a tedious, complex and user unfriendly configuration procedure the user has to go through, simply to be able to obtain access to a remote device.
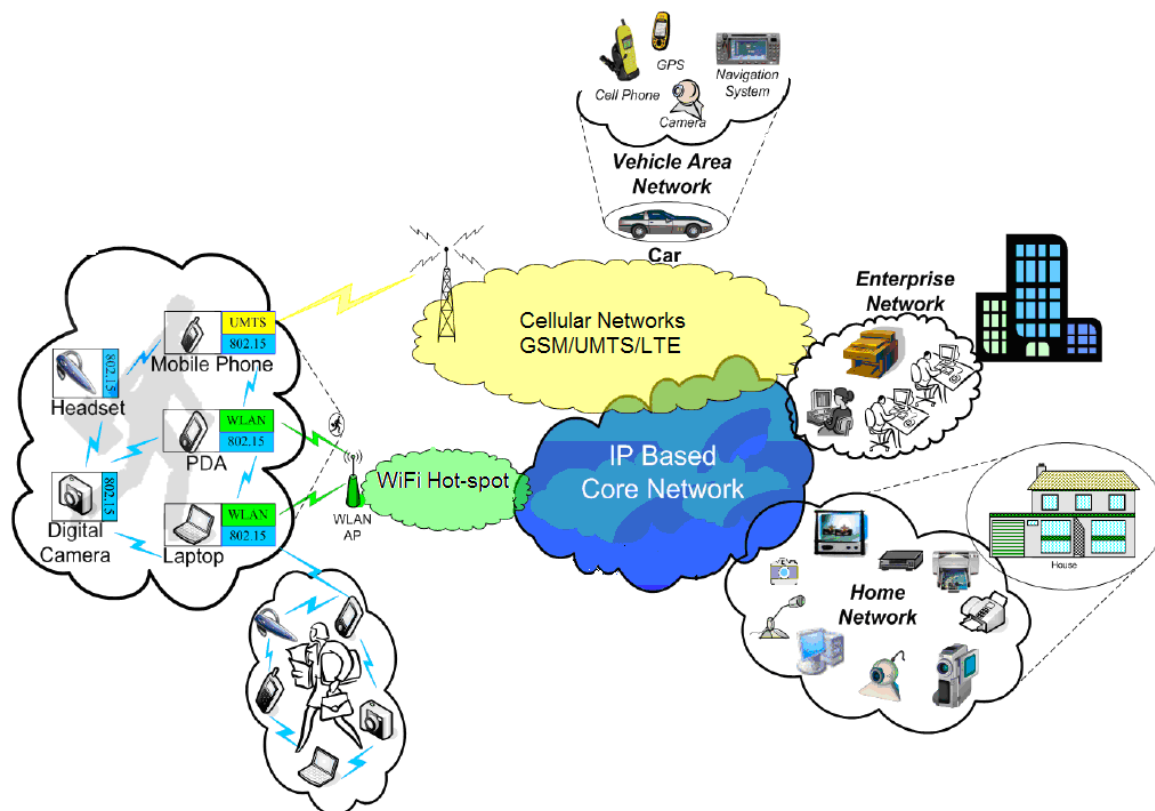
Figure 2 — Typical networking scenario of a person with various personal devices

Personal Networks (PN) offer a general solution to this challenging problem by autonomously and securely interconnecting a trusted set of Nodes and offering users access to their Services. User may access those Services through any Node in their PN. As such, users can partake in one or more PNs that each fulfils one of their specific needs and that are as such fully user-centred. Whereas a personal area network (PAN) connects the personal devices situated in a geographical area, the PN is not limited to a geographical area or PAN.

A user of a PN may require access to Services that are located in another PN in the same flexible way. In this case, the PN is extended with Services from Foreign Nodes, creating an Extended-PN (EPN). An example scenario is shown in Figure 3.

PN User 1

PN User 2

Extended PN User 1

🔴 = Service offered by Foreign Node, extending the PN of User 1
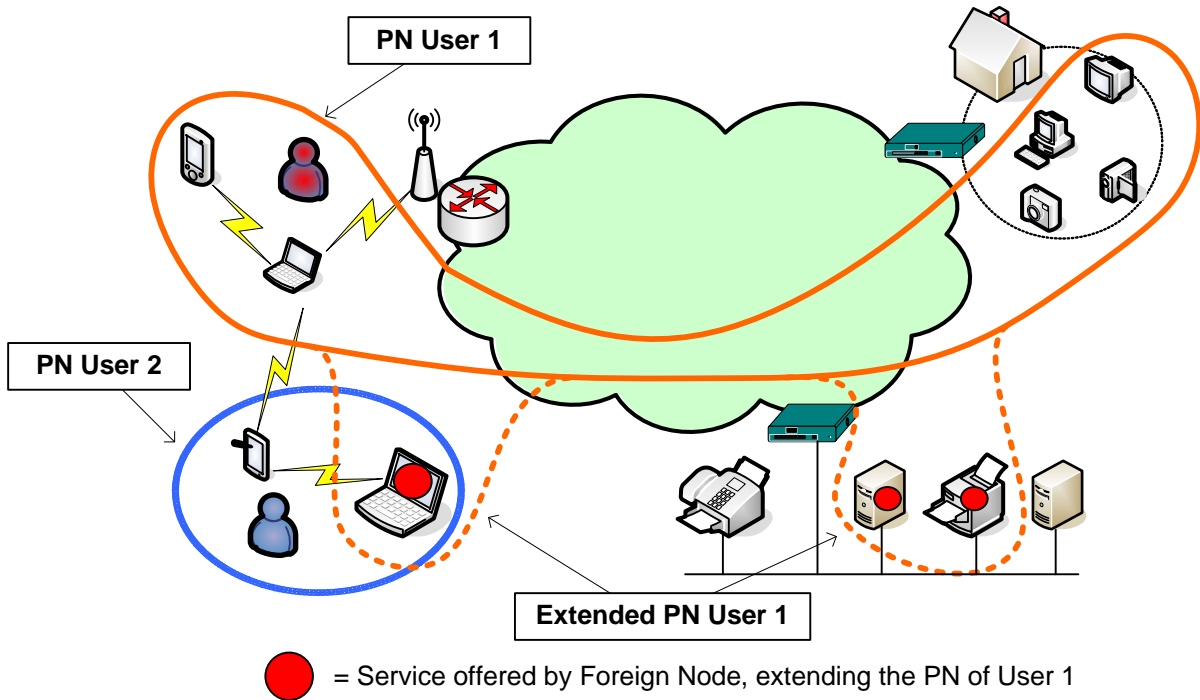
Figure 3 — PN extended with Offered Services

Additionally, the user-friendly PN environment can be enriched with Non-PN Services to fully meet the user's requirements and to help accomplish tasks not possible with a single PN.

The abstraction of the service, PN and connectivity levels that provide the context for the main PN concepts are illustrated in Figure 4. Each of the levels addresses a coherent set of issues to cope with the inherent complexity of personal networks. In the following subclauses, these levels are introduced.
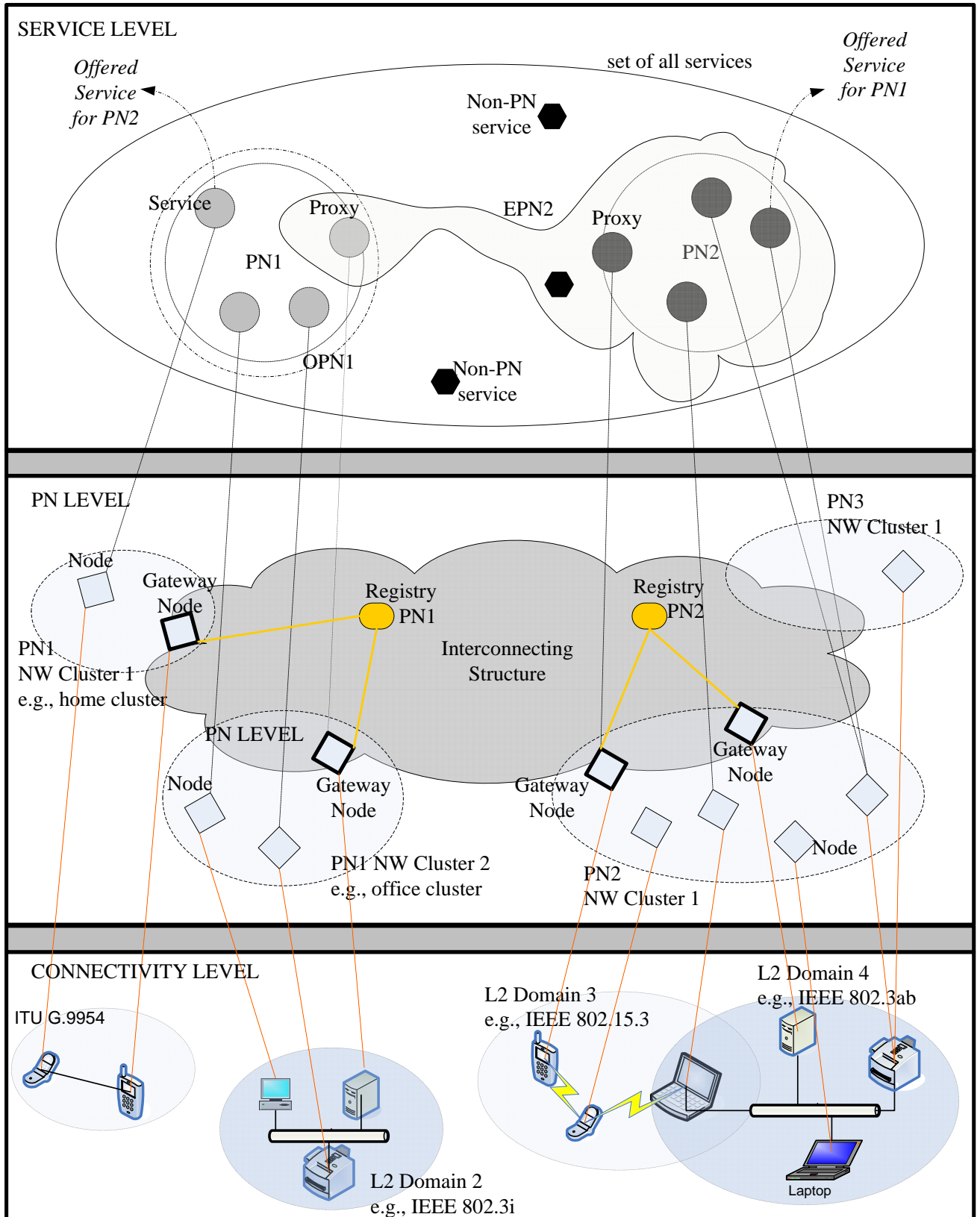
Figure 4 — Three abstraction levels of personal networks

4.1 Service Level

The service abstraction level focuses on support facilities that are related to optimizing the providing and using of Services. The service level supports Services as they become available through interfaces, which are either targeted for other Services (APIs) or for interfacing with people (e.g., graphical user interfaces). The service level provides the following support facilities:

- Name resolution so that the PN user can assign meaningful names to his Nodes and perhaps Services.

- Service discovery for authorised:

    o Services from within the PN;

    o Offered Services; and

    o Non-PN Services.

- Functionality for sharing Services, including access control and the management thereof.

- Giving access to Non-PN Services and Offered Services using Proxies.

Offering PNs (OPNs) make a subset of their Services available to other PNs that may (subject to a set of rules) then become Extended PNs (EPNs). Notice that only a subset of the Services in each participating PN is made available to the others.

4.2 PN Level

The PN level provides an efficient networking platform for the PN Services. A PN can be seen as an autonomous overlay network that runs transparently on top of existing infrastructure.

The PN level addresses how the Nodes are organized and how they communicate with each other. PN protocols are based on IP because

- IP offers abstraction across heterogeneous connectivity technologies and the network level has to be as independent as possible from the connectivity level so that current and future connectivity technologies can be supported,

- compatibility with the already developed protocols based on the IP is maintained,

- existing technologies based on IP can be reused within the PN.

The PN level detaches communication among its Nodes from communication with Foreign Nodes. The PN has its own PN level address space for its Nodes. Nodes must have an address that is unique within its PN and may receive it during the imprinting process. Applications and services can use these addresses to communicate with each other regardless of the location and topology.

A PN has at least one - or more - Network Clusters. Network Clusters do not have an address or identity.

Nodes organise themselves into Network Clusters, using a method that is to-be-standardised.

Network Clusters facilitate local communication and efficient routing.

Communication among the Nodes in different Network Clusters may be realized using IP routing, forwarding and/or tunnelling over the Interconnecting Structure. Network Clusters use their Gateways to communicate with other Network Clusters, using the Gateway PoA(s) retrieved from a (common) Registry. Gateways keep the globally addressable registry up to date when their PoAs change. The Gateways use the Registry to learn each others' PoAs initially and when they change.

Higher layer protocols, such as SIP [11], IKEv2 [12]. RSVP [13], may be required for e.g. mobility, security or QoS support.

4.3 Connectivity Level

In the connectivity level, Devices are organised in L2 Domains with communication links among them. The connectivity level covers the basic wired and wireless networks and protocols.

Concerns addressed at this level include issues at data link layer, physical layer, and their interrelationships. Solutions for this abstraction level use existing wired and wireless technologies.

A Personal Network will partly be formed on top of these L2 domains by simply using the connectivity offered by this L2 domain. Some important issues that are influential on the performance of PNs are

- Auto-configuration of interfaces: if different Nodes want to communicate with each other in a L2 domain, they may need to use the same configuration. For example, for networks based on the IEEE 802.11 standard, this means they have to connect to the same access point (in infrastructure mode) or the same ad-hoc network (in ad-hoc mode). Manual intervention to achieve this would seriously impact user-friendliness.

- Efficient utilisation of resources: For example, several wireless technologies operate in the same frequency bands (e.g., ISM bands). These technologies should share these radio resources in an efficient and fair way to improve connectivity, scalability and co-existence.

- Standardized access to L2 link properties such as bandwidth and delay to make the PN networking more efficient.

Standardized feedback about L2 events such as the detection of other devices, the breakage of links or loss in connectivity to make the PN establishment and maintenance more efficient.

5 PN Configurations

This Clause introduces some configurations for Personal Networks and their extensions.

5.1 PN with 1 User

People make use of a wide range of devices. At home, they have a variety of devices such as digital TV, stereo, PC, printer, digital camera, hard disk recorder, media server, smart phone, intercom, HVAC system, surveillance camera. Furthermore, users also carry around some devices such as smart phones, PDAs or laptops. Such devices are not easily connected to each other and access to services is difficult. PNs facilitate interconnection of these devices, access to information that is stored on them and usage of services offered whether the user is inside, around or away from home. Examples of such services are: automated file replication, remotely watching the surveillance camera, accessing digital photos stored at home, programming your hard disk recorder, controlling the heating system while driving back home.

The Owner will authorise or himself imprint these Devices. The Nodes at home will self-organize them into a Network Cluster. When the User leaves his house, carrying some Devices with him, the Nodes on these Devices will form another Network Cluster. The PN technology will automatically interconnect the different Network Clusters via Gateways and make all their Services available to each other.

It is possible that a Device, e.g. a printer, is being used by other Users at the same time. In that case, this Device will host different Nodes at the same time, each Node belonging to another PN.

5.2 PNs with multiple Users

People residing in a home for the elderly become often socially isolated. Their family members often do not have time to visit them due to time and distance restrictions. However, these elderly people really care about

how their children and grandchildren are doing. They like to watch pictures of them, listen to music, communicate with each other, or to be kept up-to-date about interesting things that happened. Within the home for the elderly, the caregivers want to keep these people informed about things happening inside the home (meals, activities, pictures of events…), but also in the outside world. Traditional technology is often too complex for these elderly people, but PN technology reduces complexity and can enrich the life of these elderly people.
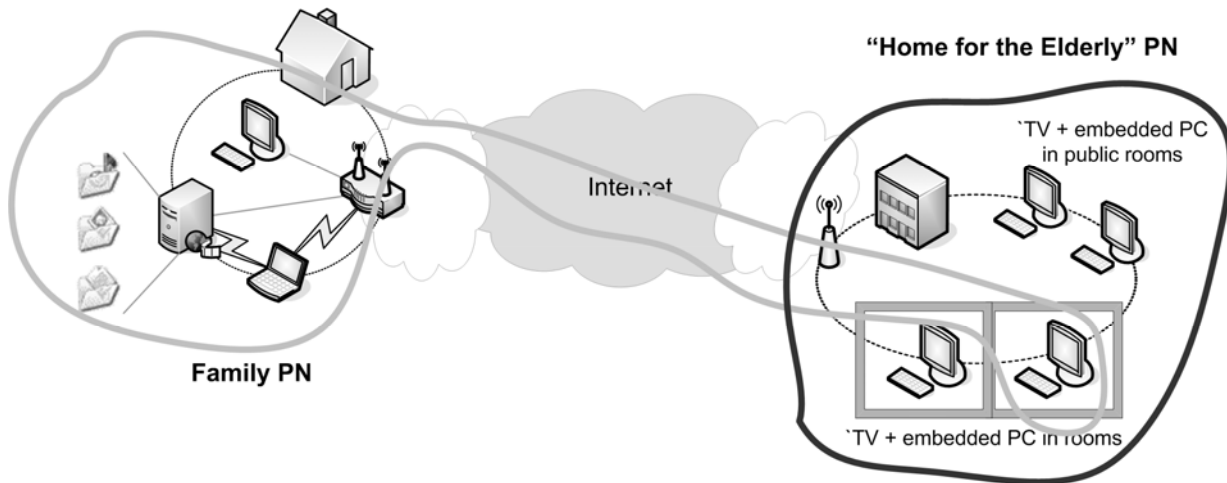

Figure 5 — 2 PNs, both having multiple users

Within the home for the elderly, Devices can be installed in the rooms of the people. On the Device of a person living in the home for the elderly and on the Devices of their family members, Nodes can be created, forming a Family PN that has multiple Users. The PN transparently makes the Services offered by the Nodes of the family members available to the Node created on the Device in the room. Then, with an easy, remote-controlled user interface, these Services can be used by the elderly people in a very simple and intuitive way. In the same way, all Devices in the home for the elderly can host an additional Node that is part of the "Home for the Elderly" PN.

The TranseCare project implemented a prototype of this use-case, see [36].

5.3 PN owned by a Legal Entity

Within a company employees are often on the road or they have to be stand-by in case of an emergency. Therefore, they frequently require access to data stored in remote databases or services located at different premises. For example, a sales person requires access to the customer database at the main office when visiting its customers as shown in Figure 6. A production engineer needs to be reachable 24 hours a day, seven days a week and, in case of an emergency, needs to be informed automatically and requires instant access to the production system independent of the location of the engineer. A truck driver stays in touch with the main office to exchange documents about the freight and the customers. Since often critical or confidential information is being exchanged, all communication needs to be secured, preventing disclosure of any confidential data.
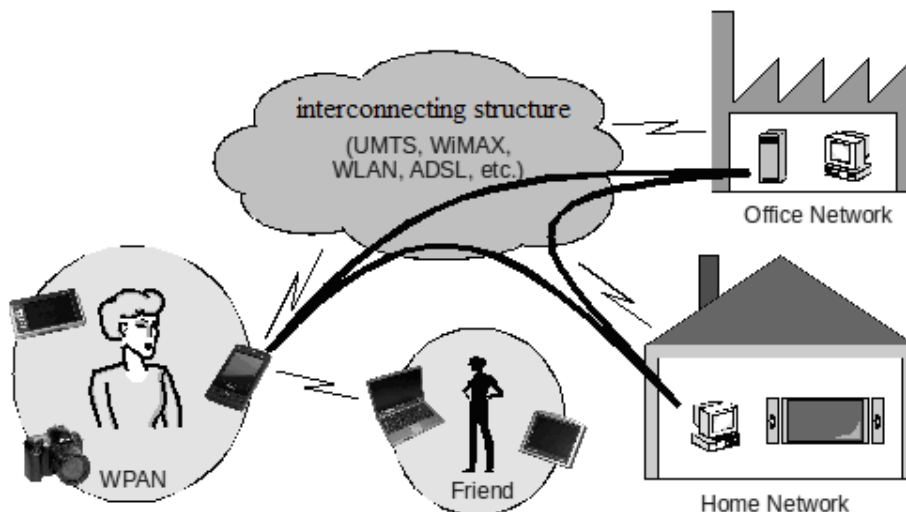
Figure 6 — Travelling salesperson scenario

The company can establish a Company PN. Nodes are created on all involved Devices. This includes servers, but also the Devices that are owned by the company, but are carried around by the employees. As such, any User that is authorized to access a Node, can easily, securely and transparently make use of all or a subset (e.g. depending on policies or rights for that User) of the Services offered by the other Nodes in the Company PN. Note that the "home for the elderly PN" in Figure 5 is another example of a PN owned by a legal entity. Access control of and authorization to Services are standardization gaps.

5.4 EPN using Offered Services

Different people can have their own PN, companies or organizations can have their own PN. In many situations, interactions between people or between a person and a company need to take place in order to achieve a certain goal, thereby crossing the PN boundaries. For example, a salesperson may need to exchange information with its customers or may need to access company information from a device not belonging to the company. Family members want to share services with each other by creating a virtual vicinity feeling: by sharing cameras, headset, speakers they can see, talk and interact with each other wherever they are or even while travelling. Think of a truck driver or business man that wants to stay in touch with its family.

In order to share Services across the boundaries of these PNs, Proxies will be used. The PN that wants to make the Service available to another PN, i.e. the OPN, will make it discoverable and accessible via a Proxy. The other PN will also use a Proxy in order to be able to discover access and finally use the shared Service, resulting in an Extended PN. As a result, a PN can make use of Offered Services in a similar way as its own Services, with all complexity transparently managed by the Proxies. EPNs offer an alternative solution for the "travelling sales person scenario" in 5.3.

5.5 EPN using Non-PN Services

In several situations, a PN user would benefit from the ability to make use of Non-PN Services from within the PN. For example, a person that is able to control and monitor her burglar alarm or fire detectors wants to get connected to an emergency service or surveillance service in case an alarm occurs. Family members who want to make use of two-way real-time communication want to make use of the (non-PN) telecommunication services from within their PN. People wearing devices that monitor their health may want to connect to an emergency service in case the monitoring device detects that something is going wrong.

In order to make use of Non-PN Services, the PN will again make use of a Proxy. The Proxy will make the Non-PN Service available to all users of the PN, in a way as if it were a normal PN Service, thereby creating an Extended PN. When making use of the Service, the Proxy will transparently take care of any translation needed, hiding the PN internals for the Non-PN Services and guaranteeing interoperability.

5.6   User to User Telecommunication – 2 PN configuration

(Two-way real-time) telecommunications may be achieved through

- Extending PNs with the Non-PN Services: The PNs may extend themselves with a common Non-PN Service which provides real-time telecommunications service.

- One of the PNs may extend itself with the Service provided by the other PN. In this case, the OPN provides the two-way real-time communications service to the other party.

For SIP, the communication devices have a User Agent (UA).

An example implementation of the two-way real-time communication using SIP is shown in Figure 7. Assume there are two PNs. PN1 would initiate a video call session with the PN2. To enable a session, UAs in the PNs register to a public SIP Proxy (via the interconnecting structure). Local SIP Proxies in Networked Clusters may register the Nodes in their respective Networked Clusters. The request would go through the public SIP Proxy which is a Non-PN Service (in this configuration). After this initial request, the SIP proxies can talk to each other and initiate sessions between User Agents in the PNs. Having a SIP Proxy inside the PN has the benefit that a Node can register with the SIP Proxy independent of its location.
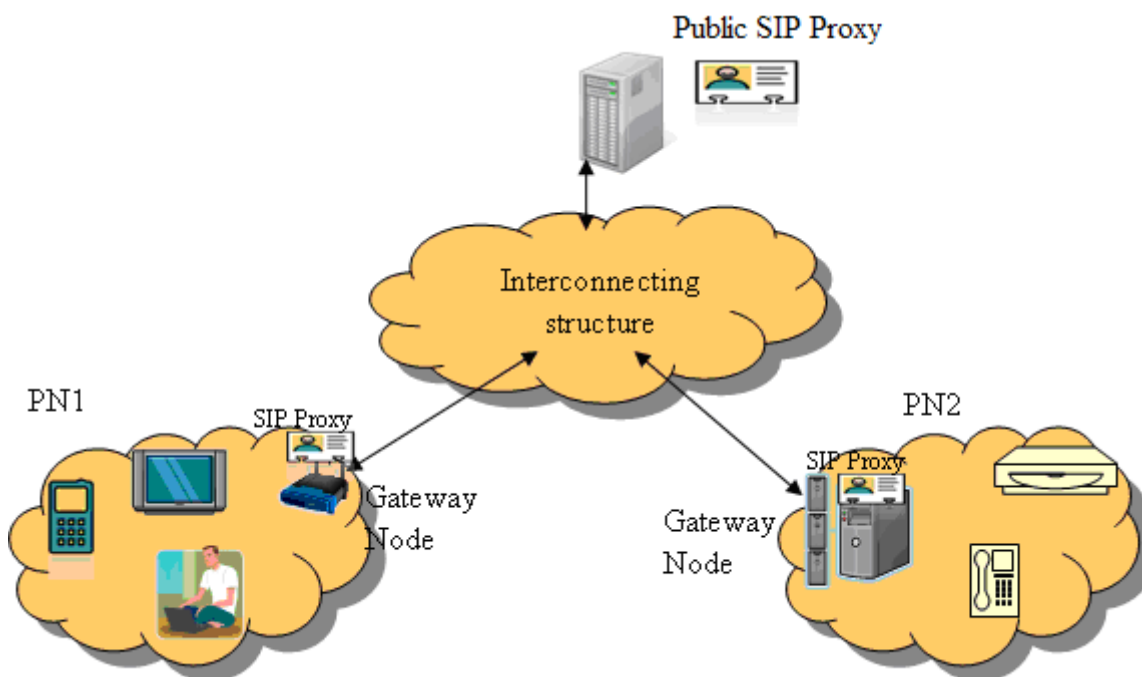

Figure 7 — Two-way real-time communication scenario

6   Requirements

While this Clause refers to the "user", in practice there are several actors having requirements on PNs and their extensions. The requirements are derived from the configurations in Clause 6; Clause 9 lists the standardisation needs.

6.1 Connectivity and Mobility Support

A PN should

- Maintain connectivity between its Nodes.

- Support communication with non-PN services and Offered Services.

- Provide terminal, user, session and Service mobility as defined in ECMA TR/92 [1].

6.2 Security and Privacy

A PN should be able to

- Guarantee secure configuration, use and decommissioning

- Protect against unauthorized access to - and visibility - of Services.

    By e.g.:
    o Provide seamless authentication mechanism such as single sign-on between a User, Node, Cluster, PN and Services,
    o Preserve privacy,
    o Facilitate Service and data integrity,
    o Facilitate trust among Nodes and among Services,
    o Provide interoperable, easy-to-use security mechanisms.

6.3 Auto Configuration and Self-organisation

A PN should

- Limit the administrative requirements for human interventions; conceal most of the network-related configurations and mechanisms.

- Self-organise joining and leaving at the connectivity, Cluster, PN and the Service level.

6.4 Quality

A PN and its Services should utilize underlying networks in a way that achieves the required quality such as bandwidth, bit error rate, latency, prioritisation, continuality, security, availability, reliability, pages per second, resolution, and location accuracy.

The negotiation of quality of Services accessed via external communication (see 8.7) is a standardisation need.

6.5 Management

NOTE   Herein we do not address device management requirements.

Actions that people and/or organisations are required to do for PN management should be brought to a minimal level. The user must remain in control of his PN and may therefore need to be able to perform certain management tasks.

PN management typically deals with management of Nodes, PN and Services, including:

- Configuration management,

- Topology management (e.g. by using registries),

- Fault management,

- Performance management,

- Access control and deployment,

- Security management,

- Accounting.

It should be possible to:

- Create and destroy PN credentials,

- Create Nodes by means of imprinting with the PN credentials,

- Un-imprint Nodes,

- discover which Services are available within a PN,

- Offer a subset of Services in a PN for use in EPNs,

- Manage the visibility of its Nodes, PN, and Services and their attributes including quality and capacity,

- delegate the PN management.

6.6   Scalability

A PN must be scalable in terms of number of Users, Service extensions for both OPNs an EPNs, Devices, Nodes, Network Clusters and Services. The number of Nodes in a PN may be in the range of hundreds, which in turn affects the addressing scheme, networking, and other functionalities.

7   PN Networking

In this clause, the scenarios are generalized into functional decomposition and relevant standardisation needs are presented in the PN level. The functionality of the PN level shown in Figure 4 is divided into two main sections.

- PN management is a prerequisite to any PN networking functionality. It includes:

  o   Imprinting,

  o   Enabling self-organisation by configuring Nodes, Clusters, Network Clusters, etc.

- PN networking includes:

  o   Network Cluster formation,

  o   Gateway discovery,

o   Intra-Network Cluster communication,

o   Inter-Network Cluster communication,

o   Inter-PN and with non-PN network communication.

7.1   PN Creation and Dissolution

PNs may be created by the Owner, the authorised User or by another authorised party. This involves initializing a "mother" device (see [37]) that can be used to imprint Devices (see 7.2). A mother" device may contain e.g. a Registry address, personal data of the User, name, affiliation, (privacy) preferences, etc. With the 1st imprinting, the (one Node) PN is created; conversely with un-imprinting the last Node, the PN no longer exists. Un-imprinting can be automated.

7.2   Device Imprinting, Node Initialisation and Configuration

The "mother" (see 7.1, [37]) imprinting device imprints any "duckling" Device. Imprinting a Device involves creating a Node belonging to the PN on the Device. As part of the Node creation, authentication data for its PN is uploaded to the Node. After imprinting, the Device hosts the new Node.

If an imprinting device needs to join a PN, it must create a Node on itself by means of imprinting.

As part of the imprinting, PN management on the imprinting device configures the Node with e.g. the configuration of the network stack, user data such as name, affiliation, set of IDs, (privacy) policies, specific initialization for Services on the Node, etc. After configuration, the Node can join its PN without additional user intervention.

Devices may support the hosting of multiple Nodes. The creation of more Nodes on a Device will not affect the already existing Nodes.

Un-imprinting removes the Node from the Device (i.e., killing the duckling) and it includes removing all PN credentials associated with the Node.

Imprinting and un-imprinting have security implications. Therefore, these activities should be protected from non-authorized use. Imprinting is controlled by the Device owner; un-imprinting may be subject to authentication.

7.3   Node Addressing

A PN maintains its own secured private network. During imprinting each Node is assigned a fixed intra-PN Node address, which will not be made public. The address is unique within a PN and All Nodes in a PN communicate using their Node addresses.

7.4   Network Cluster Formation

During the Network Cluster formation:

•   Neighbour discovery algorithms are used and subsequently Nodes authenticate each other using the imprinted credentials; and

•   If authentication is successful, secure connections among the Nodes in the cluster may take place.

7.5   Intra-cluster Routing

Network Clusters may be multi-hop and therefore need routing to identify the paths between its Nodes.

Intra-cluster routing functionality should be able to deal with the specific characteristics and dynamics of Network Clusters, such as Nodes joining and leaving the Network Cluster or having multiple L2 interfaces. To cope with such characteristics or dynamics, distributed solutions are required.

Beyond unicast routing, Network Cluster-wide multicasting and broadcasting may be required.

7.6   Gateway Node

Nodes in a Network Cluster communicate with Foreign Nodes and other Gateway Nodes through Gateway Nodes. Outside a PN Gateways are addressed by their PoA addresses as assigned by the interconnecting structure. Inside a PN, Gateways are addressed by their intra-PN Node address.

Gateway Nodes may implement special functionalities, such as

- Translation between intra-PN Node addresses and Gateway PoAs,

- filtering of unwanted traffic,

- dynamic tunnelling with Gateway Nodes in other Network Clusters in this PN.

Nodes in a Network Cluster should be able identify their Gateway(s).

7.7   Inter-cluster communication, tunnelling and Routing

The purpose of the inter-Network Cluster tunnelling and routing functionality is to connect disperse Network Clusters and offer transparent and secure communication among all Nodes with terminal mobility support.

All intra-PN communication, including inter-Network Cluster communication, must be shielded from the outside world. To form the PN and realise inter-Network Cluster communication over the Interconnecting Structure:

- Network Clusters use their Gateways to communicate with other Network Clusters in the same PN.

- Gateways contact the other Gateways by using their PoA addresses which they get from a globally addressable registry. Gateways keep that registry up to date when their PoA addresses change.

- Gateways establish secure tunnels and exchange routing information.

- Gateways maintain the communication paths by dynamically changing tunnels and updating routes in case of terminal mobility, when Network Clusters merge or split, or when Gateways change their points of attachment.

- Active Registries might facilitate Gateway communication when Gateways are behind Network Address Translation (NAT) functions by using e.g. the STUN or TURN methods.

Registries may be centralised or distributed and may reside on any of the Nodes or be a Non-PN Service. Figure 8 illustrates PN formation with a centralised Registry.
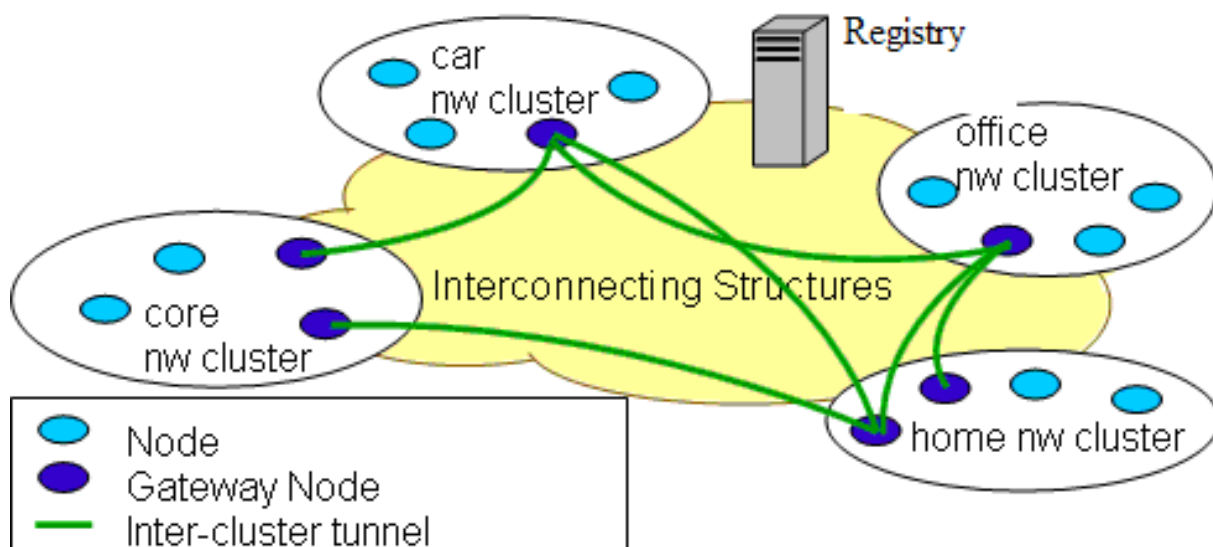
Figure 8 — A PN with centralised registry and secure inter-Cluster tunnels

7.8   External communication

External communication is Inter PN and PN to non-PN communication which includes finding, establishing, and maintaining communication via Proxies and Gateways.

7.8.1   Via proxies

A PN that offers its Services, i.e., an OPN, makes them available to other PNs by using one or more Proxies. Those OPN Proxies make Services visible, available, and accessible to (prospective) EPNs. A Proxy and a Gateway typically reside on one Node. Proxies use Gateways for communication with other Proxies or Non-PN Services.

The EPN Proxy imports Non-PN Services and Services from OPNs into the PN. To make a Non-PN Service available to all Nodes in an EPN, a Proxy in the EPN is needed. Also note that a PN can be an EPN and an OPN at the same time. In that case, a proxy may both export and import Services at the same time.

A Proxy needs to discover Services and Non-PN Services to import and export. For Services within the PN, it uses the PN-internal service discovery mechanism. For Non-PN Services and Services from OPNs, it may use any existing service discovery protocol or service directories.

A Proxy may control or secure access to Services.

7.8.2   Direct L2 communication and tunnelling on behalf of proxies

Gateway Nodes of the Network Cluster may establish a direct L2 communication link or a secure tunnel over the Interconnecting Structure with a Foreign Node or with a device hosting a Non-PN Service.

PN internal mechanisms, such as addressing, routing, tunnelling, and service discovery, should never be exposed to the outside. To this end, Gateways translate between PN internal addresses and external addresses. Foreign Nodes and PN-unaware devices will only be able to communicate at the network level with the Gateway Nodes of a PN.

In case of mobility or other reasons, direct L2 communication between the Gateway Node and a Foreign Node or a device may stop functioning. Direct L2 communication may also become available and can be used instead of tunnelling over the Interconnecting Structure. In these cases, a switch between direct L2 communication and tunnelling over the Interconnecting Structure or vice verse could be done.

A Gateway may use access control or other security mechanisms to decide whether to translate addresses of a given Node or non-PN device.

7.9 Mobility in PNs

Device (terminal), personal, session and service mobility are as defined in ECMA TR/92 [1].

7.9.1 Device (terminal) Mobility

The addressing, routing and tunnel mechanisms as described in 7.3, 7.5 and 7.7 handle the device mobility as well as changes in PN topology.

7.9.2 Personal Mobility

When the PoA of the PN user changes, the mobility is implicitly handled since all the devices have a Node that belongs to the user's PN.

7.9.3 Session Mobility

Session mobility can be implemented as a Service in the Service level. With this Service, session mobility can be preserved while a terminal is mobile.

7.9.4 Service Mobility

Service mobility in PNs is implicitly addressed by the self-organising mechanisms in the PN level.

7.10 Support for Non-IP IP or Resource Constrained Devices

Devices which cannot host a Node including sensor devices or other devices not capable of running IP never become part of a PN. However, their Services may be exported to a PN by a special Proxy running on a Node in that PN. To the rest of the PN, it will appear as if the Services are hosted by the Node with the Proxy, while in fact, they are hosted on one or more devices, with which the Node has non-IP connectivity.

7.11 Other Technical Considerations

In addition to the architectural and other concepts described above, there are many other technical considerations associated with the scenarios identified in Clause 5 including but not limited to:

- **Identity management**: When communication service based on the session initiation protocol is implemented for PNs, the identity definitions in ECMA TR/96 may be applicable to the service end points [2].

- **Security, privacy and firewalling**: Personalization of Nodes facilitates secure communications. Firewalling may be functionality on the Gateway Nodes.

- **Emergency calls**: When communication Service based on the session initiation protocol is implemented for PNs, emergency calling can be handled as addressed in ECMA TR/101 [3].

8 Standardisation Needs

This clause lists the standardisation needs for PNs and their extensions and in some cases specifications and their applicability and relevancy. Also note that some additional standardization gaps have been specified in Open Mobile Alliance (OMA) [27].

8.1 Quality

o End-to-end quality: Users require a certain level of quality from their Service that may be a combination of independent managed services and networks. There is no standardised query and negotiation mechanism for this case [7][8][9][10].

o Remote management of UPnP QoS using ECMA TR/96 [2], which is a 2007 result of PNP2008 together with IST-MUSE. The resulting contribution is HGI00863: "Remote management of UPnP devices using TR-069 auto configuration server".

8.2 Credential Management and imprinting

o Format for credentials (e.g. X.509 [6]),

o Method to generate credentials for a PN,

o Method or protocol to distribute credentials to a Device when creating a Node (imprinting),

o Method to revoke or erase credentials.

8.3 Node initialisation and configuration

o Format and elements of configuration data,

o Method to ensure a unique Node address assignment within a PN,

o Initial configuration protocol(s).

8.4 Uniform network interfacing

o How to describe the (e.g. quality, security) characteristics of a network interface, access network in a uniform way.

8.5 Network Cluster formation and maintenance

o Self-organisation and formation method,

o Discovery of other Nodes over L2 connections (e.g. IPv6ND/SeND, NHDP[16], NEMO [17]),

o Authentication and establishment of encrypted L2 connections between two Nodes using the imprinted credentials (e.g. 802.11i, RSA, AES).

8.6 Network Cluster routing

o Ad hoc routing for Network Clusters (e.g. IETF OLSR [14], IETF DYMO [15]),

o Multicasting or broadcasting (e.g. IETF SMF [16]).

8.7 Inter-Network Cluster routing and tunnelling

o Gateway to registry protocols (e.g. Host Identity Protocol (HIP) [19], Mobile IP, Dynamic DNS),

o NAT traversal (e.g. STUN, TURN [20]),

o Secure and dynamic tunnelling protocols (e.g. IKE [12], IPSec, TLS, SSL),

o Inter-Network Cluster routing protocols (e.g. NEMO [17]).

8.8 External communication

o   Automatic setup of translation between Node and external addresses (NATing).

8.9 Resource and service discovery and management

o   Service provisioning (e.g. DNLA [28], PUCC [29]),

o   Within PNs (e.g. Jini [30], UPnP [31], mDNS [23]),

o   Between EPNs and OPNs,

o   Proxy-related protocols,

o   Authorization and access control,

o   Resource location and discovery. Peer-to-peer signalling protocols, such as RELOAD [26] are being discussed in IETF.