A Network Architecture for Personal Networks[1]

Martin Jacobsson*, Jeroen Hoebeke†, Sonia Heemstra de Groot‡, Anthony Lo*, Ingrid Moerman†,
Ignas Niemegeers*, Luis Muñoz**, Mikko Alutoin††, Wajdi Louati‡‡, Djamal Zeghlache‡‡
*Delft University of Technology, The Netherlands, †Ghent University - IMEC, Belgium
‡Twente Institute for Wireless and Mobile Communication, The Netherlands,
**Universidad de Cantabria, Spain ††Technical Research Centre of Finland (VTT), Finland
‡‡Groupe des Ecoles des Télécommunications-Institut National des Télécommunications (GET-INT), France

***Abstract*— A Personal Network (PN) is a new concept related to pervasive computing with a strong user-focused view. Whereas several existing technologies can offer solutions to part of a person's future communication needs, there is very little work on combining these technologies into something a normal user can handle. It will undoubtedly be the network layer that should integrate a person's all devices and networks into one single network for the person: the Personal Network. This paper introduces a network architecture for PNs that can handle the dynamic and demanding situation a PN is facing. Discussions of some related network layer concepts, issues and possible solutions are given in the end of this paper.**

***Index Terms*— Personal Networks, Wireless Networks Architecture, Mobility, Self-Configuration, Self-Organisation**

I. Introduction

Future mobile and wireless systems have been discussed as visions for several years. New wireless technologies have been developed, such as Wireless Local Area Networks (WLAN) [4], Bluetooth [2] and other Wireless Personal Area Networks (WPAN) technologies [5]. All these technologies have triggered researchers and innovators to think about future mobile wireless systems that will address our need for communication and much more. As a consequence, new research fields are emerging, addressing different aspects of future mobile wireless systems.

A Personal Network (PN) [7] [16] is a new concept related to pervasive computing with a strong user-focused view that is being developed within the IST MAGNET project [9]. The origin of the PN concept is the Personal Area Network (PAN), which is the network that consists of devices in the close vicinity of the person. By integrating all of a person's devices and resources, not only those in his vicinity, but also those that are further away (such as devices at home, in the car or at work) and foreign devices and resources the person is granted access to, the PAN concept is extended into a PN. This extension will physically be made via infrastructure-based networks, vehicle area networks, a home network or multi-hop ad hoc networks. A person's PN is configured to support the person's applications and takes into account the person's context, location and communication possibilities. A PN must adapt to changes in the surroundings, be self-configuring and support many different types of networks and devices. The key to a successful PN realisation is a general network architecture that can bridge different technologies and offer a homogeneous and clear view to the end-user. Since a PN should address a person's all communication needs, a PN must include not only the person's wearable and wireless devices but also devices in the home, the car and in the office, etc. It will undoubtedly be the network layer that should integrate all these devices and networks into one PN and at the same time cooperate with existing networks such as infrastructure networks and other fixed networks. The network layer architecture we suggest in this paper provides a complete solution, which will make it easier for normal users to setup and maintain their PNs. The underlying link layer technologies will meet the different communication needs in the different environments. A fast wireless technology can meet the requirements of bandwidth demanding multimedia traffic in the home, whereas short-range power efficient technologies are more suitable for the network around a person on the move. The PN network layer will be the same in all these environments, but may operate in different modes to meet the requirements in the different environments. In this way, it is believed that communication between different environment and types of networks can function seamlessly.

The rest of this paper will further explain the details of the overall PN architecture and in particular the network layer architecture. Section II will describe a potential application and some motivations of PN, whereas section III lists some existing proposals. Section IV introduces the three-layer abstraction level view of a PN and some relevant terminology. In section V we discuss the requirements imposed on the PN and translate them into a general network architecture framework. Finally, section VI goes further in depth by discussing in more detail the network protocols running on top of this architecture. Conclusions are given in Section VII.

II. An Application Scenario

Transportation and logistics represent a major business industry employing millions of truck drivers. Each day, these persons spend hours in their vehicle while driving, waiting or sleeping and they are often away from home several days at a time. Offering these persons the ability to stay in touch with their family by creating a virtual home environment, offering them the ability to stay connected with their company and clients or offering them the possibility to contact their

[1]The work presented here was funded by the Commission of the European Union under the project IST MAGNET.

colleague truck drivers, could have great commercial potential taking into account the large number of truck drivers world wide.

Consider a truck equipped with a mobile phone, broadband Internet access, TFT display, headset, etc. forming a network of cooperating devices. When finished working, a truck driver could set up an Internet connection to his home. At home, a network of cooperating cameras, speakers, headsets, provides the truck driver with a virtual home environment. Through this environment, he can virtually walk around, seeing his family, talking with them, playing games? When driving, the truck driver can listen to his digital music collection by streaming it from a server in his network at home. When truck drivers stop at a parking, they can read their e-mail, search for colleagues, play a game with other truck drivers, etc. When the truck driver arrives at a client, his PAN can connect to the client's company network and exchange necessary documents. The documents can be digitally signed, handed over to the client and a copy can be uploaded to the truck driver's company, reducing the administrative burden.

Whereas several existing technologies can offer solutions to part of this scenario, there is very little work on combining these technologies into something a normal user can handle. In addition to offer the user instant access to services and communication, PN also needs to be easy to use, setup, configure and maintain as well as fast and secure. The target of PNs is to provide users with exactly that.

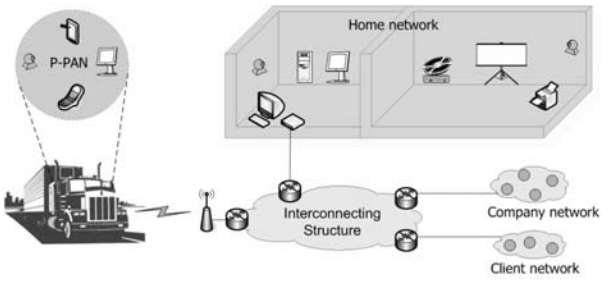

Fig. 1. Virtual home truck scenario

III. Existing Solutions

Most technologies focus on a particular aspect of future wireless communication. Here we list proposed solutions that try to meet more of a person's communication needs. In a proposal from the University of Illinois at Urbana-Champaign and the Mobius project [8], they group devices in close vicinity into so called Mobile Grouped Devices (MOPEDs). Each MOPED is connected to a proxy (some kind of home agent) via an infrastructure connection. MOPED is not suitable for PN because it is still too dependent on the proxy and the infrastructure. Furthermore, MOPED does not address direct ad-hoc communication with other person's MOPEDs and is therefore still too limited to support the PN vision. The Mobile VCE project has defined a concept called Personal Distributed Environment (PDE) [3]. PDE has a very similar vision to PN, but has no clear network architecture yet. IXI Mobile [6] has a commercial product around a concept called Personal Mobile Gateway (PMG). It is basically a mobile phone with a WPAN-technology that has been extended to better manage a person's WPAN. PMG-enabled devices can communicate with each other and can also use the PMG-enabled mobile phone to connect to the infrastructure. However, all services are controlled by the operator and all external communication has to go through the operator's networks and this will not be able to meet a user's all future communication needs.

IV. The Abstraction Level View and Terminology

A. The Three Abstraction Level View

As shown in Figure 2, the IST MAGNET project [9] [10] has proposed a PN architecture, which is composed of three abstraction levels; the connectivity, the network and the service abstraction levels.

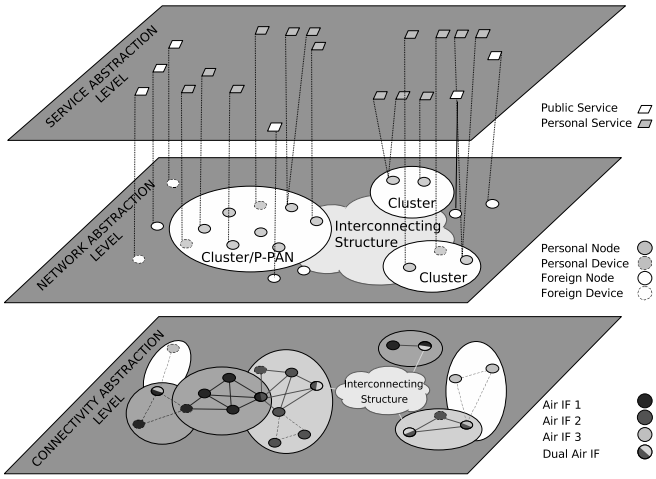

Fig. 2. The abstraction level view

The connectivity abstraction level consists of various wired and wireless link layer technologies, organised in radio domains, including infrastructure links. The link layer will allow two nodes implementing the same radio technology to communicate if they are within radio range. To allow any two nodes within a PN to communicate, a network abstraction level is needed. This level divides the nodes into Personal and Foreign Nodes and Devices, based on trust relationships. Only nodes that are able to establish long term trust can be part of a user's PN. The meaning of "my" in MAGNET should be understood in this loose sense as sharing and borrowing devices in some point of time is also taken into account (for example family devices, devices from work can also be "my devices") through long term trust establishments. Personal Nodes that have such a long term common trust relation form Clusters and Clusters can communicate with other Clusters via infrastructure. The next section will further develop the architectural concepts of the network abstraction level. The highest level in this architecture is the service abstraction level, which incorporates two types of services; public and private services. Public services are offered to anyone whereas private services are restricted to the owner or trusted persons by means of access control and authentication.

B. Network Terminology

This section gives an overview of the networking terminology that will be used in the remainder of the paper.

Device Any communicating entity.

Node A Device that implements the Internet Protocol (IP).

Personal Node/Device A Node or Device related to a given user with a pre-established trust attribute. These Nodes and Devices are typically owned by the user. However, any Node or Device exhibiting the trust attribute can be considered as a Personal Node or Device.

Private Personal Area Network (P-PAN) A Private Personal Area Network or P-PAN is a dynamic collection of Personal Nodes and Devices around a person. The privacy in a P-PAN is guaranteed by mandating a mutual trust relationship between every Node and Device in the P-PAN.

Cluster A network of Personal Devices and Nodes located within a limited geographical area (such as a house or a car), which are connected to each other by one or more network technologies and characterised by a common trust relationship between each other.

Personal Network (PN) A Personal Network (PN) includes the P-PAN and a collection of remote Personal Nodes and Devices in Clusters that are connected to each other via Interconnecting Structures.

Interconnecting Structure Public, private or shared wired, wireless or hybrid networks, such as a UMTS network, the Internet, an intranet or an ad hoc network.

Foreign Node/Device A Node or Device that is not part of the PN. Foreign Nodes can either be trusted or not trusted. Whenever trusted, they will typically have an ephemeral trust relationship with a Node or Device in a PN.

Gateway Node A Personal Node within a Cluster that enables connectivity to Nodes and Devices outside the Cluster either directly or through the Interconnecting Structure.

Edge Router A Node in the Interconnecting Structure that can communicate with Gateway Nodes and can support them by offering PN functionality. In case no Edge Routers are present or they are not trusted, the Gateway Nodes have to provide this functionality.

PN Agent An infrastructure-based management framework that keeps track of all Clusters in a PN.

V. Network Architectural Framework

The network level has to be as independent as possible from the underlying connectivity level so that current and future wireless communication technologies can be supported. In the Internet, IP was designed to meet this requirement and therefore IP is the proposed packet format also for PNs. The choice of IP also makes it easier to connect the wireless world with the Internet, which will be important also in the future.

In our architecture, the home network of a person will be one Cluster, the car network another, the P-PAN around the person a third and so on. All Clusters, including the P-PAN, work as local networks and therefore need their own independent networking solutions such as self-configuration, self-maintenance, naming, addressing, routing, etc. However, the solutions used in the Clusters and the P-PAN will be compatible so that the Clusters and the P-PAN can merge and split without extra effort. In terms of the network-level organisation, the P-PAN is just a Cluster. The formation and maintenance of Clusters is a purely local process and does not need any support from infrastructure. Clusters are dynamic in nature. Nodes are switched off and on as well as roam and might suddenly show up in a different Cluster. Clusters can split when a person leaves some devices behind and Clusters can merge when a person arrives home with his devices.

When Clusters want to communicate with remote Clusters through their Gateway Nodes, they need to be able to locate each other, a requirement that will be met by the PN Agent concept, explained in the next section. Further, inter-Cluster communication needs to be secure and maintained when Clusters merge, split and their Nodes roam or are activated/deactivated. This will be accommodated through dynamic tunnel establishment mechanisms. Again, solutions to naming, resource and service discovery, addressing, routing, etc. are needed to enable inter-Cluster communication.

Last but not least, Personal Nodes and Devices will often be battery powered and limited in computational resources. Providing and implementing a complete, secure, dynamic and fast network architecture on top of these Nodes can consume a lot of resources which can decrease the lifetime. To this end, the network architecture will introduce the notion of Edge Routers, which can support the Personal Network Nodes in providing the required functionalities such as tunnel establishment or NAT capabilities for communication with Foreign Nodes, thereby taking the burden and complexity away from the less powered Cluster Nodes and Devices.

The above discussion leads to the general network architecture depicted in Figure 3. The figure shows two Clusters of Personal Nodes and Devices connected over the Interconnecting Structure by a dynamic, secure tunnel to form a Personal Network. The PN is supported by a PN Agent and one Cluster uses the support of an Edge Router. This architectural framework will form the basis of a PN, on top of which the relevant networking protocols will run in order to meet all communication needs of the PN user.

VI. Network Solutions

A. PN Organisation and Maintenance

A PN can have multiple Clusters that are geographically dispersed, but have access to each other via the Interconnecting Structure. In order to form a PN and realise inter-Cluster communication, two requirements need to be fulfilled. First of all, the Clusters need to be capable of locating each other in order to establish tunnels between them. Secondly, once the PN has been formed, it should be able to maintain itself regardless of Node mobility.

For these requirements to be fulfilled, we introduce the concept of a PN Agent, a management framework that can be either centralised, under the control of a single provider or in a fixed Cluster, or distributed over multiple providers or operators. Clusters that have obtained access to the Interconnecting Structure announce their presence to this PN

Agent. This information should at least include which PN the Cluster belongs to, the point of attachment to the Interconnecting Structure, i.e. the IP address of the Gateway or Edge Router through which the Cluster can be reached and some credentials to verify this information. When Clusters move, this information must be kept up-to-date. As a consequence, the PN Agent will function as a database that tracks the PN Clusters. For more details see [13].

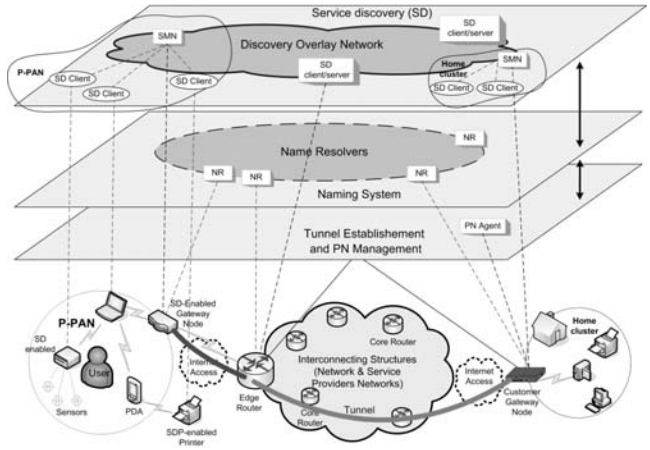

Fig. 3. General network architecture

B. Edge Router Tunnelling Capabilities

The dynamic inter-Cluster tunnelling functionality can reside completely in the Gateway Nodes in the Clusters and the PN Agent. Whenever a Gateway Node is not sufficiently capable it can delegate some tasks to the Edge Routers in the provider premises, if the user trusts the provider. This offloads the Cluster Gateway Nodes from unnecessary burden (such as tunnel establishment and management, context management, transcoding, name and address resolution, translation and more). Edge Routers can prove valuable in this sense but also for providing support to the PN in general by assisting in device, resource and service discovery. Whenever viable, the Edge Routers can house some of the PN Agent functionality. Consequently, the Edge Router tunnelling capability as well as other key functions required for networking purposes (naming, addressing, discovery and so on) can be distributed between the Cluster Gateway Nodes and the providers Edge Routers. Edge Routers could also be programmable and implement the separation principle between the router data, control and management planes. Such flexibility would allow services in the PN Clusters or in network providers to gain some secured control over the physical routers.

C. PN Addressing and Routing

In this section we will discuss two different solutions for PN addressing and routing using Edge Routers and dynamic tunnelling. Both solutions will also work without the support of Edge Routers. In that case, the Gateway Node of the Cluster has to perform the Edge Router tasks. However, if the Gateway Node is battery powered, it is better to let the Edge Router perform these tasks whenever possible.

1) Proactive routing, with flat addressing: Using a flat addressing scheme, each Personal Node will have a unique intra-PN IP address that consists of a PN prefix, which identifies a specific PN, and an identifier that uniquely identifies each Personal Node within the PN. This address needs only to be assigned the first time a Node joins the PN. This scheme has the advantage that address assignment and duplicate address detection only incur a very low overhead and could easily be managed, for instance by the PN Agent (E.g. the naming system). In addition, merging or splitting of Clusters does not lead to any additional overhead. However, such an address does not provide any information on the location of the Node within the PN. This can be solved by deploying a proactive routing protocol, based on ad hoc routing techniques, which efficiently uses the intelligence of the Edge Routers. Proactive ad hoc routing information from within a Cluster is propagated up to the Edge Routers, which exchange this information amongst each other. As a consequence, each Personal Node will have a route to all other Nodes in its Cluster and a default entry to its Edge Router and each Edge Router will know for each Personal Node, the Cluster where the Node is located.

As Edge Routers maintain and exchange PN routing information, this approach assumes that the Edge Routers actively establish and maintain tunnels between all Clusters of the PN, based on a tight coupling with the PN Agent. As not only routing information, but also naming and service information can be exchanged proactively, the different information flows can be aggregated and coupled in order to further reduce the overhead.

2) Reactive routing, with Cluster-based addressing: When deploying a Cluster-based addressing scheme, each Node will have a unique intra-PN IP address, consisting of a PN prefix, a Cluster prefix and an identifier that uniquely identifies the node within its Cluster (The Node identifier could of course be unique in the whole PN). This addressing scheme involves a higher addressing overhead as network dynamics, such as a Node is leaving or joining a Cluster or two Clusters are merging or splitting, require updating of addresses. On the other hand, the address now provides information of the location of a Personal Node within the PN. Therefore, Edge Routers do not need to exchange routing information and thus only need to establish a tunnel between two Clusters if required by the applications. Within a Cluster, both proactive or reactive routing can be used when a Personal Node wants to communicate with a Node in a remote Cluster and has obtained its address (through the naming or service discovery framework), the Node can forward the packets to the Edge Router, which then can establish a tunnel to the remote Cluster based on the Cluster prefix and the information provided by the PN Agent. As active Edge Routers are used, naming could also be tightly coupled with the PN Agent, meaning that the name resolvers will not only provide the address of the destination node, but also the IP address of the point of attachment of the Cluster in which the destination Node resides. The Node that wants to establish a connection can then send a management packet to the Edge Router that initiates the establishment of a tunnel for the communication session.

3) Addressing Conclusions: Both approaches provide a PN solution, but have completely different implications on the interaction between and importance of the different components of the PN network architecture and the functionality of the Edge Routers. Choosing one of the two solutions will depend on what the user is willing to pay for PN management to the service providers. Both solutions are currently being analysed in terms of performance and scalability.

D. Resource and Service Discovery and Naming System

Figure 3 also shows the naming system as well as the service discovery system. The role of resource and service discovery (SD) and naming is to discover Devices, Nodes, resources and services automatically and hide addressing from users by using names to describe objects. The service discovery is performed using a multi-tier approach. A Service (discovery) Management Node (SMN) discovers and manages the services in its corresponding tier, and interacts with its upper tier SMNs. As an example, the master of a Bluetooth radio domain can act as an SMN for its piconet, discovering the services within that radio domain, registering them in an upper tier SMN, i.e. the P-PAN or Cluster SMN. At the PN level, SMNs of the P-PAN and Clusters interact with each other to manage the whole set of services within the PN. The same approach can be followed for discovering resources, as well as context information. For more details see [11] [12].

Names are resolved by the naming service typically through name resolvers, such as the well known DNS or another paradigm. The reason to have names is to hide irrelevant information from users and to give a human-understandable identity of Devices, Nodes and services. As PN is continuously dynamically changing, the addresses may change. The user should not be concerned by the addresses of the Devices and Nodes but simply see the same name as a verification of using the same resource (Device/Node). To this end, the naming architecture should provide a flexible naming scheme that provides a local name space for the PN, enabling naming of the PN, its Clusters, its Devices/Nodes and services. In addition, this scheme should closely interact with the PN resource and service discovery.

When a Cluster connects to the Interconnection Structure, it propagates the names of its Nodes and Devices that consequently can be advertised by the Gateway Node or the Edge Router to other Clusters. Each Cluster could add an attribute in the naming system that identifies the Cluster. Naming systems based on intentional names such as INS [1] or other names [18] or identities [15], on DNS and rendezvous server paradigms [14] [17] are all capable of describing Devices, Nodes and services using names and binding these names to addresses to be used by transport networks for networking. Either names are resolved directly onto IP addresses or Uniform Resource Names or Locators are returned by the naming system. The name space in INS is quite powerful and is capable of providing a full description of Devices and Nodes in terms of characteristics, capabilities, location, type and even access rights. The naming systems mentioned here are currently under investigation within MAGNET.

VII. Conclusions

A PN extends and complements the concept of pervasive computing by creating a personal distributed environment where persons can interact with various devices not only in the close vicinity but potentially anywhere. The network layer is the glue that binds all a person's devices together into one PN. We proposed a general network layer architecture that can bridge different technologies and offer a homogeneous and clear view to the end-user. The network layer is based on a long term trust relationship that can offer communication between a person's all devices in a secure way. In the end, solutions were presented to some of the most important networking issues needed to realise intra-PN communication.

Acknowledgment

The authors would like to acknowledge the contributions of the MAGNET consortium (IST 507102) and specifically the networking work package of the project for the contributions to this joint paper that is a synthesis of the ongoing research and development activities in the project.

References

[1] William Adjie-Winoto, Elliot Stewart, Hari Balakrishnan, Jeremy Lilley, The design and implementation of an intentional naming system, In *Seventeenth ACM Symposium on Operating Systems Principles (SOSP'99)*, Charleston, United States, December 1999.

[2] Bluetooth SIG, *Specification of the Bluetooth System - Version 1.1 B*, http://www.bluetooth.com/, 2001.

[3] John Dunlop, R.C. Atkinson, James M. Irvine, D. Pearce, A personal distributed environment for future mobile systems, In *IST Mobile & Wireless Communication Summit*, Aveiro, Portugal, June 15-18, 2003.

[4] IEEE 802.11 - The Working Group for Wireless Local Area Network (WLAN) Standards, http://www.ieee802.org/11/.

[5] IEEE 802.15 - The Working Group for Wireless Personal Area Network (WPAN) Standards, http://www.ieee802.org/15/.

[6] IXI Mobile, http://www.ixi.com/.

[7] Martin Jacobsson, Jeroen Hoebeke, Sonia Heemstra de Groot, Anthony Lo, Ingrid Moerman, Ignas G. M. M. Niemegeers, A network layer architecture for personal networks, In *The First MAGNET Workshop*, Shanghai, China, October 17, 2004.

[8] Robin Kravets, Casey Carter, Luiz Magalhaes, A cooperative approach to user mobility, *ACM Computer Communications Review*, Volume: 31, Pages: 57–69, October 2001.

[9] IST MAGNET project, http://www.ist-magnet.org/.

[10] IST-507102 MAGNET/WP2.1/INT/D2.1.1/PU/001/1.0, *Conceptual secure PN architecture*, January 2005.

[11] IST-507102 MAGNET/WP2.2/UniS/D2.2.1/PU/001/1.0, *Resource and Service Discovery: PN Solutions*, December 2004.

[12] IST-507102 MAGNET/WP2.4/AAU/D2.2.2/PU/001/1.0, *Context Discovery: PN Solutions*, December 2004.

[13] IST-507102 MAGNET/WP2.2/IMEC/D2.4.1/PU/001/1.0, *Architecture and Protocols for Ad-hoc Self configuration, Interworking, Routing and Mobility*, December 2004.

[14] Michael Mealling, *The Network Solutions Personal Internet Name (PIN): A URN Namespace for People and Organizations*, IETF RFC3043, January 2001.

[15] Robert Moskowitz, Pekka Nikander, *Host Identity Protocol Architecture*, IETF Internet-Draft (Expired), draft-moskowitz-hip-arch-06, June 27, 2004.

[16] Ignas G. M. M. Niemegeers, Sonia M. Heemstra de Groot, Research issues in ad-hoc distributed personal networking, *Wireless Personal Communications: An International Journal*, Volume: 26, Issue: 2-3, Pages: 149–167, Kluwer Academic Publishers, August 2003.

[17] Paul Vixie, Susan Thomson, Yakov Rekhter, Jim Bound, *Dynamic Updates in the Domain Name System (DNS UPDATE)*, IETF RFC2136, April 1997.

[18] Qiaobing Xie, Randall R. Stewart, Maureen Stillman, Michael Tuexen, Aron J. Silverton, *Endpoint Handlespace Redundancy Protocol (ENRP)*, IETF Internet-Draft, draft-ietf-rserpool-enrp-11, February 18, 2005.