# New Role of Policy-based Management in Home Area Networks – Concepts, Constraints and Challenges

Annie Ibrahim Rana, and Mícheál Ó Foghlú, *TSSG, WIT, Ireland.*

*Abstract*— **The management of Home Area Networks (HANs) is problematic. On the one hand there are increasing numbers of IP enabled devices that are connecting to the HAN (wired and wirelessly), some of which need to be managed, especially in terms of granting external access to certain services running on certain devices (e.g. home security, home monitoring, external media access). On the other hand, of any area of network management, the home network is the one where there is least likely to be a capable network manager physically there. So the Internet Service Providers (ISPs) have an interesting challenge: do they leave the management to the user and risk the degraded user experience that results, or do they offer to help manage the network for the home users, at potentially very high costs? This means that automated or autonomic (self-governed) network management approaches could potentially offer a solution. Policy-based Network Management (PBNM) is a promising network management paradigm that potentially makes administration tasks easier and lessens the complexity involved in the management process for the end user. In this article, we present the potential for PBNM in HAN. Significant concepts, constraints and challenges related to the PBNM implementation are discussed. The potential is that ISPs can use PBNM to improve end user experience in HANs without incurring excessive support costs.**

*Index Terms*— **Network Management, Policy, Policy-based network management, Home area network. Policy-based traffic management, autonomic network.**

## I. INTRODUCTION

MANY papers cite Mark Weiser's seminal article on ubiquitous computing [12] published nearly 2 decades ago, that predicted the disappearance of the computer as more devices became networked within the home and other environments. Much progress has been made towards this vision, and many devices are now more networked than previously, including many devices in Home Area Networks (HANs), and people's mobile phones. This paper argues that the key challenge is today is less about the design of exciting new such devices with non-traditional interfaces that are embedded everywhere. Instead most of us face the more mundane challenge of how to integrate and access the existing slightly clumsy devices we have that are already network capable. At its heart, this is a network management challenge. For example how many of us can access our music collections from inside the home on various devices, and how many of us can do so remotely? How many of us can watch the TV we have paid for at home, from a remote location? The problem is that, even though many (though by no means all) HAN devices are IP enabled, there is a lot of network management involved in setting up these devices to work, and to be accessible externally in a secure way. This there is a prevalence of single service solutions: one solution for home security video monitoring, one for remote TV access (e.g. SlingBox), and so on.

Thus the growing complexity of Information and communication technologies (ICT) infrastructure involved in HANs and services threatens to undermine the very benefits that ICT aims to provide. Complexity leads to difficulty in management, and this potentially leads to unreliability. In a complex network of heterogeneous systems, management of different network resources is a highly complicated and nontrivial task. Management involves configuration of network resources, assurance of quality of service, provision of dynamic network changes and resources, and implementation of security measures and access rights; performing and repeating these management tasks for every network resource can be time consuming, involve complexity, and be error prone.

The promise is that, by introducing one intelligent gateway device into the home network, it could potentially help configure the devices and services, within the constraints of an overall policy.

Policy-based Network Management (PBNM) [4, 5] is a promising network management paradigm to potentially make administration tasks easier for end users. It is often part of a wider autonomic networking approach (i.e. self-governing) [1] that aspires to reduce the human intervention, reduce cost and reduce errors. In this article we present a new role of PBNM in

Manuscript received October 31, 2009. This work is supported by the SFI SRC FAME award (Ref: 08/SRC/I1403).

A. Ibrahim is with the Telecommunications Software and Systems Group, Waterford Institute of Technology, Waterford, Ireland. (e-mail: arana@tssg.org).

M. OFoghlú is with the Telecommunications Software and Systems Group, Waterford Institute of Technology, Waterford, Ireland. (e-mail: mofoghlu@tssg.org).

HAN management, which is more user requirements' centric, essentially a lighter weight approach focused on managing a small home access network, from the ISPs' perspective.

This article is structured as follows: we briefly summarize current research in the area of policy-based management; then we present the role of PBNM in HAN to manage user requirements, e.g. Quality of Service (QoS). Finally, we summarize the article and discuss open PBNM related issues in HAN management.

## II. Policy-based Network Management

Policy-based Network Management (PBNM) is management paradigm in networking that separates administration operations from other basic network operations. It provides a flexible and robust mechanism to allocate network resources and services like bandwidth allocation, quality of service, access rights, traffic prioritization and security to different network elements. It results in increasing quality of work, efficiency, adaptability, coherent network behavior, flexibility and reduced maintenance cost regarding to network management [4, 5].

### A. *Historical Background*

Policy-based Management gained widespread attention in late 1990s when Internet Engineering Task Force (IETF) formed a Policy Framework Working Group (PFWG) to define architecture and information model for policy-based management of Quality of Service (QoS) in IP networks. Distributed Management Task Force (DMTF) also developed information models for network and policy management applications and later joined IETF Policy Frame Working Group to standardize IETF policy information model. Many IETF and DMTF standards have been introduced for policy-based management of networks [4].

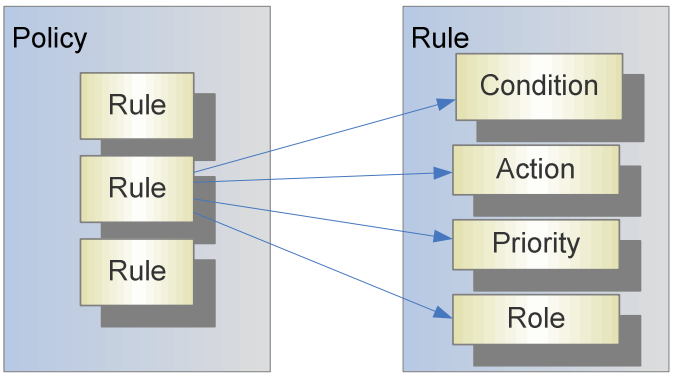


Fig. 1: Policy anatomy.

### B. *Policy Definition*

There is no standard way of defining policy but there are some definitions put forward by academic researchers. According to [6], policy is predetermined action statement for such action patterns that are repeated by entities involved in a network under certain systems conditions when they are met. The paper [7] defines policy as a goal or course of action to guide present and future network decisions. More concisely, policy is set of rules to administer, manage and control the access to network resources and services.

There are mainly two types of network operations: Core network operations, management operations. Network management can be further broken into three major types of management tasks: Network QoS Management, Network Security Management, and Network Configuration Management. QoS and security, both requires configuration management and are dependent on it. However network policies can be classified generally into the following six broad categories [5]:

1. Performance Management Policies
2. Security/Access Control Policies
3. Quality of Service Policies
4. Administrative/Configuration Management Policies
5. Fault Management Policies
6. Customized/Event Condition Action Policies

In this report we are focusing on QoS management policies for home area network. A policy gives abstraction to control network resources/elements. By the using policy-based QoS management, network resources can be used efficiently. We would discuss the benefits of this approach in later sections.

### C. *PBNM Architecture*

IETF PFWG has defined a policy management architecture that is considered as best approach for internet policy-based management.

#### 1) *Components*

Following are the major components of policy-based management model with few additional components indicated with asterisk [5]:

Policy Management Service (PMS) / Policy Console (PC): This service provides an interface for specifying, editing, and administering policy for network management.

Dedicated Policy Repository (DPR): This is location to store and retrieve policy information, rules and standards.

Policy Decision Point (PDP): This is a resource manager also called as policy server that is responsible for handling events and making decisions based on those events

Policy Enforcement Point (PEP): It enforces the policies based on the "if condition then action" rule sets it has received from the PDP.

Local Policy Decision Point (LPDP): This is smaller version of PDP that exists within a network node and is used in cases when a policy server is not available. Basic policy decisions can be programmed into this component.

Policy Communication Protocols: Two types of protocols are involved: a protocol to read / write data from the policy repository (e.g. LDAP), and a protocol to communicate between PDP and PEP (e.g. COPS, SNMP).

According to [9], the functionality of a Policy Enforcement Point can be further subdivided into:

Policy Execution Point (PXP): This is location for carrying out specified policy actions.

Policy Verification Point (PVP): This is a location for ensuring that the policy actions executed correctly and, more importantly, do they meet the desired requirements.

*2) Policy Anatomy*

The IETF and DMTF organizations are jointly developing a standard model for policy data [2, 11] as shown in figure 1.

A policy rule contains four major components: Condition, Action, Priority, and Role. The Role indicates the context in which a policy rule is relevant. The Priority indicates the relative importance of the policy rule to avoid policy conflicts. The Condition indicates the state when policy rule will be applicable. The Action part of a policy rule specifies the action to be taken if the rule is applicable.

### *D. Policy Abstraction Levels*

There are a number of levels in a policy specification. This is sometimes called a policy hierarchy [10] or abstraction levels, and represents different views on policies, relationships between policies at different levels of this hierarchy, or abstractions of policies for the purpose of refining high-level management goals into low-level policy rules whose enforcement can be fully automated.

TABLE I
POLICY ABSTRACTION LEVELS

| Abstraction Level | Description |
|---|---|
| Business | These policies are domain, mechanism, devise and instance independent. They contain no specification how policy would be realized and no system and network elements are mentioned to support the policy. |
| Domain | These policies are mechanism, device and instance independent, and they are translated into domain specific format. Policies are not assigned to any specific device or network element, nor does it describe how to implement. |
| Mechanism | These policies are device and instance independent, specified to realize a mechanism. They cover mechanism implementation details. |
| Device | These policies are instance independent. These policies involve device specific parameters and mechanism implementation details. |
| Instance | This is the most specific expression of a policy. All parameters are expanded to all network elements that are involved in enforcement process of this policy. |

The paper [10] considers there are three major levels but paper [5] considers five policy abstraction levels and [8] refers them as policy continuum. Each abstraction level defines policy scope within network. These abstraction levels are interrelated and can be defined in terms of each other. Abstraction levels are defined in table 1.

### *E. PBTM Work Model*

Policies are created, modified and stored in repository through policy management service using policy management console. Policies are stored in repository. Stored policies are retrieved by policy decision point server and enforced at policy enforcement points, the network elements (router, bridges, servers, desktop etc.) Figure 2 shows very simple PBNM work model.

High level/Abstract policies are translated into specification level policies. Policy translation can be done by using policy specification language, rule based approach or formal logic based approaches.

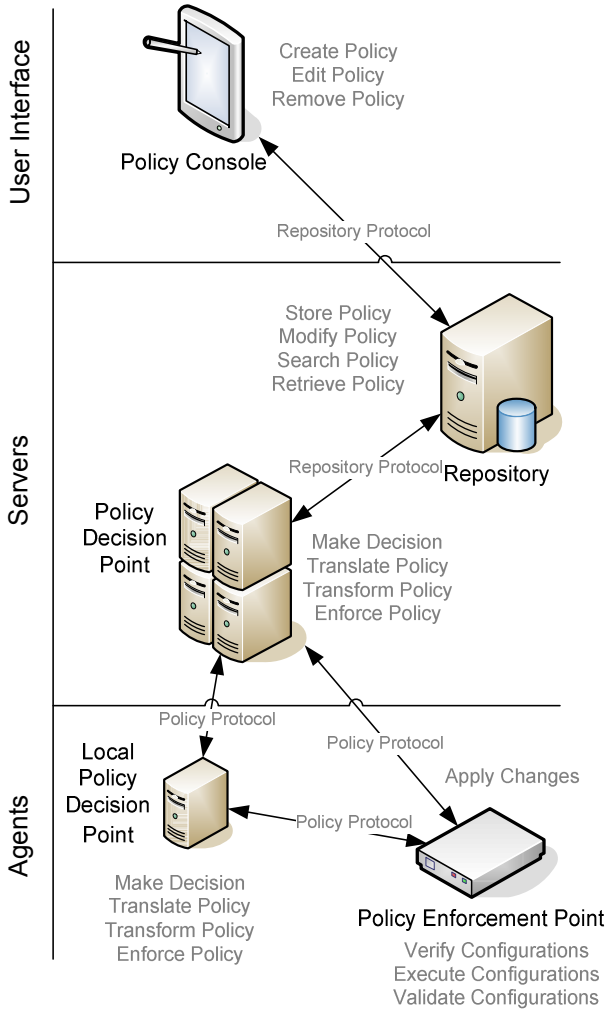


Fig. 2: PBTM work model.

Specification level policies are further transformed into low level policies / configurations, which are applied to network devices/agents. When any triggering event happens, new policy decisions are made and applied to network automatically as shown in figure 2.

### *F. PBNM Communication Methods*

PBNM communication between PDP and PEP can be implemented in many ways [5], HTTP, COPS and SNMP etc. Two most commonly used methods COPS and SNMP are discussed below. The figure 3 shows communication between PDP and PEP through SMTP and COPS.

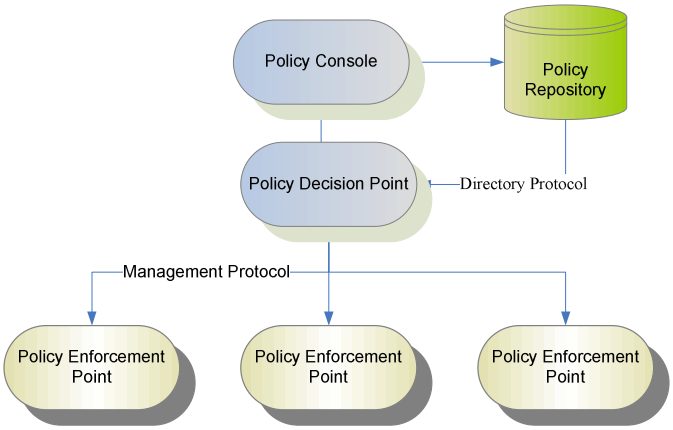


Fig. 3: PBNM typical architecture.

*1) Common Open Policy Services (COPS)*

In COPS approach, policies are translated into configuration rules or instructions that are downloaded to network devices via a protocol 'common open policy services'. These instructions are stored in a directory for decision making and sharing. The directory is 'Lightweight Directory Access Protocol' compliant and it is updated dynamically. Network learns the changes dynamically and enforces the updates on managed devices.

*2) Simple Network Management Protocol (SNMP)*

In SNMP approach, management system contains several network nodes (also called as SNMP agents) which have access to management instrumentation, command responder and a notification originator, at least one manager (also called as SNMP entity) that contains a command generator and notification receiver. It also contains a management protocol to convey management information between the SNMP entities.

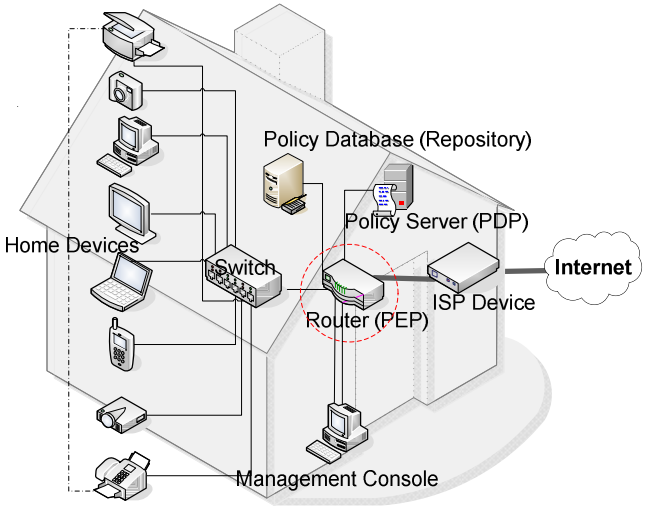


Fig. 4: PBTM in HAN.

## III. DISCUSSION

A network usually has two types of network operations: core and management operations. According to [16], network management is a set of activities, methods, procedures, and tools that is related to the operation, administration, maintenance, and provisioning of networked system. A home area network (HAN) is a residential local area network that connects different devices within a home; it may also connect the devices to another network. Based on this definition, home networking can be divided into two groups keeping in mind the scope of management:

1. Access network / device networking
2. Device / device networking

Network management in the later type of networking is significantly different from the management in access or core networks. Home networking uses a wide variety of existing cabling or wireless access points using technologies that have varying underlying bandwidth. HANs are no less complex than any other networks; in fact, there is usually no control upon what is deployed in a network management perspective. Potentially the HAN is the most extreme case of a heterogeneous network.

Users without much network management knowledge often install the home networking equipment and they usually do not desire to actively manage their networks. The applications in the HAN tend to be multimedia intensive with a wide variety of bandwidth requirements, which sometimes are beyond the network capability and the complexities are hard to understand for the HAN users. The latest trends in the usage of HAN -i.e. multimedia applications, intelligent home appliances etc, have opened a great deal of work in the domain network management in HAN. Fulfilling the HAN users' requirements and ensuring QoS on the network require different techniques than the traditional techniques used in managing the core and access networks infrastructure. However, very less focus has been given to QoS issues in HAN. Most of QoS state-of-art focuses on access and core network but we know that edge networks also need equal attention to achieve end-to-end QoS. PBNM can play a significant role in managing home networks focusing on users' requirements. One intelligent gateway device to control all outgoing and incoming traffic, which can be configured according to user requirements through a policy manager, can make HAN management much easier. The paper [3], proposes similar solution but it focuses more on intelligent control centre (ICC) to connect all other networks with in HAN e.g. Power Line Network, PC Network, Wireless Network, Home Automation Network, and Home Gateway. But it doesn't discuss that how that ICC would be managed by the HAN users.

We suggest an intelligent residential gateway device by introducing a policy manager to enforce the policies and an autonomic manager to supervise the gateway device. Figure 4 shows an autonomic PBNM model, this model would allow HAN users to configure their gateway device according to their requirements .e.g. user can prioritize different types of network traffic. The role of autonomic manager is to configure the gateway device automatically. We have deployed a HAN testbed [17] in our research lab and successfully executed the experiments to observe the effect of policies in managing the

home area network traffic. In this paper we have listed the issues and problems that we came across during our experiments. In following sections some of PBNM advantages and constraints in HAN are discussed.

*A. Management Advantages*

Following are some of the advantages of using PBNM in HAN:

- Controlling resources: Policies can be used to control different network resources e.g. printers, directory folders etc. Access to different resources can be made limited to different network users -e.g. Children computers can not access internet after 8 PM.
- Deploying and configuring resources: Policies can be used for auto deployment and configuration of different devices -e.g. backup certain folder contents on my computer onto the disk server when my computer gets connected to the network.
- Monitoring resources: Policies can be defined to monitor performance of the network devices -e.g. printer should not accept more than 2 printing job at a time.
- Bandwidth allocation: Policies can be defined to allocate fixed bandwidth to particular network service or user applications -e.g. all video network traffic would get X Kbps bandwidth after 5 PM and Y Kbps bandwidth after 8 AM.
- Load balancing: Policies can be defined to balance the network load on a particular resource or the load on the network itself -e.g. if there X number of jobs at Node A then send all other jobs to Node B.
- Authorization: Policies can be defined specifying access rights to network resources, which are related to network security -e.g. XYZ person can not access network resources after 5 PM.
- Configuration management: Policies can be defined to establish and maintain consistency of network resources, their functional and physical attributes with the network requirements.
- Fault management: Policies can be defined to detect, isolate, and correct malfunctions in the network.
- Security management: Policies can be defined to protect network from unauthorized access by employing security services and mechanisms.
- Performance management: Policies can be defined to evaluate and report the behavior of network resources and the effectiveness of the network services.
- Bandwidth management: Polices can be defined to measure and control the network traffic on a network link to avoid congestion, which would result in poor performance.

*B. Management Constraints*

Traditional network management approaches lack the flexibility to configure/reconfigure the network elements according to network requirements unless it is accomplished manually. PBNM is promising network management paradigm to make administration tasks easy and less complex. However there are certain constrains implied by the home network requirements:

- Lack of Standards: There is no standardized approach for management of heterogeneous home networks.
- Lack of Simplified Techniques: Techniques and tools play a great role in network management but unfortunately there are not many simple techniques and tools available for managing home networks.
- Lack of Expertise: Usually lack of technical skills and the level of expertise of HAN users in the domain of network management make it more complex because traditional approaches require high level of skills and domain knowledge.
- Static Configurations: Static configurations of network resources make network management static as well, which lacks the adaptability of network with the change in network requirements.

*C. PBNM related Challenges in HAN*

Probably the biggest issue is that the HAN devices may be so cheap that it is typically sold as "unmanaged". However, there are still some basic network management issues, which are required to be addressed to make policy-based network management / configuration a reality in HAN. PBNM has emerged as a new paradigm for managing network elements, although it is beyond its infancy and its emergence in 1999 does not equate to maturity but there are some challenges associated with it, which require immediate attention.

Following are two types of PBNM challenges: generic PBNM challenges and HAN-specific PBNM challenges. Some of the generic PBNM challenges are listed here:

- There is no standard policy specification language to specify common policies to multiple and heterogeneous implementations e.g. configuration across multiple administrative domains and diverse network devices (from different vendors). There are number of attempts and good initiatives taken by PONDER [13], HP [14] and REWERSE [15] but they are not widely adopted. There is no need to reinvent the wheel but need of the hour is to standardize the existing policy specification languages.
- Standard techniques and mechanisms are required to resolve inter-policies conflicts at all different levels of abstraction, conflicts can also arise at same of level.
- Autonomic approaches are required for refinement of policies from high-level to lower-level policies and ultimately translation or transformation of policies into configurations (machine or vendor specific).
- Techniques to validate and verify policies and configurations are also required. Validation is required to make sure that policy has come through the right channel and confirm its validity of syntax and semantics. Verification is to check if a policy has met its goals after it is enforced.
- There is also lack of generic tools to author policies for network management. PONDER has developed a policy editor that can be plugged in with other applications but policy authoring through the editor would be a great challenge for HAN users.

And now here are some of the HAN-specific PBNM issues:

- HAN users are usually naive to the technical complexities of network management. Ease of use of the tools and techniques becomes very important when it comes to HAN management because mostly HAN users themselves are managing their home networks. HAN users must be able to define different network goals and policies without getting into complexities of authoring the rules and writing configuration scripts to manage their networks.
- HAN devices are usually cheap and not manageable sophistically. At the present there is no solution exists to manage such devices. Auto configuration of network resources would be necessary to make HAN users' life easy but such devices even can not be configured manually.
- An intelligent autonomic manager would be required to detect contextual changes in network and to configure resources according to the user requirements. However very few observers or monitors can be used for certain checking certain conditions because great number of observers would put extra workload (resulting in memory issues), which would degrade the performance of the management system. Concept of aggregate conditions can be one potential solution, meaning aggregating conditions under one monitor agent.
- A policy engine would be required to retrieve policies from the repository. But most challenging work is the transformation of policies into the configurations rules. Configurations would vary device to device depending on the vendor specifications. One good solution is to device a policy virtual machine for the transformation of policies into device specific configurations.

## IV. Conclusion

After a number of decades of research in PBNM there are still no widely adopted standards and techniques for PBNM, other than some adoption of COPS in the industry. No doubt PBNM has great potential to solve many of the complex management issues in HANs but implementation of a flexible enough PBNM system that can cope with all of the potential devices and services in a HAN (and be flexible enough to be updated to deal with future devices and services) is non trivial task. The authors have presented the key challenges being addressed in their research.

## REFERENCES


[1] B. Jennings, S. van der Meer, S. Balasubramaniam, D. Botvich, M. ÓFoghlú, W. Donnelly, and J. Strassner. “Towards autonomic management of communications networks.” *Communications Magazine, IEEE Publications*, 45(10):112–121, October 2007.

[2] D. Agrawal, S. Calo, J. Giles, K. Lee, J. Lobo, and D. Verma. “Policy management for networked systems and applications on integrated network management.”, *In 9th IFIP/IEEE International Symposium*, pages 455–468, May 2005.

[3] G. Liu, S. Zhou, X. Zhou, and X. Huang, 2006. “QoS Management in Home Network.”, *In Proceedings of the international Conference on Computational intelligence for Modelling Control and Automation and international Conference on intelligent Agents Web Technologies & international Commerce* ( November 28 - December 01, 2006). CIMCA. IEEE Computer Society, Washington, DC, 203.

[4] R. Boutaba and I. Aib. “Policy-based management: A historical perspective.”, *ACM Journal of Network and Systems Management*, 15(4):447–480, December 2007.

[5] S. Boros. “Policy-based network management with snmp”, *In Proceedings of EUNICE*, pages 13–15. University of Twente, Netherlands, September 2000.

[6] J. Saperia. “IETF Wrangles over Policy Definitions”, *Network Computing*, IETF Policy Framework Working Group, 2002.

[7] A. Westerinen. “Terminology for policy based management.”, *ACM IETF* RFC 3198, 2001.

[8] S. Davy, B. Jennings, and J. Strassner. “The policy continuum - a formal model.”, *In Proceedings of the Second IEEE International Workshop on Modelling Autonomic Communications Environments*, pages 65–79. MACE, March 2007.

[9] S. Davy, K. Barrett, S. Balasubramaniam, J. Strassner, S. van der Meer, and B. Jennings. “Policy-based architecture to enable autonomic communications - a position paper”, *In Proceedings of IEEE Consumer Communications and Network Conference.* CCNC, January 2006.

[10] N. Damianou. “A Policy Framework for Management of Distributed Systems.”, *PhD Thesis*, Imperial College London, 2002.

[11] Hewlett-Packard. “A Primer on Policy Based Network Management.” *Open View Network Management Division*, Hewlett-Packard Co., 1999.

[12] M. Weiser. “The computer for the twenty-first century.” *Scientific American*, pages 94–10, September 1991.

[13] L. Kagal. A policy language for the me-centric project. http://www.hpl.hp.com/techreports/2002/HPL-2002-270.pdf.

[14] N. Damianou. “The ponder policy specification language.” http://www.doc.ic.ac.uk/mss/Papers/Ponder-Policy01V5.pdf.

[15] P. Bonatti. “Policy language specification.” http://rewerse.net/deliverables/m12/i2-d2.pdf.

[16] Cisco, “Quality of Service (QoS) Notes”, *CiscoPress*, Cisco, 2006.

[17] A. Ibrahim and M. ÓFoghlú, "Policy Refinement for Traffic Management in Home Area Networks – Problem Statement". *In Proceeding of 9th Information Technology & Telecommunications (IT&T) Conference*, 150–153, October 2009, Dublin, Ireland.