

Policy-based Network Management in Home Area Networks: Interim Test Results

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

Abstract— This paper argues that Home Area Networks (HANs) are a good candidate for advanced network management automation techniques, such as Policy-Based Network Management (PBNM). What is proposed is a simple use of policy based network management to introduce some level of Quality of Service (QoS) and Security management in the HAN, whilst hiding this complexity from the home user. In this paper we have presented the interim test results of our research experiments (based on a scenario) using the HAN testbed. After using policies to prioritize different traffic, packet loss decreased to 30% and VoIP quality improved dramatically without employing any intelligent bandwidth allocation technique.

Index Terms— Network Management, Policy, Policy-based network management, network traffic prioritization. Policy-based traffic management, autonomic network.

I. INTRODUCTION

HOME Area Network (HAN) management is problematic for a number of reasons:

- HANs typically comprise cheap hardware (e.g. ADSL router provided by ISP) that have few if any advanced management features;
- HANs are typically owned by end users with little or no management expertise;
- HANs devices used to be simpler, often a single networked home PC, but are now growing in complexity to include games consoles, networked music and video media devices, home automation equipment;
- HAN connectivity now typically comprises both wireless and wireline networks, and may also including IP over powerline and other types of networks.

The problem is that, even through most HAN devices are now IP enabled, there is still a lot of knowledge required to set up these devices to work according to user requirements. For

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

example how many users can setup their home VoIP call to take priority over a large p2p file transfer?

Policy-based Network Management (PBNM) [1] is a promising network management paradigm that has the potential to make network administration tasks easier; one important aspect of this is the configuration management. PBNM is often part of a wider autonomic network management approach (i.e. self-governing, self*, that includes self-configuration) (c.f. [3]). Such approaches generally aspire to reduce human intervention and complexity involved in the process. In a large telecommunications core network, such solutions may be justified in terms of a reduction in operational costs, and a reduction in errors introduced by manual intervention. In a HAN the argument is mainly based on provision of added functionality with minimal user involvement required. In this article we present the role of PBNM in 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 paper is structured as follows: In first part we briefly summarize network management issues in home area network; in the second part we discuss the interim results of our experiments using low level policies in home area network and lastly conclude the research work with future work directions.

II. BACKGROUND AND RELATED WORK

The Internet Engineering Task Force (IETF) has defined a policy management architecture that is considered as best approach for internet policy-based management. The architectural components define the work model and the framework for policy-based management. These are defined in RFC2748 [2] and RFC2753 [5]. Since the initial IETF RFCs were published in 2000, other research has built on this, and there is now a rich history of investigation of policy-based network management, though the deployment in real networks has been more limited.

In a HAN, the aim is to have a single intelligent gateway device that controls all network services and devices, and that can be configured according to user requirements through a policy manager. The paper [4] proposes such a solution for HAN management that focuses on an intelligent control centre (ICC) connecting all other networks within a HAN (e.g. power

line network, PC network, wireless network, home automation network, and home gateway). However, the focus of our research has been an intelligent home gateway that controls services and devices, as well as networks. In addition our work aims to upgrade any existing ADSL router to have the additional capability of acting as the intelligent home gateway.

III. POLICY TESTBED FRAMEWORK

The objective of our initial research experiments was to establish a platform for experimenting with HAN traffic management. As a first step, we deployed a HAN testbed in our research lab, using a small number of machines. This testbed comprised a single Linux router connecting a HAN to the Internet, and a single client Windows XP client on the HAN. Various services on this machine emulated other machines on the HAN, and the necessary data. Figure 1 shows the testbed framework [6, 7] used for policy experiments in home area network. The framework has following components:

1. Policy Builder
2. Policy Engine
3. Traffic Conditioner
4. Traffic Controller
5. Queue Manager
6. Queues Analyzer

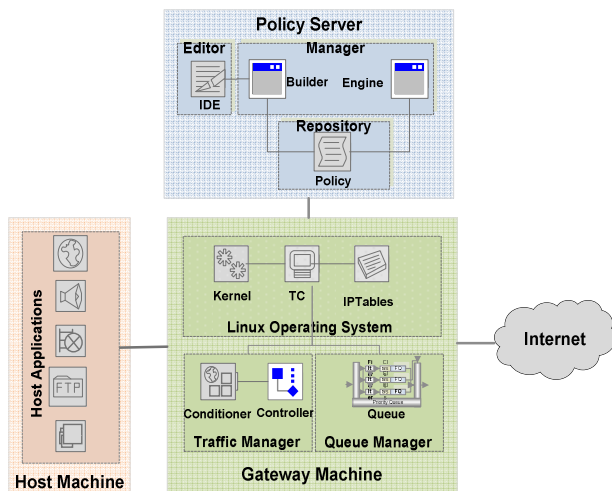


Fig. 1: Testbed Framework.

On the router:

1. iptables (<http://bit.ly/FacQ6>) was used for implementing IPv4 NAT;
2. tc-ng (<http://bit.ly/12ESXV>) was used to implement QoS traffic control (implementing four levels of service based on service type);
3. tcpdump (<http://bit.ly/DrYLG>) was used to capture data for subsequent analysis;
4. perl was used to monitor the queues created and generate descriptive statistics;
5. bash shell scripts were used to manage the configuration, simulating a policy-based network management of the iptables rules.

On the client:

1. Web Traffic Generator (<http://bit.ly/4mSFfs>) was used to generate background TCP web traffic;
2. Traffic Emulator (<http://bit.ly/MJ7y9>) was used to generate background UDP traffic;
3. XLite (<http://bit.ly/6rP7U>) was used to make VoIP calls. An existing Asteisk SIP VoIP service (<http://bit.ly/RePb>) was used to generate the VoIP traffic, with a call to an external PSTN via the SIP gateway from the XLite client in the HAN.

4. INTERIM TEST RESULTS

The experiments run to establish this testbed were based on a scenario that assumed a HAN user was conducting a VoIP call and other Internet activity simultaneously, and that, without some form of QoS management, the VoIP call's quality was adversely affected (including packet loss, delay and jitter). After using policies to prioritize different traffic, packet loss decreased to 30% and VoIP quality improved dramatically. The results produced were able to demonstrate this, providing a baseline for future experimental work on the policy-based network management of the configuration.

Figures 2 and 3 show the network bandwidth utilization graphs. We generated four types of IP traffic: VoIP, UDP Streaming, HTTP and FTP. Initially we created three queues of equal priority and with maximum bandwidth availability for each queue. We assigned VoIP and UDP stream packets on one queue. Most of the bandwidth was utilized by UDP stream. HTTP and FTP traffic was almost negligible and VoIP quality was extremely poor due to great packet loss.

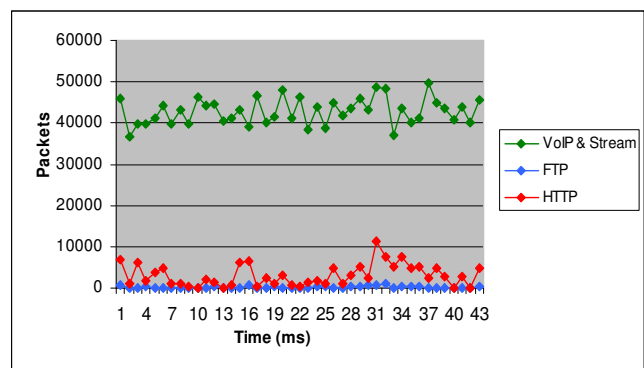


Fig. 2: Bandwidth utilization before policy

HAN users' generated traffic has equal priority with no bandwidth constraints; this means the packets are queued on the gateway device in a first-in first-out (FIFO) queue (depending on default configuration). When two UDP traffic flows (e.g. VoIP and Video streaming) of equal priority compete for bandwidth, their quality can suffer because of varying bandwidth availability, which can result in great packet loss and unwanted packet delays. We know that policies can be used to manage QoS requirements, therefore by separating the VoIP and streaming traffic into two different priority queues, with optimal flow rates, this can potentially

improve the quality both traffic flows. Although, we did not employ any intelligent bandwidth allocation technique but bandwidth utilization improved by using low level policies as shown in figure 3.

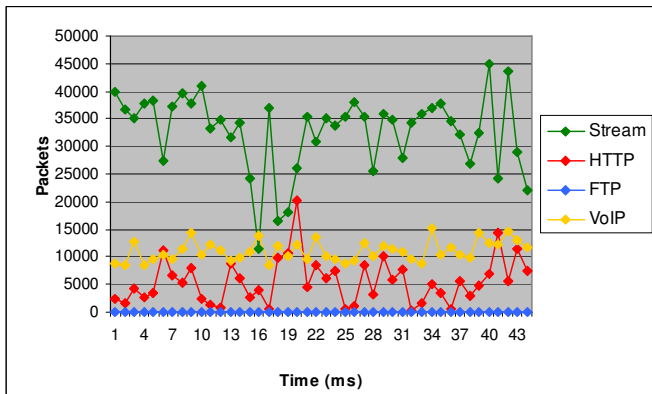


Fig. 3: Bandwidth utilization after policy

IV. DISCUSSION & FUTURE WORK

The next step is to implement a real policy language that can map between a high level specification of a priority (e.g. VoIP is important), to the lower level configuration management that enables this behavior (e.g. specify a particular service class has having a specific queuing priority in iptables). There are a number of candidate policy languages, and the current working assumption is that a language derived from DEN-ng [3] will be used and some initial work in this direction has been done. The aim is then to demonstrate this with QoS management, and to expand it to implement security configuration, such as the management of the firewall rules that allow services to be accessed externally (and potentially also using some for of NAT traversal or IPv6 to avoid the NAT issues). Thus the aim is to demonstrate, on a testbed with real measurements and metrics, the auto-discovery of new devices and services on a HAN, and their automatic configuration with a higher level set of constraints expressed in a suitable policy language. So, an illustrative example is that a new media server is automatically discovered, and is given a suitable priority on the HAN, and that external access is enabled if the end user answers a simple question, generated by the system.

This is the initial work for our project; this was to setup a test environment for our future research work. However, this testbed would be further refined and built to the next level for future research requirements. The testbed will be further refined to allow investigation of PBNM in HAN.

REFERENCES

- [1] S. Boros. "Policy-based network management with snmp," *In Proceedings of EUNICE*, pages 13–15. University of Twente, Netherlands, September 2000.
- [2] R. Boutaba and I. Aib. "Policy-based management: A historical perspective," *ACM Journal of Network and Systems Management*, 15(4):447–480, December 2007.
- [3] 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.
- [4] B. Jennings, S. van der Meer, S. Balasubramaniam, D. Botvich, M. OFoghlu, W. Donnelly, and J. Strassner. "Towards autonomic management of communications networks". *Communications Magazine, IEEE Publications*, 45(10):112–121, October 2007.
- [5] G. Liu, S. Zhou, X. Zhou, and X. Huang. "QoS management in home network," *In CIMCA '06: Proceedings of the International Conference on Computational Intelligence for Modelling Control and Automation and International Conference on Intelligent Agents Web Technologies and International Commerce*, page 203, Washington, DC, USA, 2006. IEEE Computer Society.
- [6] 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.
- [7] A. Ibrahim and M. ÓFoghlú, "Policy-based Traffic Management in Home Area Network – An Elementary Testbed Model ". *In Proceeding of 7th Frontiers of Information Technology (FIT) Conference*, December 2009, Abbotabad, Pakistan.