Intelligent Devices in Rural Wireless Networks

Daniel Fuentes[a,b,c], Rosalía Laza[c], António Pereira[a,b]

[a] Computer Science and Communications Research Center, School of Technology and Management of Leiria, Polytechnic Institute of Leiria, Portugal
[b] Information and Communications Technologies Unit, INOV INESC Innovation - Delegation Office at Leiria, Portugal
[c] ESEI: Escola Superior de Enxeñaria Informática, University of Vigo, Ourense, Spain

KEYWORD

Intelligent devices
Distributed architecture
Automatic configuration
Rural wireless networks
Sustainability

ABSTRACT

The rural wireless networks are increasingly in demand by associations and autarchies to expand Internet access in this type of areas. The problem of such solutions centers not only in network deployment and its maintenance, but also in the equipment installation on clients, which always has big costs. This installation and configuration must be performed by a technician on site, so that the equipment can be integrated in the infrastructure. To try to mitigate this problem, it is presented a solution that allows the clients to install, with transparency, the device at home, reducing not only the cost for the management entity but also for the clients. This way, for info-excluded people or with new technology low experience level, it is the user that integrates himself in the network, making him part of the process, fostering the network usage.

In this article are specified not only the system architecture but also the way that it works and how it obtains the desirable result. The tests made to the solution show the quickness, reliability and autonomy in the execution of the tasks, making it a benefit for rural wireless networks.

This solution, by its robustness and simplicity, allowed an uptake to the IT by people who never thought to do it, namely an advanced age group (elderly) who want to join the world of the new technologies.

1 Introduction

The growing demand for Internet access has led communications operators to bet strong in its infrastructures. The problem is that these same structures are only being optimized where there is a large concentration of population. Rural and dispersed areas, because of their few population, are not a good financial return for the operators, which lead them to not invest in the infrastructure located in these areas [Mishra, S. *et al*., 2005]. Because of this, the younger population, that is connected to IT, does not have the easy access that exists in large urban centers. Sometimes, there are locations where there is not even a minimum Internet access, which lead some villages to implement wireless networks to meet this need [Ranga, M. *et al*., 2010]. These networks provide users with a variety of technology services that are regarded essential for the younger population. The challenge for this kind of networks is that they have to cover many populations scattered over a wide area [Selada, R., 2008], this raises many problems in terms of cost of installation and maintenance, making them a non-sustainable solution.

This kind of networks, called rural wireless networks, consists in several geographically dispersed distribution points interconnected via wireless links. The configuration of these distribution points must be made during the installation of the network, this to link the various points of the infrastructure.

The installation itself and configuration of network infrastructure is sometimes difficult, since there may be some configuration problems on some equipments, which must be reconfigured on site. Problems exist not only when the infrastructure is built, but they also manifest during the operation of the same,

DOI: http://dx.doi.ort/10.14201ADECAIJ2013172330

including deconfiguration of equipments and mandatory changes in the network topology. All this shows that there are too high costs in maintaining a rural wireless network [Surana, S. *et al*., 2007].

The above facts associated with the rural location of this type of networks leads its maintenance cost to be aggravated by the distance of the specialized teams. In order to minimize these obstacles are implemented monitoring and network management systems to help to reduce the maintenance costs. This is achieved through a centralized management of the whole network, where all the devices are monitorized [Frazão, L. *et al*., 2013]. The limitation of these monitoring systems lies on the fact that the devices must be reachable on the network in order to function properly.

The evolution of communication networks has led to several studies in the area of future networks, including the features that a network must have to be considered as such [ITU, 2001]. Two of these features are self-sustainability and the ability of the network to be autonomous, needs that are found in rural wireless networks.

In the work presented in this article is intended to minimize intervention by specialized technicians when installing new client devices on the network, delegating this function to the client itself. This not only helps make this type of networks autonomous and sustainable, but above all makes them more usable by the most technologically illiterate people, growing their number of users.

In addition to this section, the article is structured as follows: the section II presents the work related to projects of dynamic configuration of client devices in wireless networks; The section III presents the system architecture. In section IV is presented the test scenario, the objectives and the correspondent results. In section V are presented the conclusions of all the work done.

2 State of the art

The automation in communication networks early awakes large interests by the searchers aggregated to that area, factor due to the exponential growth, both in size of the networks, in area that embraces and in associated services [Strassner, J., 2004] [Prehofer, C. *et al*., 2005]. This has raised the need to study new concepts and technologies that were in accordance with the resolution of the problem of the equipment autoconfiguration and communication networks optimization [Agoulmine, N. *et al*., 2006] [Lehtihet, E. *et al*., 2005].

The research conducted in this area, aggregated to the demand from network managers, led to the emergence of several studies related to this topic, particularly in terms of paradigms to be adopted in the creation of self-configuring wireless networks and approaches to take in the disposition of access points on the network [Mullany F. *et al*., 2004] [Zimmerman, K., 2004].

The information inherent to the processes above described, aggregated to the increasingly urgent need for large quantities of data in these devices, led to the emergence of the concept of distributed architectures [Zarandi, M. *et al*., 2008] [Manzoor, U. *et al*., 2008] [Ilarria, S. *et al*., 2007], whose aim is to decentralize the processing of the information by distributing it among all the devices on the network.

The evolution of these autonomous systems directed the researchers to apply knowledge of other areas in this kind of networks, such as artificial intelligence, creating systems based on multi-agent architectures, whose main function is to provide the devices of an own intelligence that allows them to be autonomous [Kephart, J. *et al*., 2004] [Gavalas, D. *et al*., 2002] [Weiss, G., 1999].

Dynamic configuration of equipments in wireless local area networks (WLAN) has already taken steps, but there are only a few specific cases. This feature is used by some manufacturers to enable equipments, such as computers, mobile phones or tablets to connect to the wireless network in an easy way. With this is simple to get access to a protected network with little knowledge of wireless networks, or even none.

The Wi-Fi Protected Setup (WPS) [Wi-Fi Alliance, 2010] provides a mechanism for configuring small office / home office (SOHO) networks. This allows users with little knowledge in wireless network configuration to be able to add new devices to the network safely.

The products with WPS provide two types of configuration - through a Personal Identification Number (PIN) or via a Push Button Configuration (PBC). The access points provide both types of authentication and client devices must have at least the PIN authentication.

In the PIN mechanism, the user enters the PIN of the access point on the client device, and then the connection is made. In the case of the PBC, the user presses a button on the access point and the connection is made between the two devices.

The AirStation One-Touch Secure System (AOSS) [Buffalo Technology, 2004] works similarly to WPS, but only provides the PBC mechanism. This system was developed by Bufallo Technology and is in almost all of their SOHO wireless network equipments.

Given the goals we set ourselves with this solution, the studies in the area and type of system where it will focus the development, we propose an autonomous system that: aims autoconfiguration of client equipment present in rural wireless network, making them smart and providing cost reduction in the implementation and maintenance of the same; minimizes the need for intervention by specialized teams on the ground; reduces the problems inherent with the geographic dispersion of the equipment and its accessibility; do not impose limitations in terms of scalability of the infrastructure.

3 System Architecture

The infrastructure of a rural wireless network consists mainly in clients, distribution points, servers and gateways. Clients are the equipments installed at the end user's home, as the name implies. The distribution points are the devices distributed over the area to be covered, are interconnected via wireless links and provide a point of connection to clients. Servers are the devices that provide various services to network users and are usually located at the center point. Gateways are the equipments that are responsible to interconnect the internal network to the outside world, providing Internet access for network users.

To be able to implement autoconfiguration of the client devices is necessary to develop a distributed architecture that allows these same equipments to auto-configure. This requires creating agents in those devices that are in charge of automatically configure it.

An agent is a software-based entity which, in this case, can access to the equipment information. The agents are also responsible for maintaining the proper function of the devices and, to this goal, have to ensure communication between devices.

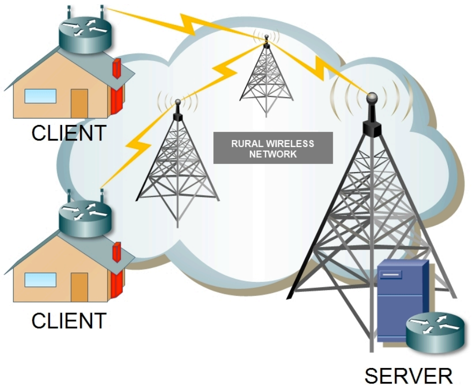


Figure 1 - System architecture

In **Figure 1** we can see the defined architecture and where are located the respective agents. The Client Agent and Server Agent form this system, each one is required for the correct operation of the network and system.

3.1. Agents

The Client Agent, shown in **Figure 2**, is present in the equipment that is at the end user's home. It is this device that connects the user to the core wireless network. The equipment starts in a state of pre-registration configuration and the Client agent connects to the Server agent to get the respective settings to configure the device.

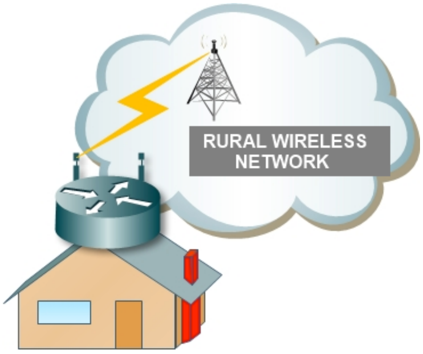


Figure 2 - Client Agent

The Server Agent, visible in **Figure 3**, responsible for maintaining the functionality of the network, storing all the information inherent in the configuration and enables the management of the system by the administrator, also adds an element of web services. Through this web service component becomes available the necessary settings to the client Agents present in the infrastructure, thereby enabling its configuration.

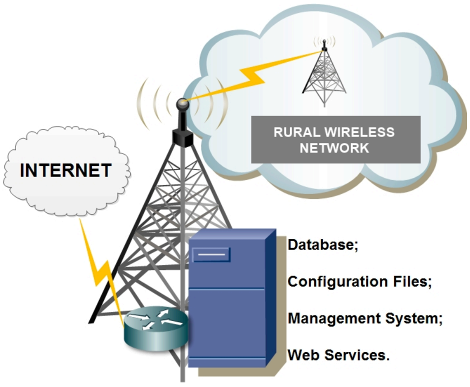


Figure 3 - Server Agent

3.2. Pre-registration configuration

A key point in this architecture is the system of pre-registration present in the devices. This pre-registration allows the end users to be able to configure their own device in an easy and fast way, without the intervention of an administrator or a technical expert. This pre-registration is built-in on the equipment via firmware modifications of the same, which allows the device to connect to a registration network, allowing the Client agent to configure it-self using the Server Agent.

One of the major concerns is the system security, this because we want to avoid to the maximum the faillures in the network.

In order to solve this problematic, this registration network is protected with Wi-Fi Protected Access II (WPA2) encryption [Wi-Fi Alliance, 2012], using 128 bits passwords.

For a superior protection there are also used the device's firewalls in the distribution, this to only allow configuration traffic to the server.

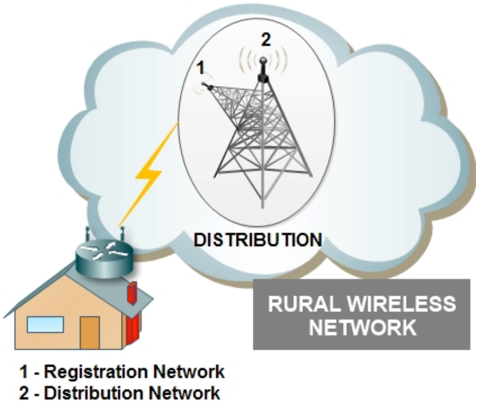


Figure 4 - Registration network

The pre-registration network, exemplified in **Figure 4**, can be created in two ways: through an adicional Wi-fi radio, being an idependent network, or through configuration of a Virtual Access Point (Virtual AP). The "Virtual AP" can be created using a radio that performs functions as access point. In this case, since all the nodes have a distribuition network for the clients to connect, this can be used for that effect.

3.3. Algorithm

To be able to send and receive data to self configure, the devices need to follow the algorithm presented in **Figure 5**, which represents the client side system function.

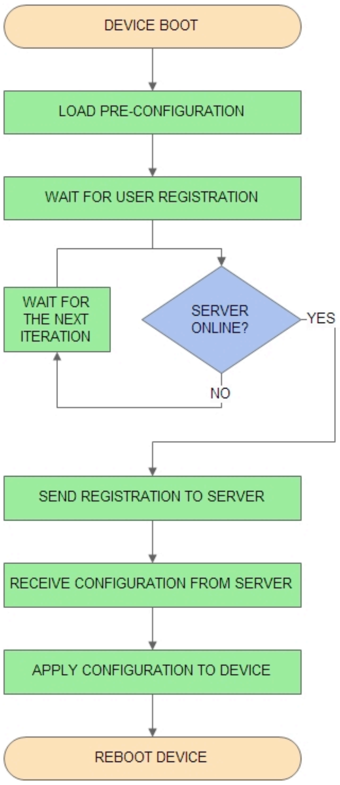

DEVICE BOOT
LOAD PRE-CONFIGURATION
WAIT FOR USER REGISTRATION
WAIT FOR THE NEXT ITERATION
SERVER ONLINE?
YES
NO
SEND REGISTRATION TO SERVER
RECEIVE CONFIGURATION FROM SERVER
APPLY CONFIGURATION TO DEVICE
REBOOT DEVICE

Figure 5 - Algorithm

On the device startup, the client Agent loads the pre-registration settings to the equipment and waits for the user to register the device. After the registration is done, the agent verifies the connectivity with the Server agent, if do not exists it waits for the next iteration to check it again. If there is connection to the server the registration is sent to the server where the respective agent creates the configuration file that is sent back to the device. The agent on the device receives the configuration file, applies it and reboots the equipment.

3.4. System Central Point

The system central point is what most concerns any architecture, because it is a crucial failure point. To mitigate this possible failure it has been implemented in the server a cluster to guarantee high availability of the services.
In **Figure 6** is represented the cluster present in the central point.

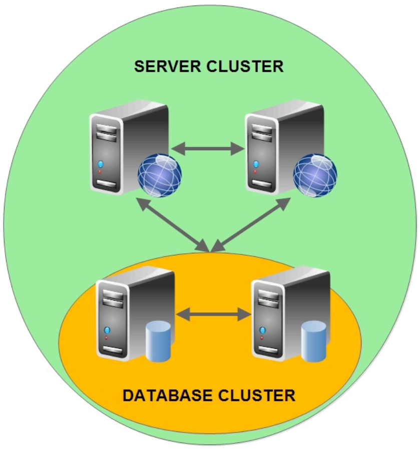
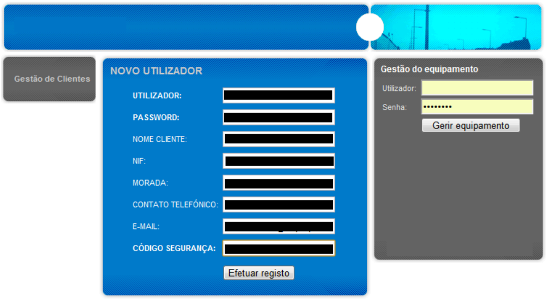


Figure 6 - Configuration system

This cluster is composed by two machines that implement a Virtual Router Redundancy Protocol [IETF, 2010] (VRRP) and share the same IP of the server. The services are guaranted by the two machines, being one as a master and the other as a slave and in case of failure of the main machine, the secondary assumes the command. The database also implements a redundant system that is directly connected to both machines.

3.5. System Function

To be possible to implement the registration system it is needed a network that allows connectivity between the client and the server, allowing an automatic configuration of the device. This network is provided by the core devices can be a real network or a virtualized one. The client equipment boots with the registration configuration, and after the respective user fills the registration form, the device communicates with the server using the registration network. It is noteworthy that this pre-registration can be done by the management entity when the requesting adhesion to the infrastructure is done.
An example of that pre-regitration is shown in **Figure 7**, where are presented the fields needed to request a configuration file for the device.



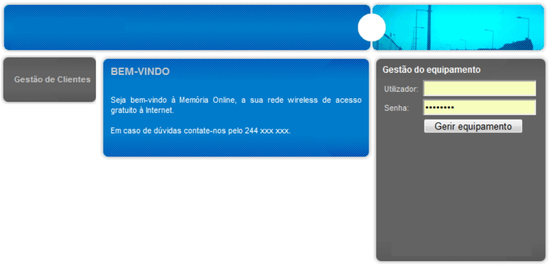
NOVO UTILIZADOR

UTILIZADOR: [redacted]
PASSWORD: [redacted]
NOME CLIENTE: [redacted]
NIF: [redacted]
MORADA: [redacted]
CONTATO TELEFÓNICO: [redacted]
E-MAIL: [redacted]
CÓDIGO SEGURANÇA: [redacted]

Gestão do equipamento
Utilizador:
Senha: •••••••••

Figure 7 - New client registration

After the Server agent has received the data, this creates a new client in the database and sends back the configuration file for system device. The Client agent receives the request settings, applies them and reboots the device. After that, the device is configured and ready to be used, displaying that information to the user, as shown in **Figure 8**.



BEM-VINDO

Seja bem-vindo à Memória Online, a sua rede wireless de acesso gratuito à Internet.

Em caso de dúvidas contate-nos pelo 244 xxx xxx.

Gestão do equipamento
Utilizador:
Senha: •••••••••

Figure 8 - Registered client

4 Tests and Results

In this section are described in detail all the tests that were made to the configuration system, such as configuration and recovery tests.

4.1. Test scenario

To perform all the necessary tests it was implemented a small laboratory setting consisting of a wireless distribution, several clients and the respective configuration server, which is shown in **Figure 9**.

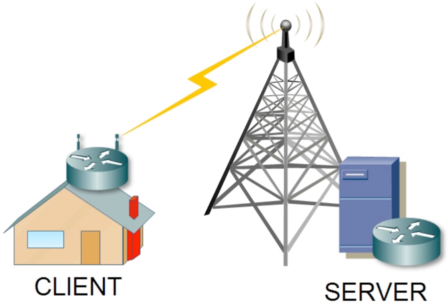


Figure 9 - Test scenario

The devices used are based in the OpenWRT system [OpenWRT, 2013] which is a linux-based firmware very used in wireless networks environments.

4.2. Tests objectives

The tests were intended to verify the proper function and detect possible failures that existed. In order to do that the tests were divided into three groups:

- Client registration tests;
- Comunication tests;
- Cluster failure tests.

4.3. Client registration tests

The client registration tests serve to observe whether the system can correctly register a new client on the network. **Table 1** shows the average times that the devices took to auto-configure starting at the registration point.

	Client
Get configuration	7 seconds
Device configured	49 seconds

Table 1 - Registration times

The results come check the response speed of the automatic configuration, which in less than a minute after the registration the devices were configured and ready to use.

4.4. Comunication tests

The communication tests serve to verify the connectivity between the Client and Server agents. This is necessary to prove that clients can communicate with the server to acquire its configuration. To do that new clients were connected simultaneously and performed the registration in the equipment. After that there were made a QoS marking to all the packets from the registration network to check if any information were lost.

These tests proved that the system could communicate whitout problems with the server, and only with it, due to the restrains configured in the firewall.

4.5. Cluster failure tests

The cluster failure tests are used to observe how long it takes the cluster to recover from a failure of one of the servers. In **Table 2** are shown the different tests and their respective times of downtime.

	Service downtime
Failure in main serve	2 seconds
Failure in secondary server	0 seconds
Failure in the connection between the main server and the database	2 seconds
Failure in the connection between the secondary server and the database	0 seconds
Failure in the secondary server after failure in the main server	Undefined
Failure in the connection between the secondary server and the database after failure in the mais server/connection with the main server with the database	Undefined
Failure in the connection between servers	0 seconds
Failure in the cluster connection	Undefined

Table 2 - Downtime times

As can be seen in the results obtained, the existing downtime in case of failure in some cases is zero, since the fault does not directly affect the system. The problem is when there are consecutive failures covering either servers or both of the database, where the downtime will happen until there is a technical intervention.

4.6. Results

With the results obtained in the tests previously presented we can conclude that the system shown gives administrators of a rural wireless network a tool for unattended installation of equipments. The times achieved in both the registration of clients as in the downtime were within the expected.

5 Conclusions

In this paper we proposed a system for automatic configuration of equipment for rural wireless networks. This system aims to automate the installation of client equipment within the infrastructure, automatically and quickly, making it autonomous, sustainable and a usable network by the population with lower computer literacy.

The advantages that this system brings to rural wireless networks are in particular reducing costs in terms of installation and maintenance, the network automation and the ease of integration offered to clients. This allows an adhesion by a range of people who never would use, with all the benefits that this will bring in the future with the widespread use of new technologies.

The results of tests performed, demonstrated the speed of the system, the reliability and the autonomy.

6 Acknowledgment

This work was partially supported by the Rede de Inovação da Região Centro (RICE), INOV - INESC Innovation delegation of Leiria and supported by the Memória Online project.

7 References

[Mishra, S. et al. 2005] S. Mishra, J. Hwang, D. Filippini, R. Moazzami, L. Subramanian, T. Du. “Economic analysis of networking technologies for rural developing regions”. Internet and Network Economics. Springer Berlin Heidelberg. 2005.

[Ranga, M. et al. 2010] M. Ranga, Mamello Thinyane, Alfredo Terzoli. “Exploring Cost-Effective Reinforcements for Rural Telecommunication Networks: Dwesa Case

Study”. SATNAC. 2010.

[Selada, R. 2008] Rodrigo Selada. “Redes Wireless de Banda Larga”. Universidade de Trás-os-Montes e Alto Douro. 2008.

[Surana, S. et al. 2007] S. Surana, R. Patra, E. Brewer. “Simplifying fault diagnosis in locally managed rural WiFi networks”. Proceedings of the 2007 workshop on Networked systems for developing regios. ACM. 2007.

[Frazão, L. et al. 2013] Luís Frazão, Silvana Meire, Carlos Rabadão, António Pereira. “Modelo de Gestão de Rede Wireless de Banda Larga em Ambientes Rurais”. Sistemas e Tecnologias de Informação – CISTI. 2013.

[ITU 2001] International Telecommunication Union. “Future Networks: Objectives and design goals”. ITU-T Y.3001. 2001.

[Strassner, J., 2004] J. Strassner. “Autonomic Networking – Theory and Practice”. IEEE Tutorial. 2004.

[Prehofer, C. et al., 2005] C. Prehofer, C. Bettstetter. “Self-Organization in Communication Networks: Principles and Paradigms”. IEEE Comunication Magazine. 2005.

[Agoulmine, N. et al., 2006] N. Agoulmine, S. Balasubramaniam, D. Botvitch, J. Strassner, E. Lehetihet, W. Donnelly. “Challenges for autonomic network management”. First Conference on Modelling Autonomic Communication Environment. 2006.

[Lehtihet, E. et all., 2005] E. Lehtihet, H.Derbel, N. Agoulmine, Y. Ghamri-Doudane, Sven van der Meer. “Initial approach toward self-configuration and self-optimization in IP networks”. Management of multimedia network and services. 2005.

[Mullany F. et al., 2004] F.J. Mullany, et al. “Self-Deployment, Self-Configuration: Critical Future Paradigms for Wireless Access Networks”. WAC 2005. 2004.

[Zimmerman, K., 2004] K. Zimmerman. “An Autonomic Approach for Self-Organising Access Points”. Diploma Thesis, University of Ulm – Germany. 2004.

[Zarandi, M. et al., 2008] M.H. Fazel Zarandi, P. Ahmadpour. “Fuzzy agent-based expert system for steel making process”. Expert Systems With Applications 36(5). 2008.

[Manzoor, U. et al., 2008] U. Manzoor, K. Ijaz, A. Shahid. “Distributed dependable enterprise business system – DDEBS”. Proceeding of springer communications in computer and information science, vol.19. 2008.

[Ilarria, S. et al., 2007] Sergio Ilarria, Eduardo Menaa, Arantza Illarramendib. “Using cooperative mobile agents to monitor distributed and dynamic environments”. Information Sciences, 178. 2007.

[Kephart, J. et al., 2004] J.O. Kephart, W.E. Walsh. “An artificial intelligence perspective in autonomic computing policies”. Proceedings of POLICY’04. 2004.

[Gavalas, D. et al., 2002] D. Gavalas, D. Greenwood, M. Ghanbari, M. O’Mahony. “Hierarchical network management: A scalable and dynamic mobile agent-based approach”. Computer Networks, 38(6). 2002.

[Weiss, G., 1999] G. Weiss. “Multiagent systems a modern approach to distributed artificial intelligence”. The MIT Press Crambridge. 1999.

[Wi-Fi Alliance, 2010] Wi-Fi Alliance. “Wi-Fi CERTIFIED Wi-Fi Protected Setup”. 2010.

[Buffalo Technology, 2004] Buffalo Technology. “AirStaion One-Touch Secure System”. 2004.

[Wi-Fi Alliance, 2012] Wi-Fi Alliance. The State of Wi-Fi Security. 2012.

[IETF, 2010] IETF. “Virtual Router Redundancy Protocol” RFC5798. 2010.

[OpenWRT, 2013] OpenWRT, [http://openwrt.org], Accessed in November 2013.