DOCTORAL DISSERTATION
Sistema Inteligente para la Gestión de
Redes Wireless de Banda Ancha en
Ambientes Rurales

Luis Alexandre Lopes Frazão

2017
Universidade de Vigo
International Doctoral School

Luis Alexandre Lopes Frazão

DOCTORAL DISSERTATION

Sistema Inteligente para la Gestión de Redes Wireless de Banda Ancha en
Ambientes Rurales

Supervised by: Dra. Silvana Gómez Meire and Dr. António Manuel de Jesus Pereira

2017
Page intentionally left blank
Acknowledgements

This work would not be possible without the guidance, insights, support and friendship of many people who fill my life, to whom I greatly appreciate.

Dr. António Pereira has been a great supervisor in guiding and assisting me throughout this study. Between providing me insights of his knowledge in many topics, he introduce me to his vision and to the research problems that were the base of this work.

Dra. Silvana Meire was my second supervisor for my research. Every occasion we had been together, she always push me forward and point me to the right directions in my research and in my focus.

Dra. Isabel Marcelino was my closest partner during my research work. Through our journey in this doctoral study, I have learned a lot from her experience and knowledge. She was able to impulse my motivation on some Saturdays of hard work.

In addition to these individuals, I also had the opportunity to work with Alberto Costa, Tiago Nobre and Daniel Fuentes of which I keep on memory great discussions and brainstorming sessions to develop solutions for the deployment of the Memória Online project.

I wish also to extend my thanks to the University of Vigo, for allowing me to achieve another step in my long ride of education.

My family’s constant support, love and encouragement during the time spent working on this dissertation was precious. My parents and brother always encouraged me in all the accomplishments of my life. My little girls, Sofia and Alice, always made me focus on what is more important.

The best for last: my wife Débora. I could not have done it without your deep love and tenderness!
Las tecnologías informáticas y sus servicios están emergiendo a un ritmo muy rápido, cubriendo todos los sectores de nuestra sociedad y negocios. Internet, que una vez fue conocida como una gran biblioteca de conocimiento, es hoy una "aldea global" donde un usuario común puede comprar, vender, hablar con viejos amigos, conocer nuevos amigos, estudiar e incluso trabajar a distancia.

Los datos estadísticos nos muestran que el número de usuarios conectados a Internet está teniendo un crecimiento de alrededor del 10% cada año. Este crecimiento se ha incrementado debido a la caída de los precios de los servicios de tecnología de la información y la comunicación (TIC). Sin embargo, este crecimiento sólo se manifiesta en zonas de alta densidad de población, donde los precios son muy competitivos y la velocidad y los servicios ofrecidos son muy tentadores para el cliente habitual. En la mayoría de los casos, las zonas rurales de baja densidad de población se quedan con tecnología antigua y débil, si es que la hay. La oferta real de Internet no es igual para todos debido a la no rentabilidad de la implementación de servicios de Internet en las zonas rurales [1 - 4]. En estas, donde la densidad de población es muy baja, la tecnología debería ser tan simple y barata como fuese posible [5-8].

En la última década, las redes inalámbricas basadas en el Protocolo de Internet (IP) se han utilizado en las zonas rurales y los países en desarrollo por las comunidades y grupos de investigación, con la intención de proporcionar un acceso a Internet más barato. Estas redes suelen ser de bajo costo, bien conocidas por los usuarios, y pueden alcanzar una distancia considerable para ser utilizadas en una zona rural [2, 6, 8, 9].

Si bien este tipo de redes inalámbricas en las zonas rurales son rápidas de desplegar, también tienden a desaparecer rápidamente debido a los mismos problemas, que se explican en los siguientes subcapítulos. A partir de la revisión de la literatura se puede afirmar que al diseñar y planificar una red inalámbrica para
una zona rural, los investigadores y administradores deben centrarse no sólo en los detalles de instalación, el alto ancho de banda disponible para los usuarios, la visibilidad social y los factores económicos, sino también en los problemas que pueden surgir en el futuro y los recursos necesarios para resolverlos [2, 10]. La solución de problemas requerida en una red inalámbrica rural no siempre es un proceso fácil, especialmente cuando no hay datos o información que pueda ayudar. Incluso para los administradores y técnicos más experimentados, algunas decisiones son difíciles de definir porque la documentación disponible y los datos se olvidan cuando se planea la red. Una buena solución de gestión para las redes inalámbricas en las zonas rurales debe tener en cuenta todos estos aspectos que permiten a la red crecer y ser sostenible durante mucho tiempo.

Debido al crecimiento de este tipo de redes, también se están implementando otros tipos de servicios y redes en las zonas rurales. El intercambio de información entre máquinas no es suficiente para lo que podemos lograr. Hay una necesidad de recibir y enviar información de las "cosas" en nuestra vida cotidiana. Internet de las cosas (IoT) se está convirtiendo en presente en nuestra vida cotidiana moderna de las telecomunicaciones. El concepto es la presencia omnipresente en cosas y objetos alrededor de nosotros para recopilar datos e interactuar unos con otros. Esta presencia en "cosas" abre oportunidades en proyectos en diferentes campos de interés (agricultura, militar, logística, transporte, seguridad, medicina, industria, domótica y robótica).

Los últimos avances en zonas rurales se está haciendo con las redes de sensores inalámbricos en agricultura a través del control de las características del suelo y el aire, como la humedad o la temperatura del suelo, pero también en los campos médicos y de seguridad proporcionando sensores que controlan a los ancianos y otras personas que necesitan asistencia constante en sus hogares. Sin embargo, la mayoría de los dispositivos utilizados en el IoT tiene recursos limitados, no sólo en la capacidad de proceso y de memoria, sino también en la potencia de la batería y la intensidad de la señal de comunicación. Los dispositivos típicos en IoT están equipados con muy pocos microcontroladores que tienen baja capacidad de memoria RAM y de almacenamiento.
Administrar y monitorizar esta red de IoT puede ser un desafío mayor, debido a las muchas restricciones y limitaciones mencionadas anteriormente. Una visión de Ericson [11] es que en 2020, más de 50 millones de dispositivos cambiarán la forma en que interactuamos unos con otros, incluyendo nuestras "cosas" y objetos. Con un número tan alto de dispositivos, es imposible gestionar cada nodo individualmente. Una solución de gestión adecuada es necesaria para estos tipos de redes, especialmente las que coexisten con la red inalámbrica en las zonas rurales.

**Alcance y Motivación**

Esta tesis contribuye a la investigación en múltiples áreas, muchas de las cuales están experimentando un gran desarrollo y dirigirán nuestro trabajo a futuras investigaciones en el futuro.

La investigación en el desarrollo de condiciones y la implementación de tecnología informática en las zonas rurales es un problema difícil debido a las limitaciones de estas áreas. Para implementar tal escenario es necesario investigar todos los aspectos del despliegue de una red inalámbrica y todos sus servicios asociados. Hay una amplia gama de líneas de investigación en esta área que motivó profundamente nuestro trabajo de investigación.

Una de las características clave de nuestro trabajo es el uso de la inteligencia artificial para crear funciones que ayuden a los administradores de las redes a lograr una buena calidad de red inalámbrica para los usuarios finales. Las redes informáticas y todos sus dispositivos y servicios generan muchos flujos de información que pueden ser utilizados en la inteligencia artificial, como el reconocimiento de patrones para generar acciones automáticas en la red y sus dispositivos. Los algoritmos implementados deben provenir de una experiencia de aprendizaje y un conocimiento previo de los servicios y dispositivos de la red.

Otra característica de nuestro trabajo es el despliegue de un caso real. Esto fue muy motivador porque nuestro trabajo contribuyó a ayudar a una comunidad de personas y negocios. Al desplegar una red inalámbrica en una zona rural que se conecta a Internet, estábamos mejorando la vida de muchas personas. En estas áreas, Internet puede disminuir el aislamiento y la soledad que la mayoría de los ancianos
tienen en sus hogares. Esto potencia la igualdad entre personas de diferentes generaciones y lugares.

También ha contribuido a crear muchas oportunidades de investigación que nos permitan seguir investigando y creando servicios e implementaciones para el escenario implementado.

**Objetivos y metodología**

El objetivo principal de esta tesis es identificar los requisitos para administrar y monitorizar una red de área rural inalámbrica y crear un modelo de gestión que apoye la administración de la red inalámbrica lo más fácil, económico y sostenible posible.

Con base en estudios recientes en áreas rurales, identificamos los problemas y resultados de cada estudio para obtener nuestro modelo de gestión.

Los objetivos de esta tesis son:

- Estudiar e identificar problemas y resultados obtenidos en proyectos de redes inalámbricas en áreas rurales o en países en desarrollo;
- Estudiar e identificar, usando diferentes enfoques, como administrar y monitorizar dispositivos de bajos recursos usados en redes de sensores inalámbricos;
- Creación de un modelo de gestión capaz de:
  - Supervisar todos los dispositivos de red activos y sus servicios, con el fin de identificar problemas;
  - Realizar una constante recolección de datos de todos los dispositivos de red activos y sus servicios con el fin de detectar, anticipar y ayudar en el diagnóstico de problemas;
  - Crear una base de datos para almacenar toda la información a fin de servir de base para herramientas de diagnóstico y prevención de problemas (modelo predictivo);
- Identificar sistemas inteligentes que podrían ser utilizados para mejorar la red para ser autónomo y autosostenible, minimizando así su costo y maximizando su longevidad y sostenibilidad;

- Utilizar herramientas gráficas para presentar toda la información recopilada de manera fácil y efectiva a los administradores;

- Monitorizar el comportamiento de los usuarios para establecer procesos de calidad de los servicios;

- Proporcionar una herramienta gráfica para mostrar eventos o problemas importantes para todos los usuarios de la red;

- Implementar el modelo de gestión en un área rural para demostrar su importancia en la sostenibilidad y para mostrar la importancia de estas redes inalámbricas.

Para cada objetivo de esta tesis, se requirió una investigación sobre el estado del arte. En primer lugar, se realizó una investigación sobre las tecnologías inalámbricas para identificar posibles soluciones, pero también para transmitir algunos conocimientos al proceso de implementación de nuestros resultados. Por otro lado, se utilizó el trabajo realizado por los investigadores en el despliegue de redes inalámbricas en zonas rurales para identificar las limitaciones y dificultades que tenían, pero también para aprender de sus errores y soluciones en la gestión y monitorización de estas redes inalámbricas.

Como resultado, el modelo propuesto para la gestión de una red inalámbrica se basó en este estado del arte. La implementación de este modelo en un proyecto real permite obtener datos y retroalimentación de las personas que utilizan la red. Con la cantidad de información disponible, se hizo una investigación adicional para estudiar qué métodos se podrían utilizar para aplicar inteligencia en la red usando algoritmos, técnicas probabilísticas y de aprendizaje automático.
Hemos propuesto un innovador modelo de gestión de redes inalámbricas en las zonas rurales, en donde hemos podido concentrar nuestro esfuerzo creando alternativas a los problemas identificados anteriormente. Las características de las redes inalámbricas rurales requieren que las soluciones de gestión sean económicas y no requieran equipos especializados a tiempo completo ni visitas sistemáticas de campo.

La arquitectura del modelo de gestión se divide en varios módulos que tienen los mismos objetivos: reducción de costes y automatización de una gestión remota. La monitorización de dispositivos y servicios, junto con las herramientas de diagnóstico y prevención, permiten al gestor de red conocer en tiempo real la red, los dispositivos y su estado de servicio. La creación de informes históricos y gráficos de valores de los dispositivos y sus servicios, son herramientas que ayudan al administrador a prevenir y resolver problemas.

El modelo también propone soluciones automatizadas de resolución de problemas a través de herramientas de recuperación automática que, aunque no pueden ser 100% eficaces, son capaces de realizar tareas de resolución de problemas sin necesidad de presencia humana. Al aplicar inteligencia a las funciones de monitorización, el modelo garantiza a los administradores un mantenimiento seguro y libre de tensión de la red. Además, la solución permite instalar un nuevo dispositivo en la red sin necesidad de la presencia de un administrador o personal especializado, reduciendo así los costes y maximizando la sostenibilidad de la red. Esta solución también permite actualizar constantemente los dispositivos.

Cuando estas herramientas de recuperación no son efectivas, el modelo proporciona accesos alternativos de diagnóstico de copia de seguridad que permiten a los administradores alcanzar zonas de la red que, debido a algún problema, pueden haberse vuelto inaccesibles. Esta solución puede ahorrar tiempo de desplazamiento a los lugares de ubicación de los dispositivos, algunos de los cuales son difíciles de acceder debido a las topologías de terreno en las zonas rurales.
Se presenta también un portal web de información para proporcionar información relevante y objetiva a los usuarios de la red. Siendo un portal de visita obligada para los usuarios, se puede utilizar para crear espacios publicitarios virtuales para que el proyecto sea financieramente todavía más autosostenible.

Finalmente, el modelo propone la monitorización de usuarios para evitar abusos de tráfico y el uso de sistemas de calidad de servicio (QoS) para crear prioridad en algunos tipos de tráfico de aplicaciones, como Voz sobre IP o transmisión de video. La solución permite mejorar el rendimiento de la red mediante la toma de decisiones inteligentes basadas en el estado actual de las variables de tráfico de la red que resultará en un uso justo de la misma y mejorará la calidad de la experiencia para todos los usuarios.

Las ventajas que estos sistemas inteligentes pueden aportar a las redes inalámbricas de las zonas rurales se centran en reducir los costes de instalación, mantenimiento y mejora del rendimiento de la red. Esto permite a la red crecer sostenible y crear condiciones para que los usuarios sigan utilizando la red con su máximo rendimiento.

**Resultado en la implementación del modelo de gestión**

El modelo de gestión se aplicó mediante el despliegue de una red inalámbrica en el proyecto "Memória Online" ubicado en Memória, un pequeño pueblo del centro de Portugal. Las características del pueblo elegido y su localización están clasificados como área rural.

Para este proyecto, se instaló una solución de monitorización de código abierto con el fin de permitir la configuración de todo tipo de dispositivos y servicios, independientemente del fabricante o la arquitectura. Este software permite la creación de plugins para monitorizar cualquier servicio o información que sea necesaria. Esto permite que el software sea escalable y su funcionalidad casi interminable. Se ha realizado la interacción de este servicio de monitorización con otras aplicaciones permitiendo aprovechar los datos de monitorización para otras aplicaciones. El uso del histórico y la creación de gráficos y mapas disponibles para el administrador a través de interfaces gráficas intuitivas y fáciles de usar, facilita la
monitorización, la identificación rápida y resolución efectiva de problemas así como la prevención de los mismos. A través de la comparación de comportamientos entre dispositivos, el administrador puede adoptar una actitud proactiva sobre eventos y comportamientos futuros, evitando así movimientos innecesarios y pérdida de tiempo.

La configuración realizada en estos dispositivos permite la ejecución automática de comandos predefinidos en caso de fallo, permitiendo en algunos casos resolver problemas en el momento exacto en que se producen.

Los usuarios pueden ser monitorizados y supervisados debido a la configuración de proxies y la creación del portal web. El primer proxy tiene como objetivo controlar el tráfico web con el fin de evitar abusos en la descarga de ciertos tipos y tamaños de archivos. Aunque las velocidades se reducen en descargas de archivos grandes, permite que la red sea viable para todos los usuarios. Dado que la conexión a Internet es de 8Mbps con una tasa de contención de 1 a 50, es necesario racionar muy bien el acceso al ancho de banda. Los resultados han sido satisfactorios, ya que el tráfico generado por los usuarios es elevado, teniendo en cuenta las restricciones de tráfico aplicadas. El segundo proxy tiene como objetivo redirigir la primera acción del usuario al portal web. En este portal, es posible poner a disposición de la comunidad mensajes importantes y dar a conocer a las entidades que hacen posible la ejecución del proyecto. Además, en el portal web, los usuarios se registran automáticamente en una base de datos que monitoriza constantemente su tráfico en la red. El resultado de esta monitorización permite obtener un conocimiento estadístico sobre el uso de la red.

La puesta en práctica del modelo de gestión ha dado como resultado una infraestructura de red sostenible y estable en el área rural de Memória. La gran retroalimentación dada por los residentes que utilizan la red son satisfactorios para el proyecto. Las autoridades locales también están disfrutando del excelente servicio que está disponible para toda la comunidad. Sin el estudio y desarrollo de este modelo de gestión, la longevidad de esta red estaría en peligro.
Abstract

Communication technologies have evolved and grown exponentially in recent years. Unfortunately, this growth is not the case in rural areas, where the small population density does not justify the investment made by internet providers.

The creation and development of projects in rural wireless networks are often a cheap and effective alternative. However, these projects tend to disappear soon after their implementation mainly because of poor quality of electricity, lack of specialized teams, lack of periodic and predictive maintenance and the absence of money to keep the project sustainable for many years.

Based on these issues, a proposal was prepared for a management model that aims to eliminate the difficulties inherent to wireless networks in rural areas through the creation of intelligent system for monitoring devices and services that allow efficient diagnosis and troubleshooting as well as proactive maintenance.

The management model succeed in decreasing the cost of specialized personnel and unnecessary travel to the network location, by creating solutions for automatic recovery and dynamically manage the configuration of the devices.

The management model also presents an intelligent distributed system that can help the network administrators in maintenance tasks by applying automatic intelligent actions and decisions, ease the installation of new network devices for end users, automatically update existing devices, and manage network traffic by applying algorithms that will decide based on intelligence. This is achieved by using an intelligent distributed system that is executed in every device of the network and is capable of making decisions and actions that will help administrators with problem-solving, automatic configuration of devices, proactive bandwidth and network traffic management, and reduction of costs in maintaining the network.

The results obtained by implementing the management model in a rural wireless network, allow to prove the effectiveness in the diagnosis and the resolution
of problems, beyond ensuring a reduction of costs associated with specialized personnel.
# Contents

1  INTRODUCTION ......................................................................................................................1

1.1  SCOPE AND MOTIVATION ..........................................................................................3

1.2  OBJECTIVES AND METHODOLOGY ........................................................................4

1.3  RESEARCH EVOLUTION .............................................................................................6

1.4  STRUCTURE OF THE WORK ......................................................................................9

2  LITERATURE REVIEW ........................................................................................................11

2.1  WIRELESS NETWORK TECHNOLOGIES IN RURAL AREAS ......................................11

2.1.1  802.22 - Wireless Regional Area Networks (WRAN) .......................................12

2.1.2  802.16 - Wireless Metropolitan Area Networks (WMAN) ................................13

2.1.3  802.11 - Wireless Local Area Networks (WLAN) .............................................14

2.2  WIRELESS NETWORKS DEPLOYMENTS IN RURAL AREAS ....................................28

2.2.1  Case Studies ...........................................................................................................29

2.2.2  Common Problems ...............................................................................................35

2.3  MANAGING AND MONITORING WIRELESS SENSORS NETWORKS ....................41

2.3.1  Monitoring Methodologies ....................................................................................44

2.4  SUMMARY ....................................................................................................................69

3  MANAGEMENT MODEL FOR WIRELESS AREA NETWORKS .......................................71

3.1  SUSTAINABILITY OF A WIRELESS NETWORK IN RURAL AREAS ............................72

3.2  ARCHITECTURE OF THE MANAGEMENT MODEL ....................................................73

3.3  MONITORING DEVICES AND SERVICES ................................................................74

3.4  DIAGNOSIS AND PREVENTIVE MAINTENANCE ....................................................75

3.5  INTELLIGENT MONITORING FOR AUTOMATIC RECOVERY ...............................77

3.6  DEVICE AUTOMATIC CONFIGURATION .................................................................80

3.7  INFORMATION AND ADVERTISEMENT ....................................................................81

3.8  USERS AND PROACTIVE BANDWIDTH MANAGEMENT ...........................................81
3.9 REVIEW OF THE MANAGEMENT MODEL ..................................................93
3.10 SUMMARY .........................................................................................94

4 RESULTS IN APPLYING THE MANAGEMENT MODEL .................................97

4.1 PILOT DEPLOYMENT (MEMÓRIA ONLINE) ...........................................97

4.2 MONITORING SOFTWARE ......................................................................100
   4.2.1 Configuration Files ........................................................................102
   4.2.2 Objects ..........................................................................................105
   4.2.3 Plugins .........................................................................................106
   4.2.4 Hierarchy and Dependency of Objects .............................................108
   4.2.5 Monitoring Devices ........................................................................109
   4.2.6 Network Services for Management ...............................................115
   4.2.7 Internal Device Information ............................................................121
   4.2.8 Notifications ..................................................................................127

4.3 SIMPLE NETWORK MANAGEMENT PROTOCOL ....................................129

4.4 MONITORING HISTORY ........................................................................131

4.5 MAP USAGE IN MONITORING ..............................................................134

4.6 WATCHDOG ..........................................................................................135

4.7 WEB PROXY ........................................................................................137

4.8 NETWORK USAGE ..............................................................................139

4.9 LESSONS LEARNED ...........................................................................139

4.10 SUMMARY .........................................................................................140

5 CONCLUSIONS .....................................................................................143

5.1 FUTURE WORK ....................................................................................146

6 REFERENCES .........................................................................................147
List of Figures

Figure 1 – Overview of the most important links in the Akshaya network ....................................................... 31
Figure 2 - Representation of Aravind Network ........................................................................................................ 33
Figure 3 - AirJaldi network topology ..................................................................................................................... 34
Figure 4 – Architecture of the management model for a low-cost rural wireless network .............................. 74
Figure 5 - Monitoring network services and internal services of a wireless router ................................. 75
Figure 6 - Example of a network dependency: the red zone of the network is unreachable due to an error with a wireless router ................................................................. 76
Figure 7 - Monitoring System Core ..................................................................................................................... 78
Figure 8 - Algorithm for automatic device configuration ................................................................................. 80
Figure 9 – Algorithm to prevent network congestion ......................................................................................... 86
Figure 10 – Algorithm to prevent congestion on high QoS classes ............................................................... 88
Figure 11 – Algorithm for “happy hour” QoS management ................................................................................ 89
Figure 12 – Algorithm to act when congestion is set on high priority classes .............................................. 90
Figure 13 - Theoretical results of signal coverage (red = great coverage; green = no coverage) for the village of Memória ........................................................................................................ 99
Figure 14 - Hierarchy of file categories used by the Nagios service ............................................................... 103
Figure 15 - Example of a device hierarchy ........................................................................................................ 108
Figure 16 - Web interface with presentation of services in the LAR1_10 devices ........................................ 120
Figure 17 - List of LAR_10 services in the monitoring software web interface .............................................. 127
Figure 18 - Signal level change on one of the wireless links between two routers ........................................ 132
Figure 19 - Example of a chart created through a history of checks made to the processor of a wireless router ...................................................................................................................... 133
Figure 20 - Example of problem identification ................................................................................................. 134
Figure 21 - Example of a small map created representing zone LAR1_10 and its information .......... 135
Figure 22 - Web portal in the Memória Online project .................................................................................... 138
Page intentionally left blank
List of Tables

Table 1 – Summary of the main evolutions in 802.11 ...............................................................17  
Table 2 - Selected passive monitor studies ..............................................................................45  
Table 3 - Comparative Analysis of Passive Monitoring Studies ..............................................50  
Table 4 - Selected active monitor studies ..................................................................................52  
Table 5 - Comparative Analysis of Active Monitoring Studies .................................................56  
Table 6 - Selected active monitor studies using SNMP protocol ............................................58  
Table 7 - Comparative Analysis of Active Monitoring Studies using SNMP protocol ..........64  
Table 8 - Selected hybrid monitor studies ...............................................................................66  
Table 9 - Comparative Analysis of Hybrid Monitoring Studies .............................................68  
Table 10 - Commands for monitoring device status .................................................................110  
Table 11 - Services to be monitored on MikroTik Routers .....................................................115  
Table 12 - List of services to monitor in Ubiquiti APs .............................................................116  
Table 13 - Commands for service monitoring ........................................................................116  
Table 14 - List of internal services to monitor on Mikrotik routers .......................................121  
Table 15 - List of internal services to be monitored in Ubiquiti AP .......................................122  
Table 16 - Commands for monitoring via SNMP protocol ....................................................122
Page intentionally left blank
"The new information and communications technologies are among the driving forces of globalization. They are bringing people together, and bringing decision-makers unprecedented new tools for development. At the same time, however, the gap between information ‘haves’ and ‘have-nots’ is widening, and there is a real danger that the world’s poor will be excluded from the emerging knowledge-based global economy.” – Kofi A. Annan [12]

Computer technologies and its services are emerging at a very fast pace, covering all the different sectors of our society and business. The Internet that once was known as a large library of knowledge is today a “global village” where a common user can buy, sell, talk with old friends, meet new friends, study and even work remotely.

Statistical data show us that the number of users connected to the internet is having a growth of about 10% each year. This growth has been pushed up due to the falling prices for services of information and communication technology (ICT). However, this growth is only manifest in high density population areas, where the prices are very competitive and the speed and the services offered are very tempting for the usual customer. Rural areas of low population density are in most cases, left with old and weak technology, if any at all. The actual Internet offer is not equal for everyone due to the non-profitability of implementing Internet services on rural
areas [1–4]. In rural areas, where the population density is very low, the technology should be as simple and cheap possible [5–8].

In the last decade, wireless networks based on Internet Protocol (IP) have been used in rural areas and developing countries by communities and research group, with the intent of providing a cheaper Internet access. These networks are usually low cost, well known by the users, and can achieve a considerable distance to be used in a rural area [2, 6, 8, 9].

While these types of wireless networks in rural areas are fast to deploy, they also tend to disappear quickly due to same problems which will be explain in the following subchapters. From the literature review, when designing and planning a wireless network for a rural area, the researchers and administrators must focus not only on the installation details, the high bandwidth available for users, the social visibility and the economic factors, but also on the problems that may emerge in the future and the resources needed to solve them [2, 10]. Troubleshooting required in a rural wireless network is not always an easy process, especially when there is no data or information to help. Even for the more experienced administrators and technicians, some decisions are hard to define because the available documentation and data are forgotten when the network is planned. A good management solution for wireless networks in rural areas must take into account all these aspects that allow the network to grow and be sustainable for a long time.

Due to the growth of these types of network, other type of services and networks are also being implemented on rural areas. The exchange of information between machines is not enough for what we can accomplish. There is a need to receive and send information from the “things” in our everyday lives. Internet of Things (IoT) is becoming present in our everyday modern telecommunication life. The concept is the ubiquitous presence in things and objects around us to gather data and interact with each other. This presence in “things” opens up opportunities in projects on different fields of interests (agriculture, military, logistics, transportation, safety, medical, industry, home automation and robotics).

Recent development is being made with wireless sensors networks in rural areas on agriculture through the control of the soil and air characteristics, such as
humidity or soil temperature, but also on medical and safety fields by providing sensors that control elders and other people that need constant assistance in their homes. However, most computing devices used in the IoT are expected to be resource constrained, not only in processing and memory capabilities, but also in battery and signal strength for communication. Typical devices in IoT are equipped with very few microcontrollers that have low capacity of RAM and storage.

Managing and monitoring these IoT network may be a greater challenge, because of the many restrictions and limitations mentioned earlier. A vision from Ericson [11] is that in 2020, more than 50 billion devices will change the way that we interact with each other, including our “things” and objects. With such a high number of devices it is impossible to manage each node individually. A proper management solution is required for these types of networks, especially the ones that co-exist with wireless network in rural areas.

That being said, the focus of this work of investigation is to develop intelligent systems and management modals for wireless networks in rural areas. This chapter focuses on presenting the scope and motivation of the research made and also identifies the problems related to implement and deploy a wireless rural area network and its services.

1.1 Scope and Motivation

This thesis describes intelligent systems and management models for wireless networks in rural areas. This thesis contributed to a research in multiples areas of investigation, many of which are undergoing a great development and will lead our work to further research in the future.

The research in developing conditions and implementing computer technology in rural areas is a challenging problem due to the limitations of these areas. To implement such as scenario there is a need to research all the aspects of deploying a wireless network and all its services associated. There is a wide range of research lines in this area that deeply motivated our investigation work.
One of the key features in our work is the use of artificial intelligence to create functions that help the administrators of the networks to achieve a good wireless network quality for the final users. Computer networks and all its devices and services generate many flows of information that can be used in artificial intelligence, such as pattern recognition to generate automatic actions in the network and its devices. The algorithms implemented must come from a learning experience and a previous knowledge of the services and devices of the network.

Other feature in our work is the deployment of a real case scenario. This was very motivating because our work contributed in helping a community of people and business. By deploying a wireless network in a rural area that connects to the Internet, we were improving many people lives. In these areas, the Internet may diminish the isolation and loneliness that most of the elders have at their homes. This potentiates the equally among people from different generations and locations.

It has also contributed in creating many research opportunities that allow us to further investigate and create services and implementations for the scenario deployed.

1.2 Objectives and Methodology
The main objective of this thesis is to identify the requirements to manage and monitor a wireless rural area network and to create a management model that supports the administration of the wireless network as easy, economic and sustainable as possible.

Based on recent studies in rural areas, we identified the problems and results from each study in order to obtain our management model.

The objectives of this thesis are:

- Study and identify problems and results obtained in projects of wireless networks in rural areas or developing countries;
- Study and identify using different approaches how to manage and monitor low resource devices used in wireless sensor networks;
- Creation of a management model capable of:
o Monitoring all active network devices and its services, in order to identify problems;

o Constant data collection of all active network devices and its services in order to detect, anticipate and aid in the diagnosis of problems;

o Creation of a database to store all the information in order to serve as a basis for diagnostic and problem prevention tools (predictive model);

o Identify intelligent systems that could be used to enhance the network to be autonomous and self-sustainable, therefore minimizing its cost and maximizing its longevity and sustainability;

o Use graphical tools to present all the information gathered in an easy and effective way to the administrators;

o Monitor users’ behavior to establish quality of services processes.

o Provide a graphical tool to display important events or problems for all the users of the network;

o Implement the management model in a rural area to demonstrate its importance in the sustainability and to show the importance of these wireless networks.

For each objective of this thesis, a research was needed in the state of the art. First, a research was made to the wireless technologies in order to identify possible solutions but also to transmit some knowledge to the process of deploying our results. Also the work done by researchers in deploying wireless network in rural areas was used to identify the limitations and difficulties they had experience, but also to learn with its mistakes and solutions in managing and monitoring these wireless networks. After this, the proposed model for managing a wireless network was based on this state of the art. The implementation of this model in a real project allow to obtained data and feedback from the people using the network. With the amount of information available, a further research was made to study what
methods could be used to apply intelligence in the network using algorithms, probabilistic and machine learning techniques.

1.3 **Research Evolution**

The cause of this research began with the proposal of creating a wireless network in a rural area in Portugal. To achieve a good result the first efforts were understand the difficulty and problems that could arise in these remote locations, where the access to the Internet was slow and expensive.

A literature review was done in two stages. The first stage was researching what wireless communication technology should be used in order to achieve a stable and economic solution. The second stage of literature review was researching projects implemented in rural areas and developing countries. Our research identified major problems that had been experienced in some deployments, but also possible workarounds. The main problems found were: (i) the cost of the technology of the solution can compromise future operation and high cost of maintenance; (ii) the low quality of electric power causes power outage that may corrupt files in devices and in some cases destruction of the device’s power supply; (iii) bad diagnose and lack of information usually reported by staff or users with little knowledge and skills in computer networks may cause unnecessary and expensive visits of expert staff; (iv) non-existent remote management leaves the administrators and expert staff in the dark with no information about the overall status of the network and with no service to perform remote tasks for updating of implement new services of features in the network; (v) poor maintenance due to the lack of information may cause a small problem in a device to grow in to a huge problem for the network; (vi) lack of automatic recovery could cause unnecessary and expensive visits of staff and long outages of the network; (vii) slow internet access caused by a big contention ratio configured by the internet providers; (viii) lack of quality of service (QoS) implementation can permit the abuse of traffic by a single user; (ix) network dependency and an unique gateway creates a single point of failure in the network.
After the literature review, the architecture for management and monitoring of the wireless network was created keeping in mind the problems that could be found during and after the deployment. The biggest importance was given to create a self-sustainable and long-lasting model for future projects. Prior works showed that these projects must include management and administration solutions to avoid the overall failure of the network. Our management model focus is based on the following characteristics: (i) automatically monitor all devices and services offered to the users, and send out alerts to the administrators in case of problems; (ii) diagnostic solutions to help the administrators to get information of current or past values of the devices or services that allow them to provide a good diagnose of the problem and act precisely; (iii) preventive maintenance can be achieve by constantly read information gathered from the network that could point to a future problem allowing the administrator to act and provide a preventive maintenance with the goal of maintaining the network operating; (iv) provide a mechanism to automatically recover devices or services that stop working properly; (v) create an intelligent system that can predict problems based on probabilistic or machine learning techniques (vi) create an intelligent system to automatically configured new or replaced devices in the network, to allow staff with no expertise to do maintenance tasks and add new users in the network; (vii) create visual interfaces that allow the users of the network to be informed about the status of the network; (viii) this previous visual interface for the end users could also be used to apply virtual advertisement of local events and business that could generate some profit that help the network to be economical sustainable for the future; (ix) create an authentication system to fully register users actions in case of legal actions against the network; (x) implementation of quality of service to guarantee that the low bandwidth available could be shared by all the users and by all the applications fairly and equally; (xi) create an intelligent system that proactively manage the bandwidth available to all users when the network is congested.

The deployment of the network was done in a small village in the center of Portugal, and some features of the management model were successful implemented.
Later after the deployment of the wireless network it was decided to research how to deploy and use wireless sensors network in elders and agriculture business. This decision lead us to a second literature review on managing wireless sensor network, to identify how can the devices used in these network can be managed without interfering with their normal operation. Being devices with resources constrained, the common monitoring and managing services cannot be used fully. From the studies researched, a proper management planning must consider: (i) the management system must be able to monitor a large number of devices, which may be network segmented; (ii) the management system must be able to work with different types of devices or to have the ability to interoperate with different systems; (iii) in some cases, the constrained devices must be able to establish connectivity (auto configuration) and be able to deal with a sudden loss of neighbors or being moved to other location. The managing system must be able to discover the devices on the network and recognize it as a trustily or unknown device in the network; (iv) a monitoring application must be prepared for different scenarios. In some use cases (environment, infrastructure), the monitoring application must be designed to tolerate a number of failures, a high number of hours in order to detect a fault and a couple of days for manual repair. In other use cases (industrial, energy, medical, military) a monitoring application must be designed to be constantly monitoring the state of the devices and to detect a fault in a few minutes or in a small number of seconds for critical services (real time detection); (v) the monitoring information must be simple and able to work at critical conditions; (vi) in most cases it may be more cost effective not to repair the device, but substitute it. In cases where the devices are difficult to access, a self-healing feature could be of good use. Also, these devices should have a minimum configuration, or none; (vii) the management protocol could include security protections such as access control, confidentiality, integrity and availability of data.
1.4 Structure of the Work

From the previously proposed objectives, this document starts with the current chapter introducing the scope and motivation of the thesis. It also introduces the objectives to reach and the evolution of the research made.

Chapter 2 presents the literature review on the main concepts of this thesis in the subchapters: wireless network technologies, management of wireless networks in rural areas and management of wireless sensors network. This chapter presents some of the technology used in rural area, as well as the work made by other authors and their findings, problems and difficulty encountered.

Following the analysis carried out, the proposed management model, its architecture, and its intelligent services are presented in Chapter 3. The proposal aims to provide solutions to the most common problems of wireless networks in rural areas. The management model focuses on: (i) monitoring devices and services; (ii) diagnosis, preventive maintenance and automatic recovery; (iii) information and advertisement for end-users; (iv) users authentication and user traffic management; (v) applying intelligence in managing devices and services;

Chapter 4 presents the implementation and results of some modules defined in the management model in an existing rural wireless network projects called “Memoria Online”, deployed in a small village of a rural area in center of Portugal.

The conclusion of the dissertation is made in chapter 5 which presents the conclusion of the proposed management model and its implementations. Some information of future work is also presented.
Chapter 2

Literature Review

This chapter presents the literature review on the main concepts of this thesis. Initially, the latest communication technologies that could be used in a rural area will be presented, with specially focus on the unlicensed standard 802.11. The 802.11 standards and their amendments will the described in detail.

After this introduction to the technologies, a literature review is made at deployments of wireless networks in rural areas. Some case studies documented by the scientific community are presented and the common problems of these deployments are identified in depth, which will be the foundation of the management model presented in this thesis.

Finally, a literature review on managing and monitoring wireless sensors networks will be presented. This study will focus on methodologies used to monitor the resources constrained devices without interfering with the low resource wireless sensor network and to try to gather as much information as possible for diagnose and managing purposes. It presents for each methodology its strong and weak key features. A comparative analysis is done for each methodology.

2.1 Wireless Network Technologies in Rural Areas

Over the past 20 years, there has been an exponential growth in communication technologies. This great evolution has been mainly noticed in the speed of
transmission and reception of information reached. In late 1990s, the 56kbps connections reached the developed countries and since then, the speed of communication have been increasing through the implementation of new technologies. However, this growth in quality and speed of access has been limited to urban areas where there is a large population density. Nowadays in Portugal, speeds of about 100Mbps through fiber optics is available for about 30% the population, most of which living in urban centers [13]. Since the year 2007, the appearance of mobile broadband access has given to rural areas an alternative method of communication, but this has proven to be insufficient due to the slow speed of access. It is necessary to wait a few more years until these mobile network technologies evolve and propagate better through the installation of new antennas with higher performance and capacity of users.

Taking into account the limitation and difficulties of rural areas, the emergence of wireless technologies has made possible in the last decade to create broadband access in rural areas. In next subchapters, some wireless technologies are being presented as a possible usage in rural areas projects.

2.1.1 802.22 - Wireless Regional Area Networks (WRAN)

IEEE 802.22 is a technical standard by an IEEE (Institute of Electrical and Electronics Engineering) working group that was created in 2004. This standard is intended to use the whitespaces of the spectrum normally used by VHF and UHF frequencies of television broadcasters between 52 and 862 Megahertz’s (MHz). When this spectrum was assigned to televisions broadcasters, the existing technology was not optimized, so the channels were very large which lead to a great waste of the spectrum available. In addition, given the number of VHF and UHF channels used, there are significant holes or white spaces between channels to fill. This situation in a rural setting is still more evident, since the usage of these frequencies is even smaller.

The standard could play a key role in the spread of wireless internet rural areas as low power (200mw) radio signal at a frequency of 100MHz that can reach
tens of kilometers of range, including line of sight connections. Obviously, there are always setbacks in all systems. In the case of the 802.22 standard, TV broadcasters are not very favorable to the use of so-called white spaces, as minimal interference will jeopardize all the emission in that region. The IEEE working group proposed various mechanisms to ensure that such situations do not occur.

One method for avoiding undesirable interferences is using frequency detection. The idea is simple: the device listens to the frequency bands to use to ensure that it will not interfere with the emissions using the same frequency. However, television broadcasters sometimes use other frequencies sporadically. In these cases, the system would have to continually tap the medium so that as soon as it detects any signal on its channel, it stops transmitting [14]. However, this would put significant delays on the technology and would allow serious security breaches.

The published studies focus on the resolution of this problem in cognitive radio channels [15, 16]. Cognitive radio is an intelligent wireless communication system that is aware of the environment around it and changes its transmission parameters based on the interaction it makes with the environment in which it operates, with the following objectives: highly reliable communication and efficient use of the radio spectrum.

This technology uses Time-Division Duplex (TDD) and Frequency-Division Duplex (FDD). By using a 6MHz channel, it is possible to reach a bandwidth up to 23Mbps. If more channels are used the bandwidth can be up to 70Mbps. Regarding quality of service and security issues the model is not yet defined, but everything indicates that it will be identical to those already existing in similar technologies.

2.1.2 802.16 - Wireless Metropolitan Area Networks (WMAN)

The working group for the 802.16 standard was formed in July 1999. The initial purpose of this group was to create a wireless technology based on in-line connections that would offer the end-user speeds in the order of 100Mbps in areas where it would be impossible to place infrastructures such as optical fiber. The first version of the standard was adopted in 2001, but amendments (a, b and c) which addressed problems related to spectrum, quality of service and interoperability soon
followed. The principle of operation of the technology is point to multipoint (a base station communicates with several client stations).

The project was completed in 2004 with the release of the final version of the document. The 802.16-2004 standard (802.16d) is part of the model initially developed and from which it was published. An amendment was made to 802.16-2004, the IEEE 802.16e-2005, which included mobility. This standard added a number of improvements to the previous standard that included better QoS support and the use of Scalable Orthogonal Frequency Division Multiplexing (SOFDMA) to allow line-of-sight connections. This technology was later termed mobile WiMAX after the creation of the WiMAX forum. It is important to note that the 802.16 standard is not WiMAX. WiMAX is a group that works on the search for interoperability of devices to work with standards defined by the IEEE 802.16 group.

The great evolution of 802.16 is mainly in the normalization of the first layers of the Open Systems Interconnection (OSI) model (PHY and MAC) of the device. Later, the 802.16m and 802.16h standards aimed to support a throughput of up to 1Gbps in order to be recognized as a 4G NGMN (Next Generation Mobile Network) technology.

In the end of 2009, it was launched in Portugal an auction for bidding of operating licenses for the provision of broadband services in the frequency spectrum between 3.4 and 3.8 Gigahertz’ s (GHz). Although it was presented as an alternative to optical fiber due to the considerable bandwidth over long distances, the usage of this technology was not as high as the initial perceptions.

2.1.3 802.11 – Wireless Local Area Networks (WLAN)

The 802.11 (Wi-Fi) standard group is today the most widely used wireless technology in the world for IP communications. One can easily find an 802.11 wireless network at a friend’s house, at corporate office, on campus and at public parks. This technology will be presented detailing its standard as well as its current advantage to be used in a wireless broadband network in rural areas.
2.1.3.1 History of WLAN

In 1990, IEEE started a group to create a standard for wireless connections. After 7 years of research and development, the first IEEE 802.11 standard was approved. This standard considered the use of the frequency range between 2.4GHz and 2.4835GHz. This initial version of the standard allowed 1Mbps to 2Mbps transmissions, and like the other 802 standards, its structure is based on the OSI model, which was compatible to an ordinary wired network. This was undoubtedly the great advantage of this standard, and the reason it is still the most used until today. Of course, any network, application, operating system or protocol would work on an 802.11 wireless network just as it would work on an Ethernet network.

2.1.3.2 Features

The 802.11 standard took into account some differences between the existing physical network and the wireless networks, such as:

- **Power:** The first wireless network cards used PCMCIA technology so they can be used in any existing mobile device. However, the problem is that this device are dependent on a battery. When adding a wireless card in a laptop computer, the batteries lasted much less time. The 802.11 working group decided to create a standby mode, where power consumption was minimal when there were no transmissions. The MAC layer implements power saving functions when there is no transmission during a predefined period, but the problem with this implementation is that when there is a transmission, the device does not receive it because it is in standby mode. The 802.11 standard solved this problem by creating buffers for the waiting messages; Periodically "sleeping" stations wake up to check and process waiting messages;

- **Bandwidth:** The spectrum used until this standard did not offer the possibility of having a nice bandwidth and the transmission rates were insufficient for the applications used. 802.11 through data
compression methods managed to achieve sufficient bandwidth using the best possible spectrum available;

- **Security:** The signals from a wireless connection reach undesired areas and therefore are susceptible to being seen by other users. Thus, these networks have a much larger area to protect than cable or fiber optic connections. All this work began with the 802.10 working group, which was responsible for security research on all 802.11 standards. Later, this group joined the 802.11 working group.

In recent years there have been successive improvements made to the lower layers of the OSI model that have contributed greatly to the success and longevity of 802.11 networks. The priority has always been to ensure more and more speed, but this was just the top of the iceberg. The 802.11 is today a robust technology, capable of supporting the most varied and demanding applications (e.g., voice, video), guaranteeing quality, safety and stability.

Other standards that are still under development will continue to streamline and improve existing services. The following topics will present all developments in this technology as well as the future trends of newly created working groups to develop the new standards.

### 2.1.3.3 Key Evolutions

The initial standard was widely accepted by hardware and software companies, which led to major developments in the research of new standards. On the other hand, the initial 802.11 standard has quickly become obsolete in terms of transmission speeds. The next few topics will present some of the most important standards that have emerged, some of which are still used today. These evolutions are summary in Table 1.
2.1.3.3.1 802.11a

The 802.11a standard was created in 1999. This standard had as main novelty the use of frequency near the 5GHz. Although this frequency allowed higher transmission values (54Mbps), its main disadvantages is the use of an unlicensed frequency, and therefore not accessible for all, in addition to a short signal range[17].

Although it was created in 1999, it was only in 2001 that the first device available for use of this standard began to exist. This delay in the creation of device has made the newly created 802.11b standard grow faster, making it global. The incompatibility between them meant that only one had an impact at a global level, and the high price of 802.11a device made it secondary, since its advantage lay only in short-range speed.

2.1.3.3.2 802.11b

The 802.11b standard published at the end of 1999 was the first amendment to the initial 802.11 standard. The main upgrade was the speed increase to 11Mbps (as opposed to the initial 2Mbps) and also a range far greater than the previous one [18]. Thanks to these improvements and the emergence of numerous devices from different manufacturers, it quickly became a technology of great acceptance and

<table>
<thead>
<tr>
<th>IEEE STANDARD</th>
<th>802.11</th>
<th>802.11B</th>
<th>802.11A</th>
<th>802.11G</th>
<th>802.11N</th>
<th>802.11AC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max. Data Rate</strong></td>
<td>2Mbps</td>
<td>11 Mbps</td>
<td>54Mbps</td>
<td>54Mbps</td>
<td>600Mbps</td>
<td>1300Mbps</td>
</tr>
<tr>
<td><strong>Channel Bandwidth</strong></td>
<td>20 MHz</td>
<td>20 MHz</td>
<td>20 MHz</td>
<td>20 MHz</td>
<td>20/40 MHz</td>
<td>20/40/80/160 MHz</td>
</tr>
<tr>
<td><strong>Frequency(s)</strong></td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
<td>2.4 GHz</td>
<td>2.4/5 GHz</td>
<td>5 GHz</td>
</tr>
<tr>
<td><strong>Spatial Multiplexing</strong></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 1 – Summary of the main evolutions in 802.11
use. The increased demand for this technology has significantly lowered the price of hardware, making it a technology available and accessible to anyone.

802.11b wireless cards run at 11Mbps, but also at 5.5Mbps, 2Mbps and 1Mbps depending on signal quality. Since lower speeds use less complex methods of encoding, they become less susceptible to interference and signal loss.

2.1.3.3.3 802.11g
In June of 2003, a new standard was created: 802.11g. Identical to its predecessors, 802.11g uses the 2.4GHz frequency, but operates at a significantly higher speed (54Mbps), identical to 802.11a. This announced speed is significantly higher than that observed in real environments, since the maximum real throughput for a transmission is 24.7Mbps. In addition to the high speed of 802.11g, its interoperability with the 802.11b standard was its greatest asset for market acceptance and commercialization. Quickly, dual-mode devices (802.11b and 802.11g) were created, which supported both technologies [18].

Although 802.11g was expected to be at high speeds and stable environments, the 802.11g standard was disappointing due to several factors: first, the conflict with 802.11b-only devices exposed the new device to the same 802.11b interference; second, the limitation of the number of channels available (3 channels without overlapping frequencies); and third, the fact that the 54Mbps transmission rate is much more susceptible to interference, caused transmission speeds to fall to values close to 802.11b.

2.1.3.3.4 802.11n
In 2004 a new working group (TGn) emerged with the aim of developing a new standard that would improve performance, provide greater coverage, and improve reliability. In 2007, the draft of this standard announced that it would be able to have real speeds greater than 100Mbps, much higher than the current 24.7Mbps of the 802.11g standard. Identical to its predecessors, the 802.11n standard continues to use Orthogonal Frequency-Division Multiplexing (OFDM) modulation, although it allows bandwidths in the order of 65Mbps using 52 subcarriers instead of the 48 previously existing ones [18].
What stands out most from this standard is the new technology called Multiple Input Multiple Output (MIMO). When a radio wave propagates through space, it does not always have the same direction. When it strikes or reflects in an obstacle, its path is different from another wave that crosses the space in a straight line to the receiver. In a normal transmission, this effect is sometimes considered a destructive signal because the signals arriving at the destination are time-shifted which lead to new retransmissions and cause instability, delays and poor quality.

MIMO transforms this problem into an advantage: the transmitter divides the signal to be sent in several parts which are sent by several antennas (2 to 4) and are received by one or more antennas [19]. This new method of propagation would identical to having several directional antennas on one side to transmit and as many directional antennas on the receiver. The MIMO makes it possible to realize the same idea but using omnidirectional antennas radiating the signal in all directions. The transmitter and the client use a series of sophisticated algorithms to calculate all reflections and attenuations of the signal at the destination, thus making a signal that was previously considered noise, in an excellent signal [18].

Thanks to this system and to other improvements in existing technologies, it was possible to increase transmission speed and range. The speed has risen to 300Mbps and can reach 600Mbps when using 4 transmit antennas and 4 receiving antennas (4x4). In addition, with the use of multiple streams in the transmission, the signal range is about twice as high as the previous standards. Of course, such a system requires a large amount of processing to perform these calculations, which means an increase in energy consumption. In mobile terminal device this means faster battery consumption [19].

Thanks to the interoperability of the 802.11n standard, it is possible that users who own device with the 802.11g standard can connect to these new devices. However, when 802.11g clients are connected, the announced speeds are impossible to achieve. Another interesting aspect of this standard is the possibility to operate in 2.4GHz and 5GHz frequencies. However, to operate at 5GHz, it is mandatory that all customers are using device with the 802.11n standard. With the
usage 5GHz frequency, the signal distance will be significantly lower compared to 2.4GHz [20].

2.1.3.3.5 802.11ac

The 802.11ac standard was announced in 2013 and is an evolution of the 802.11n standard. The speed of the transmission can reach 1.3Gbps due to the addition of 80MHz and non-contiguous 160MHz channels of bandwidth and a maximum of 8 MIMO channels. The channel is dynamic and can vary from 20MHz to 160MHz. [21] This standard only works in the 5GHz frequency that suffers from less interference than the 2.4GHz. A higher order modulation scheme called 256-Quadrature Amplitude Modulation (256-QAM) is also used that allows a bigger amount of data in each waveform, which result in a cleaner signal between the end user devices and the access point (AP) [21].

One of the most important evolutions is the introduction of Multi User Multiple Input Multiple Output (MU-MIMO) that enables the use of beamforming that is a way of directing the signal to the user device by increasing the power in their direction. This standardization forces the usage of only one type of beamforming in all manufacturers [22].

2.1.3.4 Other Evolutions

The standards already presented were the most significant for communication performance (bandwidth) between the devices. The appearance of these standards automatically meant a demand in the market for devices that supports them.

However, in recent years, other standards have been created to improve all aspects of communications between devices such as security, reliability and others. Although these standards were not so important to most end users, their appearance allowed other features and applications to be used over wireless communication.

2.1.3.4.1 802.11e
With the emergence of voice over IP (VoIP) technologies, and streaming video and audio applications (web-conference and audio/video streaming), the need for quality of service was increasingly evident.

The initial 802.11 standard used two functions to implement quality of service: Point Coordination Function (PCF) and Distributed Coordination Function (DCF). However, these two functions were quite limited because they could not predict the type of traffic or guarantee response times. The 802.11e standard presented in 2005, aims to minimize latency, maximize bandwidth, and define traffic patterns [23].

This standard defines a new way of access called Hybrid Coordination Function (HFC), which uses two mechanisms: Enhanced Distributed Channel Access (EDCA), and HCF Controlled Channel Access (HCCA). Each of these mechanisms is responsible for identifying the type of traffic, based on a certain pre-established category based on the containment values and the interval value between frames [24].

2.1.3.4.2 802.11i

The purpose of this standard is to improve the security of wireless communications, as well as the authentication mechanisms already in place for MAC layer modifications. The appearance of this working group was due to the already detected vulnerabilities of the Wired Equivalent Privacy (WEP) algorithm.

In order to struggle all known failures of WEP, in 2003 the working group for the 802.11i standard Wi-Fi Protected Access (WPA) was created. One of the major changes to WPA was made in encryption, where a 128-bit key and a 48-bit Initialization Vector (IV) were used. By combining these two elements, it is possible to have \(2^{80,000,000,000,000,000}\) different keys. In addition to these innovations, the standard offered another novelty: the Temporal Key Integrity Protocol (TKIP). This protocol is based on the concept of temporal key, that is, the key is used for a certain time, and is generated again through an algorithm. In WEP, the same key was used time after time. However, the basis of the encryption used remained the RC4 system.
(used in WEP), which is widely used in Web security protocols, Secure Sockets Layer (SSL) [25].

At the authentication level, WPA uses two methods: Personal (WPA-PSK) and Enterprise (802.1x). The 802.11i standard also offers a Robust Security Network (RSN) with two new protocols, the 4-Way-Handshake and Group Key Handshake. Both are responsible for managing the master keys that both devices (client and server) need to communicate with each other.

Although WPA was very similar to the level of operation with WEP, it brought significant changes in data security. However, information quickly emerged that the system was vulnerable to attack. One of the main mistakes was in the construction of keys that were exchanged in the authentication but remained with the same values, which increased the chances of success for systems of brute force attack.

To combat these new problems and other, this standard was updated in 2007 with WPA2. The big difference for its predecessor was mainly in encryption. Thus, instead of RC4 used in WEP, the Advanced Encryption Standard (AES) was used. AES allows the use of 128, 192 or 256-bit keys, which together with TKIP makes the attack process very difficult. In WPA2 it is normal to use 256-bit keys, which meant an improvement of the existing hardware to be able to process this data as quickly as possible, without compromising quality of service mechanisms [25].

2.1.3.4.3 802.11k

The main purpose of the 802.11k standard is to measure radio communications data between devices so that new services such as roaming can be used in the best possible way [26].

These measurements are performed in the first two layers of the OSI model, in which it is possible to characterize the medium (radio electric environment), and to identify the device that is affecting the performance of others. The measurements are made in several characteristics of the signal, the most important being the load on the radio channel, signal noise, beacon frames, hidden nodes, and sensitivity to the medium, temporal histogram, among others.
In the case of roaming, the AP can analyze the information of the measurements through the beacon frames, analyze them and send them to the clients in list form, from the best to the worst existing AP at that moment. Until this standard, the devices had no information about the radio channels of other neighboring devices, causing several problems of interference. With the 802.11k standard, through analysis of signal noise, channel load, and time histogram, an AP can perform an evaluation of the quality of a respective radio channel.

Something previously identified in the measurements is the hidden nodes. Hidden nodes are those that are not accessible, or are not "heard" by other clients. With 802.11k, clients who can identify these hidden nodes pass this information to neighboring APs by sharing that information. Due to this, APs can identify which customers are at the limit of their reach.

Previously, only APs were able to access statistical data generated by themselves, but with 802.11k, when there is shared information from clients to APs and vice versa, all devices can now the state of the network in terms of performance, congestion, usage of channels, etc.

With these improvements, radio configurations become simpler, the diagnosis of radiofrequency problems is easier, frequency automatic planning is possible which enabling traffic distribution and a consequent increase in customer performance. Other existing services, such as VOIP, have benefited from the introduction of this standard thanks to improved roaming conditions, especially in the way customer handoff is handled.

2.1.3.4.4 802.11p

The 802.11p standard was created in 2010 to allow communication between mobile device and/or base stations moving at a minimum of 200km/h and whose distances can go up to 1000 meters [27]. This standard is called Wireless Access for the Vehicular Environment (WAVE).

This standard only support communications within the 5GHz frequency range, specifically between 5,850 and 5,925GHz with the particular aim of
increasing the mobility and safety of all surface-based communications, including trains and boats.

The main cause for the development of this standard are the radio communications behavior when the devices are moving at high speeds and low latency values (4ms to 50ms) are required.

2.1.3.4.5 802.11r

The 802.11r standard was published in 2008 to ensure that transition, or roaming, between two APs was as fast as possible. In the initial 802.11 standard, the transition was smooth, with only 4 messages for roaming devices. However, with the introduction of 802.11e (QoS) and 802.11i (WPA), restrictions on transitions became more demanding and time-consuming. For a service like VOIP, where the maximum delay time should be 50ms, these transitions must be simpler, in order to be faster.

The 802.11k standard introduced earlier made the roaming function easier by increasing the information each device has on the surrounding environment and neighboring device. Even so, the 802.11r standard was necessary to solve completely the delay times in the transitions.

One of the major issues identified in the delay was related to the 802.11i standard, which required that when a transition occurs, the client is required to renegotiate the keys with the authentication server, causing further delays. The solution was to split the transition in stages. When a client device needs to transition to another AP, authentication is performed on that same AP, but data from the normal transmission continues to be sent by the current AP. Once the authentication is done, the client device makes the transition knowing that it is already authenticated in the AP to which it will transit. However, this authentication is only effective when the device completes the transition, which is still sufficient to save precious milliseconds [28].

2.1.3.4.6 802.11w
The 802.11w standard was published in September 2009, and aims to increase security in Layer 2 frames of the OSI model, more specifically in management processes such as authentication, decoupling and association. During these processes, the 802.11 standard is subject to Denial of Service (DoS) attacks, because frames are sent in plain text. Although these attacks are not for invasion or theft of data, they make the network unavailable to users.

With 802.11w, these frames are encrypted, thus making all management processes secure [29].

2.1.3.4.7 802.11z

The 802.11z standard was announced in October 2010, and aims to define a new Direct Link Setup (DLS) in which users can exchange data without accessing APs, as it happens with other technologies, for example Bluetooth [18].

The initial standard already had something very similar: the ad-hoc. However, this type of connection had several problems and limitations. The main limitation was the inability of interoperability between devices from different manufacturers. In addition, these connections did not have an encryption and security system suitable for all other current communications.

More and more peripheral devices such as televisions, printers, phones and game consoles have 802.11 wireless interfaces. With the 802.11z standard and the new DLS system, these types of peripherals can connect directly to other devices. Once the connection is active, it is possible for the device to "fall asleep" to save energy and be "awake" only when needed.

2.1.3.4.8 802.11s

The 802.11s standard created in 2011, aims at the mesh networking by leveraging the capabilities of the MAC and PHY layers to support broadcast, multicast and unicast communications, thereby enabling network communication in mesh. These networks are denominated Wireless Mesh Network (WMN) [30].

Thus, the main objective is to create an automatic distribution system, which automatically learns topologies and network paths. The standard is focused on low
/ medium dimension networks with approximately 32 nodes, although this number may be larger. One of the main advantages of using a mesh network is the rapid installation and configuration of a backbone network. Due to its scalability, it is possible at any time to add nodes to the network, for example, to cover an area not previously planned.

Another advantage of great importance is the ability of the network to adapt itself to problems. Since there are several paths that will go to the same destination, the fact that one device, stops working may harm some clients, but not the other nodes in the network because they will "find" alternatives.

2.1.3.4.9 802.11u

The 802.11u standard was completed in 2011. The 802.11u standard is aimed at interconnectivity with networks other than 802.11 [18]. This is especially useful for hotspots. A normal user when searching for wireless networks in a hotel, garden, airport, does not want to know the names of the networks (SSID - Service Set Identifier), but rather what kind of services they can perform in each one. For example, in most cases it is more important for the user to know in which of the networks can access the internet. Thus, the 802.11u standard allows a device to access network information even before the user authenticates. In this way, when the user visualizes the networks, it will already know in advance what network services are available, emergency services and commercial services of the zone.

Other proposals for this standard include integration with high-level applications to provide more complete and user-focused experiences. An example of this is the use of device near a store in a mall. The store network could provide advertising services, with promotions and discounts on time, which would be viewed automatically as soon as the user searched the wireless networks.

2.1.3.4.10802.11v

The 802.11v standard was published in 2011 and was developed to centrally manage all device through a layer 2 mechanism of the OSI model. Very similar to the 802.11k that aims to obtain device data, 802.11v has the objective of configuring devices and its management.
Consequently, other interesting goals are possible with 802.11v, such as power saving, automatic firmware update, among others. In terms of energy savings, the most attractive function is wake on WLAN. The device may be suspended if it has no information to receive or send. This feature is extremely important on devices where battery management is critical, as with smartphones.

2.1.3.4.11 802.11aa

The 802.11aa standard was created in 2012 and aims to allow video stream transport over wireless networks with high performance and reliability by providing innovation to some mechanisms. It improves the multicast and broadcast transmission in order to offer a better link reliability and very small delays. It allows the streams of video to lower its quality if the channel capacity is insufficient by discharging packets [31].

2.1.3.4.12 802.11ad

The 802.11ad working group worked in conjunction with the 802.11ac working group, but using a 60GHz frequency. This standard is also known as WiGig. This standard is considered a wireless personal area network (WPAN) due to the short range of communication. One can think of this standard for use in substitution of television (HDMI) cables or transmitting uncompressed video [32].

   The frequency of 60GHz is barely used and has a wide bandwidth available (speed of up to 7Gbps), however the range is short and any obstacle may decrease substantial the strength of the electromagnetic radio signal.

2.1.3.4.13 802.11af

The 802.11af standard proposes the usage of the frequencies allocated for television broadcasters known as Very High Frequency (VHF) and Ultra High Frequency (UHF). Most of these frequencies are idle and unused. These frequencies are usually denominated TV white spaces. In order to allocate unused TV channels, the cognitive radio defines modifications to Media Access Control (MAC) and Physical Layer (PHY) layers.
The physical layer must have the ability to adapt to different conditions and have the flexibility to switch from one channel to another depending on the communication requirements and to adjust to the available bandwidth. With the aid of cognitive radio, which consists of each element of the network doing spectral sensing before transmitting, it is possible to use the white spaces. Channel power management is also used to update the list of available channels so that the respective base radio changes the maximum transmit power, channel, and channel width. Because it operates in a frequency range below 1 GHz, the IEEE 802.11af standard allows a greater coverage area. This standard can operate with up to four 6 MHz bandwidth channels, which can be adaptively aggregated according to availability. This adaptation or aggregation of channels is a task of cognitive radio, which can verify which channel has the best conditions to be used [33].

In practice, this technology is considered hazy because the effort to organize the radios dynamically without generating interference in the primary television service is still difficult. In addition, the proposed 802.11af in local area network (WLAN) conflicts in several respects with another working group that studies the so-called cognitive radios of geographic reach of the order of 100km through the standard 802.22 of WRAN (Wireless Regional Area Network).

In the next section, a literature review will be made at deployments of wireless networks in rural areas. Some case studies documented by the scientific community will be presented and the identification of the common problems of these deployments are showed in depth.

2.2 Wireless Networks Deployments in Rural Areas

In the last decade, wireless IEEE 802.11 deployments have been made all around the world in rural areas and developing countries. Some of these deployments focus on providing services for the local community such as health services or education services. However, network management is not always planned before the deployment of the network. Raman and Chebrolu [7] describe the experiences in using wireless technologies of the Digital Gangetic Plains (DGP) in India. Although they have identified most of the challenges and problems when deploying a rural
wireless network, five years after the start of the project, Raman et al. says that they “are in the process of putting together a network management tool”.

2.2.1 Case Studies

In this section, some case studies documented by the scientific community are presented. Initially a case study will be presented that focus on the financial aspect when choosing the technology to use on a project in a rural area. The remaining case studies will highlight the importance of rural networks for the development of social communities in these areas.

Based on these case studies, the common problems in wireless networks in rural areas will be presented, which will be the basis for the presentation of our management model that will solve them.

2.2.1.1 Akshaya, India

Although mobile phones are revolutionizing telecommunications in large cities in India, this is not the case in rural areas, where both the low population density and small income of users are an obstacle for telecommunications companies to invest in these areas. In order to implement a sustainable infrastructure, it is necessary to overcome some barriers, especially financial. Thus, the cost of technology is always the most important subject when planning a wireless network.

India is the most populous country in the world, accounting for 17% of the total land population. The population is mostly young (1 in 3 are under 15), 72% of the population live in villages and 20% live in extreme poverty. The number of computers is 2.7 per thousand inhabitants. Beyond these troubling figures, education and health are equally poor development and access areas for the average citizen [34].

An alliance between the Kerala state government and the Tulip IT Company was launched in 2002 to implement a wireless network in Malappuram district with 630 access points with education centers, equivalent to 1 per 2,000 households. The cost estimate is approximately $ 1 USD per person. Each of these centers is supported by local entrepreneurs ($ 20 per month for the network connection paid
to Tulip), who receive a government-subsidized loan. One of the main goals of these centers is to teach a member of each family to use a computer and access the internet.

In addition to these centers, the Akshaya network aims to create government portals, create collaborative tools for government services, provide medical, educational and social communication services such as voice over IP, and/or teleconferencing.

Several technologies were considered in the implementation to create network access and backbone, such as:

- 802.11 WLAN;
- CDMA450 - 3G solution that operates on frequencies between 410MHz and 470MHz
- WIPLL (Wireless IP Local Loop) technology that operates up to 10km distances with line of sight at speeds up to 4Mbps;
- 802.16 WiMAX
- Optical fiber.

In [5] the authors made a study on the total cost of implementing each technology as well as installing and configuring all the devices. The composite solution of Wi-Fi with directional antennas and WiMAX was considered the most economical.

In 2003, bidding was purpose to for the purchase of services for the entire district interconnection solution. About 75 solutions were presented, some of which included backbones using wireless and wired technology. According to the financial study, the solution of covering the whole territory with fiber or cable solution would be a very high investment due to the 3500km² of territory with dense forests.
The winning solution was based on the use of wireless technology. The backbone as seen in Figure 1 uses point-to-point, point-to-point wireless connections that connect to the Network Operation Center (NOC) to about 40 district-wide Points of Presence (POP). The connection between POPs, use a technology based on 802.11a and VINE (Versatile Intelligent Network). Some peer-to-peer connections can go as far as 30km, but most of them are below 10km. These connections operate in the range of 5.3GHz to 5.8GHz, achieving bandwidths up to 24Mbps, which are used for the most critical point-to-point connections that require the highest bandwidth.

The remaining connections use proprietary VINE technology, which serve terminal connections, or which serve as repeaters. A Canadian company called Wi-LAN, which developed some significant changes in layer 2 of the OSI model, developed the VINE. These connections use the 2.4GHz frequency range and support bandwidths up to 11Mbps, using 1Watt power. The advantage of using this technology is its scalability, since it allows at any moment to add a network interface to the device, increasing twice its available bandwidth.

Access links for users are made directly to POPs. This connection uses another technology, called WIPLL (Wireless IP Local Loop), which allows

Figure 1 – Overview of the most important links in the Akshaya network
connections up to 4Mbps. This technology has sophisticated mechanisms to support quality of service. The device used is from the English company Airspan Networks. Each POP has a WipLL radio interface with an omnidirectional or sectorial antenna, which connects directly to educational centers. These centers in turn have devices with directional antennas, which are pointed at the nearest POP. These devices are installed in towers that are about 20 to 30 meters, depending on the vegetation and topography of the terrain [34].

The estimating cost for each center was $3000 to $4000 USD. This included equipment ($400), antenna ($100), communication tower ($500 to $1000) and office equipment with several computers, printers, scanner and webcams (2000$ USD to $2500). The total network cost, as quoted above, was less than $1 USD per person covered.

2.2.1.2 Aravind, India

In India, studies indicate that about 15 million people are blind [35]. Cataracts are the main cause of these bulky numbers, where diabetes also contributes significantly to the problem. There is a health service in India to treat eye problems, called Aravind. This health organization tried in various ways to provide diagnostic and curative services to the entire population, but the vast area as well as the lack of specialists made it difficult for the system to have satisfactory results.

To eliminate these problems, Aravind conceived the idea of setting up rural ophthalmology centers where specialized physicians via videoconference through a high-speed wireless network could diagnose patients remotely. In 2005, the wireless network that would link 5 rural ophthalmology centers to the central hospital in Theni, India, began to be installed.
The initial network had 11 wireless routers, and 9 were used in point-to-point connections. These connections are at least 1km and at most 15km. The routers use 266 MHz processors and three Atheros 802.11a / b / g interfaces with power from 200mW to 400mW. 24dBi directional antennas are used to reach the largest connections. These routers use about 4.5W when they are set with energy-saving feature, and can reach 9.5W when they are transmitting as much bandwidth as possible using two radio interfaces. The operating system is Linux based (kernel 2.4), running from a 512MB memory card.

The routers are placed in watertight enclosures near the antennas to minimize cable loss. They are powered through the PoE (Power over Ethernet) by a single network cable connected to an Uninterruptible Power Supplies (UPS) to provide stable power.

The most used applications for the ophthalmology service in the Aravind network are those based on videoconferencing. Video conferencing sessions are used not only between patients and doctors, but also among the staff of the centers for training and help. Videoconferencing only requires 256Kbps in each direction,
but the connections have about 5 to 7 Mbps of bandwidth, which is more than enough. These features make it possible for the network to be used for other, more demanding applications in the future [36].

Some retinal exams are done locally in rural centers, which are sent to the central hospital in images that have an average size of 4MB, which are delivered very quickly thanks to the existing bandwidth. At the end of 2007, around 3500 consultations per month were held in all active rural ophthalmology centers. The success of the network has enabled its managers to increase the network to other locations and it is expected that the entire project will be able to offer more than 500,000 tests per year, covering a population of more than 2.5 million in the coming years.

### 2.2.1.3 AirJaldi, India

The AirJaldi wireless network is a non-profit community in the Himalayas, India, which began to be implemented in 2005. The AirJaldi network provides Intranet access and voice over IP services to over 10,000 users spread over a 70km radius in the area Mountainous and rural Dharamsala. The network has 8 point-to-point links, some of them with tens of kilometers, the largest being 41km - see Figure 3.

![AirJaldi network topology](image)

**Figure 3 - AirJaldi network topology**

The device located in the mountainous and remote region is powered by solar energy. In addition to the backbone, the network also has hundreds of other
low-cost access device adapted to the AirJaldi network, which use different types of antennas depending on the location and distance of the nearest antennas.

The devices are mostly Linksys WRT56GL or Buffalo routers, to which changes have been made to their operating systems. The advantage of this device is its ease of use and its low cost (50€). These routers are placed in watertight boxes, and mounted as close as possible to the antennas in order to avoid signal losses in the cable. These devices have a 200 MHz processor with 16MB RAM, 4MB Flash memory and Broadcom 802.11b/g radio interfaces. The most commonly used operating system on routers is OpenWRT. Other free software are used to handle routing, security, logging, authentication, QoS, and remote administration protocols. For higher distance connections, other higher performance devices such as MikroTik and Ubiquiti, based on Atheros interfaces, are used.

The Internet connection of the entire AirJaldi network consists of 5 Asymmetric Digital Subscriber Line (ADSL) connections, resulting in a total of 7Mbps download speed and 1Mbps upload speed. The longest 41km connection achieves bandwidths between 4Mbps and 5Mbps with a loss of signal between 2% and 5%. However, the biggest problem is in a 21km connection that only achieves bandwidths between 500Kbps and 700kbps due to not having a line of sight completely free from interference. Even in this worst case possible, the connection is more than sufficient for internet access and voice over IP services [36].

The cost of the network is shared by all users that allow the network to be a self-sustaining network with strong possibilities for expansion to other adjacent areas.

2.2.2 Common Problems

When planning a wireless network for a rural area it is necessary to study the problems that tend to occur and require effort, personnel, and money to resolve. Planning a solution can imply the difference between a short and long lifespan of a rural wireless network. Many projects that are designed and planned by communities or groups of friends, with the greatest intentions, inevitably fail because of the factors that were not initially foreseen [10].
Based on the previous study and our experience, we have identified the main problems that may occur when planning and deploying a wireless rural area network: (i) cost; (ii) low quality electric power; (iii) bad diagnoses and lack of information; (iv) non-existing remote management and poor maintenance; (v) lack of automatic recovery; (vi) slow access to the internet (vii) network dependency; (viii) traffic management. These problems are detailed in the next subchapters.

2.2.2.1 Cost

In 2001, United Nation secretary-general Kofi Annan announced the creation of a task force comprising government officials, industry experts, and nongovernmental organizations leaders to suggest ways to strengthen access of communications and network technologies. He appealed to the private sector to “help build digital bridges to the billions of people who are now trapped in extreme poverty, untouched by the digital revolution and beyond the reach of the global economy”[12]. Unfortunately, these digital bridges still do not exist in rural areas and developing countries as neither private companies nor governments are interested in high-risk investment areas.

Installing a wireless network in rural areas is not cheap because these areas are difficult to access and involve high costs for transporting the specialized teams which are often very far from these rural areas. Cost is the primary factor in a rural wireless network. The planning of the project must be based on technologies that do not require special licenses to operate. Technologies such as IEEE 802.11 operate in license free frequencies and therefore, are cheaper than others to install and operate [6, 7].

As previously mentioned [10], the longevity of a network is based on the types of actions and management that are used after the project has been implemented. When the project is starting, the devices will obviously have fewer problems, and the entire network will work efficiently. To manage and maintain the network at a low cost price, it is important to avoid visits from the specialized team. This can be accomplished by applying strict maintenance and proactive management.
By taking advantage of a local community of users using the network, it is possible to implement a few advertisement strategies based on the browsing experience of the users in order to accumulate funds to support the network.

### 2.2.2.2 Low quality electric power

It is common knowledge that power outages are frequent in rural areas, especially in remote and isolated places [6, 37]. In some rare situations, the loss of power may cause corrupted files in the network routers. Although this is rare, the chance of continuous reboots is greater in areas where the loss of power is a recurring event. In some areas far from the central points of energy transformation, there is an even greater likelihood of losing power. However, the worst case is when the voltage is unstable and reaches values from -1000 volts to +1000 volts in devices that should function within a range of 40 to 240 volts [10, 37]. In the Airjaldi network presented in the previous subchapters, in short time 50 power supplies, 30 Ethernet interfaces and 5 routers were ruined due to power outages. One of the routers in Aravind project rebooted 1700 times in a year due to power outages.

While an Uninterruptible Power Supply (UPS) system in each router is a great solution for providing a stable power supply, it is almost as expensive as the router itself.

### 2.2.2.3 Bad diagnoses and lack of information

Sometimes a problem is easy to solve if the person who reports the problem knows how to provide detailed information. Unfortunately, however, users are not computer or network experts and their status report on the network is often simply: “The network is down” [10, 38]. Most of the time, our experience tells us that it is more likely for the problem to be on the user’s computer than on the network itself. If a network engineer is sent out every time someone reports a problem in the network, it would be impossible to maintain the costs of travel, not to mention the cost of the expert staff. Since most of the wireless rural networks are far from the development centers, it implies very high expenses in travel costs alone.

Previous work shows that user reports are not the kind of we need for this type of network [10]. For example, in the Aravind project in India, a situation arose
at the central hospital, where the central router could be accessed, but the link to a rural eye center was inaccessible. After two months of testing, no member of the technical team was able to figure out what the problem was, simply because it had not verified the connection correctly. An elevator duct was built on the roof in front of the antenna that served as a link to the rural center, completely obstructing the line of sight.

A rural wireless network needs to have solutions to confirm and understand what could be happening remotely when someone complains.

2.2.2.4 Non-existing remote management and poor maintenance

As previously stated, wireless rural networks are usually located in a remote location far from the urban areas where the administrators and expert staff are located. These remote locations are sometimes hard to reach because of the distance or the condition of the access roads. Obviously, travelling to the rural area where the project is located implies time and travel costs for each person [2, 39]. When local action is needed, it is best to take full advantage of the time spent there. That said, it is important for administrators to be aware of possible problems that although may not affect the network now, but will eventually cause major problems in the near future. An example could be the decrease in the signal strength of a wireless router. The signal could be decreasing due to a number of possible problems, such as cable damage, small movements of the antenna caused by wind, or other factors. If the administrators are aware of such situations they can plan the trip to the area with a list of specific items to review that will not only fix existing problems, but also resolve problems that have not yet emerged [10]. This type of proactive management of the network can reduce costs over time.

Some maintenance work could also be done remotely, such as updating software or implementing new functionalities in every router[40]. Over time, new versions of firmware will become available and have important updates for the stability and security of the system. To avoid unnecessary travelling and the corresponding expenses, it is important for these tasks to be implemented online remotely, or during scheduled visits to the area.
Surana et al [10] identified the lack of management in rural area by saying that “remote management solutions for wireless networks that are located in remote rural regions has not received a lot of attention”.

### 2.2.2.5 Lack of automatic recovery

Computer devices tend to freeze suddenly without much explanation. Any computer administrator has been in a situation where there is no reason to explain why something does not work, with a simple reboot being the only way to fix it. As previously mentioned the power in rural areas is very bad and often causes the device to freeze. The only solution is a power-off-power-on action. However, someone who has access to the router must do this action. Although it is an easy action that could be done by someone with no technical knowledge, it takes time, especially when the device is in remote locations in the middle of a forest, or at high altitudes [38].

The use of automatic recovery systems is normal in most hardware for wireless networks. The configuration of these systems could save precious time in recovering the device, because if successful, the administrator does not even have to be alerted to the problem. The automatic recovery is often an easy method to deploy.

### 2.2.2.6 Slow access to the internet

Internet access in rural areas is far from ideal. The bandwidth is low, and the rates that are announced by the internet providers are always fractioned by a large number of users. This is referred to as the contention ratio. In some countries, the contention ratio is 1:20 to 1:50, but in rural areas this value can go up to 1:100. For example, an 8MB internet access is, in worst case scenario, shared by 100 users with a maximum bandwidth of 80KB per user in extreme situations; this is a very low bandwidth for today’s use of internet browsing.

Surana et al [10] describe their experience in deployments of rural wireless networks and focus on sustainability in projects used by thousands of users. They have deployed rural wireless networks to offer health services in Aravind project.
and voice communication and Internet in Airjaldi project, but didn’t mention solutions for traffic management.

Sharing a single internet access to a wireless network in a rural area is challenging. A user can consume all of the available bandwidth if no quality of service is configured in the network. Some applications, such as peer-to-peer networking, can consume large amounts of bandwidth and flows, which reduce the performance of other applications. Furthermore, some types of user behavior may compromise the quality and performance of the network. It becomes necessary to implement QoS, and to monitor traffic behavior and patterns that use and abuse the available bandwidth. QoS must be implemented to create restrictions in some types of traffic that abuse the network, such as peer-to-peer applications. These types of connections push the network to its limit. However, other types of traffic, such as that created by audio/video telephony applications, should have a higher priority than others types of traffic.

Implementing QoS in wireless networks is challenging because of the wireless medium where the communication takes place. There is no guarantee that the medium is clear at all times, especially in a license-free spectrum [2, 39].

2.2.2.7 Network dependency

Although not all problems can be solved remotely, a few could be solved if the network had a backup access in different physical places within the network topology. For instance, a router in the middle of the network may be unreachable because of a bad configuration on the network card. All the users and routers that depend on this router may be working well, but the administrator cannot access them. This network dependency may force unscheduled visits to the site to understand what has happened with that specific area of the network. In a wireless network, the problem on a wireless link could be affected by the performance of the antenna. If an obstacle interrupts a wireless link, the administrator does not have sufficient information to understand that the routers are working well, and that the problem is with the wireless link.
In the next section, a literature review on managing and monitoring wireless sensors networks will be presented by analyzing the methodologies used to monitor the resources constrained devices of the wireless sensors networks. A comparative analysis is done for each methodology analyzed.

2.3 Managing and Monitoring Wireless Sensors Networks

Managing a network require the query and setting of different values of the devices present in the network. When managing the network, information need to be collected, measured, calculated, processed, and evaluated in order know the overall state of the network. Monitoring is generally assumed to be periodic [42]. This evaluation of states, may lead to a problem or fault detection that can trigger a solution that will adjust and set new parameters or configuration in the devices and services of the network. The main objective of a network management is to continuously monitor values and states of all devices in the network and act when it assumes a critical value in order to keep and maintain the network operating at its best. When managing computer networks these values must be full of information and should be collected and delivered as fast as possible.

However, in IoT networks the constrained network and its devices offer different challenges. When compared with traditional IP based network the traditional operations and methods needs to be adjusted to be used in IoT networks [43]. Because of their limited power (small batteries) and low processing capability and bandwidth, these constrained devices cannot be queried and accesses as often as a traditional IP based device. Due to this network capabilities, the management data should have low overhead in order to avoid the congestion of these low bandwidth and resource constrained networks [44]. In addition, the energy consumed by the management system must be used wisely.

Although the existence of simulators, tools, and lab testbeds are helpful in testing the deployment of new sensor networks, the results are not as real as the real world. Also, real experiments in lab testbeds are often costly and difficult to run [45]. Even when tests are executed before deploying it, the network and the sensors usually does not perform as well as it did in the lab. The influences of the real world
environment are different from the environment created and planned in laboratories with simulators, emulators or test-bed.

In [46] the authors discuss the difficulties and requirements of managing resource constrained devices by looking at different types of use cases, such as environmental monitoring, infrastructure monitoring, industrial applications, energy management, medical applications, building automation, home automation, transport applications and community network application. For each application scenario, we have gathered the most important features that should be considered when planning management in network sensors such as:

- The management system must be able to monitor a large number of devices, which may be network segmented.
- The management system must be able to work with different types of devices or to have the ability to interoperate with different systems.
- In some cases, the constrained devices must be able to establish connectivity (auto configuration) and be able to deal with a sudden loss of neighbors or being moved to other location. The managing system must be able to discover the devices on the network and recognize it as a trustily or unknown device in the network.
- A monitoring application must be prepared for different scenarios. In some use cases (environment, infrastructure), the monitoring application must be designed to tolerate a number of failures, a high number of hours in order to detect a fault and a couple of days for manual repair. In other use cases (industrial, energy, medical, military) a monitoring application must be designed to be constantly monitoring the state of the devices and to detect a fault in a few minutes or in a small number of seconds for critical services (real time detection).
- The monitoring information must be simple and able to work at critical conditions.
In most cases, it may be more cost effective not to repair the device, but substitute it. In cases where the devices are difficult to access, a self-healing feature could be of good use. In addition, these devices should have a minimum configuration, or none.

- The management protocol could include security protections such as access control, confidentiality, integrity and availability of data.

In [47], authors observed that managing a network of wireless sensors must include the monitoring, configuring and controlling of these devices, even with their resources constrained and very limitations in hardware. The operational system must include functions to detect faults, configure devices, accounting of devices, performance and security. In networks with resource constrains a good management system must take into account that the devices do not have the processing power and network bandwidth enough for being constantly monitored and queried about its status and other operational values. In addition, the networks in which they operate are often unreliable and have limitation in the data rate available. Finally, many of these resource constrained devices are not always online, but that does not mean they are experiencing problems.

In [48], the author summarize the management requirements for these networks as follows:

- Need for fault tolerance: power status, battery status, physical problem;
- Need for scalability due to the high number of nodes;
- Low Cost;
- Low Complexity;
- Energy efficiently;
- Traffic managing for network performance.

The methods of managing IP-Based networks are designed to manage devices whose characteristics and challenges are very different from the resource-constrained devices in IoT. The most used and known protocol for managing
networks, Simple Network Management Protocol (SNMP), is very heavy for the characteristics of most devices used in IoT. In some sensor networks, the lack of TCP/IP support and the low bandwidth of the network make it impossible to use these well-known protocols for monitoring.

Two approaches have been studied in order to monitor the status of the sensor devices and sensors networks: active monitoring and passive monitoring. We will discuss both of these approaches on the next sub section.

2.3.1 Monitoring Methodologies
In order to provide information on wireless nodes and their networks, several monitoring systems have been proposed by authors in recent years. We can divide these studies in two approaches: active monitoring and passive monitoring.

The active monitoring acts directly in the sensor network and devices, and can interfere with the normal operation of the network. A common example of active monitoring is usually done by requesting specific information and waiting for the answer in a determined timeframe, like when using the SNMP protocol.

The passive monitoring only observes or sniffs the information generated by the wireless nodes, but has no interference in its operation.

The following section will show the recent studies based in these two monitoring methodologies.

2.3.1.1 Passive Monitoring
The main objective in using a passive method is to achieve management and control of resource constrained devices without overload the network and nodes limited resources [49].

A passive monitoring technique is used when there is no interfering with the monitored device or service. This type of monitoring captures or sniffs information in messages and communications that already exists in a normally activity of the sensor network. It means that no extra communication is added to the network and the monitored device requires no extra processing. For these reasons, a passive method is extremely useful when monitoring constrained devices and networks.
because it does not use any resource from the existent network and its devices. When devices have very limited resources, it is impossible to communicate through request and response interaction, like a normal SNMP query/response operation in a computer network.

To achieve a passive monitoring technique, a separate network is created only for sniffing purposes. This network could be fixed (to constantly monitor the network) or portable (to help in diagnostic or test-labs). Some authors use the same sniffing network to diagnose different wireless sensors.

The research made in recent years shows that in some cases, a passive monitoring is the only way to efficiently monitor some types of WSN [50]. Table 2 shows the list of the selected studies that focus on passive monitoring methodologies and their implementation.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>[50]</td>
<td>Estimation of Physical Layer Performance in WSN Exploiting the Method of Indirect Observations</td>
<td>2012</td>
</tr>
</tbody>
</table>

Table 2 - Selected passive monitor studies
In [51] authors present the Sensor Network Inspection Framework (SNIF), which is a distributed network sniffer for analyzing and overhearing the network traffic of the sensors in any multi-hop WSN. It uses decision trees that can detect problems related to individual nodes, wireless links and paths. They also implemented a framework for online analysis of the results gathered from the sniffers. This framework provides flexibility in adding code for detection of other WSN specific problems. The sniffer is composed of two network interfaces: one collects the data networks of the sensors, and the other sends this information to a central device of the network using Bluetooth.

In [52] authors present the Sensor Network Troubleshooting Suite (SNTS) which performs automated failure diagnostics in WSN. It gathers data through sniffers that capture network packets and are manual transfer to a computer for post processing and analysis. Using data mining it extracts conditions on the network state that can be correlated with faults in order to find the cause of the problem. This system must be used in scenarios where the access of the devices must be easy to reach (not suitable for military or environment monitoring applications).

In [49], Awad presents Pimoto, a passive monitor system for debugging and analyzing WSN. It is based on hierarchical structure that allows the monitoring of different networks at the same time. In the first stage it intercepts the radio packets, forwards it to a gateway (usually a laptop PC) using other communication network in order to avoid interferences with the WSN (example: Bluetooth). The gateway tags it with a timestamp and transfers all the information received to a central computer using a communication network based on TCP/IP. The monitoring network is subdivided in small networks each one with each own gateway. This subdivision avoids redundant packets in the final merge of captured packets, however it may not be a suitable tool for large scale WSN because of the all the infrastructure needed. A human in a dedicated computer using a plugin for well-known software, named WireShark, analyzes all the packets. The tool does no event detection based on the analysis of the captured packets.

In [53] authors describe a set of tools and analysis methods for reconstructing the behavior of a WSN – named LiveNet. Their principle is passive
monitoring by collecting packet traces using a small number of passive packet sniffers deployed in different places of the network instead of using intrusive hardware in the sensors. Doing this, they get a global picture of the entire network operation and use the trace gathered to get different points of view of the critical problems. Its results show that they can reconstruct an entire network topology, determine what bandwidth is being used and the routing paths. Unlike previous studies in passive monitoring, LiveNet is focused in gathering information about dynamics in network behavior, such as routing path dynamics, traffic load and hotspot analysis, network connectivity and recovering the sources of path loss. It does not analyze captured packets to detect fault events that do not affect the network traffic. While the data is collected at real time, the processing and analysis is done afterwards in offline. When the sniffers are installed temporarily, the log packets are recorded locally. When the sniffers are installed permanently, it must be connected to a network, or backchannel for the delivery of the log packets. Because LiveNet stores the information locally or in a computer using a wired network, its use must be on scenarios where a local access to devices is possible and easy.

In [54] authors present the Sensor Network Distributed Sniffer (SNDS). Like other passive monitoring systems, its objective is to monitoring WSN with large traffic, synchronize all the sniffers accurately and analyze protocols with efficiency and flexibility. The sniffer-monitoring network is based on Ethernet, which interconnects all sniffers. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocols are used for transmission and synchronization. After gathering the information, its send the data to a central service program which analyze it and display the results to the users. Being a cabled solution, it could be problematic with large network or very dispersed nodes.

In [55] authors propose a passive monitoring system for WSN named PMSW for solving issues such as, trace merging, inference and event detection. They propose the improvement of passive monitoring by using clock adjustment and fine-tuning to solve clock drifting when trace merging. For missing packets, a finite state machine is used to infer the missing packets and the state of packet receptions in
multi-hop networks. In PMSW, each sniffer present in the network sniffs the information sent by the nodes at its coverage area and sent it to a local gateway through a different wireless network. This gateway receives the captured data, record the current timestamp, and send it to a central server through TCP/IP. The central server receives the captured data of each gateway and generate a unique global gathered data, which is then analyzed in order to remove duplicate entries and detect errors. When this analysis is concluded, it is showed to the users through a software application made by the authors.

In [50] authors present a process for the monitoring of the physical layer of WSN using passive methodology and indirect observations. Using external nodes to sniff data, the authors compute the information of signal strength, and use this to estimate the position of the nodes by applying the Weighted Least Squares to the method of indirect observations. After knowing the estimated position of the nodes, the system estimates the status of the network links between nodes using the propagation model. The analysis of the network performance is done offline.

In [56] authors presents a network monitoring and packet sniffing tool for WSN named NSSN. This tool can gather network packets from the nearby nodes by using local nodes for sniffing. The sniffer nodes examine the network status, detect problems and can optimize the network configuration without interfering in the normal operation and behavior of the sensor nodes. After collecting data from the sensor nodes, the information is sent to a monitor server through a wired or wireless connection, such as 3G. The main server receives the data, parses it, pre-processes it and stores it in the data in the database. A remote monitor client performs the analysis and visualization of the data to complete the monitoring functions. The tool also include functions such as network monitoring, protocol parsing, network diagnosis and performance measurement, data mining and statistical analysis.

In [57] authors identified the lack of passive monitoring systems for WNS with the aim of reducing the energy consumption, which is a benefit for the longevity of the network. Their proposed system is Energy-efficient Passive MOonitoring SysTem for WSN (EPMOST) with the main objective of reducing the energy consumption and providing monitoring information through an SNMP
agent developed. By electing a sniffer, it guarantees that one sniffer only captures the packets of a certain node of the WSN in order to reduce the transmission of redundant packets. The usage of SNMP enables the integration of this tool with widely well-known software to facilitate the management of the network, such as Nagios.

2.3.1.1 Comparative Analysis

In order to compare the previously selected studies for the passive monitoring methodologies, we present in this section a set of items to be compared between each study. Those items are:

- **Data**: The information that is gathered/monitored in order to extract the network and/or node status.

- **Deployment**: in passive monitor, the sniffers may be deployed using different techniques. One can deploy one sniffer to each node, or use one sniffer to listen many nodes. In addition, the communication between the sniffer networks may have different topologies (star, scatternet, etc).

- **Analysis**: this item answer the question: “Is the processing of the data is done in real time (online) or processed later (offline)?” An online solution is able to detect failures on real time, although it needs a good processing capability and network infrastructure to process the information and send it to a remote server. Offline analysis are usually done in testbeds or developing scenarios where the results are processes later to analyze what was wrong during a test.

- **Method**: The information that is gathered needs to be processed. Depending on the inputs and preprocessing information, one can use various machine-learning algorithms to identify potential problems or to infer rules.

- **Features**: the mains objectives of each solution studied.
<table>
<thead>
<tr>
<th>Ref.</th>
<th>Data</th>
<th>Deployment</th>
<th>Analysis</th>
<th>Method</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>[51]</td>
<td>Network traffic</td>
<td>Distributed sniffers in scatternet formation</td>
<td>Online</td>
<td>Decision Trees</td>
<td>Detects problems in nodes, wireless links and paths</td>
</tr>
<tr>
<td>[52]</td>
<td>Network traffic</td>
<td>Distributed network sniffers, One sniffer listen 4 nodes.</td>
<td>Offline: Data processes later at a backend</td>
<td>Data mining</td>
<td>Troubleshooting; automated failure diagnostics</td>
</tr>
<tr>
<td>[49]</td>
<td>Network traffic</td>
<td>Distributed network sniffers, One sniffer listen 3 nodes.</td>
<td>Online. Data is sent to a server</td>
<td>Packets analyzed manually in Wireshark by a developed plugin</td>
<td>Debugging</td>
</tr>
<tr>
<td>[53]</td>
<td>Network traffic</td>
<td>Temporarily or permanent distributed network sniffers</td>
<td>Offline: traces of sniffers are merged to create a global picture (single trace)</td>
<td>Series of algorithms to compute the results required</td>
<td>Provides information on network traffic, network path, network topology and traffic load</td>
</tr>
<tr>
<td>[54]</td>
<td>Network traffic</td>
<td>Distributed Ethernet network sniffers</td>
<td>Online. Data is sent to a service program to graphically display the result</td>
<td>Not Available</td>
<td>Network running status and operating efficiency</td>
</tr>
<tr>
<td>[55]</td>
<td>Network traffic</td>
<td>Distributed network sniffers</td>
<td>Online</td>
<td>Algorithm to merge multiple traces</td>
<td>Trace merging: missing packets, clock sync. Detection of abnormal events in networks, network performance evaluation and fault diagnosis</td>
</tr>
<tr>
<td>[56]</td>
<td>Network traffic</td>
<td>Distributed network sniffers</td>
<td>Data is gathered and sent to a local server to be stored. Further analysis is done remotely.</td>
<td>Data mining techniques and human analysis using visual tools.</td>
<td>Monitoring network operating conditions, assessing network performance, detecting network failure and optimizing network operation</td>
</tr>
<tr>
<td>[57]</td>
<td>Network traffic</td>
<td>Distributed network sniffers</td>
<td>Offline. Data is sent to a local server and stored in a MIB to be accessed by a SNMP agent</td>
<td>human analysis using visual tools</td>
<td>Monitoring information using a (SNMP) agent; Energy efficient monitoring.</td>
</tr>
</tbody>
</table>

Table 3 - Comparative Analysis of Passive Monitoring Studies
Table 3 shows the summary of these items compared between the selected studies.

**Key benefits** of using passive monitoring:

- Sensor nodes do not need to be altered for debugging purposes and monitoring;
- Data gathering for monitoring does not use valuable resources from the sensors;
- Avoidance of probe effects (any software for monitoring the sensors, will interfere with the monitoring itself; bugs may come and go when active monitoring is used).
- The same sniffing network could be used for debugging other networks.

**Drawbacks** of using passive monitoring:

- More hardware is needed. A new network has to be added;
- The cost of implementing a new network;
- Large networks are very difficult to monitor using passive monitoring;
- When monitoring is only used to debugging, the network must be added and removed after the problems are solved;
- There is no guaranty that the monitoring network captures all packets.
- Lack of security, since the sniffing processes could be altered by a foreign network;
- Some monitoring information is unable to be verified (internal services status such as battery levels or the status of disk/memory);
- No performance metrics can be evaluated;
- Synchronization problems (such as redundant/duplicated packets) when merging traces from multiples sniffers;
2.3.1.2 **Active Monitoring**

Active monitoring involves adding hardware or software in the nodes of a wireless sensor network. When hardware is added the nodes it can alter its normal operation and behavior, but in comparison with passive monitor, the information gathered directly in the nodes is more accurate and detailed, similar to monitoring protocols such as SNMP. In active monitoring, the exchanged information between the nodes and the monitoring system uses the sensor network which can cause traffic congestion.

Table 4 shows the list of the selected studies that focus on active monitoring methodologies and their implementation.

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>TITLE</th>
<th>YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[58]</td>
<td>Sympathy for the sensor network debugger</td>
<td>2005</td>
</tr>
<tr>
<td>[59]</td>
<td>Design of an application-cooperative management system for</td>
<td>2005</td>
</tr>
<tr>
<td></td>
<td>wireless sensor networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>networks</td>
<td></td>
</tr>
</tbody>
</table>

Table 4 - Selected active monitor studies

In [58] authors present a tool named **Sympathy** for detecting and debugging failures in WSN in both simulation and deployment. This detection and diagnosis is done in a centralized node (sink) by just analyzing the node status and network information, such as routing tables, neighbor list and flow information. Using the information acquired by the nodes, Sympathy detects failures and determines their causes by using a decision tree algorithm. Each node needs to keep executing the software in order to obtain the conditions of the sensor node and send it to its sink at periodical intervals. This means that the node send redundant messages to the sink. Because of these continuous updates, the tool increases the network traffic overhead [63] using about 30% of the network bandwidth[51]. Due to this heavy
network usage, Sympathy is more suitable for lab experiment-based debugging. There is no GUI or protocol analysis provided. The framework of detection only supports a fixed set of problems (not extensible).

In [59], Tolle presents **SNMS** a Sensor Network Management System that has the objective of being simple, functional with any sensor network, and be low on network and memory usage. It provides a query based network health data (failure detection, neighbor tracking and reporting inconsistent routing state) and event logging while using low RAM memory and can be integrated into TinyOS applications. The querying system allows the user to gather information about the condition of the nodes. The event logging allows the user to set thresholds in which the nodes will report their data. It also includes lightweight network architecture for collecting and dissemination. It only generates network traffic in response to direct human queries. On [64], Fenghua improved the SNMS by minimizing the overhead of memory and network usage. It incorporates an RPC (Remote Procedure Call) mechanism that enables the user to access functions and variables of application running on the sensors during runtime.

In [60] authors present a system named **Memento** to provide failure detection and alerts based on symptoms on WSN. In this approach, the sensor nodes cooperatively monitor each other implementing a distributed node failure detector. Each child sensor sends its neighbors information (heartbeats) to its direct parent, which aggregates all the information received by all its child’s sensors in the form of a bitmask (simple bitwise OR operation). This aggregation and optimization of information saves bandwidth and processor. Every parent node sends the bitmask of the sub-tree summary information to the main sink at regular intervals. However, to save bandwidth, a cached mechanism is used to ignore further updates when there are no changes in the health condition of the nodes. The sink creates a list with the sensors information and determines which of the sensors have failed based on various reports of different nodes. This system only supports a fixed set of problems and the nodes keep sending redundant messages to the above nodes in the topology.
In [61] authors present an active monitor system with low intrusion for WSN. Although its title, Passive Diagnosis (PAD), the system is active. In this approach, a probabilistic diagnosis is suggested based on Bayesian Network. Each sensor node has a probe that marks the packet with relevant data for the sink to collect and analyze the data, constructing and maintaining the inference model. The sink can automatic generate diagnosis information such as packet loss. However, the system may be delayed in cases where the sensors only communicate to each other sporadically. The system has to wait for a packet to be sent to be able to communicate with the sink.

In [62] authors present DiMo, a distributed and scalable lightweight network managing solution for monitoring nodes and network topology, including a redundant topology solution. This solution was designed to be used in event-triggered networks, which only transmits to the sink when an event occurs. The monitoring is done by heartbeat messages exchanged between the nodes in which one is the responsible (observer node) for the other. There is at least one observer responsible for every node. If a node is down, the observer node will send a message to the sink. This allows the sink to know the states of all the nodes in the network. While this action requires some processing locally at the node itself, it greatly reduces the transmission overhead and energy consumption. Through maintaining a redundant topology, each node is able to communicate at least with two node neighbors.

2.3.1.2.1 Comparative Analysis

In order to compare the previously selected studies for active monitoring methodologies, we present in this section a set of items to be compared between each study. Those items are:

- **Data**: The information that is gathered/monitored in order to extract the network and/or node status.

- **Deployment**: this item describes where the code collects metrics or data from, and how it is deployed.
• **Analysis**: this item explains what type and/or how information is sent to sinks (servers) that gather and compile the results.

• **Method**: The information that is gathered needs to be processed. Depending on the inputs and preprocessing information, one can use various machine-learning algorithms to identify potential problems or to infer rules.

• **Features**: the mains objectives of each solution studied.

Table 5 shows us the summary of these items compared between the selected studies.

**Key benefits** of using active monitoring:

• Accurate access to internal state of nodes;

• There is no need to add extra hardware for monitoring purposes;

• Suitable for much dispersed networks or network with high number of sensors.

• The information acquired is safely inside the network;

• Good for debugging in lab tests.

**Drawbacks** of using active monitoring:

• Problems in the node also affects the monitoring mechanism;

• The limited resource available is used for normal operation and monitoring;

• Monitoring interferes in the sensor network;

• Probe effects (any software for monitoring the sensors will interfere with the monitoring itself; bugs may come and go when active monitoring is used);

• Monitoring software may need to be updated often in order to capture relevant data to help diagnostics.
<table>
<thead>
<tr>
<th>REF.</th>
<th>DATA</th>
<th>DEPLOYMENT</th>
<th>ANALYSIS</th>
<th>METHOD</th>
<th>FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>[58]</td>
<td>Metrics at the node; Active in each node</td>
<td>Periodically sends important data to a sink.</td>
<td>Decision tree algorithm at the sink</td>
<td>Failure detection on nodes, and network communication</td>
<td></td>
</tr>
<tr>
<td>[59]</td>
<td>Metrics at the node;</td>
<td>Queries are generated when needed by programmers or when thresholds are triggered in event logging.</td>
<td>Functions programmed at the node</td>
<td>Failure detection; logger for analysis further.</td>
<td></td>
</tr>
<tr>
<td>[60]</td>
<td>All nodes monitor one another: distributed node failure detector, a symptom alert protocol and a logger Node neighbor heartbeats Periodically send heartbeats to the node above in the routing topology. The top nodes in the topology aggregate the information in the form of a bitmask and send it to the sink.</td>
<td>Functions programmed at the node</td>
<td>Failure detection and alerts. Can detect problems in a node by using the information provided by their neighbors. Fixed set of problems (needs programming)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[61]</td>
<td>Packets at the sink. Active in each node.</td>
<td>Each node marks packets with small relevant data for the sink to analyze</td>
<td>Probabilistic diagnosis approach (Bayesian network)</td>
<td>Failure detection based on the received data and hints on possible causes</td>
<td></td>
</tr>
<tr>
<td>[62]</td>
<td>Node neighbor heartbeats Active in each node.</td>
<td>Each node heartbeats other nodes to check the topology. Only sends to sink errors or suspects of failure</td>
<td>Algorithms</td>
<td>Network topology maintenance and network health status monitoring</td>
<td></td>
</tr>
</tbody>
</table>

Table 5 - Comparative Analysis of Active Monitoring Studies
2.3.1.3 Active Monitoring based on Simple Network Management Protocol (SNMP)

The SNMP [65] protocol was developed 30 years ago with the main purpose of managing traditional TCP/IP networks. SNMP is widely known for collecting information, diagnose and configuring network devices. It can manage a large amount of devices and it is very flexible and extensible to any kind of network and device[66].

However, the SNMP protocol is currently not suitable for resource constrained networks because of a couple of important factors [67][68]. First, the size of information exchanged is too big for the low bandwidth network of WSN. The energy used could be also a problem, because SNMP is configured to pool frequently the same device and service, repeatedly. Lastly, the Management Information Base (MIB) used in SNMP is large and needs to be stores at each device, which in WSN have very limited storage [44].

However, since most WSN are supporting IP for interoperability with the IoT concept, the SNMP must be a protocol to consider when choosing how to manage and monitor a network. In the selected studies, the use of the SNMP in resource-constrained networks shows us that the protocol is being used in a different way, as one would think. The SNMP architecture allows the use of a few set of features that are enough to manage resource constrained devices [69].

According to a pool done by authors in [70], most of the managing (44%) is done using a custom application on top of application layer protocols, but 49% expect to be using SNMP in a near future.

Table 6 shows the list of the selected studies that focus on active monitoring methodologies using the SNMP protocol and their implementation.
<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>[71]</td>
<td>ANMP: ad hoc network management protocol</td>
<td>1999</td>
</tr>
<tr>
<td>[72]</td>
<td>Shaman - An Environment For Distributed Management Applications</td>
<td>2001</td>
</tr>
<tr>
<td>[73]</td>
<td>The Guerrilla Management Architecture for Ad hoc Networks</td>
<td>2002</td>
</tr>
<tr>
<td>[76]</td>
<td>LNMP- Management architecture for IPv6 based low-power wireless Personal Area Networks (6LoWPAN)</td>
<td>2008</td>
</tr>
<tr>
<td>[78]</td>
<td>Evaluation of the resource requirements of SNMP agents on constrained devices</td>
<td>2011</td>
</tr>
<tr>
<td>[80]</td>
<td>Cost effective WSN Network Monitoring and Control using Modified SNMP</td>
<td>2013</td>
</tr>
</tbody>
</table>

Table 6 - Selected active monitor studies using SNMP protocol

In [71] the authors presented a protocol for ad hoc network, ANMP, that is based on SNMP and it’s fully compatible with the version 3 of SNMP, using the same Protocol Data Units (PDU) to gather information. ANMP includes MIB extensions, dynamic configuration of agents, and security modules. The protocol uses hierarchical clustering of nodes to reduce the volume of information exchanged between manager and agents. Nodes in the network elect a cluster head
where it will manage information from other clusters as a central point. This division of cluster is done by geographic localization and topology. When grouped by localization, the nodes are periodically redefined and its master node can apply personalized management policy to its group. When grouping by topology, the protocol uses the number of hops to group the nodes. The protocol understands the mobility of nodes, and updates its clusters and all the network topology.

In [72], Sethi presents SHAMAN, a framework based on SNMP for hierarchical management of networks. This framework allows distribution of control and management over the hierarchical management structure in order to provide a dynamic and flexible management of the network. This is done by a custom MIB installed in a multiple top-level manager. The top manager can have several child, or intermediate managers that periodic polls MIB objects at agent in nodes to find their location and gather the data required for monitoring. The top manager answer directly to the programmer requests/queries.

In [73] Shen describes the Guerrilla Management Architecture for adaptive and autonomous management of ad hoc networks. It is based on SNMP, but adds a layer management scheme. The architecture is scalable and heterogeneous and capable of auto adapt to all types of network. In addition, it can be used by any other information access protocols, such as SNMP. The architecture divides nodes in nomadic managers, active probes (agents) and nodes with only SNMP agents. This division is done according to each node capability in energy, processing power, etc. To scale, nodes are grouped in clusters with at least one nomadic manager in each group to reduce the messages exchanges between nodes. A nomadic manager has the management intelligence to adapt to the network, collaborate with other nomadic manager and serve as the main point to other nodes around them. The active probes are programmable scripts that can be deployed in remote nodes to perform local management activities and probe other remote SNMP agents. All the data from the nodes are stores in an adapted MIB database.

In [74], the authors proposed a proxy-SNMP for WSN in which a PC hosts a proxy-based service for SNMP. The data is centralized by an application on the WSN and creates a log file that is then translated to a SNMP agent. This is done by using
a gateway to translate SNMP queries and responses between the IP base network and the WSN. The WSN sensors use software named CodeBlue that then displays and store the gathered data on a PC. This data is available for remote access via the SNMP-proxy connection. On a remote server, a network management system analyses the data and process it. The delay between the gathering of the data and the visualization on the remote server could be a disadvantage. Although the proxy is not used for monitoring the network, the method of acquiring data could be used for managing and monitoring a sensor network using SNMP.

In [75], the authors propose a management tool for wireless sensors networks entitled: LiveNCM: LiveNode Non invasive Context-aware and modular Management, which has similar functionalities to the SNMP, but reduces the volume of exchanged information between the entities, the volume of stored information and the energy consumption. The reduction of data is made in a non-invasive context-aware diagnosis by estimating some data with linear models or interpreting data message exchanges. The tool uses the SNMP to centralize all data and to ease the management of devices. With the use of a gateway, they implement a translator, or SNMP-proxy, that listen to SNMP queries on one side, and retrieves the information from the sensors using a custom process. They also implemented a custom MIB extension for their objects.

In [76], Mukhtar propose a LoWPAN Network Management Protocol (LNMP) which is an operational and an informational architecture management of a 6LoWAPN based WSN. They also propose the design of a management information base. The operational architecture aims to reduce the overhead of transmission and the informational architecture defines the MIB used by the devices in the network. In their architecture, the SNMP is supported only on the IPv6 network and a 6LoWPAN gateway is used to translate between the SNMP and LNMP used on the 6LoWPAN network. Whenever a SNMP request is submitted to the gateway, it is translated to a simplified query via UDP to the destination device. Clusters of devices are created, assigning coordinators devices that are responsible for their child devices. The coordinates keep the information of their child and report it to the gateway. This reduce the communication overhead.
In [69], authors propose an extended modification of the SNMP in order to enable the transmission of the SNMP messages over 6LoWPAN. The proposed 6LoWPAN-SNMP protocol objective is to be fully compatible with the standard SNMP and be resource-efficient by reducing the number of SNMP messages generated and reducing the SNMP header. Authors also purpose the introduction of new protocol operation to push management information periodically from SNMP agents and the use of UDP multicasts. The compatibility with the standard SNMP is achieved by implementing a forwarder proxy on 6LoWPAN gateway.

In [77], Chaudhry presents a lightweight network management protocol named EMP, based on SNMP for IP-based WSN. It consists of an operational architecture focus in reducing the communication cost, reducing network queries and traffic optimization. A MIB extension was also defined for the management of the devices. The EMP assume a coordinator node in the WSN which communicate with the other nodes and a gateway which provides ZigBee to IPv6 translation as well as SNMP queries and responses translation to local management protocol.

In [78], Kuryla implemented the SNMP for resource constrained devices using Contiki operating system. Their solution supported the Get, GetNext, and Set operations, and the message processing models used in versions 1 and 3 of the SNMP protocol. They measured their evaluation by looking at the request processing time and transfer time. Results showed that this metric is increased when using authentication protocols, while encryption protocols do not have a significant impact on this metric. They also estimate the memory usage by using three different approaches. Their solution is a native SNMP operation without using gateways for translation of protocols and messages. On a further study [79], authors investigated how to implement known protocols, such as SNMP and Network Configuration Protocol (NETCONF) to manage restrained devices. For the SNMP protocol, a request took 40 to 120 ms to be processed, while using a NETCONF implementation it took 500 to 900 ms. By adding some security features to these implementation, significant overhead is added increasing on the order of seconds the total processing time.
In [80], the authors designed an efficient modified lightweight SNMP-W for monitoring, managing and control a single-hop WSN. They have done it by removing the encoding of the Type Length Value (TLV) before transmission that reduces the packet size more than 50%. They also proposed a new MIB extension for improvement of their protocol. They also use a proxy to translate the data TLV encoded SNMP packets for the WSN through a gateway device.

Already presented in the passive monitor section, in [57] authors proposed a system named Energy-efficient Passive MOnitoring SysTem for WSN (EPMOS) that provides monitoring information through an SNMP agent developed, where all the data gathered are stored in a MIB.

2.3.1.3.1 Comparative Analysis

In order to compare the previously selected studies for active monitoring with SNMP methodologies, we present in this section a set of items to be compared between each study. Those items are:

- **Data**: The information that is gathered/monitored in order to extract the network and/or node status.

- **Deployment**: this item describes where the data is collected from, and how the gathered nodes are deployed inside the network.

- **Analysis**: this item explains how the data gathered is transmitted to a central server, and what types of improvements are made.

- **Method**: This item describes the type of processing that is made or what types of techniques are used to achieve a customized SNMP query/response transmission.

- **Features**: the mains objectives of each solution studied.

Table 7 shows us the summary of these items compared between the selected studies.
<table>
<thead>
<tr>
<th>REF.</th>
<th>DATA</th>
<th>DEPLOYMENT</th>
<th>ANALYSIS</th>
<th>METHOD</th>
<th>FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>[71]</td>
<td>Management data of each node</td>
<td>Distributed clusters by geographical location and topology</td>
<td>A node is elected in a cluster and is responsible for collecting and forwarding data, reducing the number of packets</td>
<td>clustering algorithm</td>
<td>SNMP v3; MIB extensions, dynamic configuration of agents, and security modules; uses the same PDU and UDP protocol;</td>
</tr>
<tr>
<td>[72]</td>
<td>Management data of each node</td>
<td>Distribution of control and management over the hierarchical structure</td>
<td>Nodes are elected as intermediate managers to gather data and send it to the top-level manager.</td>
<td>Framework built and graphical user interface (GUI)</td>
<td>Flexible and autonomous hierarchical management structure.</td>
</tr>
<tr>
<td>[73]</td>
<td>Management data of each node</td>
<td>Distributed agents in clusters depending on their capability</td>
<td>Active probes gather information from other nodes, process it, and send the results to a supervisor node.</td>
<td>decision-making mechanism and probabilistic reasoning mechanism</td>
<td>Adaptive, scalable and autonomous monitoring; minimize overhead;</td>
</tr>
<tr>
<td>[74]</td>
<td>Health parameters (heart rate, oxygen, pulse...);</td>
<td>Distributed nodes connected to a gateway node;</td>
<td>Gateway node connects to a PC and sends a log file with the sensors gathered information;</td>
<td>SNMP proxy; A remote PC reads SNMP values;</td>
<td>SNMP v3;</td>
</tr>
<tr>
<td>[75]</td>
<td>Management data of each node</td>
<td>Cluster architecture to send information and a server to collect all data.</td>
<td>SNMP agent in only installed on the supervisor (WSN Gateway – SNMP Proxy);</td>
<td>SNMP proxy; Linear models; interpreting data messages exchanges; compression algorithms; custom MIB extension;</td>
<td>Efficient messaging; context-aware; reduced database size;</td>
</tr>
<tr>
<td>[76]</td>
<td>Management data of each node</td>
<td>The task of monitoring is delegated to coordinators nodes;</td>
<td>Each node report to the coordinator periodically or in response to a direct query; Coordinators maintain the state of its subordinates and report to the upper level coordinator or gateway;</td>
<td>SNMP proxy; custom MIB extension;</td>
<td>Reducing the cost of communication; network discovery; interoperability with SNMP;</td>
</tr>
</tbody>
</table>
Management data of each node; Each node with a SNMP agent; Each node respond to custom SNMP queries;

SNMP Proxy; compression on SNMP v1/v2c header; Multicast SNMP messages; custom MIB extension;

Fully compatible with SNMP; Resource efficient; reduces the number of SNMP messages and the size of the SNMP header;

Management data of each node

The task of monitoring is delegated to coordinators nodes; Coordinators maintain the state of its subordinates and report to the gateway; SNMP proxy; custom MIB extension;

Resource efficient; Increase network lifetime;

Management data of each node

SNMP agent in nodes using Contiki operating system Each node respond to custom SNMP queries;

Various implementations made to compress and reduce usage of RAM memory

Interoperability with SNMP messages; memory efficient;

Management data of each node

SNMP agent in nodes Modified version of SNMP v2c and new MIB tree extension;

SNMP-proxy/gateway;

TLV encoding avoided; controlling nodes through SNMP agents;

Network traffic

Distributed network sniffers. Offline. Data is sent to a local server and stored in a MIB to be accessed by a SNMP agent

Human analysis using visual tools Monitoring information using a (SNMP) agent; energy efficient monitoring;

Table 7 - Comparative Analysis of Active Monitoring Studies using SNMP protocol

**Key benefits** of using active monitoring with SNMP:

- The use of a known standard with many visualization tools;
- Accurate access to internal states of services using MIB;
- Usage of a SNMP proxy minimizes the amount of traffic and requests;
- When SNMP v3 is available it adds an extra layer of encryption and security useful for sensitive and/or confidential data (such as healthcare / hospital network);
- There is no need to add extra hardware for monitoring purposes;
• Suitable for much dispersed networks or network with high number of sensors.
• The information acquired is safely inside the network;
• Good for debugging in lab tests.

**Drawbacks** of using active monitoring with SNMP:

• SNMP agents use the limited resources of the devices;
• The usage of SNMP proxy introduce a single point of failure;
• SNMP transmission protocol is UDP which does not provide reliability needed for healthcare / hospital networks;
• Problems in the node also affects the monitoring mechanism;
• Limited resource is used for monitoring;
• Monitoring interferes in the sensor network;
• Probe effects (any software for monitoring the sensors will interfere with the monitoring itself; bugs may come and go when active monitoring is used);

2.3.1.4 **Hybrid Monitoring**

Hybrid monitoring is a mixed methodology of active and passive monitoring, and can be divided in two types: semi-active or semi-passive. In semi-active, the sensor nodes are programmed internally to send messages containing additional information about the state of the sensor node (ex: battery level). These messages are received by the sniffing devices and ignored by the other nodes. In semi-passive, the messages can also be injected in the sensor network to detect how the sensors react and behave. Although no processing is used to generate the packets, the nodes are used for computing and analyzing the packets injected/received. [51]

Table 8 shows the list of the selected studies that focus on active monitoring methodologies using the SNMP protocol and their implementation.
In [82] and [83] authors propose a passive distributed assertion (PDA) as a tool for identifying failure in WSN and provides hint on the causes. This tool allows the programmers to make formulated assertions on the distributed system nodes causing the sensors to send information to be captured passively and evaluated. After capturing the trace, the system can detect failed assertions and give a possible cause to the failure. As long as the sensor can send messages, assertions can be checked. The system also provides mechanisms to deal with incomplete traces. Although the authors named this tool as passive, the tool is also active because the nodes were programmed to send messages about their status to be sniffed by the sniffing network.

In [84] the author purpose DIF, a framework that uses a semi-active method by inserting packets tags in the communications of the nodes. Its objective is to minimize the effort and increase the speed of developing diagnosis tools for a variety of WSN, as well as simplify the diagnosis of the network. The tool developed was made to be used for debugging development scenarios due to its complexity for large networks.

In [85] and [86] the authors developed an low intrusion hybrid monitor. Both passive and active monitoring methods are used. It has two main components: monitor software running in each sensor node, and a monitor node attached to the node which receives software traps in order to obtain the status of the node. Using a passive methodology, the sniffing nodes capture the frames of the sensor wireless

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>TITLE</th>
<th>YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>[82][83]</td>
<td>Increasing the visibility of sensor networks with passive distributed assertions</td>
<td>2008</td>
</tr>
<tr>
<td></td>
<td>PDA: Passive distributed assertions for sensor networks</td>
<td>2009</td>
</tr>
<tr>
<td>[84]</td>
<td>DiF: A diagnosis framework for wireless sensor networks</td>
<td>2010</td>
</tr>
<tr>
<td></td>
<td>Active Low Intrusion Hybrid Monitor for Wireless Sensor Networks</td>
<td></td>
</tr>
</tbody>
</table>

Table 8 - Selected hybrid monitor studies
nodes. In addition, using an active methodology, the sniffing nodes collect information from the monitor nodes, that are connected to the sensor nodes using a serial or parallel connection. Both these types of information gathered are sent to the monitor server by the sniffing nodes, using the wireless sniffing network. The monitor server is responsible to analyze the collected data and to display information. The result is information mainly focused on WSN operation and node state. It can be used to detect failures on nodes or identify intrusion attacks using specific inference techniques. When the monitor nodes are removed the software on the sensor node become non-operational and thus doesn’t impact the sensor node’s performance. The programmer can define what events should be monitored. The proposal model has great advantages at implementation stage or for debugging purposes.

2.3.1.4.1 Comparative Analysis

In order to compare the previously selected studies for active monitoring with SNMP methodologies, we present in this section a set of items to be compared between each study. Those items are:

- **Data**: The information that is gathered/monitored in order to extract the network and/or node status.

- **Method**: this item describes how the data is gathered in nodes.

- **Analysis**: this item explains how the data gathered is transmitted to a central server, and what types of improvements are made.

- **Method**: This item describes the type of processing that is made or what types of techniques are used to achieve a customized SNMP query/response transmission.

- **Features**: the mains objectives of each solution studied.

Table 9 shows us the summary of these items compared between the selected studies.
### Key benefits of using hybrid monitoring:

Advantages in using semi-active observation: the system does not need to be prepared to know all the messages exchanged by the protocol used in the WSN.

- Good for debugging in lab tests.
- Reduces interference in the sensor node compared to active monitoring;
- Flexibility in obtaining detailed data from different hardware / labs;
- Reduction of energy consumption in the sensor nodes;

### Drawbacks of using hybrid monitoring:

- Complexity and difficulty in deploying large network;
- Need to add extra hardware for monitoring;
- Problems in the node could also affect the monitoring mechanism;
- Limited resource is used for monitoring;
- Monitoring interferes in the sensor network;
- Probe effects (any software for monitoring the sensors will interfere with the monitoring itself; bugs may come and go when active monitoring is used);
2.4 **Summary**

The literature review on wireless network technologies presented some technologies that were reviewed at the start of our research. Both the 802.22 and 802.16 are technologies that work in frequencies that require licenses from the government. This is a great disadvantage when the project is intended to be as cheap as possible, because the license and the devices are very expensive. However, the most interesting feature in these standards is the usage in large distance, which is ideally for rural areas with low population density.

The unlicensed standard 802.11 was also presented, with special emphasis on the standards that enabled an increase of the bandwidth. The 802.11 is today a robust technology, capable of supporting the most varied and demanding applications (eg, voice, video), guaranteeing quality, safety and stability. The standards still under development will continue to raise the quality and stability of these networks.

In the literature review on wireless network deployments in rural areas, a survey was made of some case studies in the usage of wireless networks in rural areas. From this study, we learned the main motivations in the use of technologies and the main problems in the administration and management of these networks. Some projects were presented to implement wireless networks in rural areas. These projects provided a scientific understanding of the existing difficulties and possible solutions implemented. In one of these projects a financial study on the use of various technologies was carried out, among which 802.11 is the right choice for this type of network. Finally, based on the case studies, the main problems in the administration and management of wireless networks in rural areas were identified. This analysis will result in the proposal for a centralized management model for wireless networks in rural areas that will be presented in the chapter 3.

Finally, the literature review on managing and monitoring wireless sensors network presented the methodologies of monitoring sensors. The devices used in these networks are resource constrained and offer different challenges for managing. The study made has showed that managing these networks have two
goals: (i) reducing the side effects in the sensor network; (ii) the ability to gather information to detect failures at node and link level to evaluate the network performance metrics as well as the network availability. The presented methodologies have pros and cons. The active monitors usually creates side effects in the network, while passive monitors only can monitor some transmitted data, which could be inconclusive to infer a proper diagnose. Some monitors systems relay on only software while other are hardware based which may be limited to other networks. The IoT domain is still highly heterogeneous because of the different systems used. Gateways and proxies for other networks are still used in order to interconnect these systems. The future seems to be a convergence for the use of IPv6 and a simplified version of a management solution such as SNMP. However, as the study showed, there are still a lot of research challenges to be solved in wireless sensors networks.

Following this analysis, a management model, its architecture, and its intelligent services are presented in the next chapter. The proposal aims to provide innovative solutions and unique features to the most common problems of wireless networks in rural areas in order to achieve a self-sustainable and long-lasting wireless network in rural areas. The next chapter will focuses on these main objectives: (i) monitoring devices and services; (ii) diagnosis, preventive maintenance and automatic recovery; (iii) information and advertisement for end-users; (iv) users authentication and user traffic management; (v) applying intelligence in managing devices and services
Chapter 3

Management Model for Wireless Area Networks

This chapter presents the proposed management model for wireless networks in rural areas. Initially, the basic characteristics of a rural wireless network will be indicated and what are the main concerns for its sustainability and viability. Taking into account these characteristics, the proposed management model aims to create a self-sustainable and long-lasting model for future projects of wireless networks deployments in rural areas.

Following, the architecture is presented and its main objective is to monitor the network and their devices and respective services through automated and constant processes in real time. Taking advantage of the information gathered from the monitoring system, the creation and use of tools for diagnosis, prevention and intelligent automatic recovery of devices and services to assist administrators and technical experts in the prevention and resolution of problems are proposed. Subsequently a module that proposes the creation of alternative gateway to the Internet will be presented. This alternative connection aims to allow remote connections of specialized technicians to the network, even when the main gateway is experience problems that may leave the entire network unreachable remotely. An automatic configuration of devices is also presented as a process to save costs and ease the installation and replacement of devices.
A user monitoring and control module will be presented, which aims to register users’ behavior. This module also proposes a web portal aimed at providing information to users, and creating a virtual advertising space that could make the network and project even more self-sustaining.

Finally, a proactive bandwidth management is presented to improve the quality of the network, by applying intelligence in the QoS parametrizations of the devices in order to achieve a dynamic network. This solutions aims to adjust the QoS through a series of algorithms that provide a fair and satisfactory quality of experience for all users and services.

The following subchapter will present: (i) the essentials of a wireless network in rural areas for its sustainability and its challenges; (ii) the architecture of the management model and all its components; (iii) how the monitoring of devices and services are considered in this management model; (iv) the diagnosis and preventive maintenance that a system based on this management model can achieve; (v) the use in the management model of intelligent systems to automatic recover devices and its services; (vi) the ability of automatically configure and update devices in the network; (vii) the use of web portal to provide information and advertisements for the management model to grow into a sustainable model for the future; (viii) the use of intelligence to manage the bandwidth fairly and wisely, by applying QoS adaptations dynamically; (ix) a review of the management model.

3.1 Sustainability of a Wireless Network in Rural Areas

The creation of projects for the implementation of wireless networks in rural areas is tempting. At a first sight, the deployments of these networks in rural areas may seem easy due to its characteristics. Many scientific documents study the technologies to be used, and what type of devices are suitable for these rural areas. In chapter 0, we have identified some technologies that are being used precisely for the purpose of implementation in rural areas. However, the feasibility and sustainability of the projects do not only depend on the communication technologies used but also on the management. In order for these projects to be
sustainable, the implementation of network management and administration solutions must be mandatory. According to Surana and other authors, the lack of monitoring solutions is the main reason why most projects in rural areas do not remain operational for many years [10, 41].

Usually the global values for this type of solution do not cover much more than the network installation and deployment period. Thus, in rural networks, operational costs in management and monitoring should be reduced and, if possible, nonexistent. Any management model for a rural wireless network should be based on the search for solutions that do not require qualified full-time staff and cheap software solutions in order to keep the project financially sustainable.

3.2 Architecture of the Management Model

The proposed architecture for the management model is based on solutions that require almost no human interaction for collecting and processing data, and minimal costs for its implementation and maintenance.

As observed in Figure 4, in a typical rural wireless network, the users devices and/or home routers are connected to a wireless AP or router that is connected to other wireless routers, each one connected to a default gateway router for the Internet provider.

The architecture takes in consideration the possible presence of IoT networks. The sensors in the wireless sensors network could be inter connected by a different technology (ZigBee, Bluetooth, or other), however, in these cases, a Things Proxy is needed to serve as a gateway or proxy from the wireless sensor networks and its services to the wireless rural area network.

The gateway router is often connected to Wide Area Network (WAN) – Local Area Network (LAN) Border Servers, such as web proxy servers or firewalls, which are responsible for securing the local network and providing services for a better Internet use. Other central servers are often used to deploy essential services, such as: (i) network monitoring; (ii) diagnose and maintenance; (iii) user control and authentication; (iv) traffic / bandwidth management; (v) intelligence algorithms;
If possible, alternative backup WAN accesses are used with the aim of providing backup access in case of failure. As usual, the administration team is remotely located, and has a vast interest in remotely managing the entire network and its services.

![Diagram of network management model](image)

Figure 4 – Architecture of the management model for a low-cost rural wireless network

The management model is divided into several modules. The objective of each module of the proposed architecture is explained in the following subsections.

### 3.3 Monitoring Devices and Services

A proper network management requires the constant monitoring of all active devices and services offered to the users, and of the device itself. In a wireless system, external devices may easily produce interference in the environment in which the communication occurs. These factors demand a strong monitoring of data from the devices [7, 37].
Prior research [7, 10, 41, 87] shows that an accurate diagnosis is a difficult task to accomplish, even for the most experienced administrators. There are a number of commercial and open source applications to monitoring a systems [88]. The monitoring system cannot only rely on network services to decide if the network and their components are working well. Figure 5 demonstrate the importance of both network services and internal services monitoring. For example, a device could respond well to a ping command, or a Secure Shell (SSH) query, but if the CPU is at 100%, this may be causing delay for the users. On a wireless link, all the essential and critical information, such as signal level, number of lost packets, noise level and interference, need to be monitored through the network.

![Diagram of monitoring network services and internal services of a wireless router]

In the cases where the result of a service monitoring result is very specific (example: signal level in dB of a wireless link), it is important to define thresholds that correspond to different alert signals. A good planning and definition of these thresholds may help the administrator to know where the network is performing badly and where users may be affected. Using these thresholds, the monitoring software has to be able to send out alerts and notifications of any type to the administrators whenever a critical value is reached.

3.4 Diagnosis and Preventive Maintenance

For an excellent diagnose, the administrators must include the use of historical values. When compared to other devices values the administrators can reach faster
conclusions and also recognize patterns that indicate a known and frequent problem. This historical information may allow the administrator to predict behavior in similar types of devices and services by looking at certain trends and values that arise in the monitoring software [38].

In a wireless network, the topology usually follows a tree hierarchy model, where an area of the network depends on a single router connection, and that router depends on another router connection, and so on. In our management model, the system must be able to identify the device tree hierarchy. As represented in Figure 6 some areas of the network may be entirely dependent on an interior router. When this router is experiencing problems, the monitoring system must be aware of this hierarchy and their respective dependencies, and therefore, the system is notified of the existence of an unreachable network and all its users. If a mesh network topology is used, there is no need of the system to know the dependencies between routers.

Figure 6 - Example of a network dependency: the red zone of the network is unreachable due to an error with a wireless router.
Another feature that is possible with a historic database of values is the ability to create graphs or charts based on these values. The visualization of graphs is an excellent source of help to detect declines or tendencies in a specific service value. It could lead to identifying problems before the problem actually happen (preventive), and allows the administrator to schedule a visit to the site [10]. A greater challenge is automatically detecting misalignment in the antennas by checking the signal variation over time; that is, by looking at the average levels over a specific period of time [2, 87].

Due to the tight budget, a rural wireless network normally has only one access to the Internet. Therefore, all the routers and users depend on that single access. An alternative access or gateway on different and geographic distributed parts of the network could help the diagnosis [7, 38].

3.5 Intelligent Monitoring for Automatic Recovery

As presented in the previous subchapter 3.4, the patterns obtained from historical values may help to detect declines or tendencies that could lead to identify problems before they exist (preventive) [10]. All these values acquired by the monitoring system, and the data information that it can achieve are extremely useful for the administrators to plan their maintenance.

The next logical step after diagnosis is recovery. Once a well-known problem has been detected, it is necessary to determine which steps the system should automatically execute in order to resolve the issue, without involving the administrators [89]. Solving problems, even the easiest ones, is a complex task that requires attention and focus. These identified and successful recovery tasks could be done automatically by the system, if the indicators suggest that it is the same problem happening over and over again. The richer the acquired data is, the better the decision for a successful recovery.

Related studies [2, 87] suggest that network management is moving towards the implementation of self-managing network functions with aim of eliminating or
drastically reducing human intervention in some complex tasks of network management.

One way to achieve this is to have a quick recovery system on all the devices that would do simple tasks, such as a hard reset or reboot. This is possible by implementing an independent monitoring service in every router (watchdog) that runs a series of scripts in case of problem [38].

Other way to achieve it is to create an intelligent system that not only alerts the administrator of possible problems or trends, but also creates actions to solve them. To better clarify our approach, Figure 7 illustrates the organization and components of the monitoring system.

If the system for monitoring the network is based on SNMP MIB queries the monitoring system queries the most important variables that could affect the network performance. When SNMP isn’t available, an intelligent agent is installed in each device that runs local commands in order to get the variables needed by the monitoring system. This module is presented in the figure as the Acquisition Module, and its objective is to receive information from the agents. This data acquisition is done automatically and repeatedly after a defined wait time, depending on the type of service monitored.
The **Process Entries** module is responsible for gathering all the information received by the acquisition module and then insert it in a database. This information is inserted in a raw state meaning that there is no additional information whether this service is working normally or not.

The **Analyzer** is the main module of the system. Using the same data inserted on the database, it is responsible for analyzing it. This data is analyzed searching for anomalies on the service monitored using the information given by the intelligent module. If a value is out of its threshold limits, the system will send out alerts. The administrators insert most of the values defined for these thresholds. For instance, link wireless signals strength for most wireless routers cannot be less than -80dBm, meaning that, anything below this value should send out an alert. Other values could be automatically learned by the system. Using the same example, a wireless link could be working at an average value of -65dBm in the last 6 months, and all of a sudden, it dropped out to an average value of -78dBm. Although this is not a value that is caught as a warning in the normal thresholds, looking at the data information, the historical values, and the pattern its flowing, it means that a problem may be on the rise, and so the intelligent system may decide to send out an alert and take action.

The **Decision Module** is responsible for the decision of the actions to be taken, whether an alert to be sent by email, or an action to be sent to the agents in the network devices. Based on the input received by the Analyzer, this module decides the actions to take by looking in its database the alerts configuration and others, given by the intelligence module.

The **Intelligence Module** it is the brain of the system. It could store information manually configured by the administrator, but also could perform problem prediction and prevention, based on previous problems. This can be achieved by comparing the values acquired at a certain time with previously acquired and defined patterns. The decision is based on history data. If a certain pattern is repeated, actions could be taken in order to avoid the same results as before. Predictions like these can be created based on probabilistic or machine learning techniques.
3.6 **Device Automatic Configuration**

Rural area networks are often geographically dispersed over a large area, where the main nodes are interconnected via wireless links to the local user devices. These nodes are often in remote locations of difficult access. Scheduling local visits to these nodes is expensive and hard to accomplish. This solution of configuring and updating the devices automatically plans to minimize the cost of maintenance by specialized teams and solve possible problems on non-configured devices.

This architecture uses agents on each device to allow a complete independent solution. An agent is deployed on every device. The agent working on the device it is responsible to keep a good configuration on its device or to deploy a new configuration. The automatic configuration algorithm is given in [Error! Reference source not found.].

![Diagram](image)

**Figure 8 - Algorithm for automatic device configuration**

When the devices boots up, it can start in one of two modes: (1) Configuration Mode or (2) Update Mode.

The configuration mode is applied when using the device for the first time. When the device boots up, it looks up for a configuration wireless network that it is configured in all devices (3). This wireless network is often configured as a virtual network on the wireless router with a hidden service set identifier (SSID) and protected with Wi-Fi Protected Access II (WPA2) encryption using 128 bits password.
The device will then choose the best signal of the configuration network it receives, marks that device as its parent and tries to connect to it (4). If the connection to this configuration wireless network is unsuccessful, the device will retry later. If the connection is establish to its parent, the device tries to connect to the server where the configuration are stored (5). If this connection fails, it will retry later, otherwise, it will search for a fresh new configuration file in the server (6). If a configuration is available, the device automatically apply the configuration file and reboots itself.

The update mode is used every time a device reboots (2). Before the device initiates its normal operation, the agent will look for new configuration parameters or updates on the server (6), and apply it immediately.

3.7 Information and Advertisement
The creation of a web portal in the network is a great way of displaying information about the state of the network, future investments, and downtime warnings for maintenance or tests. In some communities, the police or any other authority uses the portal to display important news for the population, or warnings. However, a web portal of this kind will have to be visited daily by everyone. One way of ensuring that, is to redirect the users’ navigation to the web captive portal. This is easily done with some firewall rules and a proxy server. The objective is that the first page the user tries to visit each day is redirected to the web captive portal of the rural wireless network. Obviously, after their first visit users can return to any other page they want. This method ensures that everyone sees alerts and other information. More importantly, with such a high number of views, it could be worthwhile for a local company or an event to invest in advertisement on the web captive portal. The sale of these virtual advertisements may help in the economic management of the rural wireless network, creating solid economical sustainability for the future. This solution may be used to create profit for the network.

3.8 Users and Proactive Bandwidth Management
Network users are usually the most unstable element in a network. Their actions, no matter what their intentions, can be dangerous to the sustainability and viability of
a network. Implementing authentication on the network is mandatory. Only users with correct credentials can use the network. This authentication module must be centralized on a server where a database of users is available, making it possible for users to change their geographical location without losing access to it.

By using authentication, it is then possible to obtain a summary of network usage for each user, as well as statistical information of that use. Traffic statistics by each user are important to evaluate the overall amount of network usage. Therefore, some types of traffic, such as peer-to-peer, may be limited at peak hours to allow other types of traffic to have higher priority. Traffic control is associated with QoS. Because transmission is conducted over a free license band, there is no guarantee that the wireless frequencies on which the information is being carried are clear and free of interference. To achieve a good service, there are a few network information values that must be collected in order to evaluate the performance of the network [39]. The QoS must be implemented to create restrictions in some types of traffic that abuse the available network bandwidth. Rules for these types of services should be created when beginning the implementation of a project for a rural wireless network.

An automatic system for management of the network bandwidth needs input data to allow it to make decisions and launch alerts with details of the actual state of the network. The network state may be defined as one the following: high congested network, less congested network or no congested network. Each one can be defined as:

- **High Congested**: The network is congested when the packet loss hits the minimum value threshold at a defined timeframe. This timeframe must be enough to the system overcome burst of major traffic rates. If a small time period is defined, the system may send out false alerts for network congestion.

- **Less Congested**: When there’s no network packet lost, the network bandwidth is between 25% and 75% of the available Internet Service Provider (ISP) bandwidth, and the actual bandwidth it is similar to
the average bandwidth registered on historical records with the same timeframes.

- **Not Congested**: The network is not congested when the bandwidth is low (<25% of the ISP available bandwidth) for a long period of time.

With these three defined network states, the system must gather data through time that will enable it to know what the state of the network was at a certain timeframe. For example, considering a timeframe of 24 hours, it will be possible to identify on which periods of time a network was highly congested, less congested or not congested. The same will be possible to achieve regarding week periods, month periods, annual periods, and also special periods like holidays and vacation seasons.

The automatic system gathers a variety of information available on the network packets that flow through the network, as well as all the information available on the network devices. After a good collection of data gathering, the system must decide through algorithms what the acceptable threshold levels for information are. This means that the more data the system receives, the better the thresholds levels are calculated or adjusted through the comparison of previous similar periods and network states (historical data). With these adjustable thresholds levels the system makes decisions about the network actual state and launch alerts and events to improve the network performance. When these fixes are executed, based on the thresholds level defined, the system will then gather the results of its solution to validate its success on the network. This evaluation of the solution provides a valuable feedback and enables the system to look back to previously actions and learn from them, creating a history of actions and results. Based on this historical data, the system may also anticipate problems on some periods and act on them early (proactive).

Not all types of traffic may have the same importance when the delivery priority it is assigned. All traffic must be divided in classes of traffic that represent its importance on the network. This classification will decide the quality, and delay of each type of network flow [15].
QoS classification must be defined according to the priority of each type of traffic. The priorities classes will range from “mission critical” (high priority class) to “best effort” (low priority class). Each class of traffic will have in its queues, network packets that have the same attributes and priorities defined by the network administrators. This means that different type of active flows from different application may share the same priority in one class of traffic. In resume:

\[ \sum_j \text{upload traffic type } flow_j = \text{Qos upload class}_i \]

\[ \sum_j \text{download traffic type } flow_j = \text{Qos download class}_i \]

Each class of traffic will be assigned with a reserved bandwidth and a maximum bandwidth limit. The reserved bandwidth is a guarantee that a minimal bandwidth is being assured. Applications that require no packet loss, low delay and low jitter, such as live video or voice transmission, requires a good amount of reserved bandwidth. Some classes of traffic may have a reserved bandwidth of zero, meaning they operate in any minimum speed and so, no reserved bandwidth is required. This maximum bandwidth enables the class to reach that maximum value of bandwidth available, if it exists, and if is not needed by higher priority classes. The reserved bandwidth for all classes of traffic must be less than the available bandwidth at the ISP. Each class may operate at its maximum reserved bandwidth value at any time. If two or more classes are “fighting” for more bandwidth than their reserved bandwidth, the class with more priority is the first to use it. In resume:

\[ 0 \leq \text{QoS Upload Class}_i \text{Bandwidth} < \text{Upload Bandwidth}_i, \text{ and} \]

\[ \sum_{i=1}^{N} \text{QoS Upload Class}_i \text{Bandwidth} = \text{Normal Available Upload Bandwidth} \]

\[ 0 \leq \text{QoS Download Class}_i \text{Bandwidth} < \text{Download Bandwidth}_i, \text{ and} \]

\[ \sum_{i=1}^{N} \text{QoS Download Class}_i \text{Bandwidth} = \text{Normal Available Download Bandwidth} \]
\[ QoS \text{ upload } Class_i, \text{ Maximum Bandwidth} \]
\[ = ISP \text{ Available Upload Bandwidth} \]
\[ - \sum_{i=1}^{N} Class_i \text{ Reserved Upload Bandwidth Used} \]

\[ QoS \text{ download } Class_i, \text{ Maximum Bandwidth} \]
\[ = ISP \text{ Available Download Bandwidth} \]
\[ - \sum_{i=1}^{N} Class_i \text{ Reserved Download Bandwidth Used} \]

With defined classes, the system is able to separate each flow to its respective class type and priority. For this classification, the system must identify each type of traffic. This information must be gathered by analyzing the network packets header, network packet payload (by deep packet inspection) and also flow information and flow behavior detection [90]. After this analysis, all the flows must be classified by priority and be assigned to one of the available defined traffic classes on the network. This collection of variables is acquired from packets, flows, QoS classes, network stats, and user activities. All these variables are recorded historically.

With a constant monitoring and classification of network traffic, the system is able to identify and predict behaviors of the network traffic. With all this information available and stored, the automatic system must learn from it and adjust the QoS configuration. Different machine learning algorithms (Bayesian networks, Decision Trees) could be used for traffic classification. The system is always learning and adjusting dynamic parameters. After a good collection of data, the system must adjust automatically the network QoS [90] by executing pre-defined algorithms.

Figure 9 shows an algorithm to prevent network congestion using the data gathered from previous situations. By analyzing previous congestion situations, the system can identify which timeframes are most likely of producing network congestion (1).
Therefore, the QoS can be adjusted automatically before that timeframe, using the following steps:

- Reduce the number of permitted active flows per user (2) to start limiting the users that have too many active flows. When there is no limit of permitted active flows abuses may occur. With this reduction, this means that all users have a limit, making it equal for everyone. Sometimes, one user can occupy a big percentage of bandwidth with multiples flows, like peer-to-peer applications;
- Reduce the number of permitted active flows per user on higher QoS classes (3). This may allow the higher classes to be fairly used by all the users in case of congestion.

- Reduce the maximum bandwidth each user may use (4); by reducing each user limit, the overall bandwidth must be smaller, thus, reducing the congestion.

- Reduce the reserved bandwidth of lower classes (5); this will guarantee that the higher classes have more bandwidth available when congestion occurs.

After this cycle of adjustments, the system evaluates (6) the congestion of the network to analyze if it is between the defined thresholds that allows a good quality of experience for users and services. If the network is still very congested, the same cycle of adjustment are made. When the congested drops below the limit, the configuration is saved and the system collects information about the values defined in each cycle in order to use it in the future (7).

Figure 10 shows an algorithm to prevent network congestion on higher QoS classes using the data gathered from previous situations. Congestion on higher classes means that the overall network is congested and that the quality of experience may be affected in the most important applications, such as multimedia applications. By analyzing previous congestion situations on higher QoS classes, the system can identify which timeframes are most likely of producing network congestion (1). Therefore, the QoS can be adjusted automatically before that timeframe, using the following steps:

- Reduce the number of permitted active flows per user on the QoS class (2) to start limiting the users that have too many active flows on that class; when there is no limit of permitted active flows abuses may occur. With this reduction, this means that all users have a limit, making it equal for everyone.
Figure 10 – Algorithm to prevent congestion on high QoS classes

- Reduce the number of permitted active flows per user on lower QoS classes (3). Lower classes are the firsts to be denied in case of congestion in high priority classes.

- Increase the guaranteed bandwidth on the higher QoS class (4); this is achieved by reducing (borrowing) the guaranteed bandwidth from a lower QoS clas, even if it means that the lower QoS class has a zero guaranteed bandwidth (best-effort QoS class).

After this cycle of adjustments, the system evaluates the congestion of the higher QoS class to analyze if it is between the defined thresholds that allows a good quality of experience for users and services on that specific QoS class (5). If the QoS class is still very congested, the same cycle of adjustment are made. When the congested drops below the limit, the configuration is saved and the system collects information about the values defined in each cycle in order to use it in the future (6).
Figure 11 – Algorithm for “happy hour” QoS management

Figure 11 shows an algorithm to create a QoS “happy hour”. At the early hours of the day when most of people are sleeping, the bandwidth used can be very low at higher classes. This situation open up the opportunity for the bandwidth to be used unrestricted in all QoS classes. By analyzing previous situations, the system can identify which timeframes are most likely of producing very low bandwidth usage in higher classes and some congestion on lower classes (1).

Therefore, the QoS can be adjusted automatically before that timeframe, using the following steps:

- Remove any limitation in the number of active flows per user (2). If the bandwidth available is largely unused, there are no restrictions for each user. Even if a user wants to use the network all to itself, he can do so.

- Increase the guaranteed bandwidth on lower QoS classes (3). In the identified timeframes, all QoS classes may be classified with the same characteristics. This means that, at happy hours, the users may use all kind of applications with the same quality of experience.
For a timeframe get average values of bandwidth in higher priority class (1)

Is computed value above defined threshold (Congestioned)?

- yes
  - Borrow a percentage of the guaranteed bandwidth from lower priority classes (3)
  - Reduce the number of flows permitted for users that have the most active flows (4)

- no
  - Does all users have on average the same amount of active flows? (6)
    - yes
      - Reduce the active flows with higher packet size and higher lifetime (7)
    - no
      - Is class still congested? (5)
        - yes
          - Reduce the maximum bandwidth value for all users in this class (8)
        - no
          - Save configuration values and learn. (10)

Is computed value below defined threshold?

- no
  - Mark this class has a possible lend class (12)

- yes

Figure 12 – Algorithm to act when congestion is set on high priority classes.

After this cycle of adjustments, the system evaluates the congestion of the lower QoS class to analyze if it is between the defined thresholds that allows a good quality of experience for users and services on that specific lowered QoS class (4). If the QoS class is still congested, the same cycle of adjustment are made. When the congested drops below the limit, the configuration is saved and the system collects information about the values defined in each cycle in order to use it in the future (5).
These algorithms presented a dynamic QoS management that depends on the historical data collected to act and apply new configurations. A different type of approach is to constantly monitor higher QoS class and act instantly when the conditions of the network bandwidth change.

When a high priority class is dropping packets for a certain amount of time, this class must be adjusted according to its priority. Mainly, a high priority class may increase its bandwidth by decreasing the bandwidth of a lower priority class automatically, and adjusting the number of active flows that each user may create on the lower and higher priority classes. The system must adjust automatically the network QoS, by executing the algorithms presented in Figure 12.

At a defined timeframe, the average values of bandwidth on high priority QoS classes are monitored (1). If the latest result monitored shows no congestion on those classes (2), and if the average value is lower than the threshold defined (11), this QoS class may be marked as a lend class (12), which means that other QoS classes may “borrow” some guaranteed bandwidth when needed.

However, if the latest result monitored shows a state of congestion on those classes (2), the QoS can be adjusted automatically, using the following steps:

- Borrow a percentage of the guaranteed bandwidth from lower priority classes (3); this is achieved by reducing (borrowing) the guaranteed bandwidth from a lower QoS class, even if it means that the lower QoS class has a zero guaranteed bandwidth (best-effort QoS class).
- Reduce the number of flows permitted for users that have the most active flows (4); restricting the users with high values may be enough to control the congestion on the QoS class.
- If the class is still experiencing congestion (5), and there is still users with a high number of active flows (6), the last step (4) is repeated.
If the class is still experience congestion (5), and the users have on average the same number of active flows (6) these steps are performed:

- Reduce the active flows with higher packet size and higher lifetime (7); this acts directly on the flows that are consuming more resources from the network.
- Reduce the maximum bandwidth available for all users in the identified QoS class (8); this means that each user traffic will be slower on this class.
- Block all traffic in the lower classes (9); Starting with the best-effort QoS class, the traffic of these classes have no guaranteed bandwidth to be used; therefore, all the resources are being given to the higher QoS classes;
- After this cycle of adjustments, the system evaluates the congestion of the QoS class to analyze if it is between the defined thresholds that allows a good quality of experience for users and services on that specific QoS class (5). If the QoS class is still congested, the same cycle of adjustment are made.

When the congested drops below the limit threshold defined, the configuration is saved and the system collects information about the values defined in each cycle in order to use it in the future (9). Ideally, the lower classes will run out of available bandwidth, before the numbers of active flows on all users reach a minimum defined value. When this threshold is reached, all the lower classes defined as a non-priority traffic class, must have no bandwidth available. If a high priority QoS class is near its maximum capacity and more bandwidth is needed, it is important to control how much share of that class each user has. When the QoS class reaches peak values, the number of active flows must be as equal as possible for all the users on that class.
3.9 **Review of the Management Model**

The proposed management model is intended as a basis for an effective, cheap and sustainable management solution in rural areas. The availability of specialized teams in rural locations is almost zero. However, with centralized diagnostic tools specialized teams that have a minimum knowledge of the network can provide remote assistance.

The proposed diagnostic and preventive tools allow preventive maintenance to be fast and effective through the visualization of graphic components. Proactive management with the help of intelligent agents eliminates urgent trips to the network by planning corrective maintenance, conducted in advance based on monitoring systems. The proposed alternative backup diagnostic accesses will allow access to inaccessible zones, which allows for more effective diagnostics.

Automatic recovery should be used whenever possible. In centralized automatic recovery systems, recovery tasks should be updated whenever possible according to network needs and common problems. This will allow some problems to be resolved automatically before administrators or network managers realize it. Automatic recovery solution using watchdogs with no intelligence can become harmful if the device constantly resets to solve the problem, which may cause data inconsistency or device malfunction. Because of that, an intelligent system for automatic recovery was proposal with the objective of predict action patterns in the devices and services from the collected information gathered by the monitoring system.

A device automatic configuration can be used to save significant costs of high-specialized personnel and travel expenses. Installing a software based on the algorithm proposed in each device of the network allows a simple user of the network to install or move his own device. This automatic configuration is even more important when there is a need for locally staff members to perform a replacement of a malfunction device with a new device. By executing the software at the startup boot, this new device is automatically configured. The same situation occurs for upgrading or inserting a new configuration in every device.
Information portals can serve as communication between network managers and users. Important information about the state of the network or service breakdowns can be given through a web page due to planned maintenance. The sale of virtual advertising spaces could contribute to a self-sustaining network.

The monitoring and control of users and their traffic allows us to obtain concrete data of the network usage. Abusive cases can destabilize the sustainability and quality of the network. Thus, by prioritizing existing types of traffic, it is possible to adjust the quality of services and provide satisfactory solutions to all users. The proposed solution for traffic control can be improved by implementing QoS parametrizations on all devices, avoiding the accumulation (funnel) at the central point of the network. By using an intelligent automatic system for managing the network bandwidth and a series of algorithms it is possible to create a dynamic network that is always adjusting its characteristics and limitations in order to achieve the best results for the users and services traffic and bandwidth requirements.

3.10 Summary

In this chapter, we proposed an innovative wireless network management model in rural areas, where we were able to focus our effort on creating alternatives to the problems identified in the previous chapter. The characteristics of rural wireless networks require that management solutions be inexpensive and do not require specialized full-time teams or systematic field trips.

The architecture of the management model is divided into several modules that also have the same concerns: reducing costs and automating a remoted management. The monitoring of devices and services together with the diagnostic and prevention tools, enable the network manager to know the network, the devices and its services status in real time. Creating historical reports and value graphs on device details and their services are tools that help prevent and resolve problems on the part of the administrator.

The model also proposes automated problem solving solutions through automatic recovery tools that, although they cannot be 100% effective, are capable of performing problem-solving tasks without the need for a human presence. By
applying intelligence to the monitoring functions the model guarantees the administrators a safe and stress free maintenance of the network. In addition, the solution permits that a new device may be installed in the network without the need of the presence of an administrator or specialized staff, therefore reducing costs and maximizing the network sustainability. This solution also allows the devices to be constantly updated.

When these recovery tools are not effective, the model also provides alternative backup diagnostic accesses that allow administrators to reach network zones that, due to a problem, may have become inaccessible. This solution can save unnecessary time and travel to locations, some of which are difficult to access due to the terrain topologies in rural areas.

An information web portal was presented to provide relevant and objective information to network users. Being a portal with a mandatory visit by users, it can be used to create virtual advertising spaces in order for the project to be even more self-sustaining financially.

Finally, the model proposes the monitoring of users to avoid traffic abuses, and the usage of QoS systems to create priority in some types of application traffic, such as voice over IP, or video streaming. The solution permits to enhance the network performance by applying intelligent decisions based on the actual state of the network traffic variables that will create a fair usage and improve the quality of experience for all the users.

The advantages that these intelligent systems can bring to rural areas wireless networks are focus on reducing the costs in installation, maintenance and improving the network performance. This allows the network to grow sustainable and creating conditions for the users to keep using the network at their maximum performance.

In the next chapter, the solutions implemented in a rural wireless network will be presented, based on the proposed management model.
Chapter 4

Results in Applying the Management Model

This chapter presents the implementation of the management model proposed in the previous chapter. First, it will be presented the pilot deployment made at the start of this investigation, analyzing what were the characteristics of the village and what were the choices of technology and devices used.

The monitoring software, its features and characteristics are also presented in this chapter. A quick overlook at the carefully chosen protocol for monitoring is also presented, to include some brief advantages of using this protocol for the overall monitoring functions. Later, the implemented solutions and the respective results will be presented.

4.1 Pilot Deployment (Memória Online)

The “Memoria Online” project was born out of a partnership between the Center for Research in Informatics and Communications (CIIC) of the Polytechnic Institute of Leiria (IPLeiria) and INOV INESC Inovação. The village of Memória, located in the municipality of Leiria, financed the project.

In 2006 some studies were done by the students of Computer Engineering and Communications of the Higher School of Technology and Management of the Polytechnic Institute of Leiria (ESTG - IPLeiria), with the aim of finding solutions for the lack of broadband access in several zones of the district of Leiria. The work
has evolved with some master’s theses and scientific articles at international conferences.

At the end of 2009, the laboratory pilot network was set up in the parish of Memória denominated Memória Online. The total cost of the network was estimated at 45000 euros. Any resident of the parish can request access to the network through the village council. The only cost to the user is the device that will be installed in his home, namely a wireless router and the respective antennas and physical connections. This device has an average price of 150 euros for each user. The user can connect this device to their own home or wireless router in order to propagate the access to the project network within their home. After this initial cost, the user does not need any further investment. All usage of the internet is free. Local companies and the village board support internet access. In exchange, they can advertise within the network, making the network self-sustaining and creating conditions for its longevity.

This pilot network complies with the legal requirements defined in the Portuguese legislation and has been registered with ANACOM, the Portuguese legislator in telecommunication subjects. In the village of Memória inhabit about 900 people spread in an area of 11km². The parish has about nine locations, which are part of the Memória Online project. During the commissioning of the network, about 50 houses were connected to the grid.

Before the implementation of the network, several studies were carried out to plan the positioning of the antennas in order to cover the largest possible number of residences. Through the Radio Mobile Software [91] (specific to perform site-survey), tests were performed on the antenna positions. This software uses topographic data through digital maps along with signal propagation factors to realize coverage maps of the signals.

For the point-to-point connections between the distribution devices, the frequency of 5GHz was used. The main reason for using the 5GHz frequency in the backbone is the possibility of using a high power legally. Each point in the backbone infrastructure is equipped with a router with one or more interfaces that will distribute the signal through antennas to the population. In addition, another
function of the routers is to distribute signal to the users through omnidirectional antennas.

In Figure 13 it is possible to verify the theoretical signal coverage created by Radio Mobile software based on the settings and specifications of the selected antennas for the Memória village. The areas with the warmest colors are the ones with the best reception.

![Figure 13 - Theoretical results of signal coverage (red = great coverage; green = no coverage) for the village of Memória](image)

The results of this study were important for the beginning of wireless network planning in the village of Memória. Some aspects of this initial study were reformulated a year later through a new study, creating new solutions and improving the final solution that would be implemented later.

The devices used were:

- **MikroTik Routers**: used to make backbone and distribution connections. These routers were equipped with directional and sectorial antennas according to the need and terrain topology.
- **Ubiquiti Access Points**: used to make connections between end users and distribution routers. These devices have integrated antennas, whose powers oscillate between 0dBi and 22dBi. Obviously, the choice of the power of the device depended on the distance that the end user was from the nearest distribution router.

Internet access throughout the project is done through a single point. Thus, the first phase was to create a central server that could serve for all the management and administration of the network.

A server was acquired with the following main characteristics:

- Intel Core 2 Duo E7500 @ 2.93
- 4GB Memory
- Operating System Ubuntu Server
- 2 Network Cards

The capacity of this server allows the configuration and installation of any software required for network management. The fact that it is an operating system without graphical interface, allows the performance to be greater, since it does not need to spend memory and processing to deal with local graphical components, which are not necessary for the management and monitoring software.

The wireless network of the pilot project in the village of the Memória has only one internet connection in a central area called LAR. The internet connection is ADSL with download speed of 8Mbps with a contention rate of 1 to 50.

### 4.2 Monitoring Software

Nagios [92], was the chosen software for monitoring. Nagios is one of the oldest network monitoring systems, and hailed by many as the best. Some inquiries from technology professional’s show that Nagios is actually one of the most widely used monitoring systems in the world [93]. Nagios is an open source system running on Linux operating systems.
Nagios performs verification commands to network device and its services constantly, based on a configuration file for that device or service. When a problem occurs, according to the criteria that are provided in the configuration file, the service alerts and notifies the network administrators through various methods: e-mail, SMS, chat, and others.

The way Nagios works is very complex, since it involves several processes that work together but are configured separately. This method allows the Nagios community to develop more tools and plugins for monitoring their own devices and services. This diversity of people contributing to the project make it the most scalable and configurable of all.

The Nagios base system is responsible for coordinating and scheduling all configured checks in a parallel technique. In addition, the base system holds the response information to these verification requests, and executes the actions or events based on the status of those responses.

The checks are basically execution scripts developed specifically for the type of service that needs monitoring. These scripts are called Nagios Plugins, which are installed separately. There are hundreds of plugins available, the most reliable being on the official Nagios website.

Nagios allows several monitoring methods:

- Checks for network services, such as SNMP, Hypertext Transfer Protocol (HTTP), Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), SSH, Internet Control Message Protocol (ICMP), among others. Nagios not only checks the service, but can also see if the service is well configured. For example, in DNS service verification, Nagios can verify that the service is responding to requests, but also it needs to verify that a name in the local DNS database is correct. If Nagios requests the IP address of the EXAMPLE.PT, and this address is not identical to the one configured in the DNS service configuration file, an error alert is triggered in Nagios.
• Using the SSH or SNMP communication protocol, Nagios can check the status of the processor, memory, or even a disk of an device that has these protocols configured.

• Checking the existence of dependencies between services and devices. The system can check if the device X is unreachable, all its services, and others depending on its state, will also be unreachable. However, only one alert will be issued, which corresponds to device X. All other devices that depends on X will not be verified or reported.

• History of checks for graphing and production of statistical data.

Nagios is one of the most complete monitoring software and has the main advantage for the project Memória Online, to be completely free. In addition, it is modular and scalable, since its growth in applications and functionalities depends on how many plugins it uses or develops.

4.2.1 Configuration Files

The devices and services to be monitored are configured in several configuration files, denominated Objects Definitions Files, which the monitoring software reads hierarchically – see Figure 14. These configuration files are text files, which must follow a set of rules specified in the documentation.
These configuration files are the main disadvantage in using this monitoring software. This whole process of creating configuration files, which can be extensive, takes time. In a network with hundreds of services, this process may take some time until everything is set up. However, there are some aids to facilitate and speed up the process when the devices are equivalent. First, these files can be placed in different directories, making it easier for them to be identified and related to other devices or services to be monitored. Second, it is possible to create templates for devices and services, which can be reused in devices or services that are based on the same monitoring profile. For example, when configuring SSH service monitoring on a router as a template, it can use the same template to also monitor an SSH service on an AP.

The configuration in the monitoring software is based on text files. There are several files to configure all characteristics of the monitoring software operating mode. Most of these files and their configuration options are tuned to the best performance of the service. Thus, the files most important for the basic configuration of the service are:

![Hierarchy of file categories used by the Nagios service](image-url)
• **nagios.cfg** - is the "parent" file. In this file the main the monitoring software options are configured, and all other configuration files are included by name.

• **cgi.cfg** - is the file that contains all the settings for the web server handling the Common Gateway Interface (CGI) execution files.

• **resource.cfg** - is a small file, and contains global variables for using the monitoring software. The main one is the variable that indicates where the plugins or verification scripts are located.

• **commands.cfg** - is the file that instructs the monitoring software on how to use the verification scripts.

• **contacts.cfg** - is the file containing the contacts of administrators who will be notified of any alerts. It can identify multiple people, or entities, as well as create groups of people.

• **timeperiods.cfg** - is the file that contains information about the length of time that different people should be notified of any alerts.

The monitoring software automatically configure all files during installation. Obviously, for complex scenarios, or for experienced management teams, studying and editing these files could make the monitoring software a system tailored to its administrators.

Configuration files that contain the definitions of devices and services can be created in any directory, as long as they are properly identified in the **nagios.cfg** file. The organization of the configuration files is very important because as the devices and services are added, the task to find the files and their respective configurations is harder. Thus, the organization of these files must be performed in advance and in an orderly manner.
4.2.2 Objects

Any definition of devices, services, dependencies, or commands in the monitoring software configuration files are called objects.

A device has associated services. A service must necessarily belong to a device. When all the services on a device are working properly, the monitoring software displays the device as OK. When one service fails, the remaining services are monitored separately. This way the administrator knows that there is a problem with a given device, including the service of that device. In addition, if services are dependent on each other, the administrator can identify the root of a problem. For example, a proxy service usually requires that the DNS server present on the same machine is working properly. If these services are configured correctly in the monitoring software as dependent services, in case the DNS fails, the proxy service will also fail. However, the difference is that the monitoring software will only alert the administrator that the problem is the DNS service, because the proxy is dependent on this.

If the monitoring software detects a problem in a device, service scans will continue to be performed, however, notifications of services will not be sent to administrators due to the device failure on which the services depend.

The states that an object can have are:

- **OK** - the object is working as expected;
- **WARNING** - the object is working, but presents worrying values;
- **CRITICAL** - the object is not functioning and has critical values;
- **UNKNOWN** - the object is not functioning, its status unknown;
- **UNREACHABLE** - the monitoring software cannot communicate with the object.

These states can occur in two types of situations:

- **SOFT STATE** - a state is soft, when the first error check occurs;
- **HARD STATE** - a state is hard state, when all scan attempts have already occurred.

If an object has been configured with a number of retries equal to one, that object immediately passes to the HARD state. Only transitions from SOFT to HARD, and vice versa, cause notifications to service administrators.

Regarding errors and notifications, not all services are identical, and as such, there must be specific configurations for each type of service. For example, a service that checks the state of the processor can verify at a first attempt that the processor is at 100%. The fact that a processor is 100% at a given time may be a normal situation; however, the situation changes if the processor is constantly at 100% for 1 hour. In this case, it is possible to configure the monitoring software in order to send an alert to the administrators of the service when this situation occurs after a number of times. The time between each check is also set.

### 4.2.3 Plugins

The monitoring software plugins are the essence of all communication between the monitoring service, and the objects to be monitored. Each plugin contains a series of script instructions, which are executed by the monitoring software. It is thanks to this functionality that the monitoring software is a powerful tool. Every day new plugins are added to the existing database on the official Nagios website. These plugins are created by the whole community, and are adjusted to the need of each. Anyone who needs to perform monitoring or verification to their specifications can create a new plugin, or change an existing one.

There is a pre-defined package of plugins, which are usually installed together with the monitoring software base service. About half of all plugins were written in Perl, and some in C. Only a small part are written in Bash Shell.

For this modular system to work, the monitoring software base service does not need to know how plugins are built. The documentation clearly specifies the requirements for a plugin to work correctly: input and output parameters.
In the input parameters two values are usually placed: warning (w) and critical (c) values. “Warning” is the value at which it is identified that the service is reaching very high values. “Critical” is the value at which the service is considered to be in problems. For example, when monitoring the processor state of a router, an acceptable warning value would be above 85%, while critical could be above 95%.

Other input parameters can be added to the plugin as long as they are correctly identified in the plugin’s help menu and plugin documentation as shown in this example using the Linux terminal command:

```
root@memoria::/check_ping -h
Usage: check_ping -H <host_address> -w <rta>,<wpl>% -c <crta>,<cpl>% [-p packets] [-t timeout] [-4|6]
Options:
  -h, --help
    Print detailed help screen
  -V, --version
    Print version information
  -4, --use-ipv4
    Use IPv4 connection
  -6, --use-ipv6
    Use IPv6 connection
  -H, --hostname=HOST
    host to ping
  -w, --warning=THRESHOLD
    warning threshold pair
  -c, --critical=THRESHOLD
    critical threshold pair
  -p, --packets=INTEGER
    number of ICMP ECHO packets to send (Default: 5)
  -l, --link
    show HTML in the plugin output (obsoleted by urlize)
  -t, --timeout=INTEGER
    Seconds before connection times out (default: 10)

THRESHOLD is <rta>,<p> where <rta> is the round trip average travel time (ms) which triggers a WARNING or CRITICAL state, and <p> is the percentage of packet loss to trigger an alarm state.

This plugin uses the ping command to probe the specified host for packet loss (percentage) and round trip average (milliseconds). It can produce HTML output linking to a traceroute CGI contributed by Ian Cass. The CGI can be found in the contrib area of the downloads section at http://www.nagios.org/

In the output parameters, the monitoring software accepts a line of text with information about the result of the scan. Usually this line puts the state of the device or service first, and then additional information. In the example below, a ping service request was made to a public IP address, with the input parameters required by the plugin. The result was slightly above the warning value, so the result of the check was PING WARNING, as showed in this terminal command:

```
root@memoria:/usr/local/nagios/libexec# ./check_ping -H 193.137.239.248 -w 10,50% -c 400,90%
PING WARNING - Packet loss = 0%, RTA = 45.27 ms|rt=45.259001ms;10.000000;400.000000;0.000000;pl=0%;50;90;0
```
4.2.4 Hierarchy and Dependency of Objects

The monitoring software enables configuration of object dependencies and hierarchies. There are two types of possible configurations in different objects: the devices hierarchy and the dependencies of objects or services.

It is important for any administrator in a communications network to know the overall status of your network. When the need for diagnosis arises, it is essential for administrators to know the entire topology of the network.

This configuration on the devices allows the monitoring software to be able to map the entire network topology, as identified in Figure 15. This type of configuration is extremely important for the monitoring software to be able to identify and to separate different states, such as DOWN or UNREACHABLE states.

When a routing problem occurs, the monitoring software can be aware of zones that will be influenced by this problem. The example of Figure 15 is enlightening. If a problem occurs in the Router1 device, this device is marked as DOWN, and the configured alerts to the administrators are sent. However, the remaining devices that depend on Router1 (ex: Switch2, Internet ...) will be marked
as UNREACHABLE because the monitoring software does not know its status. Without this device hierarchy configured, administrators would receive notification for each device, making the diagnostic task more difficult and confusing.

Unlike device hierarchies, dependencies do not always exist. The purpose of dependencies is to inform the monitoring software that two or more objects are dependent, and therefore their states are conditioned by each other.

For example, if the administrator wants to monitor a website, he need to consider more than one service or device. A website may depend on the web service, but also on the database service. In this situation, the web service depends of the database service. For the monitoring software to realize this dependency it is necessary to configure this type of dependency in a configuration file. The same situation occurs if the services are on two different devices.

In addition to service dependencies, there may also be device dependencies. Devices dependencies are often confused with devices hierarchies. The difference however is that in hierarchies, the monitoring software already has its own rules on how to act when certain states occur, as explained before. In the dependencies, both services and devices, the network administrator has the possibility to configure the rules for dependencies.

Therefore, it is possible to configure the monitoring software through the dependencies so that if a service has a certain state, the dependent service will not be monitored. In the device hierarchy, as long as the main device has an error (WARNING, DOWN or UNREACHABLE), the dependent device will never be monitored normally.

4.2.5 Monitoring Devices

An important factor for the good condition of the network is the state of its devices. The network of the Memória Online project has as main devices the MikroTik routers and the Ubiquiti APs.

The basic monitoring of these devices is through the known command ping. Using the check_ping plugin, the monitoring software performs several pings to the
respective device and monitors the number of lost pings and response time. Table 3 shows the commands used to monitor devices.

<table>
<thead>
<tr>
<th>CHECK</th>
<th>PLUGIN</th>
<th>WARNING</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK-HOST-ALIVE</td>
<td>check_ping</td>
<td>&gt; 80% loss</td>
<td>&gt; 100% loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 3 seconds delay</td>
<td>5 seconds delay</td>
</tr>
</tbody>
</table>

Table 10 - Commands for monitoring device status

The commands are all defined in the commands.cfg file. In the case of host-alive check this was defined as follows:

```plaintext
# This command checks to see if a host is "alive" by pinging it
# The check must result in a 100% packet loss or 5 second (5000ms) round trip
# average time to produce a critical error.
# Note: Five ICMP echo packets are sent (determined by the '-p 5' argument)

define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 5
}
```

By default, all devices have a WARNING state if they have more than 80% of lost pings or more than 3 seconds of delay. If the result shows 100% loss or more than 5 seconds of delay, the status of the device is marked as CRITICAL state.

Previously, configuration files in the form of a template for repeated uses in identical devices or services have been presented. These templates are an essential part of the good organization and management of the monitoring software.

The first step in creating the monitoring software configuration files is to create a template or generic configuration for all devices. Thus, the generic-host template appears:

```plaintext
define host{
    name              generic-host ; The name of this host template
    notifications_enabled  1 ; Host notifications are enabled
    event_handler_enabled  1 ; Host event handler is enabled
    flap_detection_enabled  1 ; Flap detection is enabled
    process_perf_data    1 ; Process performance data
    retain_status_information  1 ; Retain status information across program restarts
    retain_nonstatus_information  1 ; Retain non-status information across program restarts
    notification_period    24x7 ; Send host notifications at any time
    contact_groups        admins
    register              0 ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
}
```
This template has the following characteristics:

- **notifications_enabled**: Enables or disables notifications for administrators.

- **event_handler_enabled**: Allows activating or deactivating the functions that are performed when the device fails. These functions can be recovery scripts. For example, if a service stops, the event handler can execute a script that automatically connects to the device and restart a specific service.

- **flap_detection_enabled**: Enables or disables flap detection. The flap occurs when a device is changing its state frequently, indicating that the monitoring of the device is not correctly configured or that there are problems in the network.

- **process_perf_data**: Activate or deactivate the information collection function for external plugin processing. It is useful for storing information in a database and for creating graphs with history.

- **retain_status_information**: Allows to enable or disable the function to save the current state of the device to be monitored if there is a reset to the machine or the monitoring service.

- **notification_period**: Lets indicate the timeframe in which notifications will be given. In this case, 24x7 is a time value that indicates that notifications can be sent at any time of any day.

- **contact_groups**: identifies which contact group the notifications will be sent to. These contact groups are created in the separate configuration file contact.cfg.

- **register**: The last parameter defines that this configuration is a template. With the register value set to 0, the monitoring software does not register it as device, but as a template.

This generic configuration contains the basic settings that are identical for all devices to be monitored. However, since the main device is divided by its function.
and importance, it is recommended to divide and create two templates for each type of device: MikroTik router and Ubiquiti access point. Two templates were created:

```
define host{
    name                            generic-mikrotik
    check_command                   check-host-alive
    max_check_attempts              2
    check_interval                  1
    notification_interval           120
    notification_options            d,u,r
}
```

```
define host{
    name                            generic-ubiquiti
    check_command                   check-host-alive
    max_check_attempts              6
    check_interval                  10
    notification_interval           0
    notification_options            n
}
```

The first template (generic-mikrotik), as the name implies, is used for MikroTik devices. The second template (generic-ubiquiti) is used for Ubiquiti devices. It was necessary to create two different templates, because some parameters differ from values, such as:

- **check_interval**: Sets the waiting time between each check. On MikroTik devices, this value is 1 minute per check. In Ubiquiti devices, the value is 10 minutes since the type of connection is not as critical as that of MikroTik.

- **max_check_attempts**: Sets the number of attempts the monitoring software must make to the devices before sending a notification to administrators. In the case of MikroTik, the value is two attempts. An isolated error can be considered normal due to delay or congestion, but two errors in two consecutive minutes is an indication of failure. In Ubiquiti devices, this value is set to six attempts, which together with the value set for the check_interval means a total of 60 minutes until the monitoring software considers that there is a problem with the device.

- **notification_interval**: Sets how many minutes the monitoring software should wait until it resends a notification of the device failure. In the
In the case of MikroTik devices this value is 2 hours, while in Ubiquiti devices no notifications are sent (value 0).

- **notification_options**: Indicates the state in which the monitoring software should send notifications. One or more states may be indicated. The possibilities are d (down), u (unreachable), r (recoveries), f (flap detection), s (schedule downtime) and n (none). In the case of Ubiquiti devices, it is not a priority to receive notifications about their status. As pointed out above, it may be normal for this type of device to be switched off.

After creating these devices templates, it is necessary to create settings for each device, indicating its name and IP address. As noted earlier, it is important to have an organization of these configuration files in order to facilitate the administration process and future changes. Thus, for these devices it was decided to organize them by the geographical area where they are installed. In the same file, the zone distribution MikroTik routers and the Ubiquiti clients that connect to these routers are configured.

For example, in the LAR zone, there are two MikroTik routers and several Ubiquiti clients. The configuration file for this zone is configured as follows:

```plaintext
define host{
  use generic-mikrotik
  host_name LAR1_10
  alias Router Lar 01
  address 10.10.10.1
}

define host{
  use generic-host
  host_name LAR2_10
  alias Router Lar 02
  address 10.10.10.2
  parents LAR1_10
}

define host{
  use generic-host
  host_name MEMO1001
  alias 01001
  address 172.16.10.1
  parents LAR1_10
}

define host{
  use generic-host
  host_name MEMO1002
  alias 01002 Humberto - Farmacia LDA
  address 172.16.10.2
}
```
The configuration of a device (host) is done with the commands presented above:

- **use generic-host**: this parameter specifies which template to use. In this case the generic-host is used, which contains a list of preconfigured parameters for the type of network to be monitored. These parameters, while important, do not differ from device to device so easily.

- **host_name**: this parameter specifies the name by which this device is identified in all other configuration files.

- **alias**: this parameter specifies a description for the device that is displayed in the monitoring software web interface. When updated information is always entered the user name and his customer number.

- **address**: specifies the IP address of the device with which the monitoring software will have connectivity.

- **parents**: this parameter indicates the name of the parent device. For example, the MEM1004 relies on LAR1_10, which means that if the monitoring software cannot access LAR1_10, or if LAR1_10 is in the DOWN or UNREACHABLE state, monitoring to MEM1004 will not be performed.

The remaining configuration files will not be presented in this document, since they are in every way similar to the example presented in the LAR. In the web
interface it is possible to visualize all the devices configured and their respective state and detailed information.

### 4.2.6 Network Services for Management

Service monitoring is a very important aspect in networks where the devices have available services. For example, one of the most commonly used services by administrators in the Memoria Online project network is the SSH service. SSH is an essential service for the administrator to access the devices console and perform routine tasks, or even to automate backup tasks. The most important network services for the network management of the Memoria Online project and their respective monitoring will be presented.

In the MikroTik routers, some services (as showed in Table 11) have been identified as necessary for the good management of the network.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>NETWORK PORT</th>
<th>DEPENDENCIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>HOST</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td>HOST</td>
</tr>
<tr>
<td>WINBOX</td>
<td>8291</td>
<td>HOST</td>
</tr>
<tr>
<td>PING</td>
<td>-</td>
<td>HOST</td>
</tr>
</tbody>
</table>

Table 11 - Services to be monitored on MikroTik Routers

All monitored services are important for device management and administration. The SSH service is essential for connections between machines as already mentioned. The FTP service is used to perform software updates, and to make backups. The PING service is identical to the general device but will have a more advanced use in the services.

Finally, the Winbox service allows the connection of a management software of the MikroTik brand. This software is based on a graphical interface and allows the administrator to perform several tasks in this very complete software.

In Ubiquiti APs the list of services (as showed in Table 12) to monitor is very similar to that of the MikroTik routers.
All services monitored on this device are for management use. SSH and PING are identical to MikroTik. However, for Ubiquiti AP the remote management in graphical interface is done through a secure web page, through port 52443.

According to the identification made in the previous points, it is necessary to use several the monitoring software specific plugins to monitor these services. Table 13 shows the commands used to monitor services.

<table>
<thead>
<tr>
<th>NAME</th>
<th>SERVICE</th>
<th>WARNING</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK_SSH</td>
<td>SSH</td>
<td>-</td>
<td>connection to port 22 fails</td>
</tr>
<tr>
<td>CHECK_FTP</td>
<td>FTP</td>
<td>3 second delay</td>
<td>5 second delay</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connection to port 21 fails</td>
</tr>
<tr>
<td>CHECK_TCP</td>
<td>Winbox</td>
<td>3 second delay</td>
<td>5 second delay</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connection to port 8291 fails</td>
</tr>
<tr>
<td>CHECK_PING</td>
<td>PING</td>
<td>&gt; 80% loss</td>
<td>&gt; 100% loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; 3 second delay</td>
<td>5 second delay</td>
</tr>
<tr>
<td>CHECK_TCP</td>
<td>HTTPS</td>
<td>3 second delay</td>
<td>5 second delay</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connection to port 52443 fails</td>
</tr>
</tbody>
</table>

Table 13 - Commands for service monitoring

These commands are defined in the commands.cfg file:

```bash
# 'check_ssh' command definition
define command{
    command_name    check_ssh
    command_line    $USER1$/check_ssh $ARG1$ $HOSTADDRESS$
}

# 'check_ftp' command definition
define command{
    command_name    check_ftp
    command_line    $USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
}
```
The common point in all of these verification command definitions is the CRITICAL result to happen when connecting to services is not possible. In addition, all commands other than SSH allow the configuration of response time. Response times above 3 seconds are considered as WARNING. Response times over 5 seconds are considered as CRITICAL.

The best way to configure these services is to use the templates again. In the case of services, there is a generic template for all services with the most basic options, similar to what happens with the device and the generic-host template. For the services it was created a generic-service:

```
define service{
    name                            generic-service
    active_checks_enabled           1
    passive_checks_enabled          1
    notifications_enabled           1
    event_handler_enabled           1
    flap_detection_enabled          1
    process_perf_data               1
    retain_status_information       1
    max_check_attempts              3
    check_interval                  10
    contact_groups                  admins
    notification_options            n
    notification_interval           0
    notification_period             24x7
    register                        0
}
```

This template has the following characteristics:

- **active_checks_enabled**: Enables or disables checking for services automatically.
- **passive_checks_enabled**: Enables or disables the verification of services through commands performed by applications external to the monitoring software.
- **notifications_enabled**: Enables or disables notifications for administrators.

- **event_handler_enabled**: Allows activating or deactivating the functions that are performed when the device fails. These functions can be recovery scripts. For example, if a service stops, the event handler can run a script that automatically connects to the device and restarts a specific service.

- **flap_detection_enabled**: Enables or disables flap detection. The flap occurs when a device is changing its state frequently, indicating that the monitoring of the device is not correctly configured or that there are problems in the network.

- **process_perf_data**: Activate or deactivate the information collection function for external plugin processing. It is useful for storing information in a database and for creating charts with chronological history.

- **retain_status_information**: Allows enabling or disabling the function to save the current state of the device to be monitored if there is a reset to the device or the monitoring service.

- **max_check_attempts**: Sets the number of attempts the monitoring software must make to services before sending a notification to administrators.

- **check_interval**: Sets the waiting time between each scan. Considering that the types of services to be monitored will be mostly management services, there is no urgency in checking them.

- **contact_groups**: Identifies which contact group the notifications will be sent to.

- **notification_options**: Indicates the state in which the monitoring software should send notifications. One or more states may be indicated. The possibilities are: w (warning), u (unknown), c (critical),
r (recoveries), f (flap detection), s (schedule downtime) and n (none). In this last case, no notifications are sent from these services.

- **notification_interval**: Sets how many minutes the monitoring software will wait until it resends a notification of the device failure, if it continues. The value 0 means no notifications will be resent.

- **notification_period**: Lets indicate the timeframe in which notifications will be given. In this case, 24x7 is a time value that indicates that notifications can be sent at any time of any day.

- **register**: The last parameter defines that this configuration is a template. With the register value set to 0, the monitoring software does not register it as service, but rather as a template.

After creating these service templates, it is necessary to create settings for each service with the appropriate parameters for each. As mentioned previously, the organization of the configuration files of the device and services is organized geographically. Using these already created files for the devices, it will be added the information about the services that belong to these devices.

Using the LAR zone as an example, there will be several defined services for both MikroTik and Ubiquiti devices. The configuration file for this zone will be added with the following settings:

```plaintext
define service{
  use                             generic-service
  host_name                       LAR1_10,LAR2_10,MEM01001,MEM01002,MEM01003,MEM01004
  service_description             PING
  action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
  check_command                   check_ping!1000.0,80%!5000.0,100%
  check_interval                  1
}

define service{
  use                             generic-service
  host_name                       LAR1_10,LAR2_10,MEM01001,MEM01002,MEM01003,MEM01004
  service_description             SSH
  action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
  check_command                   check_ssh
}

define service{
  use                             generic-service
  host_name                       LAR1_10,LAR2_10
  service_description             FTP
  action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
  check_command                   check_ftp!-w 3 -c 5
}
```
The configuration of a service is done with the commands presented above. Fortunately, it is not necessary to create a file definition for each service on each device. It can be created a group of devices with the same service definitions. The parameters used in defining a service are:

- **use - generic-service**: this parameter specifies which template to use.
- **host_name**: this parameter specifies which device, or devices where this service will be monitored.
- **service_description**: this parameter defines the name by which the service will appear in the monitoring software administration web interface. This name identifies this service in any other configuration files, where it is necessary to indicate or reference this service.
- **action_url**: defines hyperlinks that will only appear on the web interface.
- **check_command**: this parameter indicates the name of the command to execute.

The remaining services of the devices of other geographical areas will be configured in a similar way as shown previously. In the web interface, it is possible to view all configured services and their status and detailed information as showed in

![Figure 16 - Web interface with presentation of services in the LAR1_10 devices](image-url)
4.2.7 Internal Device Information

The monitoring services presented in the above sections are based on networking services of the devices, such as the ping function, or the ability to connect to a SSH network port. However, for a complete monitoring solution, the service monitored should include internal device information that are not available via a network port. For example, it is impossible through an IP network service to measure the state of the machine’s memory or processor. To achieve this internal information the SNMP protocol is used.

The goal of the monitoring system is to interact with the SNMP service available on the devices and remotely request information about their internal information, such as, memory, processor, and data from the wireless connections to the users. Using SNMP Objects Identifiers (OID), a list of services (as showed in Table 14) can be monitored in the MikroTik routers.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>SNMP OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPTIME</td>
<td>.1.3.6.1.2.1.1.3.0</td>
</tr>
<tr>
<td>CPU</td>
<td>.1.3.6.1.2.1.25.3.3.1.2.1</td>
</tr>
<tr>
<td>LINK RX RATE</td>
<td>.1.3.6.1.4.1.14988.1.1.1.2.1.9.0.[mac].[interface]</td>
</tr>
<tr>
<td>LINK TX RATE</td>
<td>.1.3.6.1.4.1.14988.1.1.1.2.1.8.0.[mac].[interface]</td>
</tr>
<tr>
<td>LINK SIGNAL STRENGTH</td>
<td>.1.3.6.1.4.1.14988.1.1.1.2.1.3.0.[mac].[interface]</td>
</tr>
</tbody>
</table>

Table 14 - List of internal services to monitor on Mikrotik routers

Through the uptime service, it is possible to identify how long the device is connected. This value is very important for detecting power failures. The CPU service informs the current state of the processor. This value can be useful in cases where the router continually displays high values, which may mean that the tasks it is performing are too powerful for the processor type, or that the machine is experiencing a Denial of Service (DoS) attack. The services on the link state are perhaps the most important service of this list. The monitoring system will monitor each connection to another distribution router or client user device (Ubiquiti). Transmission rate (TX) and receive (RX) rate indicates the connection status.
Normally if this value drops to low values, it may indicate some problem with the medium access. Finally, it is essential to have information about the signal level in dB of the wireless connection. With this data of the wireless connections stored in a database it is possible to verify if there are breaks in the signal, and to try to identify any problems related to wind effects or others that interfere with the signals of the antennas.

In the Ubiquiti AP it is intended to monitor the data showed in Table 15:

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>SNMP OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPTIME</td>
<td>.1.3.6.1.2.1.1.3.0</td>
</tr>
<tr>
<td>LINK RX RATE</td>
<td>.1.3.6.1.4.1.14988.1.1.1.1.1.3.7</td>
</tr>
<tr>
<td>LINK TX RATE</td>
<td>.1.3.6.1.4.1.14988.1.1.1.1.1.2.7</td>
</tr>
<tr>
<td>LINK SIGNAL STRENGTH</td>
<td>.1.3.6.1.4.1.14988.1.1.1.1.1.1.4.7</td>
</tr>
</tbody>
</table>

Table 15 - List of internal services to be monitored in Ubiquiti AP

All data to be monitored on the Ubiquiti Aps is identical to the MikroTik routers. However, since the OIDs are different, it is necessary to create new services for the Ubiquiti device. In addition, it is important to monitor both sides of a wireless connection, so the administrator can make sure the values are correct. If there are different values, this may indicate a problem in the antenna connection cables, or a failure in the operating system of one of the devices.

For monitoring via SNMP protocol, it is necessary to use only one command, through the check_snmp plugin as shown in Table 16.

<table>
<thead>
<tr>
<th>CHECK</th>
<th>SERVICE</th>
<th>WARNING</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK_SNMP</td>
<td>SNMP</td>
<td>It depends on each monitoring. This setting is</td>
<td>made in the service definition and not in the.</td>
</tr>
</tbody>
</table>

Table 16 - Commands for monitoring via SNMP protocol
These commands are defined in the commands.cfg file:

```plaintext
# 'check_snmp' command definition
define command{
    command_name    check_snmp
    command_line    $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
}
```

The WARNING and CRITICAL states depend on the type of monitoring that is done through the SNMP protocol, and therefore must be configured in the configuration files of the services. The $ARG1$ variable shown above in the check_snmp command definition is responsible for entering values for the WARNING and CRITICAL states when they exist. For example, in the case of uptime it does not make sense to have such alert states. On the other hand, in the values of the signal level it is important to define limits of which it will be important to receive notifications.

The services that will be monitored by SNMP need to be run every minute in order to obtain the most accurate statistical data possible. Monitoring the signal level of a wireless connection every 10 minutes is not enough to detect small signal variations due to wind gusts or the influence of vegetation.

In the network services, it was defined that no notifications would be sent if the monitoring software could not monitor the FTP or SSH services, due to their importance being only for management actions. However, these services based on SNMP are very important to analyze the stability of the network, and as soon as there is a sudden change in values, the administrator should be warned. For example, if the value of the signal level of the connection received by an AP falls to low values, the user may no longer have access to the network and the administrator may not be able to connect to the device. For this reason, it is essential that the administrator be advised as soon as possible.

Thus, for these more sensitive services, it is necessary to create a service template.

```plaintext
define service{
    name               generic-paranoic-service
    use                generic-service
    max_check_attempts 1
    check_interval     1
    notification_options w,c,r
    register           0
}
```
This template has the most important characteristics:

- **max_check_attempts**: The unit value indicates that the monitoring software will send a notification as soon as the first state indicated in the notification_options parameter occurs.

- **check_interval**: The unit value indicates that this service will be monitored in a regular method, minute by minute.

- **notification_options**: the monitoring software will send notifications if any of the following states occurs in the monitored services: w (warning), c (critical), r (recoveries). Since user connections can be interrupted freely, by turning off the Ubiquiti AP power, it is essential that the monitoring software does not send notifications of these situations. It should only send when the values exist and are within the warning limits, therefore placing only the 'w' and 'c' values.

After creating the templates, the services settings are created in the files. Again, geographically organized files are used for better management of the files. Using the zone “LAR_10” as an example again, the following settings are created:

```plaintext
define service{
    use                            generic-paranoic-service
    host_name                      LAR1_10
    service_description            Link CC1_20 Strength
    action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
    check_command                  check_snmp!
                                 .1.3.6.1.4.1.14988.1.1.2.1.3.0.12.66.58.84.234.7 -udB -w -85 -c -90!
}  
define service{
    use                            generic-paranoic-service
    host_name                      LAR1_10
    service_description            Link CC1_20 TX Rate
    action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
    check_command                  check_snmp!
                                 .1.3.6.1.4.1.14988.1.1.2.1.8.0.12.66.58.84.234.7 -ubps!
}  
define service{
    use                            generic-paranoic-service
    host_name                      LAR1_10
    service_description            Link CC1_20 RX Rate
    action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
    check_command                  check_snmp!
                                 .1.3.6.1.4.1.14988.1.1.2.1.9.0.12.66.58.84.234.7 -ubps!
}  
define service{
    use                            generic-paranoic-service
    host_name                      LAR1_10
    service_description            Link SM1_30 Strength
```
define service{
    use                          generic-paranoic-service
    host_name                    LAR1_10
    service_description          Link SM1_30 TX Rate
    action_url /pnp4nagios/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
    check_command                check_snmp!
    1.3.6.1.4.1.14988.1.1.1.2.1.8.0.12.66.58.110.255.8 -ubps -lTX!
}
The parameters used were identical to the network services configured before. As explained earlier, when defining the command through the check_command parameter, variables such as WARNING and CRITICAL limits, that allow the administrator to complement SNMP monitoring. Contrary to what was done with network services, it is not possible to group the devices in the same services because they all have different descriptions. The final appearance in the monitoring software web interface can be seen in Figure 17. The presence of UNKNOWN states means that users have their devices turned off.
4.2.8 Notifications

Notifications are sent by the monitoring system to the contact list configured for the given device or service. The system allows the configuration of multiple contacts and groups of contacts that can be assigned to specific services and devices, if necessary. These settings are made in the contacts.cfg file.

However, just like services and devices, the contacts also allow the creation of templates. The template created was called generic-contact:

```
define contact{
  name: generic-contact
  service_notification_period: 24x7
  host_notification_period: 24x7
  service_notification_options: w,u,c,r,f,s
  host_notification_options: d,u,r,f,s
  service_notification_commands: notify-service-by-email
  host_notification_commands: notify-host-by-email
  register: 0
}
```

This template has the following parameters:

- **name**: name of the template which will be used in other configuration files as a reference.
• **service_notification_period**: set the length of time service notifications can be sent. In this case the value is anytime any day.

• **host_notification_period**: allows setting the time at which device notifications can be sent. In this case, the value is at any time of any day.

• **service_notification_options**: allows defining which service states the contact receives. In this case, it will be all states, since the filtering is done in the definition of services.

• **host_notification_options**: allows defining the status of the device the contact may receive. In this case will be all states, since the filtering is done in the definition of the device.

• **service_notification_commands**: defines which command will be used to send the notification.

• **host_notification_commands**: defines which command will be used to send the notification.

From the definition above the template, the last two parameters are commands that are defined in the commands.cfg file and that are used to send the e-mail. The definition of these commands is as follows:

```plaintext
define command{
    command_name notify-host-by-email
    command_line /usr/bin/printf "\n***** Nagios *****\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\nDate/Time: $LONGDATETIME$ | /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ ***" $CONTACTEMAIL$
}

define command{
    command_name notify-service-by-email
    command_line /usr/bin/printf "\n***** Nagios *****\nNotification Type: $NOTIFICATIONTYPE$\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\nDate/Time: $LONGDATETIME$ | /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ ***" $CONTACTEMAIL$
}
```

These commands use a Linux executable script for sending e-mail (/usr/bin/mail). In the notification, some global variables are sent to the administrator to complement the information as the best as possible. Thus, it is sent in the electronic mail, among other things, the IP address of the device, the name
of the service with problems, the date and time of when the problem was detected, and some additional information obtained in the response of the monitoring command.

Once the template is defined, creating contacts becomes simpler. For example, for the configuration of a contact the following definition is required:

```
define contact{
    contact_name          nagiosadmin
    use                   generic-contact
    alias                 Nagios Admin
    email                 email@example.com
}
```

This definition has the following parameters:

- **contact_name**: The name of the contact, which will be used in other configuration files as a reference.
- **use**: name of the template to use.
- **alias**: allows defining a contact description for use in the web interface or in the notifications.
- **email**: field to indicate an email for sending notifications.

The notifications in operation in the Memória Online project are all made through electronic mail. However, as presented, any other type of communication can be performed as long as it is possible to send through automated processes in the operating system. For example, a GSM connection can be configured in the operating system via a SIM card, which is used to send SMS or make calls to administrators. The possibilities are vast. Email notifications are still the cheapest and easiest solution to implement.

### 4.3 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application protocol that allows the collection of information from network devices through monitoring software called agent (RFC 1157). This collection of information is usually processed at a central point to various network devices running an SNMP agent.
The information given by the agent is diverse and specific to each device. For example, if an SNMP agent is running on a database server, this agent will probably report information about the memory, processor, and disks. If an SNMP agent is running on a router, this agent will probably report on the state of the interfaces and the existing traffic.

All devices that supports the SNMP protocol must include MIB that has a collection of information organized in a hierarchical way and that specifically defines what type of information can be collected from a given device. SNMP is the protocol used to access that information.

The use of SNMP is excellent for any network administrator because it can access through a network service the information that exists only inside the device. Without the SNMP protocol, it would be very difficult to access the state of the memory or the processor of a router in an automated way.

One of the great advantages of the SNMP protocol is the use of the UDP protocol for communication between devices. The use of UDP means that the device that sends data through the communication network does not know if the receiver receives it correctly. Many see this protocol as disadvantage; however, in use for SNMP messages it brings great advantages.

It is the responsibility of the SNMP application to determine whether the message has been delivered, and to retransmit it if it is necessary. Usually this effect is achieved through a simple timeout. The central monitoring system sends a request for verification and waits for a result. If the maximum waiting time is reached, the central monitoring system assumes that the packet has been lost and resends it.

Another advantage of using UDP is that it requires less network resources, making it easier to carry. In cases where there is a large communications network, with several devices monitored by SNMP, network performance is not disturbed by SNMP requests.

Several plugins for the monitoring system use the SNMP protocol to perform requests for scans of various internal device information. Thanks to the MIBs, the
configuration process is facilitated if the devices of a network are identical. In the same device, the MIBs are identical, even in the manufacturer’s specific information.

4.4 Monitoring History

One of the major disadvantages of the monitoring system used is that it does not allow viewing the history of monitored values in an easy way. It can check a history of the states that an object has in a given time period, which can be hours or months.

However, there are situations in which it may be extremely important to realize what happened to a given service a few minutes before the failure. With the monitoring system, this situation is impossible to know because when the plugin responds OK, it means that the service is within the parameters. This is insufficient for good monitoring.

For instance, a wireless connection between two routers is established over a distance of 2km. The monitoring system is configured to monitor the state of the connection through the signal level that each router received. The normal state of the connection signal level would be about -60db. Thus, in both, the WARNING state value is set to -85db and the CRITICAL state value to -90db. Some months after setting up the monitoring system, this connection has become intermittent. The signal levels sometimes stayed in WARNING, as some time later they returned to the OK state. This situation continued until the WARNING state was always active, with worse and worse values. The cause of this problem was pine tree growing in the middle of the link between the two routers. As they grew, the signal level was getting worse and worse. The administrator was never aware of the problem, because for him and for the monitoring system, the connection was always OK. If it had access to a chart with the signal level values, it could have identified the problem some weeks before, since the signal curve would probably be explicit in the chart. There are many other situations where it may be extremely important to have access to the history of values that the system is monitoring.
If there are many identical devices and services, history can be of great help in preventing problems. When viewing a strange behavior or behavior that has already been seen in a previous problem, early diagnosis can be of great help to a network administrator. In specific cases, scripts can be created that consistently check for values in the search for default situations, and that can help the administrators.

In one of the cases presented previously, this type of monitoring was of great help especially in the state of the wireless connections between routers. Most of the connections had stable graphs, with slight variations. However when exaggerated and abrupt variations appeared, these graphs were evident for the administrators. In one of these cases, a sudden signal decrease of 10dB happened at a link between two routers - see Figure 18. This signal breakdown motivated a site visit, where technicians could see that an antenna on one of the routers was misaligned, perhaps due to strong wind.

The data history is very important, especially when specific values are monitored via SNMP protocol. All monitoring services that returns concrete values are great for charting. A software for making these charts was used in Memória Online, named PNP4Nagios that has as main function the creation of history through an RRDTool database (Round Robin Database Tool) and the creation of the respective charts.
The software used allowed the administrators to bridge a failure in the monitoring system. This software is a framework written in Perl, PHP and C, whose main function is to capture the information returned by the monitoring system plugins, and to store it. The storage mode is done through the RRDTool databases. The final results are charts created from these databases, and are available directly in the monitoring software as showed in Figure 19.

The service interacts directly with the monitoring system, since the configuration to create the charts is done directly in the monitoring system configuration files. All graphics appearance and controls can be changed according to the administrator’s preferences.

The good use of this method of monitoring gave the administrators excellent feedback. Recently a notification came from a client, whose signal level of their connection was reaching WARNING values. By analyzing the chart in more detail, it was possible to identify a large difference from the normal values, as seen in the Figure 20.

The chart shows a reduction of about 10dB in the signal level. This type of variation usually occurs when the antenna moves or when something interferes in the line of sight between the two devices. By analyzing the MikroTik router, it was possible to conclude that the problem was not on MikroTik’s antenna, since the signal of the connections of the remaining users had not undergone any change in their mean values. The problem was on the Ubiquiti device (user device) antenna.
Figure 20 - Example of problem identification

This example helps to demonstrate that this type of solutions based on visual data (charts) can be a valuable aid in the identification of problems that would not otherwise be easy to analyze.

4.5 Map Usage in Monitoring

All administrators have mind maps of the network topology. Sometimes small scribbles are made at the time of planning are still used when the administrators need to make changes or solve problems. When networks reach a considerable size, it is impossible to expect administrators to remember all the details of the network, especially the network’s main nodes and their associated services.

It was proposed in the management model the existence of location maps that would assist the administrator in the task of diagnosis and prevention of problems in the network. The monitoring system has a function in which maps can be created based on the hierarchical distributions given in the configuration files. An extra software, named NagVis, was used to enable the creation of any type of map and to present the state of devices and services in an image pre-created by the administrator. This image may be the administrator’s mental map, or anything else that might be helpful in solving problems, such as a real map, a network diagram, or an actual photography.
The configuration is done through a web interface, in which the administrator can place objects in the image chosen. These objects will be responsible for presenting the different icons corresponding to the state of the service or device. For example, a geographic image might be the first image to show the general picture of the network. However, by clicking on specific points in that geographic image, another map with a more detailed image of that location or device can be opened, providing a more complete state view data.

The interface for creating the maps of the network is done via the web browser. As previously indicated it is possible to create maps through photographs, diagrams, drawings, as long as it is in image format. The way of using it is quite intuitive. An example of a simple map created for the project is shown in Figure 21.

### 4.6 Watchdog

It is custom action in the computer world to perform on and off operations to try to solve a problem. This type of solution, sometimes ironized by the media, solves problems in which the diagnosis are sometimes inconclusive. As discussed earlier, it
is common in rural areas for routers to remain in idle states due to momentary power outages. Sending a technician to the location to perform a restart on a router is sometimes enough. Although it is a simple solution, it involves expenses in sending technicians. Moreover, in rural networks, this type of visits is programmed from time to time, which in turn leaves the device inaccessible for a long time, until a visit is scheduled.

Fortunately, some devices already have a recovery system in case of failure: the watchdog. The watchdog is an automatic and independent system of recovering the device where it is being executed. These types of independent systems are excellent for solving small problems in which the diagnosis is easily performed through a command, or the solution only goes through a reset to the device.

The watchdog is usually a software already in the operating systems of the routers. Its function is to periodically monitor the state of a connection. An IP address is set which the machine will attempt to communicate. This IP address is one that under normal conditions, the device can reach and communicate. If it fails, an instruction is given for the device to perform, usually a reset to the router’s operating system. Other actions may be to reset the wireless connection interfaces, to perform specific diagnostics and automatic resolution commands, to send emails, among others.

The devices available in the Memória Online project allows the configuration of watchdogs or netwatchs. In MikroTik devices there is a hardware watchdog that constantly monitors the main system. This watchdog can reset the host system in the event of an operating system lock or in the event of a connectivity failure to a preconfigured IP address. In addition to these main features, it can also send an email to report the problem. In the MikroTik devices there is another functionality similar to the previous one, called netwatch. The purpose of this is to monitor one or more IP addresses. For each IP address it is possible to define a command that will be executed when the state of this IP address changes. This functionality may be very important for the implementation of the module of alternative diagnostic channels proposed in the management model. If the device detects that an IP
address is inaccessible, a command is launched that activates the GSM interface and sends the connection data to the administrator.

In Ubiquiti the watchdog is similar to the MikroTik device but much more basic in terms of functionality. The main difference is that while MikroTik has its hardware recovery system, Ubiquiti makes that through software, which means that if the operating system crashes, the watchdog will also not work. In addition, the only possible configuration in Ubiquiti is to set an IP address for monitoring, which in case of failure activates a command that resets the device.

4.7 Web Proxy

The most effective way to control users’ web traffic is by forcing them to direct their traffic through a proxy. Since it is not advisable to make settings on users’ devices, the perfect solution is that the network device itself performs automatic redirection. This is possible with the installation of a transparent proxy on the server that connects to the gateway. The only requirement for the proper functioning of the transparent proxy is the configuration of the network gateway being set to the server where the proxy is installed.

According to the management model, the visit of the users to the web portal should be something obligatory. The solution implemented in the Memória Online project was performed through a second transparent proxy instance, identical to the one presented previously, but with one difference: this second transparent proxy service is only used to redirect users to the web portal. Obviously, this redirection happens only once every 24 hours.

The management model proposes the existence of a web portal where it is possible to provide information among other things about the state of the network or local events. The model also proposes the existence of a virtual space for advertising.
At the beginning of the planning of the project Memória Online, it was contemplated the creation of a web portal with a message from the President of the Village Council. Taking advantage of this requirement it was created a page, with the President’s message and some additional information as showed in Figure 22. The virtual advertising space was offered to companies in the region that in turn support the internet connection of the project. The future objective is the continuous updating of the portal with relevant information from the network and the community where it is inserted.

Taking advantage of the fact that the first page viewed by the user is the web portal, a zone has been added on the site that describes the conditions of service. For the user to be able to enter the network he will have to accept the conditions of service and click on the "Continue" button. This is very important to triggers various actions on the server. By clicking on the button three important actions are performed:

- A record is created in the Database about the user entry into the network. This information is useful for gathering statistics on network usage. The administrator can consult the database at any time, and check who is currently using the network;
• Rules are added to the firewall to monitor all user traffic. User traffic (upload and download) is updated in the database every minute. This information is very important to detect excessive use of the network and to make usage statistics;

• Redirects the user to the page that requested it before it was redirected.

4.8 Network Usage

From all the data gathered from the network, we have decided to report the usage of the network in one year. Thus, during the average of 12 months in which this service was in operation, the wireless network usage was:

• Average number of sessions: 10000
• Average number of daily sessions: 60
• Average Total traffic: 4.2 TB
• Average traffic generated per session (24 hours): 380 MB
• Only 10 users make approximately 50% of the traffic accounted globally.
• About 75% of users use at least the internet once a day.

4.9 Lessons Learned

The alert system implemented in the monitoring software was configured to send out email messages to the remotely located network administrators. Defining new values for thresholds and alerts was an important and essential task to accomplish. Our experience tells us that we do not need to send out as many alerts as we initially thought. At the start, most of the alerts were false alarms, and after a while, the team treat them as unsolicited messages in their emails. In addition, some threshold defined for warning messages were not realty as important as we though initially.
For the automatic recovery, our usage of the netwatch process was not flawless. At the start of the project when this recovery method was tested, the basic netwatch processes for monitoring neighbor routers were constantly giving false alert states. Sometime when netwatch was executed and received information that a neighbor was down, the commands for recovery were initiated. After a while, we noticed that if we had no commands to fix it, the router continued to communicate very well with the neighbor’s routers. We have changed the scripts in order to have a “second opinion” of the problem before the commands for recovery were executed. Our experience in using the netwatch process is that it is better to confirm the state of the host more than once, before applying the automatic recovery.

Managing traffic with a low bandwidth Internet connection was our greatest challenge. After the implementation of the queue lists and assignment of bandwidth to each queue, it was obvious that the network was having difficulties with so many requests. Initially a great amount of traffic was being sent to the lowest priority queue named unknown traffic, causing some applications to be extremely slow. After the implementation of layer 7 filters, the amount of unknown traffic was reduced and the bandwidth became easier to manage. However, this solution was not perfect. During some hours of the day the network traffic was too heavy, while during others it is very light; nevertheless, our quality of service configuration continues with the same limits and filters.

4.10 Summary

This chapter presents the implementations based on the proposed management model and its results. Initially the project "Memória Online" was presented. The chosen village characteristics and localization classify it as rural area.

This section described an open source based monitoring solution that allows the configuration of all types of devices and services, regardless of manufacturer or architecture. This software allows the creation of plugins to monitor any service or information that is necessary. This allows the software to be scalable and its functionality almost endless. The interaction of this monitoring service with other applications is performed, allowing taking advantage of monitoring data for other
applications. The usage of history and the creation of charts and maps available to the administrator through intuitive and easy-to-use graphical interfaces, which results in easy monitoring, quick and effective problem identification and problem prevention. Through the comparison of behaviors between devices, the administrator can take a proactive attitude towards future events and behaviors, thus avoiding unnecessary movement and loss of time.

Subsequently, the automatic recovery options in the Memória Online project were briefly presented. The configuration made in these devices allows automatic execution of predefined commands in case of failure, allowing in some cases to solve problems at the exact moment they occur.

Lastly, users can be monitored and accounted due to the configuration of proxies and the creation of the web portal. A proxy aims to control web traffic in order to avoid abuses in downloading certain types and sizes of files. Although speeds are reduced in large file downloads, it allows the network to be viable for all users. Given that the internet connection is 8Mbps with a contention rate of 1 to 50, it is necessary to ration the access bandwidth very well. The results have been satisfactory, since the traffic generated by the users is high, taking into account the traffic restrictions applied. The second proxy aims to redirect the user’s first action to the web portal. In this web portal, it is possible to make important messages available to the community while publicizing the entities responsible for implementing the project. In the web portal users are automatically registered in a database, which constantly monitors their traffic on the network. The result of this monitoring allows obtaining a statistical knowledge about the use of the network.

All these results in putting in practice the management model brought sustainability and stability to the infrastructure created in the village of Memória. The great feedback given by the residents that use the network are satisfactory for the project. The local authorities are also enjoying the excellent service that is available for the community. Without the study and development of this management model, the longevity of this network would be in danger.

In the next chapter, the conclusions of the management model are presented as well as the available future work based on this investigation.
Page intentionally left blank
Chapter 5

Conclusions

The research domain of this dissertation was the management of wireless networks in rural areas through the implementation of intelligent solutions to minimize the inherent problems of these networks.

The longevity of a rural network is very dependent on the costs involved in maintaining it, on its ability to be self-sustaining, and on its proper functioning. Thus, the main objective of this dissertation was to propose an innovative management model for wireless networks in rural areas that was effective and economic, through the implementation of free solutions that allow a proactive management of the network.

With the management model proposed, we were able to overcome common problems identified in wireless network in rural areas, such as: (i) bad diagnoses; (ii) lack of information; (iii) non-existing management options; (iv) lack of automatic recovery; (v) high costs associated with specialized staff travels; (vi) non-existing QoS configuration for the limited and inconstant available bandwidth. The management model contributed to identify these problems and to offer cheap and innovative solutions to permit that more wireless networks can be deployed in rural areas.

By deploying this wireless network in the village of Memória, we found people that started using the Internet daily, most of it, elders that are usually lonely
and have limited contact with their relatives. The deployment of the network contributed to the improvement of many people lives, by reducing the gap between them and the people who live in big urban centers.

Having addressed the characteristics of rural networks and their main difficulties, the focus on Chapter 0 was given to the study of previous scientific documentation about deploying and managing wireless rural areas networks. The literature review started by analyzing the current wireless communication technologies available for rural areas. The most detailed analysis was done with communication technology IEEE 802.11, whose functionalities guarantee quality, safety and stability to the rural network. Based on this technology, a study of case studies that implemented wireless networks in rural areas using IEEE 802.11 technology was presented. The main difficulties in managing and maintaining these rural networks have been identified, taking into account the economic and qualitative difficulties in implementation and deployments of wireless network in rural areas. Due to the recent development and usage of wireless sensors, it was also presented recent studies of solutions for manage and monitor wireless sensors networks without interfering with its normal operation.

From this analysis of the literature, a proposal was presented for a novel management model for wireless networks in rural areas presented in Chapter 0. The management model proposes the constant and automatic monitoring of devices and services in order to allow the creation of visual aid systems based on historical data for a proper diagnose of network problems by the administrators. In addition, applying intelligence systems based on the monitoring data can help to predict maintenance tasks in the devices and provide automatic mechanism to recover services and devices. The model presented also plans to create an intelligent system to push automatically updates and configuration files for the network devices without human intervention. These functionalities are essential for the proactive management of the network, as it makes it possible to prevent problems, and to carry out rapid and effective diagnoses without the need for specialized staff expensive trips to the site. To improve the economic sustainability and the user confidence with the project, the management model makes use of a web portal to
keep the users informed and to allow the creation of virtual advertising spaces filled by local business and events agents. Finally, the management model also includes the monitoring and control of the network traffic. By implementing a dynamic QoS system based on automatic intelligent actions, the model guarantee that the bandwidth available is manage proactively for a better quality of experience for all the network users. The use of these intelligent systems can reduce the costs in installation, maintenance and improve the network performance. This allows the network to grow sustainable and creating conditions for the users to keep using the network at their maximum performance.

Finally, it was presented in Chapter 4 the implementations carried out based on the proposed management model. The testing environment was the Memória Online project, whose characteristics and location define it as a wireless network in a rural area. It was possible to achieve one of the most important objectives of the model: the implementation of free solutions. Free and open source solutions allow software functionality to grow as the community grows. The scalability of the software used allowed most of the objectives proposed in the management model to be implemented. The results presented are in line with expectations, since they allowed a proactive management of the network, predicting the behaviors of devices and being effective in the diagnosis of problems. The numbers showed for network usage indicate that the users rely on the good stability of the network. This stability comes from a good planning in solutions for managing and monitoring the network. These results are excellent, considering most users are well advanced in age and have low-level computer skills.

This network is still active and continues to serve as an example for future projects. The management model was the key to the success during the first years of operation on this project, and will remain so for the years to come.
5.1 Future Work

The management model presented covers a variety of features and solutions that are ideally projected for an IEEE 802.11 wireless network. However, in scientific projects many solutions present the use of 802.16 WiMAX as an alternative in rural areas. In the future, most of the features of the management model could be reviewed in order to be fully compatible with most of today’s wireless technologies used in rural areas.

Unfortunately, it was not possible to implement all the functionalities of the proposed management model since these were not present within the scope of the Memória Online project. In addition, some of the devices used in the project are not capable of performing the required processing capability necessary to run scripts based on the algorithm proposed. As a future work, solutions can be found for minimizing the delay of intelligent operations.

In addition, there is still much improvement to be made in the traffic analysis in order to reduce the 30% of unknown traffic currently generated.

The definition of new characteristics for the management model could be studied. For instance, the scope of our management model left out problems related with wireless network that uses the mesh topology, which has become popular in many projects deployed in villages and rural areas. This topology is considered more reliable and resilient, however, as it grows, problems such as bandwidth degradation, radio interference and network delay may appear due to the multiple hops. A proper management model for wireless mesh networks could have characteristics and features that could help the administrators to deal with these problems. Other usage of the management model could be used in power energy issues. In most of rural areas this is a significant problem. Future work could include different implementations for power supplies, such as UPS, solar panels, or other backup methods.

All future efforts on developing the management model will be driven by the motivation of providing access to information services for communities and villages in rural areas that are impaired by their location.
References


44. N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power


85. M. Navia, A. Bonastre, and J. C. Campelo, “Hybrid Monitoring Proposal for


