Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

FINAL MASTER THESIS

TITLE: Telemedicine System in the South Atlantic. Phase VII

DEGREE: Master of Science in Telecommunication Engineering & Management (MASTEAM)

AUTHORS: Alba Boj Sugrañes
Genís Mauri Baqueró

DIRECTOR: Roc Meseguer Pallarès

DATE: July 2012

TITLE: Telemedicine System in the South Atlantic. Phase VII

AUTHORS: Alba Boj Sugrañes
Genís Mauri Baqueró

DIRECTOR: Roc Meseguer Pallarès

DATE: July 2012

OVERVIEW

The information technology and communications (also known as ICT) are an essential part of the evolution in the economy and society. Access to information has become a vital tool for the development of a community. Consequently, there has been a phenomenon known as "digital divide", which refers to differences between countries that have access to ICT and those without.

This project aims to provide a small gesture to reduce the gap between what is often called "differences between North and South", providing an improvement in the telemedicine system that the NGO Telecos Sense Fronteres is developing to the Region of South Atlantic of Nicaragua since 2006.

This seventh stage of the project has tried, first of all, to make a careful maintenance of the infrastructure and equipment which currently has the Hospital Ernesto Sequeira Blanco of Bluefields; to improve their performance by incorporating a system of virtual desktops. In addition, the VoIP telephony system has been expanded to other departments of the hospital and other health centres of Bluefields, plus designing a virtual private network for their internal use.

Secondly, there has been worked in a radio-link to bring telemedicine to Monkey Point, a rural community, isolated and without access to telecommunications.

Finally, it has been emphasized the fact to bring the project to the community of Bluefields in order that they appropriate it and not see it as mere spectators. Related to this, some collaboration agreements have been closed with various local institutions that can contribute to self-management of the project, such as Bluefields Indian & Caribbean University (with engineering students) or the Sistema Local de Atención Integral en Salud (both with the economic and health sides).

TÍTOL: Implantació de la telemedicina a la RAAS de Nicaragua. Fase VII

AUTORS: Alba Boj Sugrañes
Genís Mauri Baqueró

DIRECTORA: Roc Meseguer Pallarès

DATA: Juliol de 2012

RESUM

Les tecnologies de la informació i les comunicacions (també anomenades TIC) són una part essencial dels canvis en l'economia i la societat actual. L'accés a la informació s'ha convertit en una eina vital pel desenvolupament d'una comunitat. Arran d'això, ha sorgit un fenomen conegut com a "bretxa digital", el qual fa referència a les diferències entre països que tenen accés a les TIC, i aquells que no.

Aquest projecte pretén aportar un petit gest per tal de disminuir aquesta bretxa entre el que freqüentment s'anomena "diferències entre Nord i Sud", proporcionant una millora en el Sistema de Telemedicina que la ONG Telecos Sense Fronteres està desenvolupant a la Regió de l'Atlàntic Sur de Nicaragua des del 2006.

En aquesta setena fase del projecte, s'ha pretés, en primer lloc, fer un manteniment acurat de la infraestructura i els equips dels quals disposa l'Hospital Ernesto Sequeira Blanco de Bluefields, millorat-ne les prestacions amb la incorporació d'un sistema d'escriptoris virtuals. A més, s'ha ampliat la xarxa de telefonia VoIP per tal de fer-la extensiva a altres departaments de l'hospital i a altres centres de salut de la població, concretant una xarxa privada virtual pel seu ús intern.

En segon terme, s'ha treballat en un radioenllaç per fer arribar la telemedicina a Monkey Point, una comunitat rural, aïllada i sense accés a les telecomunicacions.

Finalment, s'ha fet èmfasi en apropar el projecte a la pròpia comunitat de Bluefields amb la finalitat que se l'apropiïn i no el vegin com a mers espectadors. En aquesta direcció, s'han establert convenis de col·laboració amb diferents entitats que poden contribuir a l'autogestió del projecte, com són la Bluefields Indian & Caribbean University (amb estudiants d'enginyeria) o el Sistema Local de Atención Integral en Salud (amb la part econòmica i relacionada amb la salut).

"¿Qué sos Nicaragua?

¿Qué sos
sino un triangulito de tierra
perdido en la mitad del mundo?

¿Qué sos, Nicaragua
para dolerme tanto?"

Gioconda Belli
(Managua, 1948)

INTRODUCTION.....1

CHAPTER 1. General Context.....3

1.1. Location of Nicaragua.....3
1.1.1. Political situation.....4
1.1.2. Telecommunications.....5
1.1.3. Health system structure.....6
1.1.4. Telecommunications applied to health.....7
1.2. Current situation of the project.....7
1.2.1. Management plan.....8
1.2.2. The Hospital nowadays.....9
1.2.3. Objectives for the VII phase.....10

CHAPTER 2. Maintenance within the Hospital.....12

2.1. Trouble shooting: Actions taken.....12

CHAPTER 3. Virtual Private Network.....15

3.1. Current situation and problem definition.....15
3.2. Description of a VPN.....16
3.2.1 Advantages.....17
3.2.2 Architecture.....17
3.2.3 Server VPN.....19
3.2.4 Types of VPN.....19
3.3. Solution adopted: OpenVPN and Samba.....19
3.3.1. OpenVPN software features.....21
3.3.2. Security in OpenVPN.....21
3.3.3. Encapsulation in OpenVPN.....22
3.3.4. Samba.....23
3.4. Previous work – Lab.....23
3.4.1. VPN Scenario description.....23
3.4.2. VPN Server. Installation and configuration (Ubuntu 9.10).....24
3.4.3. VPN Windows client. Installation and configuration.....27
3.4.4. VPN Linux client. Installation and configuration.....29
3.4.5. Samba server installation.....30
3.4.6. Samba Windows and Linux clients installation.....30
3.5. Implemented solution.....31
3.5.1. Remote access.....31

CHAPTER 4. VoIP Telephony System.....33

4.1. Current situation and problem definition.....33

4.2. SIP Protocol.....34

4.2.1 SIP architecture.....34
4.2.2 SIP addressing.....36
4.2.3 SIP structure message.....36

4.3. Speech coding.....38

4.4. Previous work – Lab.....40

4.4.1. Testing with a VoIP phone.....40

4.5. Implemented solution.....42

CHAPTER 5. Radiolink HRESB – Monkey Point.....43

5.1. Design of the radio-link.....43

5.2. Technical solution.....44

5.3. Equipment configuration.....46

5.4. Test in-situ.....47

CHAPTER 6. Desktop Virtualization: NComputing.....49

6.1. Current situation within the hospital.....49

6.2. Virtual desktops.....49

6.3. NComputing.....50

6.3.1. Architecture.....51
6.3.2. Our pick: L-300 series.....52
6.3.3. Installation of the server.....52
6.3.4. Server software: vSpace.....53

6.4. Implementation.....54

6.5. Results and conclusions.....55

CHAPTER 7. Other Improvements.....56

7.1. Installation of VoIP phones Grandstream GXP280.....56

7.2. IP Network inventory.....56

7.3. Digitalization the documents of the Physiotherapy Department.....57

7.4. Collaboration agreement with BICU University.....58

7.5. Collaboration agreement with SILAIS RAAS.....59

7.6. Collaboration with GEDEOM....59

7.7. Health software....60

7.7.1. Current situation and problem definition....60

7.7.2. The software....61

CHAPTER 8. Budget and Funding....63

8.1. Budget....63

8.2. Funding....64

8.3. Project spreading initiatives....66

CHAPTER 9. Impact Project Evaluation....69

9.1. Methods and evaluation criteria....69

9.1.1. Human Scale Development....69

9.1.2. The Information Chain....70

9.1.3. Real Access / Real Impact....71

9.1.4. 12 Habits of Highly Effective ICT....72

9.2. Our pick: Real Access / Real Impact....73

9.3. Evaluation with Real Access / Real Impact....74

CONCLUSIONS....79

WEBGRAPHY and BIBLIOGRAPHY....81

APPENDIX A. Technical Issues....84

APPENDIX I. Telephony VoIP....85

APPENDIX II. IP Network Inventory....89

APPENDIX III. OpenVPN Configuration....95

APPENDIX IV. Windows 7 VPN....104

APPENDIX V. Samba....109

APPENDIX VI. No-IP 119

APPENDIX VII. Radiolink HRESB-Monkey Point....124

APPENDIX VIII. NComputing installation....128

APPENDIX IX. Deep Freeze....145

APPENDIX X. Digitazion of Reports....149

APPENDIX XI. Excel User Manual.....156

APPENDIX XII. Agreement UPC-BICU.....162

APPENDIX XIII. Agreement TSF-SILAIS RAAS.....163

APPENDIX B. Project Chronology.....170

Index of figures

Figure 1. Nicaragua within Central America....3
Figure 2. Departmental structure of Nicaragua....4
Figure 3. Structure of health system of Nicaragua....6
Figure 4. Blocked addresses from the main router....12
Figure 5. Mantis tool....14
Figure 6. OCSinventory tool....14
Figure 7. Location of health centres over Bluefields....16
Figure 8. Tunnelling architecture....17
Figure 9. VPN end to end architecture....18
Figure 10. VPN remote access architecture....18
Figure 11. VPN intern VLAN architecture....18
Figure 12. Data encapsulation in OpenVPN....22
Figure 13. IP configuration....24
Figure 14. Listing interfaces on server....26
Figure 15. IP routing table....26
Figure 16. All ports enabled and listening....27
Figure 17. OpenVPN connection....27
Figure 18. Enabled tunnel network....28
Figure 19. VPN network features....28
Figure 20. Automatically start of OpenVPN....28
Figure 21. Listing interfaces on Linux client....29
Figure 22. Scenario configured....30
Figure 23. Rerouted traffic based on ports....32
Figure 24. VoIP network....34
Figure 25. SIP architecture diagram....35
Figure 26. VoIP call completed....40
Figure 27. VoIP flow diagram....41
Figure 28. VoIP call set up....41
Figure 29. VoIP call RTP packets....41
Figure 30. VoIP call ending....41
Figure 31. VoIP call packets lost....42
Figure 32. Radio-link's design....43
Figure 33. Physical map between Cerro Aberdeen and Monkey Point....44
Figure 34. Spot chosen in Monkey Point....45
Figure 35. Radio link simulation....45
Figure 36. Antennas used....46
Figure 37. Switch installed in Cerro....48
Figure 38. Scaffold and antenna installed....48
Figure 39. Architecture of desktop virtualization....51
Figure 40. NComputing L-300 series....52
Figure 41. Features of the server....53
Figure 42. vSpace console....53
Figure 43. Network configuration....54
Figure 44. Guideline for NComputing units usage....55

Figure 45. Equipment for the conference room....60
Figure 46. Application access....61
Figure 47. Application homepage....62
Figure 48. Application manual....62
Figure 49. Leaflet for funding....65
Figure 50. Poster for funding....65
Figure 51. Screenshot of Telecos Sense Fronteres' blog....66
Figure 52. Screenshot of Telecos Sense Fronteres' Twitter....66
Figure 53. Screenshot of Telecos Sense Fronteres' Teaming....67
Figure 54. Informational circular of Col·legi d'Enginyers de Telecomunicació....67
Figure 55. Radio of Kukra Hill....68
Figure 56. The “4 As” model of the Information Chain (Heeks, 1999)....70

Index of tables

Table 1. Absolute number of phones in Nicaragua....6
Table 2. Comparison of VPN software....20
Table 3. Computer technical features....24
Table 4. Parameters to configure in server file....25
Table 5. SIP structure message (First line)....36
Table 6. SIP structure message (Header)....37
Table 7. SIP structure message (Body)....37
Table 8. SIP structure message (Codes)....38
Table 9. Codec Information....38
Table 10. Bandwidth features....39
Table 11. Equipment configuration....47
Table 12. Institutions involved and their contribution....47
Table 13. Comparison of virtual desktop infrastructures....50
Table 14. Advantages of desktop virtualization....51
Table 15. Comparison of features for L-Series 52
Table 16. Grandstream GXP280 features....56
Table 17. IP network inventory....57
Table 18. Budget 63
Table 19. Criteria for Human Scale Development theory with examples....70
Table 20. Comparison of methods and features....74

INTRODUCTION

Telecos Sense Fronteres (TSF) is an NGO created in 2003 at the hands of students, ex-students and professor of the *Escola Politècnica Superior de Castelldefels (UPC)*, with the objective of reducing the digital divide in disadvantaged countries. In 2006, they initiated a project in Nicaragua to improve communications and access to information in the field of health of the South Atlantic Region (RAAS). Over the years there have been several phases of this telemedicine project to improve the technological conditions of the region's central hospital located in Bluefields and the communication with several health posts spread all over the area. This document details the tasks performed during the VII phase of the project.

In the first chapter, the project is located in its political, social and geographical point of view, as well as specifying the infrastructure of the health ministry in Nicaragua. Also, it briefly reflects all the work done in the telemedicine system by TSF in recent years.

Along the second chapter, it is detailed the maintenance performed on the existing hospital's infrastructure.

This is followed by the study, design and implementation of a virtual private network (VPN) between the various health centres located in Bluefields. The VPN creates an internal network between the different computers without being physically together. This, on the one hand, leads to a reduction of costs; on the other, it increases the security of communications and facilitate the connection between multiple computers on different IP ranges.

In the fourth chapter it is presented the need to expand the VoIP telephony network outside the range of the hospital, in order to have a more direct communication between the parties involved in the project. One can see the details of network design, configuration of telephones and the final solution.

The next chapter details the solution implemented in the radio-link with the community of Monkey Point. This radio-link work started during the last phase of the project [3] and our task was to test *in-situ* the connectivity. Given the multiple problems, the chapter outlines the procedure followed and its final conclusions that led to that the radio link is actually not feasible.

Moving forwards, the sixth chapter explains the system of remote desktops (NComputing) implemented in the frame of the hospital to solve the serious problem of deterioration of computers due to the severe weather conditions of the area.

In the next chapter, the seventh, one can see the additional actions taken to improve the hospital network as well as the continuity of the TSF project. It is both explained the installation of new VoIP phones or the digitalization of physiotherapy department documents to facilitate the statistical work. Moreover, some collaborative agreements have been established with the BICU University and SILAIS in order to strengthened the continuity of the project. In addition, it is mentioned a software application, designed by the Ministry of Health, to unify the system of admission and patient records of various offices, hospitals and health centres in the country.

To end up the report, it was deemed necessary, as a cooperative project, to conduct an economic evaluation (such as the material used or the money spent by the aid workers in the trip to Nicaragua), and elaborate an impact study of the project to identify the weaknesses and strengths of the work done. Finally, a set of conclusions and commentaries are also addressed at the end of the document.

CHAPTER 1. General Context

This first section of the report presents an overview of Nicaragua, including the current economic, technological and health situation. It has been taken into account that this project is the seventh stage of a project that started in 2007 in the South Atlantic Autonomous Region (RAAS) in Nicaragua. So the different tasks performed during these years and the objectives for this new phase are detailed along the chapter.

1.1. Location of Nicaragua

The Republic of Nicaragua is the largest country in Central America (with an estimated population of 6 million), bordered by Honduras to the north and Costa Rica to the south. The country is situated some degrees north of the Equator in the Northern Hemisphere, which places it entirely within the tropics. The Pacific Ocean lies to the west, and the Caribbean Sea to the east. The country's physical geography divides it into three major zones: Pacific lowlands, Cooler central highlands and the Caribbean lowlands.

Figure 1. Nicaragua within Central America

1.1.1. Political situation

Nicaragua itself is considered as an independent state, free, sovereign and unitary. The current president of the country is Daniel Ortega Saavedra, belonging to the FLSN (Frente Sandinista de Liberación Nacional) political party, who is in charge of the government since 2007 and was recently re-elected.

The fact is that Nicaragua is still a country with a low level of development, marked by political instability in recent decades, natural disasters, and export policies that the country experienced in the 1980s and 1990s. Nowadays, it is the poorest country In Central America and the second poorest in the Hemisphere. Thus, 61.9% of Nicaragua's population is under the poverty line. According to 2011's World Bank statics, Nicaragua is ranked 129 in the table of countries by gross domestic product (GDP) to values of purchasing power parity (PPP) per capita.

The country is divided into 17 departments, which now only have merely administrative purposes. They have no authority and all the responsibilities are delegated by the central power. The departments are further divided into municipalities governed by a mayor and a council.

Figure 2. Departmental structure of Nicaragua

The two regions with more difficulties in their development are those located in the Atlantic coast, within an area known as "Caribbean Coast". This is due to access problems caused by a lack of infrastructure. The project explained along this report is developed in the South Atlantic Autonomous Region (from now on, RAAS). To access the regional capital, Bluefields, there are only two ways. One is by plane, which takes 45 minutes, but it is priced beyond the reach of most of the population. The other one, much more accessible in terms of expenses, is by land on a bus for a journey of six hours, then two hours of waiting in El Rama, and then "panga" (wooden boat motor) for two hours along the Río Escondido.

This region has a population of approximately 382,000 inhabitants and an area of 27,407 km^2. It consists of 12 municipalities, and to move from one of them to another, one must usually travel by boat. This, taken to our project, makes very difficult all medical tasks throughout the region.

As mentioned above, the capital of the RAAS is Bluefields, and is home to the Regional Hospital Ernesto Sequeira Blanco (from now on, HRESB). This is where TSF is placed and where the project has mostly been developed.

1.1.2. Telecommunications

Political instability in the area has caused continuous changes at the organizational level of telecommunications and service providers. The privatization of the telecommunications company in Nicaragua began in 1995, after a major effort to modernize them during the first half of the decade. However, as in some other countries in Central America and Latin America, this process greatly favored the company that acquired everything, ENITEL.

The privatization included an exclusivity clause for three years for private monopoly. The government also granted exclusivity in fixed and wired telephony (both national and international). In addition, licenses were granted for the operation of mobile telephony services and other telecommunications services.

Thus, this process meant an expansion of the coverage of all services, including mobile telephony, although this happened more due to the technological advance than a competitive market. Anti-competitive practices are common and sector regulation has been weakened by conflict.

Nowadays, ENITEL (company previously controlled by the state) owns all the country's fixed lines and is behind the trademark CLARO (mobile), Turbonett (wireless internet), AMNET (broadband and data transfer). There is only a competitor, Movistar, clearly in disadvantage in some regions of the country such as within the RAAS. It might be said that there is a virtual monopoly in telecommunications.

Looking at how people have access to telecommunications, since the privatization, access to fixed-lines and mobile-cellular services has improved but teledensity still lags behind other Central American countries. Fixed-line teledensity roughly 5% persons; mobile-cellular telephone subscriber-ships increased and approached 65% of population in 2010. In total numbers:

Telephony (2010)	
Fixed lines	258.000
Mobile cellular	3.711.000

Table 1. Absolute number of phones in Nicaragua

From the point of view of information, there are multiple privately-owned terrestrial television networks spread all over the country, supplemented by cable TV in most urban areas. Furthermore, Nicaragua owns more than 100 radio broadcast stations, nearly all of them privately owned. Radio Nicaragua is government-owned and Radio Sandino is controlled by the FSLN. Although this data seems encouraging, there must be said almost all of the services and networks are placed in the Pacific or Central departments of the country, and just a few in the Caribbean coast, once again, leaving them in a disadvantage position.

1.1.3. Health system structure

In Nicaragua, the public health system is divided into different SILAIS (Sistemas Locales de Atención Integral en Salud), similar to what in Catalunya is called CAP (Centre d'Atenció Primària). Each region or department has its own SILAIS, all of whom report directly to the Ministry of Health (from now on, MINSA). The HRESB is the main hospital of the RAAS, and must provide coverage for all health centres. The main health centre, which coordinates the rest of them, is also found in Bluefields and called Centro de Salud Juan Manuel Morales.

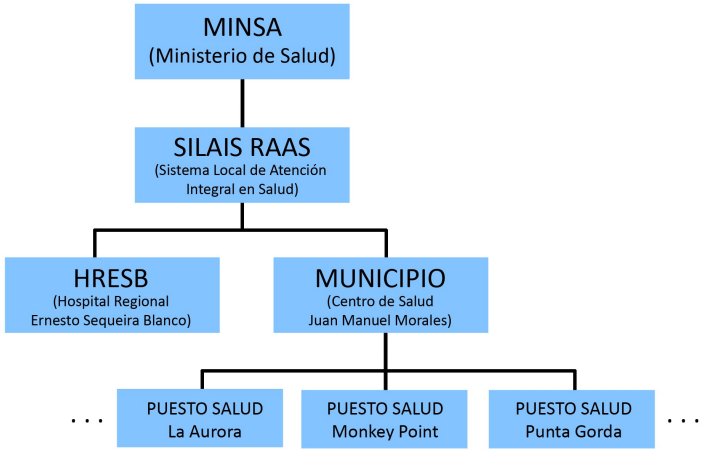


Figure 3. Structure of health system of Nicaragua

When a health post in a municipality has to have surgery or a treatment that have no infrastructure or medical supplies, patients must be referred to Bluefields. That is why communication between health centres and the hospital are so important, because health centres must apply for transfers, manage the patients, and so on.

But another factor must be also considered. Doctors working in health centres are medical students from fourth grade, as in Nicaragua is called "Social Services". As practices of their studies, they have to be two years in charge of a health post. But their knowledge, due to a lack of experience, are not as extensive as those doctors from the hospital. Therefore, they need to be in constant communication with senior doctors, for advice, opinion and support. Thus, shipments can be saved with the help of a doctor with more experience.

The main problem is that health centres are not always well-endowed in areas of telecommunications infrastructure. For instance, in the municipality of Corn Island, a very well-known tourist spot, the health centre already has a good infrastructure. But, on the contrary, there are other communities which have no access to the Internet or mobile communications or whatsoever. In other words, to broadcasting. It is here where the work by Telecos Sense Fronteres is involved.

1.1.4. Telecommunications applied to health

One of the most widespread applications that may have telecommunications in the health sector is telemedicine. Two doctors with a phone can be considered the simplest practice of telemedicine.

The development of telecommunications is continuous, very fast and can be especially useful in medicine, which allows high profits, saving time and money with increased quality and coverage. Telemedicine is applicable to all medical fields, including surgery. However, they usually pay little attention to its most practical and simple, allowing a large reduction in costs with strong improvements in efficiency, quality and coverage.

In the case TSF is dealing with, being this a project in a fairly isolated rural area of Nicaragua, the use of telemedicine is emphasized because with a relatively simple system large gains and benefits for the population can be achieved.

1.2. Current situation of the project

This project aims to continue the first phase of a global project called "*Sistema de Telemedicina del Atlántico Sur (STAS)"* [1]. Its first stage, *Plan de Telecomunicaciones para la región del kukra river. Fase I,* was developed in February of 2006. All the phases had been developed for the NGO *Telecos Sense Fronteres* (from now on TSF) with the

cooperation of telecommunication students of the EETAC (*Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels*). This phase is the fourth in which TSF promotes that the students stay for a long term where the project is held.

In the following sections, the main project STAS is described. In addition, the current situation of the project and the objectives of the new phase are also detailed.

1.2.1. Management plan

As mentioned above, the project described in this report belongs to a larger project that began in 2006. Its main target is to communicate, through an Internet network, all the health centres in the RAAS region with HRESB, as it is the most developed hospital in the area.

The reasons that encouraged the development of medicine technology in communities with fewer resources is that it provides several important advantages:

- Support and medical advice to young health professionals in rural areas through the telemedicine. This increases their self-esteem because they feel supported by other specialists.
- Strength and support the work of planning and coordination of vaccination campaigns, epidemiological surveillance, etc.
- Provide to the communities with a communication service for emergencies.
- Improve the health of the inhabitants of rural communities.
- Increase living standards in rural areas.
- Promote education and access to culture and new technologies.

All these improvements allow compliance with three of the eight Millennium Development goals:

- Reduce child mortality.
- Improve maternal mortality.
- Combat HIV/AIDS, malaria and other diseases.

In the first phase of the project, some other NGOs helped to develop it, such as *DESOS opción solidaria*, *Raíces solidarias* and *TSF,* and entities such as *Ministerio de Salud de Nicaragua* (MINSA). In 2006, TSF aid workers conducted the first stage in Nicaragua. Due to bureaucratic reasons, it was totally paralysed and they had to get back home without being able to make the goals. In January 2008, the relationships with the new MINSA were established. Thus, this first phase become active again and finally the communication between the Health Post in the community of La Aurora and HRESB was successfully made through a radio-link.

During the second phase of the STAS, it was created the necessary technological

network infrastructure for all future communications, as it was decided that HRESB would be the central point between the rural communities. The needs to improve the HRESB network were evident because the hospital was not equipped with the minimum infrastructure to support a large number of links.

Once this basic infrastructure to support new links was developed, the prioritization was focused on improving the hospital facilities and computers. So along the following stages, TSF worked out a computer room for hospital personnel; a VoIP telephony network so different departments could call among them; personal hospital e-mails; and improvements on the Internet network. Also, in the last phase of the project, two monitoring system were implemented: one for the hospital network, and a second one for the radio link established with La Aurora, in order to control the network from Barcelona during the period that TSF aid workers are not in Bluefields.

As mentioned before, one of the main goals of the project is to communicate the different Health Post of the RAAS with the HRESB, so the last action consisted of the evaluation of a radio-link between the community of Monkey Point and the hospital.

1.2.2. The Hospital nowadays

This section details the features and equipment which HRESB owns, related to the telecommunications field.

Radio-link between rural communities

The only radio-link done up to now establishes a communication between the HRESB and the community of San Francisco, La Aurora, locally known as “San Pancho”. This link presented several problems and along the phase V [2] was rebuilt. Nowadays, it correctly works. San Pancho's health post has a VoIP phone and a computer.

Feasibility studies were done to connect with other health posts within the RAAS region. Finally, it was decided to link the health post of Monkey Point as it is the community with almost direct visibility.

Infrastructure communication of HRESB

Along phase III of the project, the planning and the implementation of the infrastructure in the hospital were developed, leaving 42 connection points installed, 23 computers and 12 VoIP phones. Nowadays, the equipment has substantially changed due to the hospital's needs and because some equipment have broken down. Summing up, the hospital currently has:

- 28 computers
- 15 VoIP phones
- 44 connexions

In addition, the hospital has two servers. In one of them, there is installed the VoIP telephony on Asterisk, the hospital's internal mail and the DHCP service. In the other one, the OCSInventory application, MANTIS incident application and ZABBIX monitoring application. Both servers have a backup system.

Nowadays, HRESB has a 256Kbps Internet connection to serve the entire hospital. Furthermore, it also has a private connection of 1Mbps which is provided by an Italian NGO. This connection is barely used for some the doctors to send important statistical files to struggle against certain diseases.

1.2.3. Objectives for the VII phase

After completing the previous phases of the project, the hospital needs were assessed again. At this point, new objectives for this new stage were determined before the departure, although all of them were re-evaluated *in situ* on arrival.

For this seventh phase of the project, it was scheduled a 6 month period in which the main goals to achieve were as follows:

- **Continue the implementation of the radio-link between HRESB and Monkey Point's Health Post.** To perform it, several institutions were involved. On the one hand, the NGO blueEnergy which would supply the electrical power system with solar energy. On the other hand, the community of Monkey Point, whose inhabitants would collaborate with the construction of the tower, done by themselves. And finally, the communal government of the region, with the economical support for the fuel and the transportation.

- **Create a VPN to connect Health Centres located within Bluefields.** The main reason to implement the VPN is because the different Health Centres are continually sending and receiving documents between them, and many of that data is related to patients, thus private.

- **Expand the VoIP telephony system beyond the hospital network.** In order to include other medical centres of Bluefields to the network, so they can easily establish communication with any department of HRESB of with the Health Posts of the telemedicine project.

- **Implementation an architecture of desktop virtualization.** Since the arrival of TSF in Bluefields, it was detected a large and rapid deterioration of the computers and equipment due to its tropical damaging weather. To solve this never-ending problem that has affected us year after year, it was studied the possibility to implement N-Computing technology, which permits the centralization of the CPUs on a single server and all the clients are remotely connected to it.

- **Standardise a medical management tool for HRESB.** In previous phases, Care2x software was chosen but it eventually did not perform satisfactory results, since it is a very complex tool that did not suit the needs of the hospital. In addiction, nowadays MINSA is developing a medical software to unify and implement in all the institution of the country. So, when completed, TSF would support it and help with the implementation in HRESB.

- **Training courses for the hospital staff.** During the last two stages, some campaigns were performed, consisting of a set of courses for the personnel to learn the usage of Ubuntu and become more familiar with this SO. Education is a very important issue, so it was determined to keep everyone updated with the tools the hospital owns, specially Microsoft Office and Linux.

- **Set a cooperation agreement with BICU University.** A project is successful when the people who is helped is also involved in the labour and not just a mere spectator. That is the reason that led us to consider an agreement with the University of Bluefields, whose students could actively contribute to project and be part of the team.

CHAPTER 2. Maintenance within the Hospital

One of the initial task to take into account was the maintenance of the hospital's infrastructure in terms of equipment, devices as well as the network. During the first weeks it was vital to check out the whole system in order to fix the damages caused when no volunteers were in Nicaragua. Afterwards, we realised that maintenance was not just important during that first period but along all our stay, since problems occurred frequently.

The main shortcoming the hospital has to deal with is the fact that almost no one can guarantee an appropriate maintenance during the absence of volunteers, so many equipment fall into disuse due to a lack of knowledge.

2.1. Trouble shooting: Actions taken

- *Blocked some web sites of the Hospital's network*

Such as Facebook or YouTube due to the slow Internet connection and the misuse of that tool done by some employees during the work time. The procedure consisted of editing the privacy options within the central router.

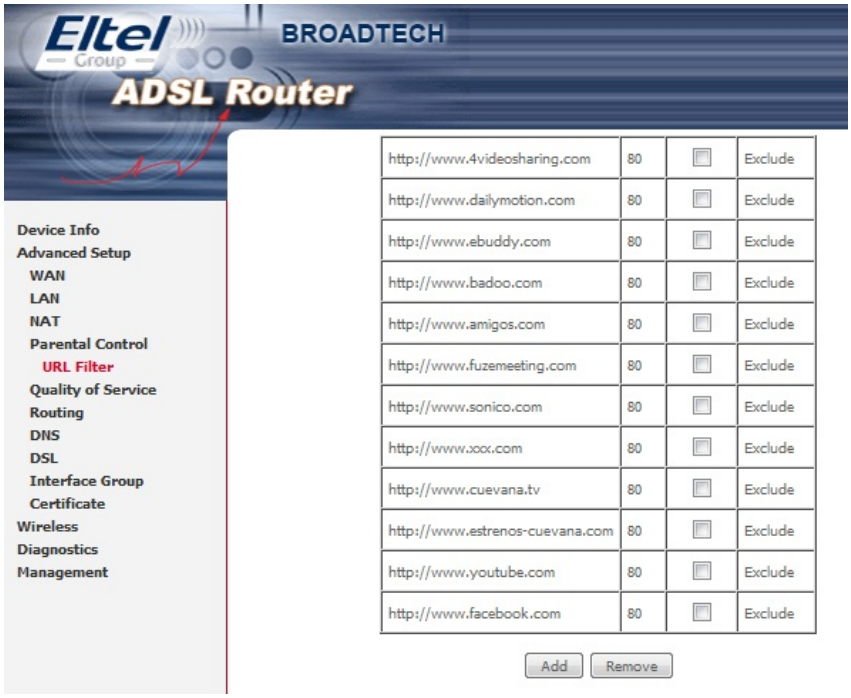


Figure 4. Blocked addresses from the main router

- *VoIP phones not working*

Checked all the VoIP telephones since many of them were not working by the time we arrived. The main problem seemed to be that they were using dynamic IP instead of static ones, so we re-configured them back into the 192.168.1.XXX rang established by the VoIP telephony. Besides this, other devices just needed to plug the wires into the correct socket (LAN vs. PC).

- *Provided Internet access in area of nutrition*

Totally absent up to the moment, the nutritionist had to move to the library to make any inquiries. We placed a switch in the closer department with Internet (Radiology, only a few feet away) and passed a wire through the ceiling, making all the installation.

- *Repaired the LAN connector in Surgery department*

Changed the LAN wall socket in Surgery department since the VoIP phone could not detect the hospital network. Afterwards, the whole VoIP network was re-established.

- *Relocated computers*

Specifically, moved a computer from the newborn room to a more comfortable environment so everybody could work in better conditions. It seemed illogical that many doctors were coming and leaving the room in order to send some files via that computer. That action included routing the LAN wire through the ceiling along 30 meters.

- *Merged two computers into one*

Humidity, high temperatures or saltpetre (among other environmental elements) are common problems for the equipments in that specific Caribbean area, so they easily get damaged. Administration department's computer powered down due to a failure in the circuit board, so we merged some components from another computer in disrepair of the Library.

- *Struggled with the Windows/Linux issue*

Any time possible, we installed the last version of Ubuntu (11.10) in the computers spread all over the hospital in order to avoid the never-ending virus problems. Mostly, the computers are only used for office automation tasks, so we added Microsoft Office for those doctors reluctant to the Operating System's change. In the cases a printer was connected to the computer, we checked out its divers and the compatibility with Ubuntu. When possible, not always, we switched OS.

- *USB virus problem*

Cleaned a very spread virus which affected and hide all the folders in the memory sticks of the employees. Apparently, it seemed that all the files were removed from the pen drive, but actually just hidden. The commands used were:

```
cmd infected unit:
ATTRIB /D /S -R -H -S *.*
```

- *Continued the use of network management tools*

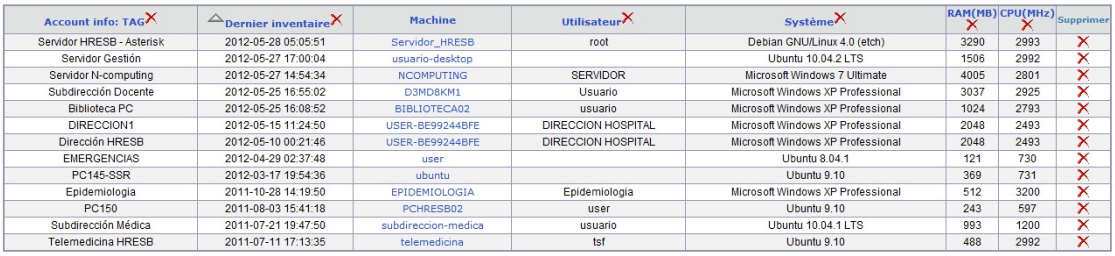
It seemed very important to us to keep using the tools installed and given by past members of TSF mainly in the phase VI (OCSInventory, Mantis and Zabbix) [3]. For this reason, we created new users in each tool in order to keep the track of all the action we had taken. The tool most important is the Mantis tool because it explains the different incidents resolved in our stay in Nicaragua. That might help the next volunteers when solving some problems which have already occurred, such as the installation of VoIP phones, etc.

Incidències (1 - 22 / 22) [Imprimeix Incidències] [Exporta a CSV] [Exporta a Excel]

P	ID	#	Categoria	Gravetat	Estat	Actualitzat	Resum
^	0000064	1	Incidencias de red	**major**	resolt (albaboj)	2012-05-14	Interconexión VoIP - Teléfonos convencionales
_	0000063	1	Incidencias de red	menor	resolt (albaboj)	2012-05-11	Nutrició - Accés a Internet
_	0000062	1	[Mantenimiento equipos] Mantenimiento equipos	menor	resolt (albaboj)	2012-02-17	Fisioterapia - Problema con el monitor
_	0000061	1	[Mantenimiento equipos] Incidencias de red	menor	resolt (albaboj)	2012-02-10	Problema connectivitat telèfon VoIP - Cirurgia
_	0000060	1	[Mantenimiento equipos] Mantenimiento equipos	**major**	resolt (albaboj)	2012-02-09	Virus PenDrive - Ocultació carpetes
_	0000057		[Incidencias de Red] General	menor	resolt (genismauri)	2012-02-09	Bloquear páginas web en hospital
_	0000059	2	[Mantenimiento equipos] Mantenimiento equipos	menor	resolt (albaboj)	2012-02-09	Ordinador Optiplex GX110 - Biblioteca no s'engega

Figure 5. Mantis tool

On the other hand, we installed in the new computers or the computers formatted the OCSInventory agent in order to monitor the characteristics of the equipment.



Account info: TAG	Dernier inventaire	Machine	Utilisateur	Système	RAM(MB)	CPU(MHz)	Supprimer
Servidor HRESB - Asterisk	2012-05-28 05:05:51	Servidor_HRESB	root	Debian GNU/Linux 4.0 (etch)	3290	2993	
Servidor Gestión	2012-05-27 17:00:04	usuario-desktop		Ubuntu 10.04.2 LTS	1506	2992	
Servidor N-computing	2012-05-27 14:54:34	NCOMPUTING	SERVIDOR	Microsoft Windows 7 Ultimate	4005	2801	
Subdirección Docente	2012-05-25 16:55:02	D3MD8KM1	Usuario	Microsoft Windows XP Professional	3037	2925	
Biblioteca PC	2012-05-25 16:08:52	BIBLIOTECA02	usuario	Microsoft Windows XP Professional	1024	2793	
DIRECCION1	2012-05-15 11:24:50	USER-BE99244BFE	DIRECCION HOSPITAL	Microsoft Windows XP Professional	2048	2493	
Dirección HRESB	2012-05-10 00:21:46	USER-BE99244BFE	DIRECCION HOSPITAL	Microsoft Windows XP Professional	2048	2493	
EMERGENCIAS	2012-04-29 02:37:48	user		Ubuntu 8.04.1	121	730	
PC145-SSR	2012-03-17 19:54:36	ubuntu		Ubuntu 9.10	369	731	
Epidemiologia	2011-10-28 14:19:50	EPIDEMIOLOGIA	Epidemiologia	Microsoft Windows XP Professional	512	3200	
PC150	2011-08-03 15:41:18	PCHRESB02	user	Ubuntu 9.10	243	597	
Subdirección Médica	2011-07-21 19:47:50	subdireccion-medica	usuario	Ubuntu 10.04.1 LTS	993	1200	
Telemedicina HRESB	2011-07-11 17:13:35	telemedicina	tsf	Ubuntu 9.10	488	2992	

Figure 6. OCSinventory tool

CHAPTER 3. Virtual Private Network

This fourth chapter defines a problem of lack of communication among several health centres in Bluefields and how was dealt by implementing a VPN. There are detailed some possible configurations and tests which were carried out in advanced with OpenVPN and Samba software, and the final implementation of the VPN consisting of PPTP protocol, as well as the results obtained.

3.1. Current situation and problem definition

Nowadays, the municipality of Bluefields embraces many health centres. Starting by the Hospital Regional Ernesto Sequeira (HRESB, where TSF is placed), there is a range of other health institutions spread all over the city which are also involved in the care of its inhabitants. Although they should be strongly coordinated, the reality shows a situation in which each institution is working by its own.

The scenario is composed of several health institutions, all of them connected to the public Internet, so it seemed vital to implement a private and secure connection to share information. The solution taken for the problem involved a Virtual Private Network (VPN).

The first step was to identify the centres which could be part of the network. The SILAIS, organization related to MINSA (Nicaraguan Ministry of Health) and responsible for managing all the institutions of the area, accorded to include in the ring those ones with reliable computers as well as Internet connection.

At first sight, it seemed that 5 of them had the reasonable features, but after visiting each centre in order to know in detail its location and equipments, we had to rule out Centro Oftalmológico since it did not fulfil the minimum requirements and, in addiction, it is expected to be closed down in a near future. Afterwards, the 4 centres considered were:

- Hospital Regional Ernesto Sequeiro Bluefields (HRESB)
- Centro de Atención Psico-Social (CAPS)
- Centro de Salud Juan Manuel Morales (JMM)
- Sistema Local de Atención Integral en Salud (SILAIS)

The following map gives in detail the location of all these centres over Bluefields. As it might be observed, all of them are relatively close, so apparently there is no

shortcoming in terms of distance.

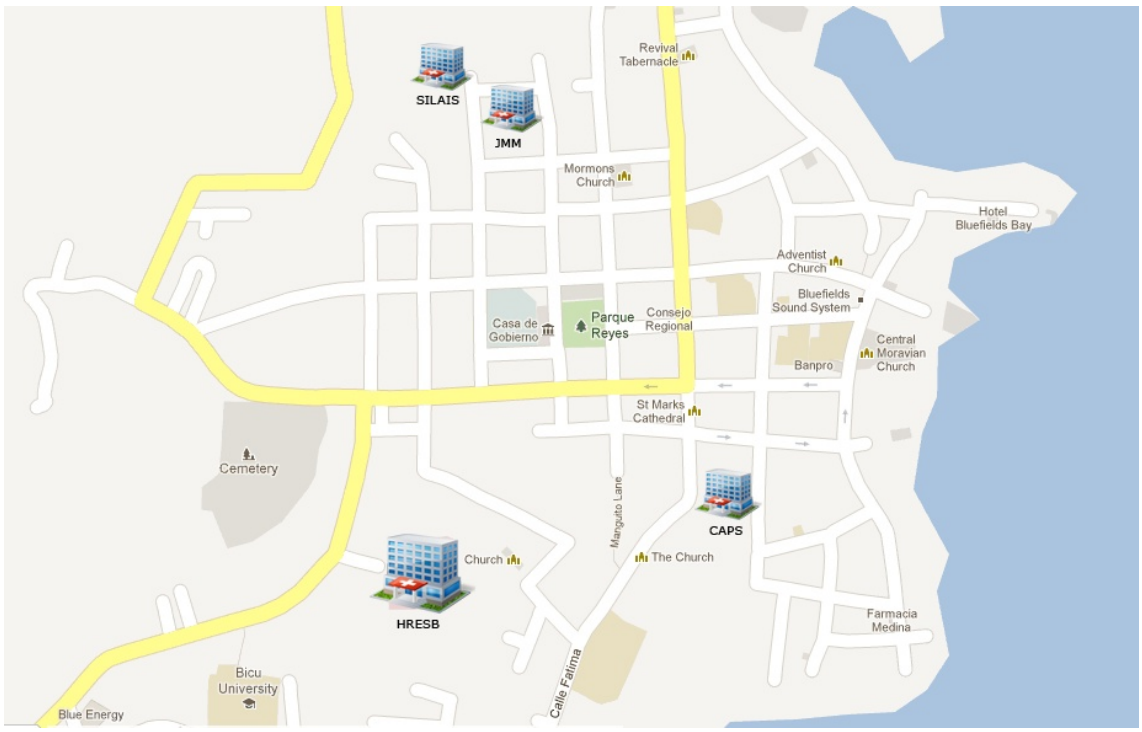


Figure 7. Location of health centres over Bluefields

Currently, TSF had created a VPN to remotely connect from Barcelona to HRESB network in order to make the network maintenance and resolve troubleshooting. This VPN was created in Phase VI of the project [3], implemented with the PPTP protocol and installed in the management server (Ubuntu).

For different reasons mentioned in the chapter 3.3, it was decided to implement a more robust VPN to make the connection between health centres more secure. Hence, it was considered the possibility of changing the PPTP VPN to the OpenVPN software, since we could adapt better to the needs of the VPN network. A first approach from a laboratory in Castelldefels was carried out during the previous months of the departure in order to test the software OpenVPN and its features, and the application Samba which will use to share files between different SO inside the VPN.

3.2. Description of a VPN

A VPN is a network that enables communication between remote users or the communication between different networks far between. This method can link two or more networks simulating a single private network, allowing communication between computers like a connexion point to point. This communication is established safely between the two extremes and is completely transparent to all users, networks, etc. that exist between the two ends of the VPN. For this purpose, the technique is called

tunnelling, data packets which are routed via the public network, such as the Internet or any other commercial network, a private tunnel that simulates a point-to point.

The tunnelling technique involves encapsulating a network protocol over another protocol, creating a tunnel in a computer network. That is to say, it opens a connection between two points (transmitter-receiver) by using a secure protocol such as might be SSL (Secure Socket Layer) or SSH (Secure Shell). This will route the data packets on intermediate nodes that are unable to see it clear the contents of those packages. To do this, the data is encrypted, then encapsulated, and finally it changes the header with information about the sender and receiver, creating a logical tunnel between the two ends of the communication.

This technology is very useful in order to establish networks which have to cover large geographic areas, such as Bluefields and its various health centres.

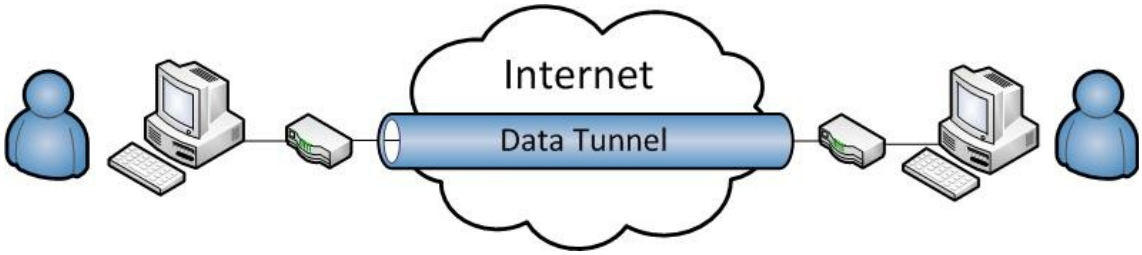


Figure 8. Tunnelling architecture

3.2.1 Advantages

Implementing a VPN has a set of advantages very beneficial to the new system:

- Data integrity, the messages sent can not be altered.
- Confidentiality, only allowed users may access to the information from the VPN.
- Encryption, encoders are implemented so that packets can not be read by outsiders.
- Easy to use for inexperienced users, transparent system to them.
- Facilitates communication between two users/sites located in distant places.

3.2.2 Architecture

There are three types of architectures to create a VPN:

- **VPN end to end.** In this model of VPN, a corporate office or headquarters is connected to the central office, where the VPN server is located, which is responsible for creating tunnels for connections and manage all traffic.

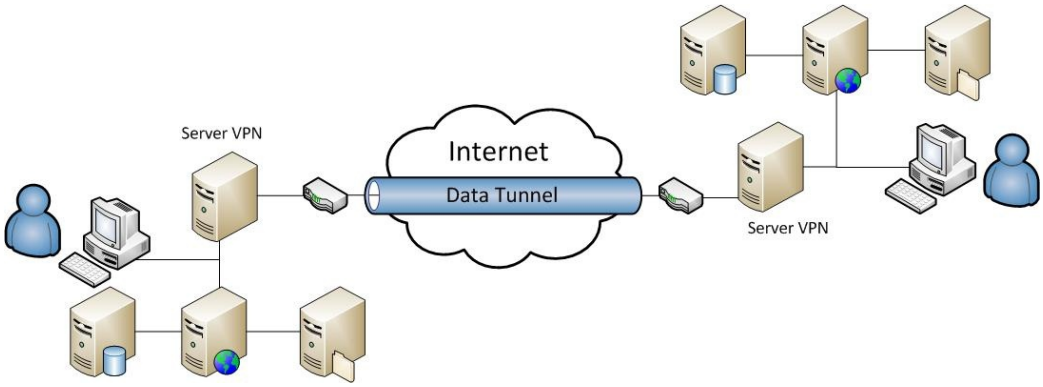


Figure 9. VPN end to end architecture

- **VPN remote access.** A user connects to a company from a remote location, such as home, airport, hotel, etc. The connection is made via the Internet with authentication between client and server.

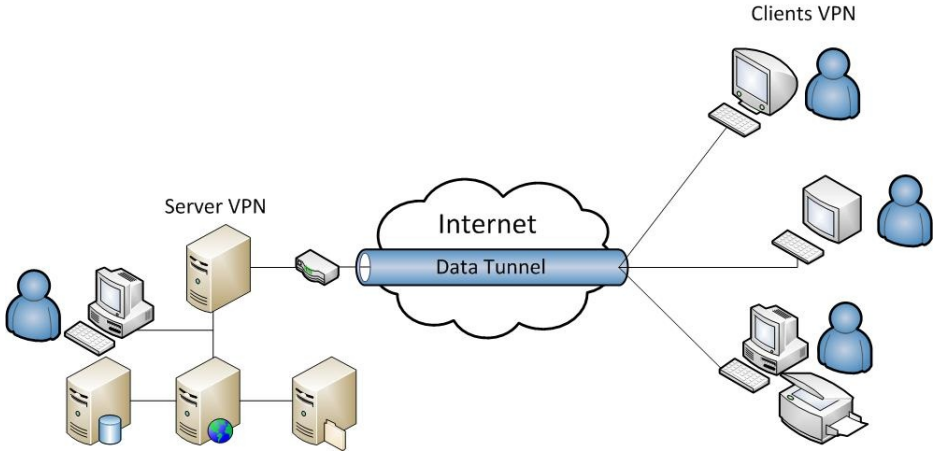


Figure 10. VPN remote access architecture

- **VPN internal VLAN.** To make connections by using the LAN in spite of Internet as in the two previous systems. Though not very spread, it is very useful to isolate areas or network resources.

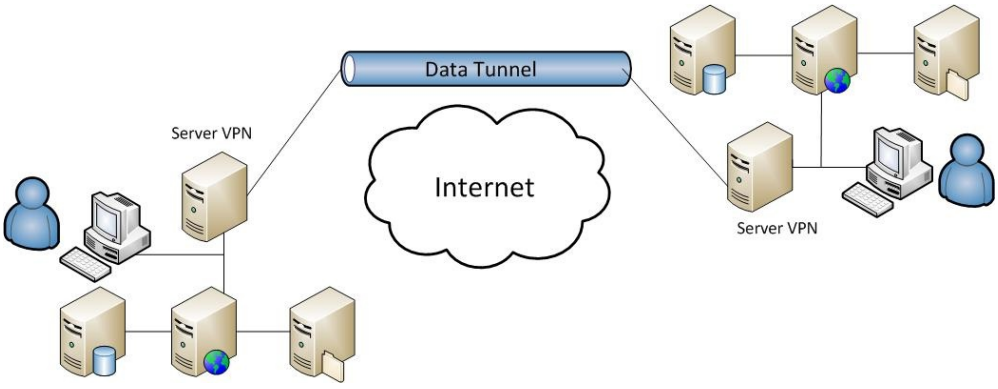


Figure 11. VPN intern VLAN architecture

3.2.3 Server VPN

There exist 2 possible configurations for installing the VPN server, which will be responsible for managing client connections:

- **Internal Server.** In this configuration, the server is physically accessible by maintenance personnel of the company itself. Thanks to this closer location, a cost savings are achieved because it is avoided to pay an outside company to administer the server, since there will be a more immediate access to set-up, or any other kind of modification.
- **External Server.** In this case, the server is outsourced to a company dedicated to host and manage servers.

3.2.4 Types of VPN

A VPN can be created by hardware or software.

Those created by *hardware* can achieve higher performance and, at the same time, are easy to configure, yet more limited than those created by software, since they have fewer configurable parameters. There exist a variety of products that enable the creation of VPN hardware, such as products from Cisco, Linksys, Symantec, Nokia, etc.

Software VPNs have a lower performance but allow more flexibility to configure them. One drawback is that they are more complex than hardware because they allow more configuration options, but this can become a plus, since it can create a VPN that best suits the needs of project. There are two ways to create a VPN software. The first is through programs that come with their own OS such as Windows XP, Windows 2003 Server, Windows Vista and GNU/Linux, but these networks tend to be somewhat limited. The other option, and recommended, are the specific applications to create open source VPNs such as OpenVPN, OpenSSH, VTun, Hamachi, FreeS/Wan, etc.

3.3. Solution adopted: OpenVPN and Samba

Considering all the architectures studied, the solution consists of a remot access VPN, that is to say, a VPN server installed that connects all the users and validates their authentication, by checking out the privacy settings of the connection.

The server will be internal and located in the HRESB (*Servidor de Gestión*), where TSF has the rest of the servers and devices. Different users will connect to the server through the VPN tunnelling. This type of architecture was chosen as discussed above due to the easy management of the server: immediate access to it and also cost savings because there is no companies involved.

Referring to the different types of VPN that can be implemented, it was decided to set up a VPN using software. This system seemed to be more appropriate to our needs, since it allows greater configuration flexibility.

For the selection of protocol, it was consulted the performance and characteristics of PPTP, L2TP/IPsec and OpenVPN. It was also taken into account the experience of professors from EETAC who had already worked and tested them. The following table shows a comparison with the features of each protocol studied.

	PPTP	L2TP/IPsec	OpenPVN
Encryption	128 bits	256 bits	160/256 bits
OS supported	Windows, Mac OS X, Linux, iOS, Android, DD-WRT	Windows, Mac OS X, Linux, iOS, Android	Windows, Mac OS X, Linux
Security	Basic encryption	Maximum encryption. Encapsulates the data twice	Maximum encryption. Authenticates data with digital certificates
Speed	Fast due to lower encryption	Encapsulates data twice making it less efficient and slightly slower than its rivals	Best performance. High speeds, even in high latency connections and long distances
Ports used	TCP port 1723 and GRE (Protocol 47). PPTP can be easily blocked by restricting the GRE protocol	UDP 500 for the initial key exchange, 50 for the IPSEC encrypted data, UDP 1701 for the configuration, UDP 4500 for NAT	Run on any port using either UDP or TCP
Configuration	Very easy to configure	Custom configuration	Requires the installation of client software
Stability / Compatibility	Not as reliable, nor does it recover as quickly as OpenVPN over unstable network connections. Minor compatibility issues with the GRE protocol and some routers	More complex than OpenVPN and can be more difficult to configure to work reliably between devices behind NAT routers	Very stable and fast over wireless, cellular and other non reliable networks where packet loss and congestion is common
Conclusion	Due to the major security flaws, there is no good reason to choose PPTP other than device compatibility	Excellent choice but falls slightly short of OpenVPN's high performance and excellent stability. Easier to block than OpenVPN due to its reliance on fixed protocols and ports	OpenVPN is the best choice for all users of Windows, Mac OSX and Linux desktops. It is extremely fast, secure and reliable

Table 2. Comparison of VPN software

Afterwards, for all the features and performance described, **OpenVPN** has been chosen as a free open source software based on SSL/TLS. The following sections details its specific characteristics.

3.3.1. OpenVPN software features

OpenVPN is a free software created in 2001. It is based on SSL VPN connexion. It is a solution which can accommodate a wide range of configurations, Including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, fail-over, and fine-grained access-controls.

It is designed to create secure networks at layer 2 or 3 of the OSI model (Tunnel or Bridge). So a customer can not make a connection to the VPN server through a Web browser, since OpenVPN does not operate at Layer 7 (Application) of the OSI stack. Some of the features and advantages about OpenVPN are:

- Support for multiple operating systems.
- Supports dynamic IP addresses and Network Address Translation (NAT).
- Scalable to the number of users.
- Configuration flexibility.
- Using certificates for authentication.
- Based security using SSL / TLS for authentication.

As mentioned above, OpenVPN is a software developed since 2001, so by not bringing many years of development it has some drawbacks:

- No support for IPSEC (Internet Protocol Security), which is the most commonly used standard for VPN solutions, though It offers support for standards like PPTP or L2TP

Although the disadvantage is significant, with time being an open source software it is expected some of them to be resolved in future releases.

3.3.2. Security in OpenVPN

OpenVPN has two methods to encrypt data. The first method is to use *pre-shared static keys*, that is to say, all users use the same key to encrypt and decrypt. The second method is to use *certificates with SSL/TLS and RSA keys*. This second method, though more complex, it is the one chosen for the implementation of our VPN due to security reasons. In the method of shared keys, if someone gets the key, could simply capture the data and install the key to its PC. From that moment, it might behave as a user over the network, and thus decrypt any information.

The security SSL/TLS mode in OpenVPN is aimed at users who will generate their own certificates and, therefore, its own Certificate Authority (CA), that is, create a trusted entity that is responsible for issuing and revoke certificates.

In our case, client and server negotiate a secret key (symmetric), commonly known as *master secret* which uses the Diffie-Hellman cryptographic protocol. This is a key establishment protocol between parties who have not had previous contact. This way each client has a private key and user-name to enable the authentication (*.key*). At this time, the OpenVPN authenticates *.key* file by checking that it is signed by the CA.

3.3.3. Encapsulation in OpenVPN

OpenVPN can be used as transport protocol both UDP and TCP for point to point connections. When using *UDP*, the client to make the connection request will wait for response from the server about 5 seconds (by default) before making another attempt to connect.

TCP also uses timers that can vary, increasing in case of expiry of the time, to avoid network congestion. This can cause problems when two layers are using this method, that is to say, it is likely that in a VPN, a TCP packet is encapsulated by another TCP so that it can send. In this case, the problem is that if the TCP of the lower layer does not receive packets that are waiting, its timer will increase as increasing its retransmission queue. On the other side, the TCP of the top layer would wait for an ACK, and with no reception, it will also increase its timer and retransmission queue. This could eventually lead to network congestion.

But the main shortcoming of using TCP is that the protocol works with the maximum packet size. Therefore, when encapsulated again by the upper layers, the packet size might exceed the dimensions and has to be fragmented. This fragmentation can cause that the router is unable to route so big packets, and that the receiver can not reassemble all the information together, as there may be packet loss or some repeated information.

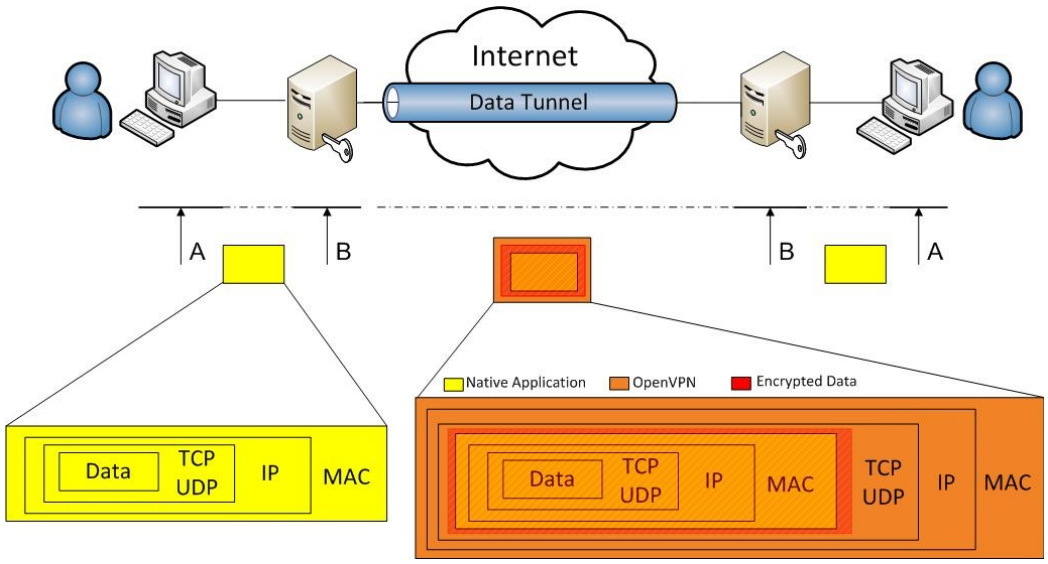


Figure 12. Data encapsulation in OpenVPN

For all these reasons explained above, OpenVPN (by default) uses UDP since it offers greater security against possible attacks, and allows OpenVPN to work more efficiently.

3.3.4. Samba

Once installed the VPN solution, and taking into account that the stage of the project involves multiple computers with different OS, it is necessary to implement a multi-platform software for sharing network resources, these being visible only to the computers connected to the VPN. The chosen solution is Samba.

Samba is a free implementation of file-sharing protocol for Microsoft Windows, called SMB (Server Message Block). This allows Linux or Mac computers act as data clients in Windows networks. It is essential that all these computers are in the same workgroup, that is to say, there is simply a group name-tag that identifies a specific collection of computers.

Once Samba is installed and running multiple shared resources for Microsoft Windows users, these will appear as normal folders within the network. Linux users can mount, in their file systems, these network drives as if they were local devices, or use the *smbclient* command to connect to them. Each directory can have different access permissions according to our interest.

3.4. Previous work – Lab

During the previous weeks before the departure, in a laboratory placed in ETAAC we set up a scenario likely to be the one found in Bluefields. So, we considered a server (HRESB) and a couple of terminals forming the network (other health centres). Each of it had different OS and features in order to estimate all the possibilities, unknown in advance. Moreover, we considered the easy escalation of the system in case it had to be larger in the future.

Although the tests were conducted in the laboratory of ETAAC, it was repeated in Nicaragua in order to see that any problem was happened with the network. The following explanations refers to the tests which were done in the HRESB.

3.4.1. VPN Scenario description

The scenario was based on two computers connected via the internal network of HRESB. One of them worked as a server and the other as a user. The technical characteristics of each computer are detailed in the table below.

	Server	Client
Model	DELL Studio	Toshiba Satellite R630
Processor	Intel Core i2 DUO CPU P8600 – 2.40GHz	Intel Core i5 CPU M450 – 2.40GHz
Memory RAM	4GB	4GB
Ethernet Card	Realtek 8192 GBE Family	Realtek PCIe GBE Family
Operating System	Linux Ubuntu 9.10	Windows 7 Home Premium (64 bits) - Linux Ubuntu 11.10

Table 3. Computer technical features

The IP configuration are detailed in the following figure. To avoid problems of routing, static IP were configured within the HRESB range.

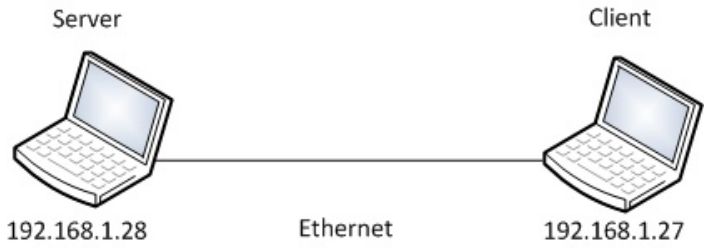


Figure 13. IP configuration

Keep in mind that the client was tested with the Windows and Linux operating system, separately. The following sections detail the steps for the installation and the configuration of both SO for the clients and for the server.

3.4.2. VPN Server. Installation and configuration (Ubuntu 9.10)

First of all, both OpenVPN and security OpenSSL packages were installed, since it was decided to use security based on SSL. To do that, opened a terminal server and type:

```
sudo apt-get -y install openvpn
sudo apt-get -y install openssl
```

Once the installation was done, it was the time for OpenVPN configuration in the server. The first step was to create *openvpn.conf* in the appropriate folder, /etc/openvpn/. In this file, all parameters for the VPN server were configured.

Parameter	Function
port 1194	Port used for connecting OpenVPN
dev tun0	To use a tunnel through a virtual interface "tun" of drivers TUN / TAP
proto UDP	UDP or TCP protocols can be implemented
tls-server	The server will establish the TLS protocol
persist-key	If OpenVPN server is restarted, it does not have to re-read keys
persist-tun	If the server is reboot, the tunnel does not have to be closed and reopened
ca ca.crt	Loads the Entity
cert server.crt	Loads the server's certificate
key server.key	Loads the server's private key
ifconfig-pool-persist ipp.txt 60	Always keeps the same IP for a client
client-to-client	Allows customers to see each other
mode server	Works in server mode to accept multiple clients
ifconfig-pool x.x.x.x x.x.x.x	Limits the IP range for clients from XXXX to XXXX
route x.x.x.x 255.255.255.0	Adds the network path to the virtual interface XXXX TUN/TAP
push "route x.x.x.x 255.255.255.0"	Related to client-to-client command of client.conf. Allows the customer to add the network path to the interface specified virtual TUN/TAP
comp-lzo	Uses the LZO compression library
keepalive 10 120	The server will send a ping every 10 seconds, and if there's no response in 120 seconds, will understand deduce the customer is dropped

Table 4. Parameters to configure in server file

After configuring the server script, another script to configure and start the VPN server was created. The following step consisted of generating:

- Diffie Hellman of 2048 bit.
- Certificates CA.
- Server certificates and keys.
- Clients certificates and keys.

After creating the certificates and keys for each VPN client, it was the right time to start configuring OpenVPN. All the scripts and commands implemented are detailed along Appendix III.

To start the server, the following command was used:

```
sudo /etc/init.d/vpnserver start
```

On the console one can see that the tunnel was succesfully created.

```
ifconfig
```

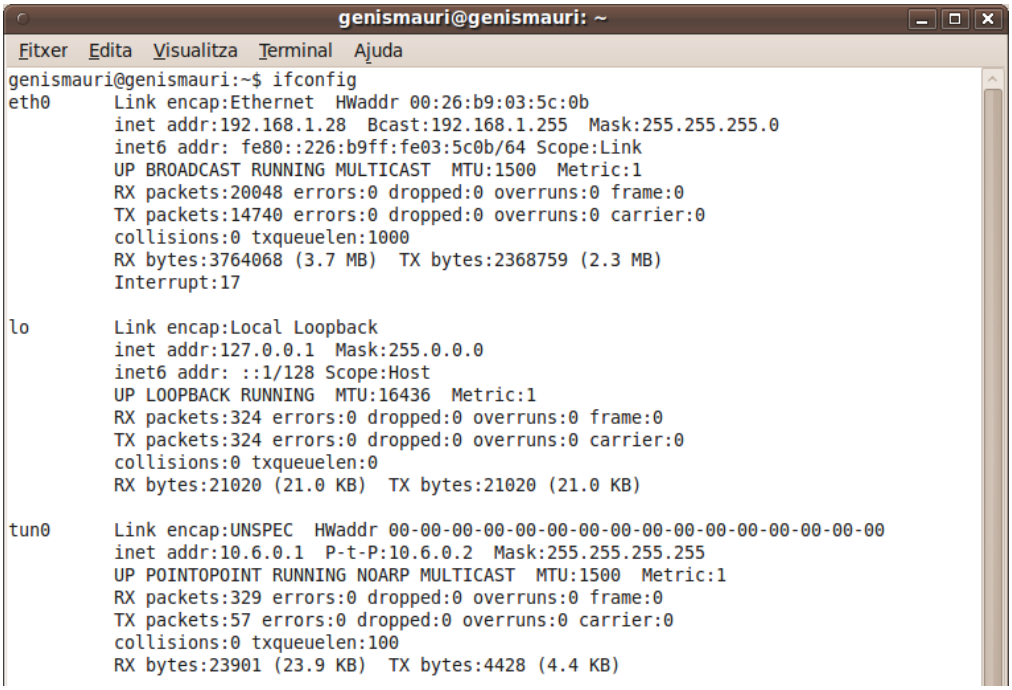


Figure 14. Listing interfaces on server

For the VPN to run automatically at start-up, there must first be installed the "chkconfig" package, then start OpenVPN and enable chkconfig on the program:

```
sudo apt-get install chkconfig
sudo service openvpn start
chkconfig openvpn on
```

If everything is correctly done, the IP routing table on server should look alike to the following figure, showing both Tunnel (tun0) and Ethernet (eth0) interfaces with their respective IP's and gateways.

```
netstat -nr
```

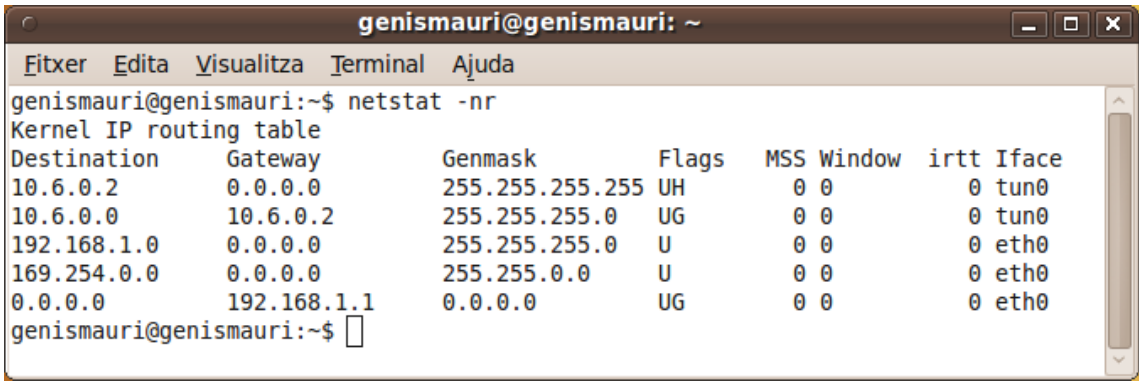


Figure 15. IP routing table

It is also interesting to check out if all the ports are enabled so the communication can smoothly flow. Otherwise, some applications such as Internet could be blocked by the server. *microsoft-ds* and *netbios-ssn* are the ones to take notice.

```
netstat -at
```

```
genismauri@genismauri:/etc$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.6.0.1:microsoft-ds   *:*                     LISTEN
tcp        0      0 10.6.0.1:1024           *:*                     LISTEN
tcp        0      0 10.6.0.1:loc-srv        *:*                     LISTEN
tcp        0      0 *:openvpn               *:*                     LISTEN
tcp        0      0 10.6.0.1:nameserver     *:*                     LISTEN
tcp        0      0 10.6.0.1:netbios-ssn    *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
genismauri@genismauri:/etc$
```

Figure 16. All ports enabled and listening

3.4.3. VPN Windows client. Installation and configuration

OpenVPN is an application that has a version for Windows, so the first thing to do is download it. In the following link can be downloaded all the versions and applications of the software.

http://openvpn.se/download.html

After the installation, the client has to be configured so it can connect to the server. All details for the configuration are set in the script *client.ovpn* which is located in the folder *C:\ProgramFiles\OpenVPN\config.* The details of the script are described along the Appendix III.

Also, as it has been described in the previous section all the certificates, keys and signatures generated by the server to identify the client should be copied to the same folder where is located the *client.ovpn.* The files to copy are:

ca.crt: certification unit
clientehresb.crt: client certificate
clientehresb.key: client key

To connect with the server it has to be run the OpenVPN GUI as administrator.

Figure 17. OpenVPN connection

Once the connection is made from the client, a new network interface for the TUN/TAP.

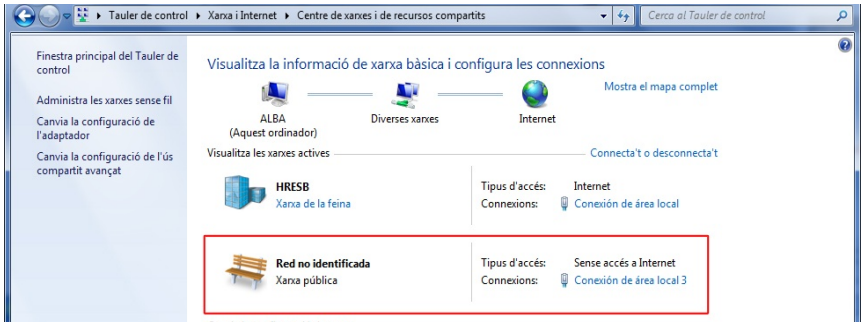


Figure 18. Enabled tunnel network

The network features with the new IP are shown in the left figure below.

It is important to take into account that the VPN connection runs when starting up the computer. To automate the process, the OpenVPN properties might be changed in: *Tauler de Control>Sistema I seguretat> Eines d'administració> Servicios*. There one have to select the software OpenVPN Service and modify the properties (right figure).

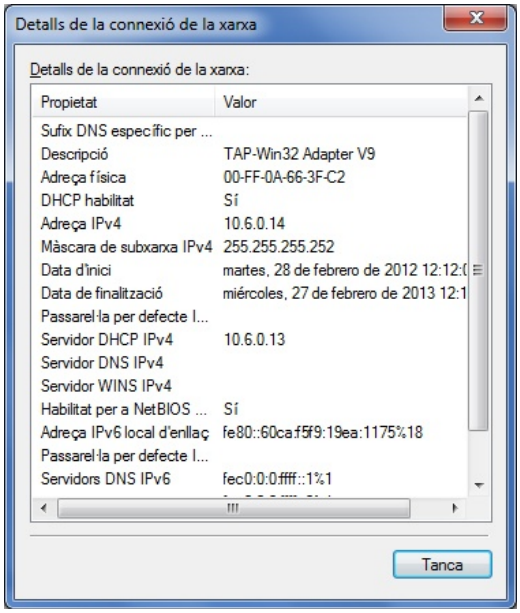


Figure 19. VPN network features

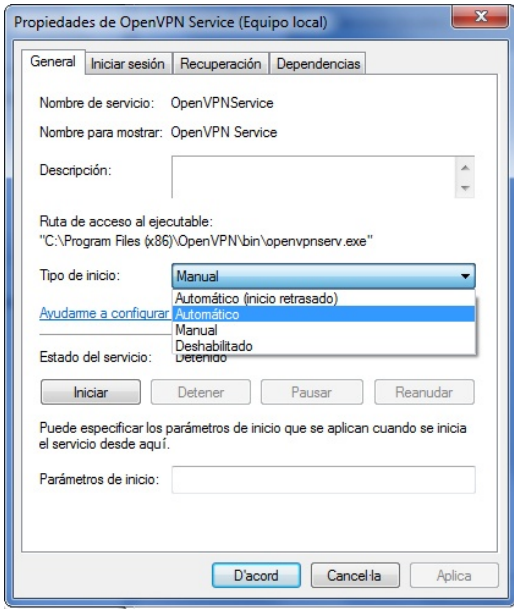


Figure 20. Automatically start of OpenVPN

3.4.4. VPN Linux client. Installation and configuration

Similarly to the server installation, OpenVPN application and the OpenSSL segurity have to first be installed.

```
sudo apt-get -y install openvpn
sudo apt-get -y install openssl
```

The next step is to configure the script *cliente_hresb.conf* which is located in the folder */etc/openvpn* and copy in the same folder the following files created by the server.

ca.crt: certification unit

clientehresb.crt: client certificate

clientehresb.key: client key

The installation is finished by running the application OpenVPN:

```
sudo service openvpn start
```

The tunnel creation can be checked out by using the ifconfig command:

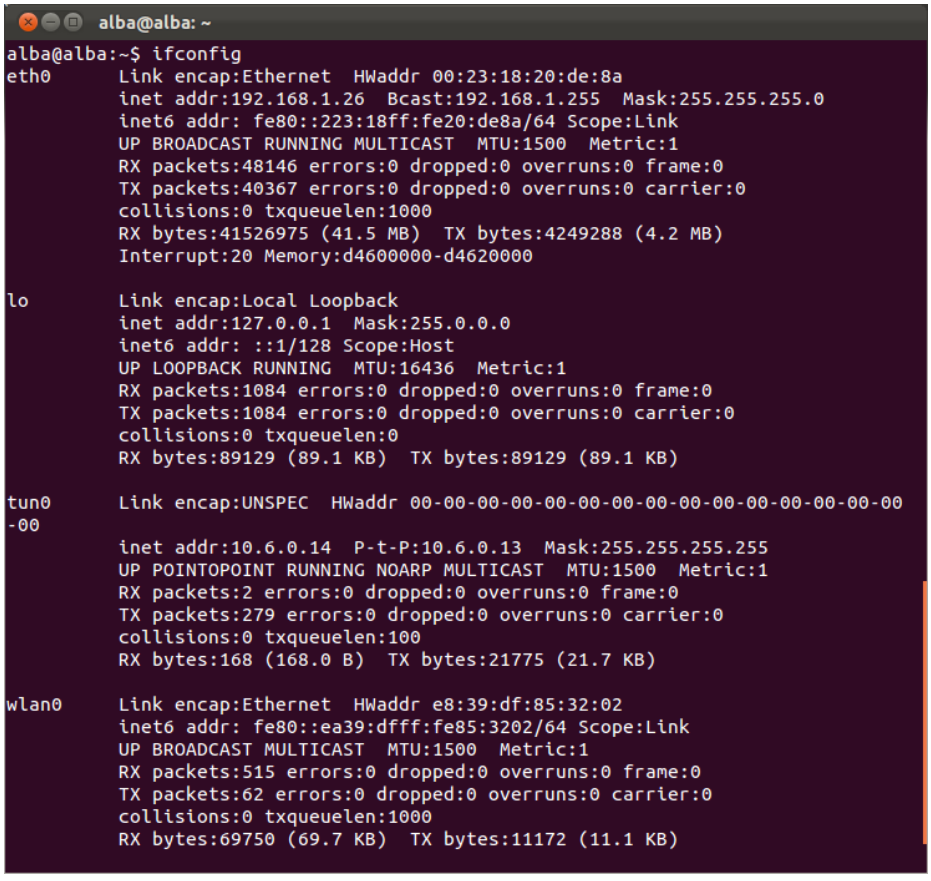


Figure 21. Listing interfaces on Linux client

All the scripts configuration implemented in the installation of the Linux client are detailed along Appendix III.

3.4.5. Samba server installation

Before doing the final implementation in the hospital and in the health posts spread over Bluefields, some tests were run in the laboratory in order to check the whole configuration and installation. Below, there are detailed all the steps followed to install Samba on the different OS. The scenario used for testing was the same to create the VPN. Thus, the VPN server will also work as a Samba server.

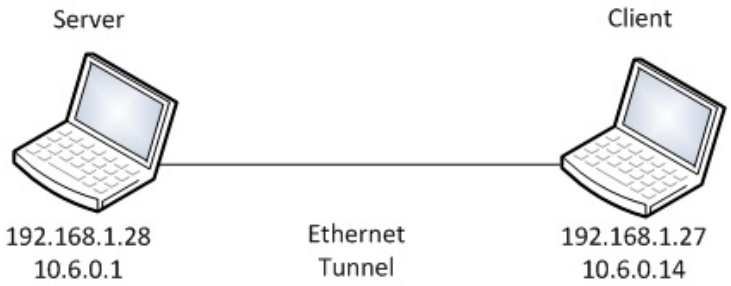


Figure 22. Scenario configured

Once installed, **Samba can be configured by editing the file *smb.conf*.** This file can be very simple or extremely complex because of the many options presented. Along Appendix V there are briefly detailed the main configuration options as well as the whole configuration used for testing it. Samba is configured to connect only to computers that are within a certain range of IP addresses (those assigned to the network OpenVPN), thereby increasing safety.

Once *smb.conf* was configured, **we set up user accounts** for each of the users involved within the VPN. That is to say, we created different profiles with user-names and passwords in order to assign them to the folders they could consult. It is possible to create as many accounts as necessary.

The last issue to take into account was related to the **security of files and folders** among users. On the one side, we gave permission to each of the folders in terms of writing or reading, so the users could only edit the content depending on the usage we were interested in. On the other side, we had to enable the firewall (Firestarter) for our VPN IP range. Otherwise, all the directions were blocked and did not have access to the shared documents. The specific setting can be read along Appendix V.

3.4.6. Samba Windows and Linux clients installation

Some of the computers within the Health Posts, due to compatibility problems with printers or specific medicine software, are running under Windows Operating System. In this OS, sharing folders is an automatic manual usage because there is no configuration file. In Appendix V it is detailed how to share a folder. Similarly, there are

the steps to follow in order to access to the shared folders in Linux.

3.5. Implemented solution

After checking out the feasibility of implementing the VPN on the different health centres involved and meeting their representative, this section details the process and the results obtained.

Centro de Atención Psico-Social (CAPS) and Juan Manuel Morales (JMM) seemed not to have Internet connection by that time, having cut their expenses during 2011, so unfortunately, the initial purpose was that neither of them could be part of the VPN. The network would be reduced to just two centres. But, since JMM is placed so close to SILAIS, it was accorded that an Ethernet wire would be crossed along the street in order to link both institutions. Afterwards, through a switch, Internet would be provided to a department of JMM. Although we consider that it would be a great idea to fix the Internet connection problem, it is not yet implemented.

Unfortunately, in the framework of this project, it was not reached to deploy the VPN. Because of these drawbacks, being the situation so unstable, it was eventually considered the creation of VPN in future phases of the project when all the centres have Internet access. However the PPTP VPN which was already configured has been maintained but with some changes, described in the following section.

3.5.1. Remote access

Fundamental to the management of the network was able to have remote access to the tools and equipment of the HRESB and radio-links to make maintenance and control from Barcelona, by the technical team of TSF.

As discussed above, in phase VI of the project [3], PPTP protocol was implemented in the management server to make a VPN. In addition, they reached to connect the hospital with ADSL in order to get a public IP.

The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks which uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. These frames are, at the same time, encapsulated into an IP packet so they might be sent over networks based on IP (such as Internet is). Between the client and the server, acting as VPN tunnel endpoints, PPTP creates a TCP connection for tunnel maintenance.

As mentioned, the hospital currently has an ADSL connection with a public IP. In the phase VI of the project [3] was applied for a private IP to ENITEL, but to prevent any IP changes it was decided to implement the tool DynDNS. **DynDNS** is a free portal in

which, after registration, one can configure a host that is associated with a domain that points to a public IP from which the user is connected. After establishing this link, it has to be installed an update the client which renews the IP in the host. Thus, although the IP changes it can always access to the network.

The problem lies in that, after a month of inactivity on the DynDNS registration, the account expires and therefore it has to be re-registered. But the biggest drawback is that nowadays DynDNS only has a free trial of 14 days, so an alternative had to be found. The selected alternative was **No-IP**.

No-IP product is a dynamic DNS service. The basic dynamic DNS service provided is a domain owned by No-IP which is free to use as long as the account remains active. The operation is the same as explained above about DyDNS: first the registration in the No-IP website; second the creation of a new host in the account (*hresbaccesoremoto.no-ip.org*); and finally the installation of the No-IP client to the server.

On the other hand, No-IP also modified the home page created when accessing to the *hresbaccesoremoto.no-ip.org* with the new links to the different systems. Along the Appendix VI one can see the steps to register our account, create the host and install the client into the management server, as well as the script configured to run automatically every time the server is switched on.

In addiction to this, the traffic was configured to the router, creating some rules. First of all, redirecting the incoming traffic through port 80, so one can have remote access to any application; second of all, redirecting the traffic from port 22 (Secure Shell Server SSH) to the server, so one, out of the LAN, can have access to the server as well; the third rule included port 443 (Secure Web Server HTTPS) so one can have access to any system installed.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Secure Shell Server (SSH)	22	22	TCP	22	22	192.168.1.252	☐
Web Server (HTTP)	80	80	TCP	80	80	192.168.1.252	☐
Secure Web Server (HTTPS)	443	443	TCP	443	443	192.168.1.254	☐
PPTP	1723	1723	TCP	1723	1723	192.168.1.252	☐

Figure 23. Rerouted traffic based on ports

Eventually, in order to access the PPTP VPN, new users had to be created, and configure a VPN on the computer. In our case, we configured the VPN client in Windows 7 following the steps described along Appendix IV.

Once the VPN was correctly created, we detected that we only had access to the server where VPN was created, and we did not access to computers on the network. It was resolved by changing the value of *ip_forwarding* file (/proc/sys/net/ipv4/ip_forward) from 0 to 1 in the server where the VPN is generated.

CHAPTER 4. VoIP Telephony System

This chapter is intended for the expansion of the VoIP telephony network the hospital currently has, with the addiction of other health centres of Bluefields into the system. That would permit fast better communication among all health institutions.

4.1. Current situation and problem definition

HRESB currently has a VoIP telephony system based on Asterisk. The Asterisk PBX is a software implementation of a traditional PBX (Private Branch Exchange). Like any PBX, it allows calls between phones connected to it, IP and analogue, for instance, it can link the IP network to the PSTN one.

The HRESB system is based on a server where Asterisk is installed, plus 14 phones spread over the different departments of the hospital. In addiction, another phone is located in the community of La Aurora. But since the last phase of the project [3], it seemed necessary that other health centres in Bluefields had a VoIP phone connected to the network. Two centres were evaluated where to place the new VoIP phones:

- Centro de Salud Juan Manuel Morales (JMM, aka Municipio)
- Sistema Local de Atención Integral en Salud (SILAIS)

Both centres (related to MINSA) are responsible for the radio-link maintenance within the community. For this reason, it was deemed advisable to install a phone to each of them in order to have direct communication with La Aurora, the HRESB and, in the future, with Monkey Point's Health Post.

Therefore, the problem relied on how to include both phones into the hospital network since they were part of other networks, following the next scheme:

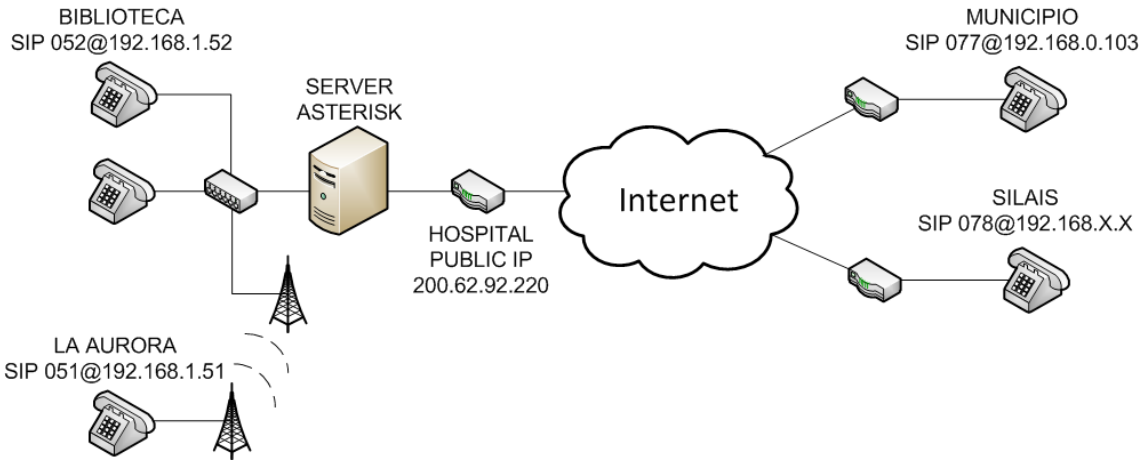


Figure 24. VoIP network

4.2. SIP Protocol

Asterisk supports various VoIP protocols: SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol) and H.323. However, this project is focused on the SIP protocol, being the most common used nowadays.

SIP is a protocol end-to-end of the application layer, used to establish, modify and close multimedia sessions, so very suitable for applications that use the concept of session, as VoIP telephones.

The architecture is based on HTTP and not associated with any protocol, so it allows any protocol in the lower layers (TCP, UDP, TLS, Ethernet, ATM, etc.). In addition, SIP re-uses the Internet addressing system based on URL and DNS; transports information of the session between the sender and the receiver, and it allows to build multiple services and sessions.

4.2.1 SIP architecture

SIP is based on a client-server architecture. The client is who generates the message and the server responds whom it transfers the message. Thus, the elements that it can be connected to the network are:

- **SIP User Agent (UA)**, are considered the terminals of VoIP telephones.

- **SIP Network Servers**, are used to find users or resend SIP forwarding messages (do not generate requests). In this case, the elements found within the network can be the Register, the Proxy and the Redirect.

- *The Register* accepts applications for client registration, therefore, it is who has a record of users which have the network.

- *The Proxy* decide the next step to make. For this reason, it acts as a client and server. Thus, it is the element that you have to connect if you want to know how to reach a destination. The Proxy can save or not the session state (Stateful or Stateless Proxy). In the first case, a request will be divided in several messages in order to detect the best path to sent the message to the client. In the second case, the proxy only send the message without checking the best path.

- **SIP Gateway (Redirect)**, knows the path to connect with a new client in other network.

From the point of view of SIP classification previously explained, the functionalities of Asterisk are several. First of all, acting as a Register and Location Server, because accepts registration requests from clients and provides a location service. On the other hand, it also acts as a Proxy Server with state (Stateful Proxy), because it knows at all times the status of the call. And even as a gateway between IP phones and the PSTN.

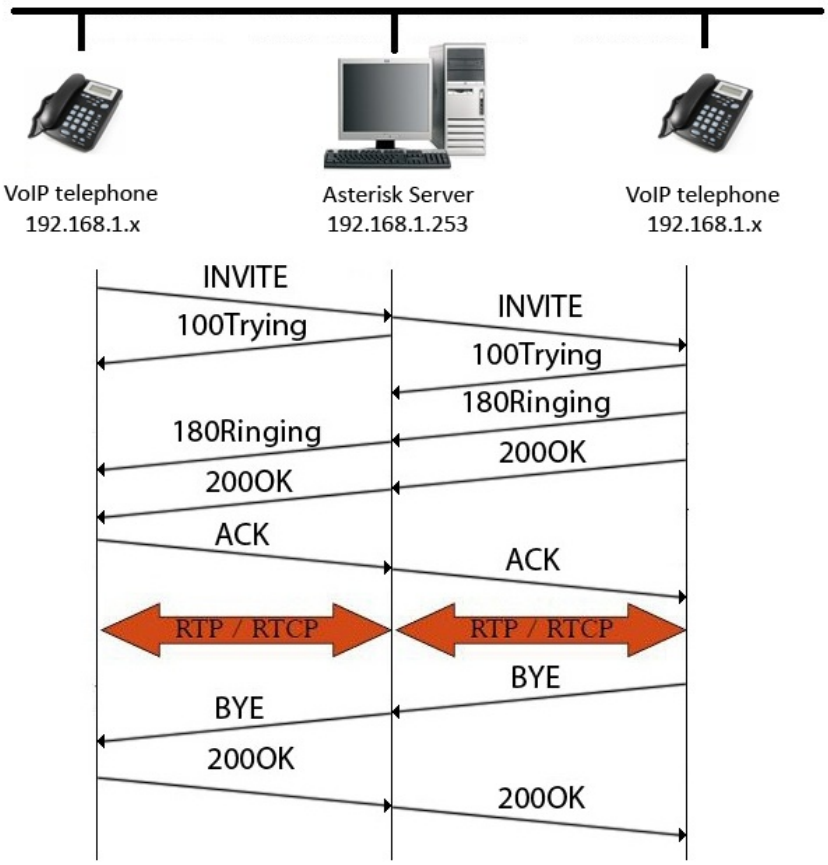


Figure 25. SIP architecture diagram

4.2.2 SIP addressing

SIP makes its routing on the Internet URLs (Universal Resource Indicators). The structure is equivalent to an address user mail represented as a URL, therefore, it uses IP addresses and E.164. In addition, other descriptive parameters can be added:

Structure without DNS: [UserIdentification] @ [Ipdirection]
Structure with DNS: [UserIdentification] @ [Domain]

4.2.3 SIP structure message

SIP messages sent from client to server have the same format and syntax of HTTP headers. These are formed, roughly, by a first line, a header and a message body which is optional.

- **First Line**
  The first line consists of an indication of the method type or request which is represented. Basically, 6 methods can be found: INVITE, BYE, ACK, CANCEL, OPTIONS and REGISTER, although others have been added such as INFO, SUBSCRIBE, UNSUBSCRIBE, NOTIFY and PRACK.

  The most common are:

Methods	Description
INVITE	Used to establish a multimedia session between two user agents
ACK	End users confirm the requests of the INVITE message with ACK. If they add a description of this session, this will be defined as default in the communication.
BYE	Used by the user agent to tell the server you want to cancel the session and release the call.
CANCEL	To cancel the requests made.
OPTIONS	Not used to establish sessions. Used to ask about the ability of the user you want to connect.
REGISTER	Allows a user to register his address in a SIP server. Customers can register from any location. This is only possible within the same administrative domain, so each network will have its users.

Table 5. SIP structure message (First line)

- **Header**

  After the first line there is the header. This describes the elements involved in the call and the path, and the message type.

  It is important to note that requests and responses are in text format, not binary, and based on HTTP/1.1. In addition, the text fields do not difference between capital letters or lower cases and, also, are ignored blank spaces. It has to be taken into account that in the first line all these exceptions are ignored.

  The most important messages in the header are:

Methods	Description
VIA	Indicates the path followed by the submission (sequence of nodes).
TO	Indicates the receiver's request.
FROM	Indicates who initiated the request.
Call ID	Unique identifier for each INVITE, and it will be contain all the log messages from a client.
CSeq	Contains the sequence number and the request message. It begins with a random number.
Contact	Contact URL for additional communications.
Expires	Time that the message could be around the network.

Table 6. SIP structure message (Header)

- **Body**

  The body message uses SDP to describe the session and make the negotiation parameters.

Methods	Description
version	Information about the message version
origin	Origin address
session names	Session name
times	Time when the message was created
connection data	Destination address
media	Data format
attributes	Encoder attributes

Table 7. SIP structure message (Body)

On the other hand, the responses to the SIP messages can also be classified into 6 types, each encoded with a number.

Structure: [SIP version] [code] [Information]

Code	Response
Informational	100-183
Success (OK)	200
Redirection	300-380
Request Failure	400-486
Server Error	500-505
Global Failure	600-606

Table 8. SIP structure message (Codes)

4.3. Speech coding

Speech coding is the application of data compression of digital audio signals containing speech. It uses speech-specific parameter estimation using audio signal processing techniques to model the speech signal, combined with generic data compression algorithms to represent the resulting modelled parameters in a compact bit stream.

Asterisk allows different speech coding in its communications: G.711 (PCMU and PCMA), G.723.1, G.726, G.729, GSM,etc. On the other hand, it is important to know that the VoIP phone used in the hospital accepts the following voice codecs: GSM, G.723.1, G.729, G.711 (PCMU and PCMA), G.726-32, G.722 and iLBC.

It is important to take into account that, according to the speech coding chosen, the conversation quality varies. The following tables compare general and technical features for the audio formats which are allowed for both systems, Asterisk and VoIP phones. In these tables, the bandwidth required to transmit over Ethernet is shown. This value is important to consider when choosing the codec for our VoIP service because of the limitation in bandwidth of the hospital.

Codec	Bit Rate (Kbps)	Sample Size (Bytes)	Sample Interval (ms)	Mean Opinion Score (MOS)
G.711	64	80	10	4.1
G.729	8	10	10	3.92
G.723.1	6.3	24	30	3.9
GSM	13	17	10	3.5

Table 9. Codec Information

Codec	Voice Payload Size (Bytes)	Voice Payload Sixe (ms)	Packets per Second (PPS)	Ethernet BW (Kbps)
G.711	160	20	50	87.2
G.729	20	20	50	31.2
G.723.1	24	30	33.3	21.9
GSM	33	20	50	36.2

Table 10. Bandwidth features

Where:

- **Codec Sample Size (Bytes).** Based on the codec, this is the number of bytes captured by the Digital Signal Processor (DSP) at each codec sample interval.

$$Bit\ Rate = \frac{SampleSize}{SampleInterval}$$

- **Codec Sample Interval (ms).** This is the sample interval at which the codec operates.

- **MOS.** MOS is a system of grading the voice quality of telephone connections. With MOS, a wide range of listeners judge the quality of a voice sample on a scale of one (bad) to five (excellent). The scores are averaged to provide the MOS for the codec.

- **Voice Payload Size (Bytes).** The voice payload size represents the number of bytes (or bits) that are filled into a packet. The voice payload size must be a multiple of the codec sample size.

- **Voice Payload Size (ms).** The voice payload size can also be represented in terms of the codec samples.

- **PPS.** PPS represents the number of packets that need to be transmitted every second in order to deliver the codec bit rate.

$$PPS = \frac{BitRate}{BitRate \cdot VoicePayloadSize(ms)}$$

- **Bandwidth Ethernet.**

$$BW = TotalPacketSize \cdot PPS$$

$$TotalPacketSize = VoicePayloadSize + 40\,bytes(Protocol\ payload) + 18\,bytes(Ethernet)$$

4.4. Previous work – Lab

Before installing VoIP phones in the new locations outside the hospital some parameters within the Asterisk PBX had to be edited, allowing SIP agents to call from external networks. Furthermore, it was considered to test connectivity by installing a VoIP phone outside the hospital network (our home) to check the proper functioning and detect possible errors.

Thus, mainly a couple of modifications were made in 'sips.conf' and 'extensions.conf' files, both configurations detailed in Appendix I.2. The 'sip.conf' file specifies the public IP available to the HRESB, although we have the public IP service provider we use DNS discussed above in section 3.5.1 Remote Access.

To create a highly secure password was made via http://www.clavesegura.org/, which specifies the type of key and length to generate the password.

Besides introducing a new phone on the Asterisk PBX, one must specify to what extension and which process will follow when establishing a call, in 'extensions.conf'.

4.4.1. Testing with a VoIP phone

Following the scenario described above, a VoIP call from Municipio to Biblioteca within the Hospital was intended and successfully completed. The exact configuration cab be seen along Appendix I. Then one can see through the next captures taken from Wireshark, how the first SIP agent established the communication with the other SIP agent.

Detected 1 VoIP Call. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State
5,990598	31,102534	192.168.0.103	"municipio"<sip:077@200.62.92.220:5060	<sip:052@200.62.92.220:5060	SIP	17	COMPLETED

Figure 26. VoIP call completed

The next figure shows the flow between both terminals and how the call was first established (Invite, Authentication, Trying, Ringing, Accepted); then the RTP corresponding to the call itself (with the flow of voice packets); eventually, the conversation closed down with *BYE request* and *OK*.

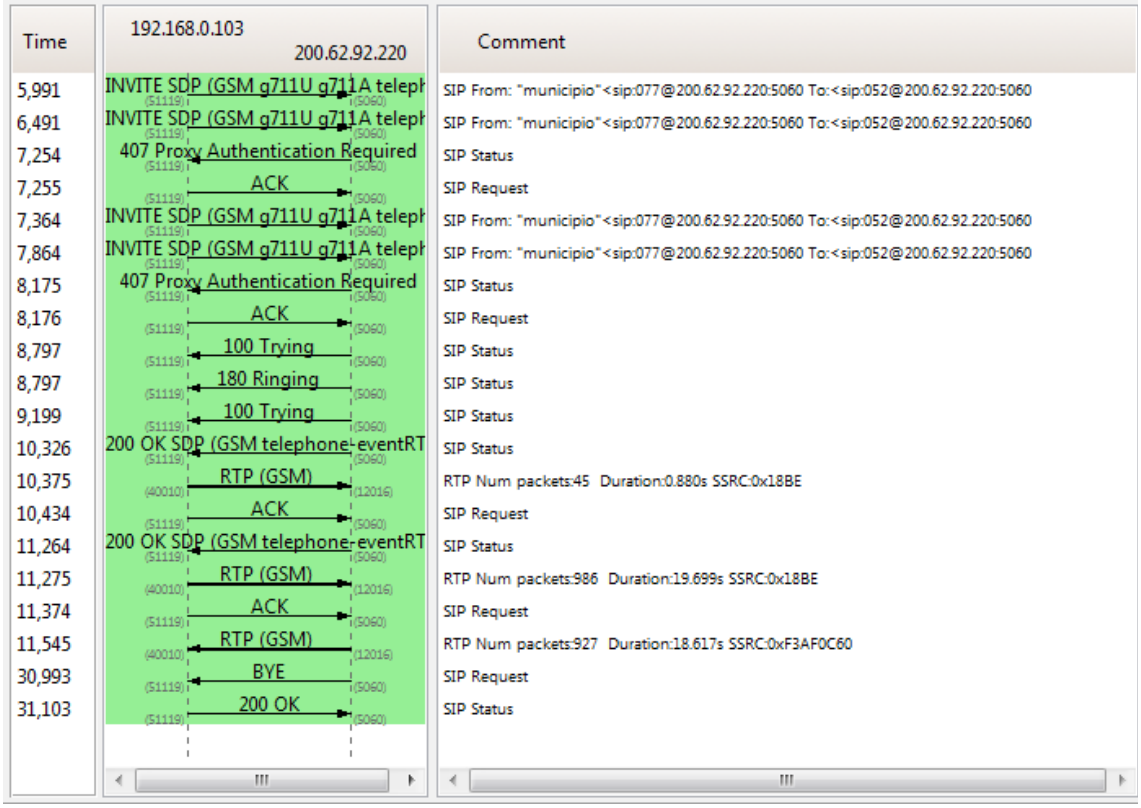


Figure 27. VoIP flow diagram

Breaking down the flow diagram, one can see the dialogue described, first of all, with the establishment of the call between the two agents.

No.	Time	Source	Destination	Protocol	Length	Info
55	7.863609	192.168.0.103	200.62.92.220	SIP/SDP	1209	Request: INVITE sip:052@200.62.92.220:5060, with session description
56	8.175137	200.62.92.220	192.168.0.103	SIP	611	Status: 407 Proxy Authentication Required
57	8.175635	192.168.0.103	200.62.92.220	SIP	393	Request: ACK sip:052@200.62.92.220:5060
58	8.796731	200.62.92.220	192.168.0.103	SIP	529	Status: 100 Trying
59	8.796735	200.62.92.220	192.168.0.103	SIP	545	Status: 180 Ringing
60	9.198730	200.62.92.220	192.168.0.103	SIP	529	Status: 100 Trying
61	10.325676	200.62.92.220	192.168.0.103	SIP/SDP	775	Status: 200 OK, with session description
65	10.434449	192.168.0.103	200.62.92.220	SIP	658	Request: ACK sip:052@200.62.92.220
108	11.264026	200.62.92.220	192.168.0.103	SIP/SDP	775	Status: 200 OK, with session description

Figure 28. VoIP call set up

Second of all, a set of packets corresponding to the exchange of voice information.

No.	Time	Source	Destination	Protocol	Length	Info
143	11.734899000	192.168.0.103	200.62.92.220	RTP	87	PT=GSM 06.10, SSRC=0x18BE, Seq=18535, Time=46089
144	11.745195000	200.62.92.220	192.168.0.103	RTP	87	PT=GSM 06.10, SSRC=0xF3AF0C60, Seq=56134, Time=223463495
145	11.755041000	192.168.0.103	200.62.92.220	RTP	87	PT=GSM 06.10, SSRC=0x18BE, Seq=18536, Time=46249
146	11.764324000	200.62.92.220	192.168.0.103	RTP	87	PT=GSM 06.10, SSRC=0xF3AF0C60, Seq=56135, Time=223463655
147	11.775191000	192.168.0.103	200.62.92.220	RTP	87	PT=GSM 06.10, SSRC=0x18BE, Seq=18537, Time=46409
148	11.789279000	200.62.92.220	192.168.0.103	RTP	87	PT=GSM 06.10, SSRC=0xF3AF0C60, Seq=56136, Time=223463815
149	11.794854000	192.168.0.103	200.62.92.220	RTP	87	PT=GSM 06.10, SSRC=0x18BE, Seq=18538, Time=46569
150	11.805074000	200.62.92.220	192.168.0.103	RTP	87	PT=GSM 06.10, SSRC=0xF3AF0C60, Seq=56137, Time=223463975
151	11.815100000	192.168.0.103	200.62.92.220	RTP	87	PT=GSM 06.10, SSRC=0x18BE, Seq=18539, Time=46729
152	11.824762000	200.62.92.220	192.168.0.103	RTP	87	PT=GSM 06.10, SSRC=0xF3AF0C60, Seq=56138, Time=223464135

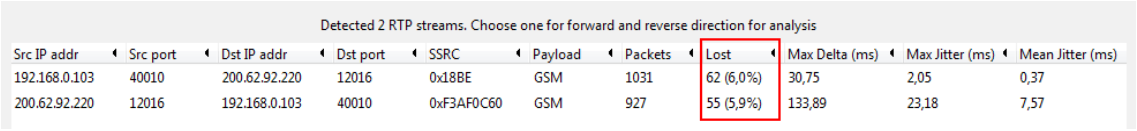
Figure 29. VoIP call RTP packets

Finally, how the call was ended up.

No.	Time	Source	Destination	Protocol	Length	Info
2028	30.993104000	200.62.92.220	192.168.0.103	SIP	493	Request: BYE sip:077@192.168.0.103:51119;rinstance=027e1bc5a23b5d1a
2029	31.102534000	192.168.0.103	200.62.92.220	SIP	430	Status: 200 OK

Figure 30. VoIP call ending

Although satisfactory, the objection relies on the fact that several packets were lost during the call, around 6% in both directions. This amount of losses did not translate into poor quality of the conversation. However, as the Internet bandwidth of the hospital is very reduced, at times of high usage of the network, the percentage is much higher and the quality of the conversation is unacceptable.



Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr	Src port	Dst IP addr	Dst port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
192.168.0.103	40010	200.62.92.220	12016	0x18BE	GSM	1031	62 (6,0%)	30,75	2,05	0,37
200.62.92.220	12016	192.168.0.103	40010	0xF3AF0C60	GSM	927	55 (5,9%)	133,89	23,18	7,57

Figure 31. VoIP call packets lost

That is an important drawback for the implementation and expansion of the VoIP telephony network, since one can not always guarantee a good communication. Two possibilities have been considered to solve this problem:

- **Have 2 ADSL lines,** keeping one of them exclusively dedicated to the use of VoIP telephony network. Though, this is not a feasible solution due to the high cost it would represent for the hospital, which always lacks of resources.

- **Save enough bandwidth** to ensure the transmission of voice packets without losses. With the implementation of a token bucket (acting as a filter), the flow of information could be limited and with that required minimum of bandwidth kept (around 80 kbps), an acceptable communication with no losses could be guaranteed. However, the modem the hospital currently has does not allow to implement that option, so a brand new one should be acquired.

4.5. Implemented solution

Finally the installation of VoIP phones was not performed for certain reasons. On the one hand, bearing the hospital's bandwidth is not sufficient to guarantee an acceptable communication with no cuts and losses of voice packets.

On the other hand, for lack of funds to buy new phones for both centres and the fact that Juan Manuel Morales has no Internet access. Thus, we left the facility to implement them along a future phase when the conditions are satisfactory.

CHAPTER 5. Radiolink HRESB – Monkey Point

Monkey Point is small rural municipality of around 300 inhabitants, belonging to the dependence of Bluefields, located 47 km south along the cost line. It is a Creole community with English-speaking and a culture deeply rooted.

Regarding the telecommunications field, these are totally absent. No phone coverage whatsoever in tens of miles around nor conventional telephony is found. So the need of providing a telephony system in order to establish a communication with the HRESB seemed obvious and vital for its citizens, since at least the health deficit that causes lack of communication or the management of patients transportation could be solved. Particularly, taking into account that the Health Post in the community has not even a doctor but just a nurse who provides the whole health care to the entire community.

In this chapter will be explained the characteristics of the radio link, the settings of the various equipment, the testing made and the conclusions drawn.

5.1. Design of the radio-link

To link the Hospital Regional Ernesto Sequeira Blanco (HRESB) with the Health Post of Monkey Point, it is necessary to establish 3 radio-links. The first, a short one from the hospital to Cerro Aberdeen; the second, from there to Monkey Point; finally, a third one from a high point within the municipality and the Health Post.

The first link was already covered by the existent infrastructure built by TSF during the previous stages of the project. The second had to cover around 50 km along the Atlantic coast, in a forested region with different slopes of the terrain and tropical climate. The third one had to cover a distance of approximately 200 meters within the village of Monkey Point.

The following map shows a scheme of the links with its coverage:

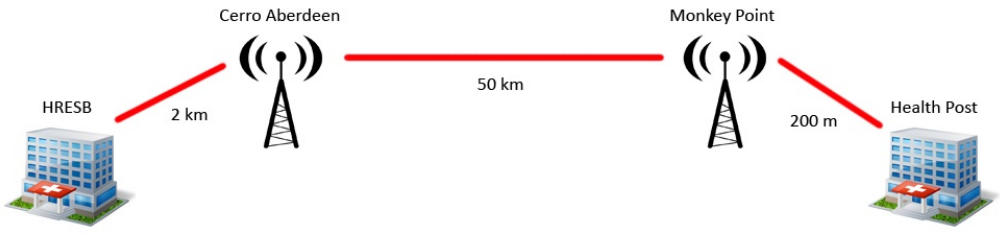


Figure 32. Radio-link's design

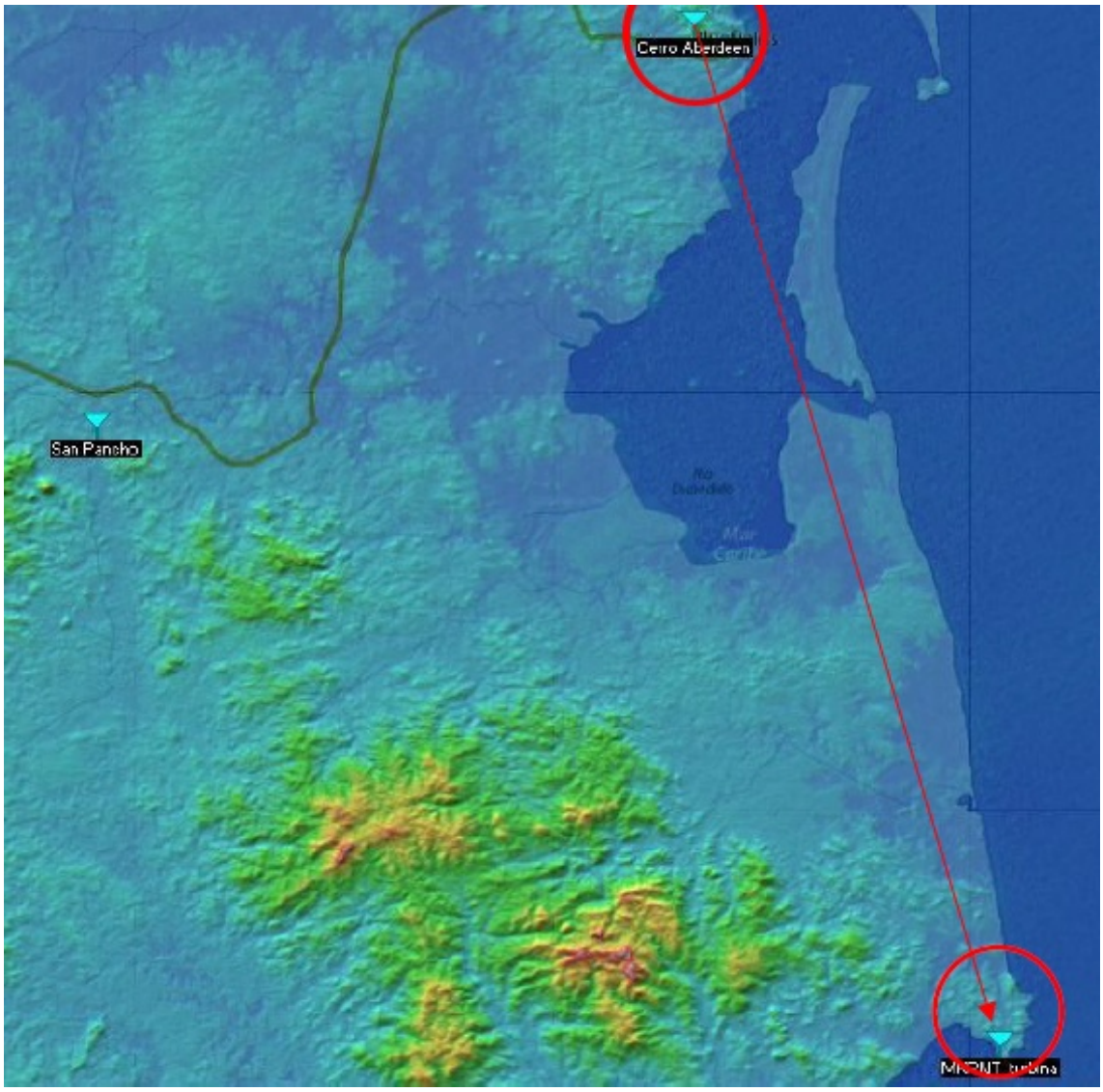


Figure 33. Physical map between Cerro Aberdeen and Monkey Point

5.2. Technical solution

Along the last stage of the project [3], the best solution to adopt in order to ensure the link was studied, both mathematically and technically. All that information and calculations can be read along Appendix V on their project.

Finally, after studying several options for the location and height of the antenna in Monkey Point, it was decided that the most optimal placement for its easy access and its height was on the hill where the wind turbine of blueEnergy is installed.

Figure 34. Spot chosen in Monkey Point

In addition, in the Phase VI [3] through the software Radio Mobile, the link was simulated to calculate the orientation of the antennas and the optimal height. Finally, it was decided to locate the antenna of Cerro Aberdeen at 20 meters and build a tower in the hill of Monkey Point with a height of 10 meters. The following figure shows the characteristics of the link.

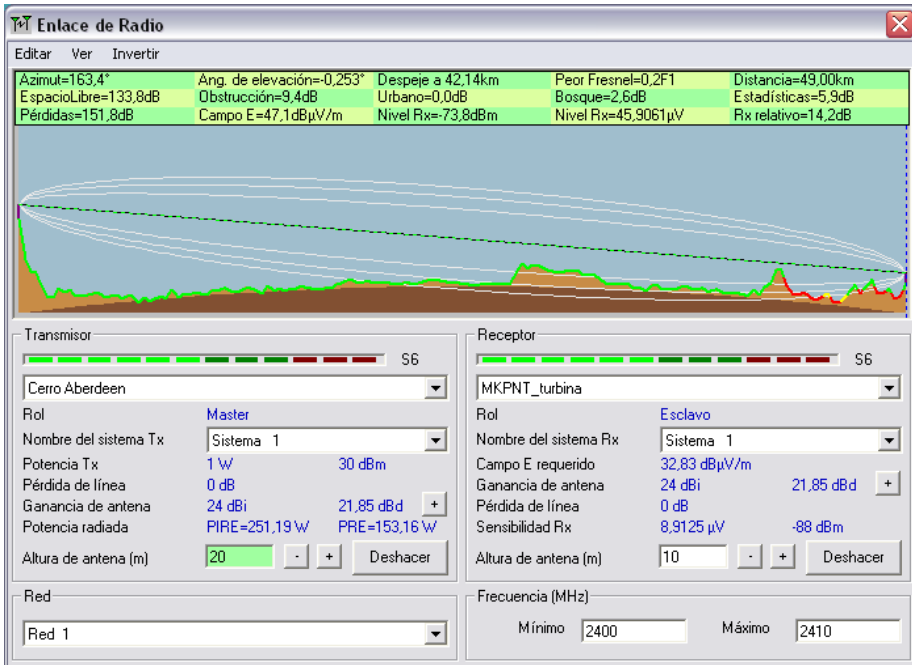


Figure 35. Radio link simulation

To summarise, different equipment was necessary for each link. That is to say, for the long one, there were used transmitters Bullet M2 and antennas H2G424G, by Hyperlink. For the short one, AirGrid M-series by Ubiquiti as the following figure shows.

Cerro Aberdeen – Monkey Point	Monkey Point – Health Post
Hyperlink	AirGrid M-series Ubiquiti

Figure 36. Antennas used

5.3. Equipment configuration

Our task began by configuring all the equipment. Following the calculations given by our colleagues, it was up a scenario likely to be the one found *in situ*, in order to check if all the devices were working correctly.

Unfortunately, one of the AirGrid seemed to be burned out, so it had to send back to the provider in Miami, FL (USA), who replaced it by a brand new one. Meanwhile, it was configured a VoIP telephone for the Health Post as well as the remaining three antennas. Once the AirGrid was back, a whole simulation was worked out, consisting of a call between the VoIP telephone from the Library to our new VoIP telephone through all the set of links. The system was ready to be implemented.

The following issues were taken into account when designing it:

- IP assignation was according to the hospital network, starting by 192.1.68.1.40.
- Channel bandwidth was set as narrow as possible, to enhance the scope of the link, since the smaller the channel bandwidth is, the greater power spectrum density has.
- Center frequency was set trying to avoid overlap of channels in adjacent nodes.
- Transmission power was set at its maximum to achieve a wider scope.
- Transmission speed (MCS table) was set to its minimum in order to increase the reception sensitivity.

The specific configuration of each device can be read along Appendix VII.

	Cerro Aberdeen – Monkey Point		Monkey Point – Health Post	
	Bullet CA	**Bullet MP**	**AirGrid MP**	**AirGrid HP**
Operation mode	Station	Access Point	Station	Access Point
IP	192.168.1.44	192.168.1.45	192.168.1.46	192.168.1.47
Bandwidth	5 MHz	5 MHz	5 MHz	5 MHz
Central Freq.	Auto	2437	Auto	2457
TX Power	28 dBm	28 dBm	28 dBm	28 dBm
MCS	MCS0 1.625 Mbps	MCS0 1.625 Mbps	MCS0 1.625 Mbps	MCS0 1.625 Mbps

Table 11. Equipment configuration

5.4. Test in-situ

Although the simulations showed good results, before the final installation some tests were run *in-situ* to verify that the radio-link would work as planned. For testing the link, the antenna in Cerro Aberdeen was first installed and in the community of Monkey Point was installed a scaffold that simulated the future tower build for the community.

Before the implementation of all the equipment, it was essential to meet all parties involved. That is to say, a couple of meetings were set up with the Ministry of Health (MINSA), the Gobierno Comunal Rama y Kreol (GCRK), the NGO BlueEnergy and TSF itself. In those meetings, the contribution of each part to the project was agreed. The following table displays the result bespoken:

Institution	Contribution
Monkey Point (Municipio)	– Scaffold rental. – Transport support (SILAIS panga). – Construction of the tower (10m), with all the material, working staff and labour. – Economic support for the panga's fuel.
Gobierno Comunal Rama y Kreol (GCRK)	– Power generator rental. – Economic support for the panga's fuel.
Telecos Sense Fronteres	– Equipment for the radio-link (antennas, bullets...). – Engineers.
BlueEnergy	– Support for the power supply equipment (30W).

Table 12. Institutions involved and their contribution

The first step was to install the antenna at Cerro Aberdeen. It was a complicated job because working at 20 meters heigh is something that we are not used to. But with the help of Nicaraguan television workers we could do the installation successfully.

An anchor to fix the antenna was necessary as it would be safer because of the strong wind could move the antenna, losing its orientation. In addition, all the outdoors connections were protected with silicone insulator and all parts of the antenna were covered with oxidant painting to protect them from oxidation. On the other hand, to interconnect all equipment installed in the Cerro, a switch was installed as shown below. To check out the correct installation of the antenna, some successful ping's were done from the HRESB in order to see the response.

After the installation of the antenna in Cerro Aberdeen, everything was set up and ready to make the trip to Monkey Point. To run the tests, as mentioned above, an scaffold was rented to simulate the future height of the antenna. In addition, it was used the solar and wind energy of NGO BlueEnergy has installed on the hill to power the antenna.

Figure 37. Switch installed in Cerro

Figure 38. Scaffold and antenna installed

After several changes in the orientation of the antenna, the signal was not received from the Cerro Aberdeen. The conclusion was that the radio link was not feasible. Possible reasons of its not correct operation could be:

- The distance of 49 km. The antennas installed have a limit of 50 Km.
- The high attenuation caused by the vegetation and the climate of the area.

CHAPTER 6. Desktop Virtualization: NComputing

This chapter details the implementation of a new technology within the hospital framework, as a stable and easy to monitor solution to the damage caused to all the computer by the severe tropical climate of the area where Bluefields is located, as well as the difficulties of maintenance the whole infrastructure.

6.1. Current situation within the hospital

As explained along Chapter 1, Bluefields is located in a very particular area, where extreme humidity, sharp high temperatures or accumulation of saltpetre (among other environmental elements) are common problems for the equipments in that specific spot of the Caribbean cost, so they easily get damaged. Moreover, there are problems of maintenance of those equipments due to a lack of knowledge among the employees within the hospital, and the budget for new equipment and repairs is low.

For all these reasons, we thought about a system that could improve the current hospital network in terms of efficiency, maintenance and energy savings. That is to say, a virtual desktop infrastructure.

We had the opportunity to visit the Seminario Pío X in Bluefields, where an architecture like this one was recently implemented by James Alaniz, a computer specialist from the city who sometimes supports and checks the network. Thanks to his help, we decided to implement a desktop virtualization within the hospital.

6.2. Virtual desktops

Desktop virtualization (also called client virtualization) is a technology that separates a personal computer desktop environment from a physical machine using the client–server model of computing. It involves encapsulating and delivering either access to an entire information system environment or the environment itself to a remote client device. The client device may use an entirely different hardware architecture from that used by the projected desktop environment, and may also be based upon an entirely different operating system.

The desktop virtualization model allows the use of virtual machines to let multiple

network subscribers maintain individualized desktops on a single, centrally located computer or server. The central machine may operate at a residence, business, or data centre. Users may be geographically scattered, but all must be connected to the central machine by a local area network, a wide area network, or the public Internet.

Among the possibilities the market of virtual desktop infrastructure (VDI) currently offers, VMware (with VMware View), Citrix (with XenDesktop) and NComputing (with L-Series) were considered as great real options to implement.

	vmware	CITRIX	NComputing
Protocol	RDP, PCoIP	RDP, ICA	UXP
OS supported	Windows, Mac, Linux	Windows, Mac, Linux	Windows, Linux
Listening	Client & Server	Client & Server	Client & Server
File transfer	✓	✓	✓
Audio support	✓	✓	✓
Multiple sessions	✓	✓	✓
Seamless window	✓	✓	✓
Average price per unit	180$	200$	160$

Table 13. Comparison of virtual desktop infrastructures

According to the general features displayed on the table above, all three VDI have similar performance. Eventually, the choice was for NComputing company due to:

1. A question of budget and its lower price as compared to the rest.
2. The system was already implemented in Bluefields so it existed the possibility to contact the person and get help with the configuration and maintenance.

6.3. NComputing

NComputing is a desktop virtualization company that manufactures hardware and software to create virtual desktops (sometimes called zero clients or thin clients) which enable multiple users to simultaneously share a single operating system instance. Currently, NComputing is the leadership in desktop virtualization worldwide thanks to its totally integrated solution, offering to the customer both software (called vSpace) and access devices.

Savings	Funcionality	Security
■ Savings of 50% in adquisition cost.	■ Easy to maitain a centralized architecture.	■ Avoids illegal extraction of information.
■ Savings in 85% in the cost of spares of PC's.	■ Easy to install the system and configure.	■ 128 bits encryption.
■ Savings in 95% in electrical power consumption.	■ Compact, small and thin.	■ Avoids the installation of virus.
■ Savings in maintenance and updates.	■ Does not generate noise nor heat; good for environment.	■ Solid and reliable.

Table 14. Advantages of desktop virtualization

Among them, there is a set of features which contributed to our decision, according to the current situation of the hospital:

1. NComputing devices **only consume 10 watt per hour** (instead of 110 watts of a standard PC), so the energy savings is around 90%.
2. Access devices are very **small dimensions** and are composed of few components, so the error **error probability decreases drastically**.
3. Operation with **standard peripherals**.
4. Lifespan **much longer** than conventional PCs.
5. **Compatible with Linux**, the operating system used in the hospital.
6. Reduction of **Total Cost of Ownership** (TOC).

6.3.1. Architecture

The architecture to implement is likely to the following figure, where there is a central computer (operating as a server) which monitors the rest of PC's (operating as clients), all of them connected to it via the Ethernet network already installed within the hospital. Each client has an access point, screen, keyboard and mouse.

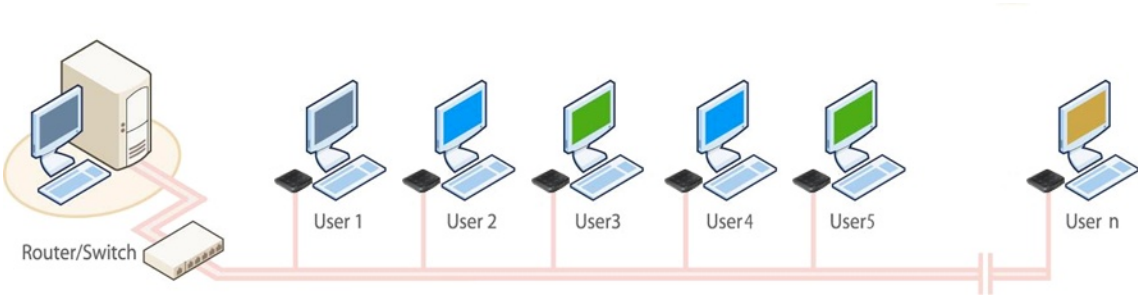


Figure 39. Architecture of desktop virtualization

6.3.2. Our pick: L-300 series

The company offers three product lines which differ in its connection. These are: the X-series (Direct connection), L-series (Ethernet connection) and U-series (USB connection). Due to the hospital's network structure, our best shoot is focused on L-series. Among them, the devices chosen are L-300, which present the best features according to our environment.

	L-130	L-230	L-300
Max. screen resol. (wide)	1440x900	1440x900	1920x1080
Max. screen resol. (4:3)	1280x1024	1280x1024	1600x1200
Max. colour depth	16-bit	24-bit	24-bit
Mouse & Keyboard port	PS/2	PS/2	USB
Microphone port	✗	✓	✓
Peripheral USB ports	✗	1 x USB	2 x USB
Full-screen video	✗	✗	✓

Table 15. Comparison of features for L-Series

Figure 40. NComputing L-300 series

6.3.3. Installation of the server

As shown above, the whole NComputing architecture is supported by a server with an specific software installed. For this case, the unit chosen was an Intel 61WW with the following features, enough to provide service to 10 devices with Windows installed and up to 20 with Linux, according to the manufacturer's specifications. Hence, this architecture might be scaled as new devices are incorporated.

Intel 61WW features	
Processor	Intel Core i5 2.8 Ghz/2300
RAM	4 Gb Kingston DDR3
Hard Drive	1 Tb Sata 7200 RPM
Operating System	Windows 7 Pro
Other characteristics	CD/DVD Burner 8 USB ports

Figure 41. Features of the server

6.3.4. Server software: vSpace

NComputing's vSpace Server virtualization software, included with the hardware, creates the virtual desktops in the shared PC by dividing the computer's resources into independent sessions that give each user their own PC experience. The vSpace software uses the communications protocol "User eXtension Protocol" (UXP) to communicate between the shared computer and the user stations. UXP serves a similar purpose as Microsoft's *RDP* and Citrix's *ICA*.

Once all the devices are set-up, it is possible to monitor them thanks to the console of the server. This tool provides an easy way to verify if the connections are enabled or see which sessions are currently running. Moreover, through the console one can edit all the settings of each user powered on and registered.

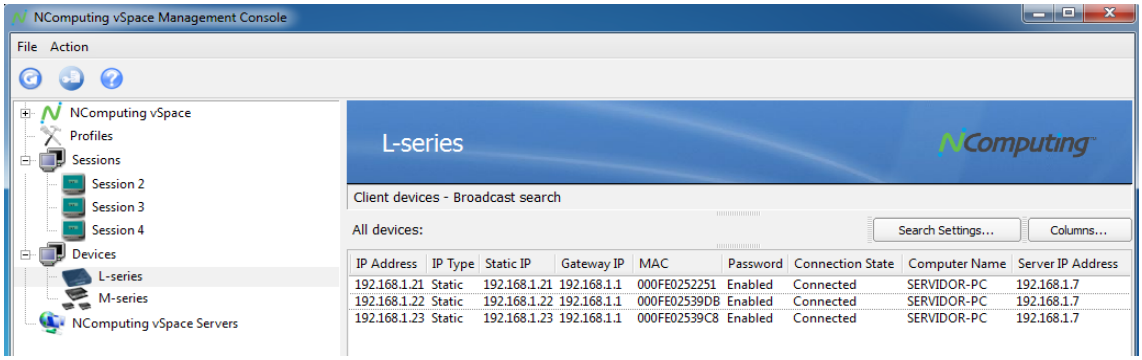


Figure 42. vSpace console

6.4. Implementation

First of all, it was necessary to set-up the server, by installing the SO (in this case, Windows 7, 64-bits) and the vSpace software, which was the last version available, 6.6.2.3 (updated February 2012). Once this first issue was running correctly, each NComputing user was created and added to a “remote group”. In total 3 users, 2 of them for the Library and the third for Surgery department: “Biblioteca 1”, “Biblioteca 2”, “Cirugía”.

Second of all, the NComputing devices were set-up, by plugging-in the keyboard, mouse and screen; pointing them to a static IP address from the hospital network range, starting by 192.168.1.21 and so on; the gateway 192.168.1.1 and DNS; a unique user-name and password to identify each department; adjusting the screen resolution. An option to *auto-connect* to the server when initialising the system was also included among the settings to simplify the process.

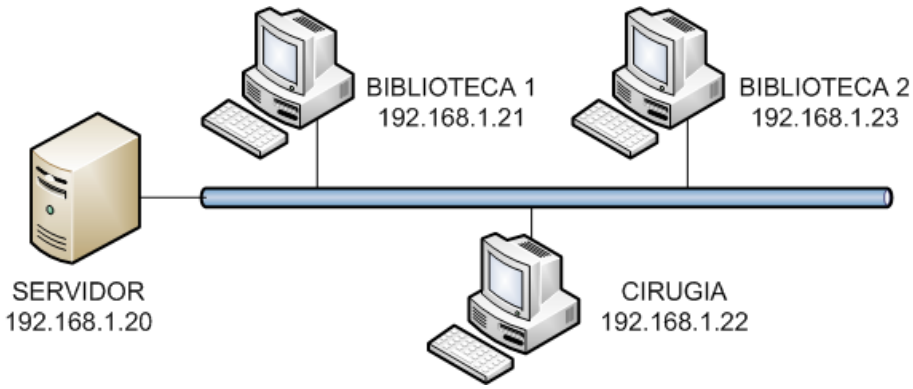


Figure 43. Network configuration

Finally, all the necessary software and applications were installed just to the server, such as Microsoft Office, Adobe Reader, WinRar... Immediately, these software are reproduced to the client units. In each client, nothing extra is necessary to be installed since all the applications are monitored from the server.

The last step consisted of freezing the server (with *Deep Freeze* software) in order to avoid that the personnel of the hospital could modify or misuse the devices. That is to say, when someone reboots the computer, all the info and changes previously done are deleted and back to the initial configuration. It strongly helps to prevent the whole equipment from virus.

All the details of installation and configuration are explained along Appendix VIII, and the use of Deep Freeze along Appendix IX.

6.5. Results and conclusions

Before the final implementation to each department, a test was run. There was a two-days conference consisting of “accurate Internet research” in the hospital, so the whole equipment was part of the computers used. The system worked out correctly.

The implementation of virtual desktop technology has lead to improve the infrastructure of the hospital. As explained before, it is easy to monitor and saves lots of energy, which translates to cutting down expenses and maintenance. This was just an initial approach but, as it seems the contribution was important, more devices might be incorporated in the near stages of the project or by the hospital themselves.

In addiction to the implementation, and following the same strategy of training, we created some posters with the basic instructions of power-on/off, how to plug/unplug a USB memory and the password to access, since the use of this technology presents no great difficulties of usage. Those posters were placed right near the devices so they can be easily seen. The following image shows an example of it.

Figure 44. Guideline for NComputing units usage

CHAPTER 7. Other Improvements

This third chapter discusses certain aspects that have helped to improve the hospital's infrastructure (installation of new equipment: a server and some VoIP phones), as well as organizational issues (for a specific department) or the collaborations established with other institutions (such as agreements with an University or GEDEOM).

7.1. Installation of VoIP phones Grandstream GXP280

Two isolated departments (Radiology and Warehouse) required the communication with the rest of them within the hospital. We configured one VoIP phone Grandstream GXP280 for each one, a similar model of the already installed Grandstream brand with the same features and functionalities.

To avoid the IP problems we had in our arrival, we established both IP being static within the rang kept for telephone use: 192.168.1.63 (for Radiology) and 192.168.1.64 (for Warehouse). The whole configuration can be found along Appendix II.

Grandstream GXP280	
Audio Codecs	PCMA, PCMU, GSM, iLBC, G.723.1, G.729A/B, G.726, G.722
Protocol Support	SIP 2.0
Display	Numeric LCD
Speaker	Available
Network	Switch Ethernet LAN/PC

Table 16. Grandstream GXP280 features

7.2. IP Network inventory

Over time, many and many units have been added to the hospital network. Eventually, this has lead to a mess of IP and devices. In order to make things clear, there was the need to separate and clarify which units have to be configured with with static IP and which running with dynamic ones.

The criteria relies on its performance. That is to say, the specific devices which strictly

need to be part of the network are set-up with static IP. The rest (all the computers spread over the departments) just by dynamic IP.

Here there is an outline of how the hospital network range have been modified and structured in order to maintain order for all the devices. Specifically each IP unit within the network is detailed along Appendix III.

	IP range	Devices
Static IP	192.168.1.1 – 192.168.1.19	Specific units of Library
	192.168.1.20 – 192.168.1.39	NComputing
	192.168.1.40 – 192.168.1.49	Radio-links
	192.168.1.50 – 192.168.1.79	VoIP Telephony
Dynamic IP	192.1.68.1.80 – 192.1.68.250	General computers

Table 17. IP network inventory

7.3. Digitalization the documents of the Physiotherapy Department

The Physiotherapy Department of the hospital suggested us to make more extensive the usage of the computer installed within their department. At that moment, the computer was only used to search on the Internet and edit some personal documents.

A meeting with the 4 members of the department was set up to evaluate their daily routine tasks in order to find a way to facilitate their work. The first intention was to digitize the information used to check their patients, but the problem leaned on they only had one computer for several rooms of consultation, and each room should have a PC to enter all the data taken during the consultations. This problem could not be easily solved because there was a limitation of the computers available in the hospital.

On the other hand, once a month they have to perform a count of the work done in the department, and it has to be delivered to the Statistical Department which performs a report for MINSA. This document shows the total amount of patients checked, treatments, etc. This work is heavy because it was done number by number, thus easily doing mistakes. The solution consisted of digitizing those files by using Microsoft Excel, so all the calculations would be automatically done. In addition, another file was designed to introduce their patient admission, in order to ease the finding of specific information about them.

The documents digitalized were:

- Patients admission (“Ingreso de pacientes”)
- Monthly report (“Reporte Mensual”)

– Monthly report of hospitalized patients (“Reporte Mensual de los pacientes hospitalizados”)

In Appendix XI, there might be seen the new Excel files created and the old documents replaced. It must be mentioned that some cells of the Excel files, which contained formulas, were protected so the personnel was unable to modify them to avoid further problems.

Moreover, we carried out some Excel training classes for all the department's personnel to ensure the correct function of the files. As some specialists did not manage the program with ease, we prepared a training course to teach the most basic skills to fill the reports.

The methodology followed for the training engaged practices based on users' computers and its corresponding application. Thus, they learnt directly to manage the application and we got better results than doing theoretical lessons. We, as educators, guided and explained them all the basic knowledge they needed to know about each tool. In order to facilitate their learning, small groups of five or six were organized.

7.4. Collaboration agreement with BICU University

TSF and UPC set out the need to reach an agreement with a university within the region to provide academic support for the students who travel to Nicaragua, and also to find new ways to guarantee the work of the NGO when there is no volunteers *in situ*.

In order to facilitate academic support for the students who volunteer as aids workers of TSF, an agreement with the Bluefields Indian & Caribbenean University (BICU) was established. This document recognizes all the work done for the students during their stay in Bluefields, that is to say, 180 hours of work as project credits. As a counterpart, a student coursing its fifth grade of Systems Engineering in BICU is able to perform their hours of practise by helping the TSF aid workers in their daily tasks.

This agreement is the first step for students or faculty exchanges between universities, but not just that. This relationship is seen as a way Nicaraguan people can get deeply involved in the project TSF is developing and not act as mere spectators of the actions taken. The lack of technical knowledge by the hospital staff has limited the maintenance of the infrastructure along the last years, but this might be supplied by the students, who could understand all the functionalities and give a hand in certain situations such it has already happened in Monkey Point's radio-link.

In the Appendix XII, the agreement signed by both universities might be seen.

7.5. Collaboration agreement with SILAIS RAAS

That SILAIS RAAS is a regional structure of the Ministry of Health of Nicaragua, under whom are held all health units, such as the Hospital Regional "Dr. Ernesto Sequeira Blanco" and the Health Centre "Juan Manuel Morales", both in Bluefields, and other units of the seven municipalities.

Since TSF has had the feeling that, for most of the time, is working with just the collaboration of the Hospital, it was necessary to seek more direct involvement by the rest of the health institutions which are also part of the project. An agreement was closed with the most important institutions, led by SILAIS RAAS. That agreement would contribute to ensure the continuity of the project thanks to a better accuracy in the equipment maintenance or the replacement of damaged one.

All the details and the collaboration agreement itself can be seen along Appendix XIII.

7.6. Collaboration with GEDEOM

GEDEOM stands for *"Grupo para el estudio de la enfermedad oncológica y malformativa"*, is a Spanish NGO focused on the surgery and malformation fields that is working since 2003 in countries such as Morocco, Rep. Dominicana, Sri Lanka or Nicaragua. Lately, this entity has established a collaboration with HRESB in order to develop a telemedicine project related to oncology, trying to move forward in a new infrastructure for the hospital to treat these cases, as well as formation of new surgery techniques for the specialists or do video-conferences between Spain and Nicaragua to analyse some cases.

However, there were several shortcomings to take into account before starting with project, all of them related to the poor facilities the hospital currently had. Taking advantage of the situation, TSF was asked to collaborate with them.

From the technical point of view, TSF gave full support to guarantee the video-conferences, so a plan and a budget were set out to improve the facilities of the conference room. It mainly consisted of:

- Raise up the Internet connection of the hospital from 256 Kbps to 2 Mbps. A new monthly contract with Enitel was signed up.
- Replace the video projector by a brand new one in order to improve the luminance, contrast and resolution of the images. EPSON EX3210 was the choice to cover all these issues.
- Set up an audio system since there was a lack of it. It consisted of 2 sub-woofers Behringer TRUTH B2031A; an audio card M-Audio Fast Track MKII; a microphone Audio-Technica-PRO49QL and some wires for the connections.

EPSON EX3210	Behringer TRUTH B2031A	M-Audio Fast Track MKII

Figure 45. Equipment for the conference room

The estimated initial budget was set about 2100$, plus a monthly amount of 575$ corresponding to the Internet contract. The funding was entirely given by some pharmaceutical companies, and TSF will contribute with the installation of the equipment. Afterwards, the hospital will certainly improve its facilities and set the first steps for the project, and the relationship between TSF and GEDEOM keeps for further collaborations.

7.7. Health software

Over time, TSF has tried (and failed) to implement a hospital management tool with the aim of digitize and modernize the current system: paper and handwriting for all.

7.7.1. Current situation and problem definition

Nowadays, the country of Nicaragua embraces many health centres across different departments. On the one hand, this is good in terms of opportunities, since each health centre offers its own cares (such as general medicine, psychiatry or ophthalmology), so the citizens can have a more accurate treat of their problems in a nearby neighbourhood.

Each health centre is organized differently to make the patient records, some have already implemented health software and other hospitals are doing all the work by hand, as is the case of HRESB. This decentralization makes difficult the share of information of the patients. That is to say, a profile of a single patient can easily be filed in 3 different institutions, each of it, with totally different data.

For this reason, MINSA saw necessary to create a single hospital software to unify the medical records and that they can be consulted from any health centre in the country. By TSF in previous campaigns was tried Care2x software implementation but without luck because it was too complex software for the needs of HRESB.

The health software was developed by the Engineer Fredman E. Vilchez Calderon, director of information systems of MINSA. TSF though interesting to participate in the

creation of software as it is a big step in the country's health system.

7.7.2. The software

The software is accessed via the following link to a user name and password:
http://www.minsa.gob.ni:8091/PORTAL/

Since June 2011, TSF can access it with a test user to see the monthly progress and thus be able to contact the engineers to discuss the operation modes. In addiction, different views were exchanged for improvement.

By the end of 2011, there was a first draft with few elementary options. During the following months, the application was changed and developed. In the following figures it can be seen the last view of the application.

Figure 46. Application access

Figure 47. Application homepage

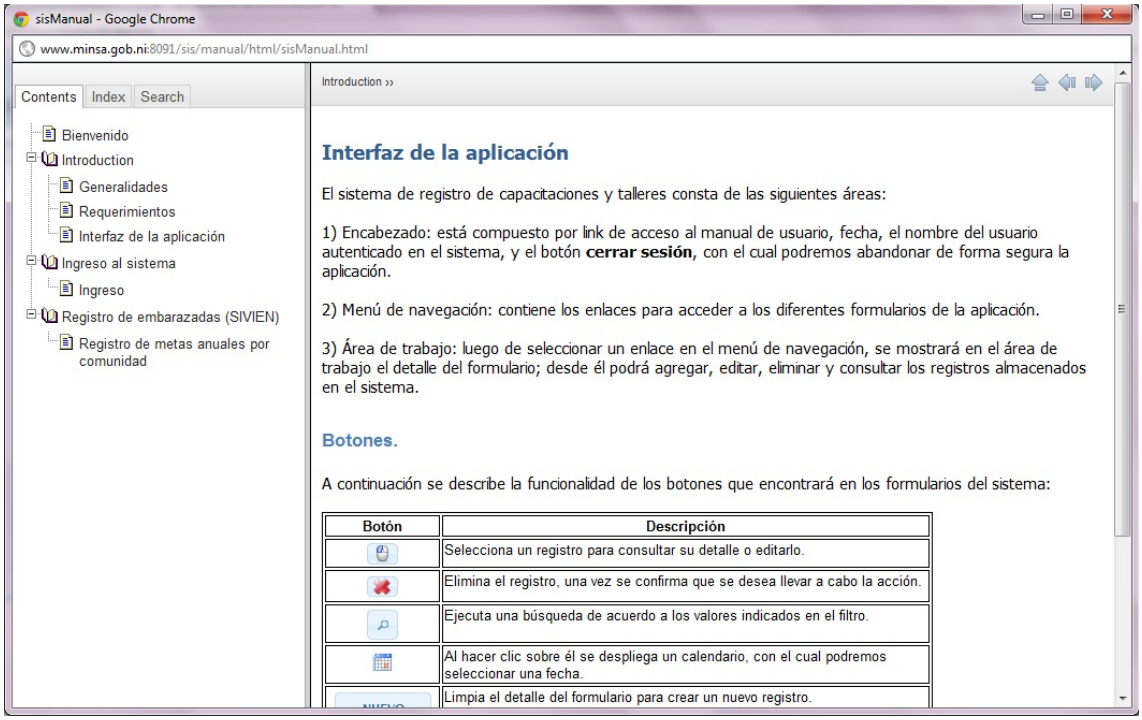


Figure 48. Application manual

CHAPTER 8. Budget and Funding

For a project, to be fully developed, it is essential to make a detailed study of the budget required to get all the goals. In this particular case, being a cooperative project, it is also fundamental to look for strategies and sources of income. This chapter shows how the funding was managed and the total estimated budget for that phase.

8.1. Budget

The following table displays the budget required to develop this stage of the project, in terms of equipment for the Hospital and the radio-link, as well as the plane tickets or the maintenance for the aid workers (lodging and subsistence).

Budget TSF Nicaragua 2012 | January - July					
Category	**Concept**	**Quantity**	**Unitary Cost**	**Total Cost**	**Source**
Plane Tickets and Subsistence	Plane Ticket BCN-Managua-BCN	2	1.097,80 €	2.195,60 €	KLM
	Plane Ticket Managua-Bluefields-Managua	2	74,90 €	149,80 €	La Costeña
	Travel Insurance	2	136,28 €	272,56 €	Caixa Nova
	Aeroport Taxes	2	8,57 €	17,14 €	Aeroport
	Visa	2	8,00 €	16,00 €	Customs
	Subsistence	-	-	1.800,00 €	HRESB
	Lodging	-	-	3.800,00 €	HRESB
	Subtotal			**8.251,10 €**	
Infraestructure HRESB	N-Computing L-300	3	151,25 €	453,75 €	Amazon
	Server Intel Core i5 2.8 GHz/2300	1	452,83 €	452,83 €	Comtech
	Sending Material	1	27,75 €	27,75 €	NicaBox
	Cleaning Spray for Computers	1	8,81 €	8,81 €	RadioShack
	Subtotal			**943,14 €**	
Radio-link Monkey Point	Various Materials	1	20,00 €	20,00 €	Bluefields
	Scaffold Hire	1	18,00 €	18,00 €	CGRK
	Fuel Supply	50	4,75 €	237,50 €	MINSA/CGRK
	Power Supply	1	50,00 €	50,00 €	BlueEnergy
	Subtotal			**325,50 €**	
Spreading initiatives	Posters	4	2,50 €	10,00 €	
	Leaflets	50	0,10 €	5,00 €	
	Subtotal			**15,00 €**	
TOTAL				**9.534,74 €**	

Table 18. Budget

8.2. Funding

One of the most important issues when developing a project is to fund it. Being part of an NGO, it is vital to do a successful campaign to promote the project and get the estimated budget.

Historically, TSF has tried and achieved that all members involved helped in the implementation and realization of the project. In this issue, the **HRESB** provides subsistence and the lodging for the aid workers. Moreover, since the last stage of the project, an agreement was created with the NGO **BlueEnergy**, which currently supplies the electrical power required in the implementation of radio links in the communities. One valuable point is the involvement of the whole **community of Monkey Point**, who gave the material and labour needed to build the tower to hold the antennas for the radio link.

Still, most of the project funding comes from the **CCD institution** which receives part of its budget through the "0.7% campaign" of the UPC. For this reason, TSF uses its virtual tools such as Twitter of Blog whenever there is the student enrolment, displaying references in their accounts, since it is the time when students and workers of the UPC have the opportunity to make a donation to the 0.7% campaign.

As it has been yearly done, TSF applied for the funding of *Centre de Cooperació per al Desenvolupament* (CCD) of 2012. The two aid workers elaborated a director plan [1] of the project with the new objectives and all the issues related to the actions taken (such as counterparts or agreements among institutions). The set of documents were delivered by the end of March 2012 and the approval resolution came out on May 21st 2012.

The last topic refers to the **donations** from individuals or private companies. To encourage and disseminate our project (in order to raise funds), several campaigns were conducted. Mainly, it has created a **poster** and some **leaflets** which briefly explained the work of the NGO and the objectives for this stage of the project. On the one hand, posters and leaflets were distributed in different areas, as well as university libraries, hospitals and places frequented by Catalunya donors of TSF. On the other hand, private companies tend to give grants to TSF, so there was presented a brief report which detailed the project and the points at which the financial support needed: the purchase of equipment.

Figure 49. Leaflet for funding

Figure 50. Poster for funding

8.3. Project spreading initiatives

TSF has a **website** *(http://www.telecossensefronteres.org/es/)* where there is reflected all the work done during the years. But in order to monitor and have a better report of the actions taken, a **blog** (http://telecossensefronteres.blogspot.com/) was created, which features the news related to the current project. During the stay of the aid workers in Nicaragua, there are weekly updates to track down the project day by day. And for the rest of the year, the blog is monthly updated to keep explaining the activities as well as funding the NGO is developing.

Figure 51. Screenshot of Telecos Sense Fronteres' blog

Furthermore, a **Twitter** account (@TelecosSF) was also created, with the same purpose as the blog, to keep everybody updated instantly.

Figure 52. Screenshot of Telecos Sense Fronteres' Twitter

Moreover, TSF has recently joined the online platform **Teaming** (*http://www.teaming.net/telecossensefronteres*). Teaming is a charitable initiative that was founded in 1998 and helps both family projects, and groups or NGOs through micro-grants of $1. People donate 1 euro per month and assign it to a social cause that they choose. TSF is part of world of Teaming since a few months ago.

Figure 53. Screenshot of Telecos Sense Fronteres' Teaming

The **Col·legi d'Enginyers de Telecomunicació** also supported us including our association and references of our project to the monthly newsletter.

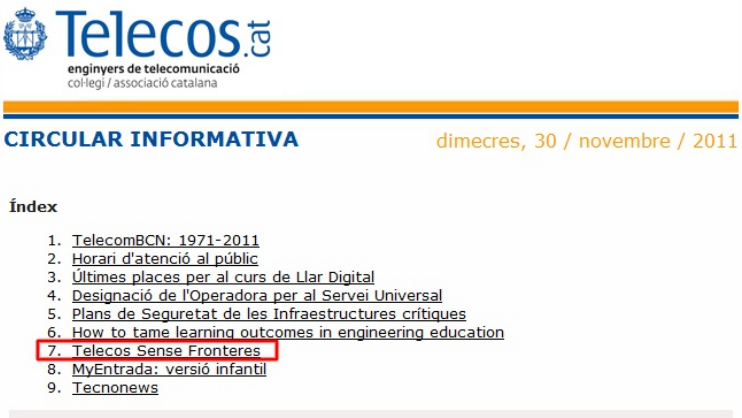


Figure 54. Informational circular of Col·legi d'Enginyers de Telecomunicació

In addition, members of **TIC.CAT community of Generalitat de Catalunya** were informed via e-mail about the project and the possibility to make donations. The following link redirects to the sent mail:

http://www.jornades.tic.cat/fileadmin/TSF/tsf_2011.html

Another initiative undertaken was the dissemination of the project through the portal **TecnoNews**, on the following link you can view the news:

> *http://www.tecnonews.info/Ayuda-para-Telecos-Sin-Fronteras-Necesitamos-recursos-para-equipar-un-Hospital/_pE0Aj1BfZN7VtoFZxcYP-KMAytk3q3yBcATxFfazYfhEjWb89GBm1D8KvOrmRNtZ*

On the other hand, when we arrived in Nicaragua we were invited to Kukra Hill Radio, Kukra Hill is a community located in the RAAS region. Through radio the communities can report the news of the region and the activities carried out. So, in the interview that we did in Kukra Hill we could explain the project which we were developing in the RAAS to inform all residents of the region.

Figure 55. Radio of Kukra Hill

To conclude, notice that this report is **presented as PFM** of students. During its presentation in July, the project and TSF itself will also be publicized. Also keep in mind that TSF works in all activities of the UPC and the CCD related to cooperation with small lectures or posters.

CHAPTER 9. Impact Project Evaluation

"Development is about people and not only with objects, and therefore the essential purpose of any type of development will be to ensure the adequate satisfaction of most basic human needs of those people".
(Postulate of M. Max-Neef et al. 1986) [5]

9.1. Methods and evaluation criteria

There exists several methods, guidelines, theories or different criteria to evaluate the impact a ICT project has over the place it has been developed. Some mainly focus on the social aspects, others emphasize more on technical issues while another group balance on both counts. For this case, 4 methods were considered and studied:

- Human Scale Development
- The Information Chain
- Real Access / Real Impact
- 12 Habits of Highly Effective ICT

9.1.1. Human Scale Development

Developed by Chilean Manfred Max-Neef in 1986 [5], states that Human Needs, self-reliance and organic articulations are the pillars supporting the Human Scale Development. But to serve its purpose they should, at the same time, rest on a solid foundation. This database is built from the real role people as a result of favouring both the diversity and autonomy of spaces in which participation is really possible. To achieve the transformation of the person-object, the subject of development is, among other things, a problem of scale, because there is no huge potential of leadership in systems organized hierarchically from top to bottom.

According to what Max-Neef proposes, this system of fundamental Human Needs can be broken down into **nine needs** that are common to all mankind, cultures, ages and groups: *permanence* or *subsistence*, *protection*, *affection* or *love*, *understanding*, *participation*, *leisure*, *creation*, *identity* and *freedom*.

Moreover it is possible to classify them according to different criteria, proposed as **four existential categories**: the needs of *being*, *having*, *doing* and *interacting*. These relate to the needs of fulfilling primarily with material goods or what would be the same with

products. From these dimensions, a 36 cell matrix is developed which can be filled with examples of satisfiers for those needs.

Fundamental Human Needs	Being (qualities)	Having (things)	Doing (actions)	Interacting (settings)
Subsistence	Physical and mental health	Food, shelter, work	Feed, clothe, rest, work	living environment, social setting
Protection	Care, adaptability, autonomy	social security, health systems	Co-operate, plan, take care of, help	Dwelling, social environment
Affection	respect, sense of humour, sensuality	Friendships, family, relationships	Share, take care of, make love	Privacy, intimate spaces
Understanding	Critical capacity, curiosity, intuition	Literature, teachers, policies	Analyse, study, meditate	Schools, families universities
Participation	Receptiveness, sense of humour	Responsibilities, duties, work, rights	Cooperate, dissent, express opinions	associations, parties, churches
Leisure	Imagination, tranquillity	Games, parties, peace of mind	Day-dream, remember, relax	Landscapes, intimate spaces
Creation	Imagination, boldness,	Abilities, skills, work, techniques	Build, design, compose, interpret	Workshops, audiences
Identity	Self-esteem, sense of belonging	Language, norms, customs, values	Get to know oneself, grow	Places one belongs to
Freedom	Autonomy, open-mindedness	Equal rights	Dissent, choose, run risks	Anywhere

Table 19. Criteria for Human Scale Development theory with examples

9.1.2. The Information Chain

According to Dr Richard Heeks (University of Manchester, UK) [4], considering the digital divide as merely digital is insufficient. To fully comprehend information-related divides one has instead to consider that information is a result of the process of accessing, assessing and applying data. People "*must be able to access data and assess if they are useful and applicable for their situation, before they could act upon them*". Data remains data unless people have the skills and expertise to transform raw data into useful information. Heeks uses a "4 As" model to illustrate this staged process. This model takes understanding beyond just access issues to the whole chain of steps that turn data into people action.

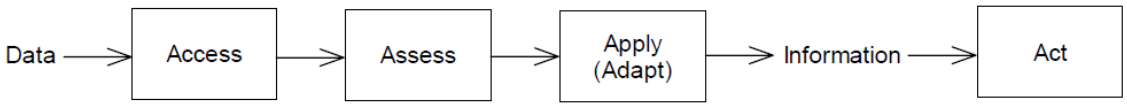


Figure 56. The "4 As" model of the Information Chain (Heeks, 1999)

The elements in the information chain can be clarified as follows. *Data* is unprocessed, raw facts and figures which might or might not be useful. When data is obtained, you *access* it. You *assess* data when you decide or estimate the value or quality of the data. You *apply* (*adapt*) data when you start using the data and make it suitable for a purpose, for particular needs or circumstances. The processed raw data then becomes *information*. Or in Checkland's and Holwell's words; "*data is transformed into information when meaning is attributed to it*".

This means that one person's information can be another person's data, for whom it has no meaning. In the Information Chain Theory, the word information is used in a special sense, simply understood as "*a physical quantity which can be stored, processed and transmitted via technical means*". Finally, when you do something with the obtained information or decide something based on that information; you *act*.

According to Heeks, the main indicator of the value of the information is the impact it makes on decision-making and action. "*The value of ICTs comes from their new abilities to handle information*".

9.1.3. Real Access / Real Impact

Founded in 2000 by Teresa Peters, bridges.org has worked hard to become one of the leading organizations in the field of information and communications technology (ICT) and development, providing the "Real Access / Real Impact" theory [4].

According to bridges.org, providing access to ICT is critical, but it must be more than just physical access and go beyond computers and connections so that ICT use makes a Real Impact on socio-economic development. "*Computers and connections are insufficient if the technology is not used effectively because it is not affordable; people do not understand how to put it to use, or they are discouraged from using it; or the local economy cannot sustain its use.*" bridges.org acknowledge that there is no single answer to what will guarantee success and achieve "Real Impact". However, looking at the project in terms of bridges.org key determining factors in whether or not people have "Real Access" to ICT or not might help.

There are twelve inter-related Real Access criteria which could be used to measure the "soft" issues surrounding ICT access and use. The questions can help outline the thinking about how to apply the criteria to ICT projects:

1. **Physical access to technology**
   Is technology available and physically accessible?
2. **Appropriateness of technology**
   What is the appropriate technology according to local conditions, and how people need and want to put technology to use?

3. **Affordability of technology and technology use**
   Is technology access affordable for people to use?
4. **Human capacity and training**
   Do people understand how to use technology and its potential uses?
5. **Locally relevant content, applications, and services**
   Is there locally relevant content, especially in terms of language?
6. **Integration into daily routines**
   Does the technology further burden people's lives or does it integrate into daily routines?
7. **Socio-cultural factors**
   Are people limited in their use of technology based on gender, race, or other socio-cultural factors?
8. **Trust in technology**
   Do people have confidence in and understand the implications of the technology they use, in terms of privacy, security, or cybercrime?
9. **Local economic environment**
   Is there a local economy that can and will sustain technology use?
10. **Macro-economic environment**
    Is national economic policy conducive to widespread technology use in terms of transparency, deregulation, investment, and labour issues?
11. **Legal and regulatory framework**
    How do laws and regulations affect technology use and what changes are needed to create an environment that fosters its use?
12. **Political will and public support**
    Is there political will in government to do what is needed to enable the integration of technology throughout society?

By paying attention to the criteria above, Real Access could be achieved. Sometimes, however, it is not enough to consider and address these issues; initiatives still fail because of poor project administration.

9.1.4. 12 Habits of Highly Effective ICT

The 12 Habits of Highly Effective ICT - Enabled Development Initiatives are a set of best practice guidelines for project management, which aim to ensure the internal health of initiatives harnessing ICT for development. Like the Real Access criteria, the 12 Habits can be used prescriptively for planning, or retrospectively for evaluation.

- **Habit 1.** Look at what has worked and what has not worked, study good practices in the area, and build on what you have learned.
- **Habit 2.** Conduct a thorough needs assessment of the community to be served so you can plan to do what is actually required.
- **Habit 3.** Make it local: ensure local ownership, get local buy-in, work with a local champion, and be context specific.
- **Habit 4.** Engage a local problem-solver with some degree of responsibility, and involve them sufficiently so they can identify and address problems.
- **Habit 5.** Form sound partnerships and collaborations.
- **Habit 6.** Set concrete goals and take small achievable steps. Be realistic about outputs and time-lines.
- **Habit 7.** Found your initiative on technology-neutral concepts so it can be adapted as needed to accommodate technology change over time.
- **Habit 8.** Involve groups that are traditionally excluded on the basis of age, gender, race or religion.
- **Habit 9.** Identify and understand the external challenges you face, and take practical steps to address them.
- **Habit 10.** Monitor and critically evaluate your efforts with effective tools, report back to your clients and supporters, and adapt your approach as needed.
- **Habit 11.** Make your initiative sustainable over the long term; either by bringing in sufficient income to be self-sustaining, or by delivering on a social mission so effectively that it is worthy of continued donor funding.
- **Habit 12.** Widely disseminate information on what you are doing and what you have learned so others can avoid your mistakes and build on your efforts.

9.2. Our pick: Real Access / Real Impact

Considering these 4 methodologies described above, one can see that “Human Scale Development” seems more appropriate for social projects, since it focuses on human needs from the point of view of “feelings”, but does not fit much with telecommunications. More or less occurs the same with “The 12 Habits of Highly Effective ICT”, a good tool since it describes 12 habits one have to face when developing a project, which does not focus on the more technical aspects.

“The Information Chain” is a a great applicable theory that is fed with their own assessments. We understand that is something one have to bear in mind as part of the steps followed, and that it helps to globally evaluate the impact of a whole project, previously defining the issues, so it lacks of specification. But the choice to evaluate this project eventually was for the “Real Access / Real Impact” method due to it fit

better according to the nature of the project and it was more complete and specific than the rest of the alternatives, giving a full conclusion of all work done and the impact it has had in all respects.

	Human Scale Development	Information Chain	Real Access / Real Impact	The 12 Habits
More social	✓	✓		✓
More technical		✓	✓	✓
More general		✓		✓
More specific	✓		✓	
Fits better		✓	✓	

Table 20. Comparison of methods and features

9.3. Evaluation with Real Access / Real Impact

Following the structure of the method given in section 9.1.3, the criteria focuses on 12 issues. Each of them, tries to answer an essential question. There it shows the responses for the project developed.

1. ✓ **Physical access to technology**
   Some equipment such as antennas and radio-links are not available to the residents of the community nor the staff of the hospital, but thanks to providing these links, all VoIP phones and computers installed within the hospital network are fully available to the personnel and students, with very easy access to them.

2. ✓ **Appropriateness of technology**
   There was a clear effect after the installation of NComputing technology within the frame of the hospital. Immediately thereafter, all the new units had full occupancy during the work-time with great feedback from the users. In addiction, the administration started to draw a plan to buy more units and add them to the network created (instead of acquiring conventional CPU), in order to replace old useless computers or cover new departments with a lack of devices. They rapidly saw the benefits according to the local conditions.

3. ✓ **Affordability of technology and technology use**
   According to the budget available by MINSA and HRESB, the technologies implemented are utterly affordable. We provided them some effective low cost ICT solutions for the problems described, always considering that in the future they will have to manage themselves these technologies. That is to say, the maintenance of the equipment, the acquisition, installation, configuration, etc.

4. ✓✗ Human capacity and training

Any technology is insufficient if people do not understand how to put it to use effectively. Furthermore, it is essential that people understand the broader potential for technology applications, so users can be empowered to creatively apply the technology to other parts of their life.

Everyone has been instructed to use the technology that could help in their specific framework. James Alaniz now manages the configuration of the antennas or Linux applications (tasks he previously did not know); doctors and nurses use NComputing units with great ease. Though, not everybody in the hospital is open to learning and some remain reluctant to change, specially in the use of VoIP phones in some departments. The cultural factor is something difficult to struggle with, but a possible solution would be more persistence in the training of the staff.

5. ✓ Locally relevant content, applications and services

Content is only relevant when its substance is interesting to users given their culture background, and accessible given their reading, writing and language skills. In the hospital environment, all the services given are tailored correctly to their needs, considering the personnel have medium-high level of culture and (although from the technological point of view) everything is related to their field: health.

6. ✓ Integration into daily routines

If technology use adds further burdens to people's lives and it is something they have to add on top of everything else they do as part of their daily routine, they are less likely to use it. Technology must be integrated into society. And that is exactly what happened with the VoIP phones and computers, because for the users these technologies daily helped them in particular moments.

7. ✓ Socio-cultural factors

People are often excluded from using technology or discouraged from using it based on gender, age, ethnic, or other socio-culturally based inequalities. But any of these issues are a barrier for the usage of our technologies. However, it is true that the lack of knowledge and fear of breaking devices reduce the use thereof.

But one should study the case in general, considering the project consisted of many different targets, some groups of people and not just one are the receivers of the actions.

On the one hand, the most direct group: the sanitary personnel of the hospital.

For instance, doctors and administrative staff who can easily establish a communication with the Health Post of La Aurora; or the personnel from the Physiotherapy Department who now is able to perform their statics in an accurate easy way. In general, everyone who uses any of the new computers or phones installed. That group is not reluctant to the use.

On the second hand, the indirect receivers: the inhabitants of Bluefields and the RAAS who, thanks to a better infrastructure within the hospital or the communication with La Aurora, now they might be getting a faster better consultation.

8. **Trust in technology**

People freely use the technologies and, in an unconscious way (probably due to a lack of knowledge), they have full confidence in the systems, so neglecting anything related to privacy or security. One can see how files, folders or important documents are sometimes forgotten in the desktops, or their e-mail accounts remain opened on the screen. There is a clear lack of understanding in issues like cybercrime.

The way to solve this problem would be to strongly insist on the possible causes, recalling the effects and consequences. Over time, this factor would definitely improve and people would be more careful with issues like privacy or security.

9. **Local economic environment**

From the economical point of view, the restoration of La Aurora's radio-link contributes in great savings of transportation by the members of the Hospital, especially in terms of fuel for the panga (very expensive nowadays). With just a single call, some trips can be avoided since some consultations might be done via telephone. The so-called “brigadas” are reduced and only proceeded when strictly necessary.

The implementation of NComputing technology definitely reduces expenses in terms of electrical energy or maintenance of the equipment. If one day all the computers in the hospital are monitored under this methodology, the effect will be noticeable. The more devices installed, the greater reduction in costs, similarly to the VoIP telephony.

Another issue that will cut down expenses to MINSA is the implementation of the medical software. Piles of papers and photocopies will be reduced since all the data will be edited and stored in the central offices in Managua (with its back-up), becoming a more reliable useful system, centralised but opened to everyone within the hospital field.

10. ✓✗ Macro-economic environment

National economic policy that creates a favourable macro-economic environment for technology integration is a critical element of bridging the digital divide. Related to Monkey Point, there is a future governmental project consisting of the construction of a deep-water harbour in that municipality, that would rise up the communication, the education or the access to information, becoming Monkey Point a key place in the Atlantic coast. If the implementation of the radio-link was achieved, our technology would be integrated to this new infrastructure. However, that is a single isolated event, since one can feel the distance and little input and investment from the government in that area of the country.

11. ✗✓ Legal and regulatory framework

The legal and regulatory frameworks that govern a country can either foster or hinder technology use. When working in an isolated environment such as the Hospital of Bluefields, one can feel there is a certain degree of freedom to do whatever, since there are almost no regulations in the Telecommunications field. It is true that an authorization by ENITEL is needed to access to the government's communications tower and install a couple of antennas. But afterwards, no one cares if the radio-link can affect the environment, the ecosystem, the communities, the tower itself, other existent radio-links, etc.

On the other hand, there are always problems with the import and transfer of new equipment at Managua's custom, usually delaying the work, what is interpreted as a lack of interest and prosperity by the authorities. A contradictory fact according to that neglect of regulation.

This situation will not get better unless the government settles some legal laws about the telecommunications field, which is something TSF can not handle.

12. ✗✓ Political will and public support

The national government can play a fundamental role in creating an environment that will foster technology use and encourage investment in ICT infrastructure, development, and a skilled workforce, but governments must have the political will to drive change and they must enjoy strong public support. And in the Nicaraguan case is not the best example of will, since it is very difficult to be coordinated with high institutions who work on their part, regardless of what is done in the smaller regional institutions as the hospital.

In this phase, we have tried to bring the project to local institutions such as the BICU University or sign a contract with health ones such the SILAIS and JMM. As mentioned along chapter 1, health and politics are closely related and it seems a logical way to gain support from that side.

Another issue out of the 12 already evaluated is related to the environment. TSF has always aimed to minimize the impact of its project in terms of environment. For instance, in the Monkey Point radio-link implementation, some issues were taken into account. On the one hand, the collaboration with blueEnergy contributed to use electrical power supplied from their solar panels, that is to say, green energy. On the other hand, the tower for the antennas was built in an area within the community where the signal coverage for the communication was acceptable, but at the same time, avoiding the cut of vegetation. In addiction, the design was made by the inhabitants themselves and the materials were trees from that specific area, becoming the visual impact barely noticeable.

CONCLUSIONS

A class project and a real project differ in several aspects. While both require good planning and knowledge of the subject, in the second case is vital its wide dissemination in order to achieve the maximum possible resources. During the months before to the trip to Nicaragua, we had to take all the decisions and get the sufficient echo so the public and private organizations supported our initiative.

Like in any other project, we had to decide the targets, although for different reasons some had to be modified. Since, in a project of this nature, it is a complicated task to achieve all the goals as they are unforeseen, so it led us to rethink the direction of the project. However, we have performed most of the tasks previously scheduled.

Our first task when we got to Nicaragua was to do maintenance and solve problems that had arisen during the absence of aid workers in Bluefields. Most of the incidents that occurred had easy solutions but, among the hospital staff, there is no technical abilities to fix the equipment, so most of them remained unused and no one cared to fix them. Since that moment, we realised that it was a huge problem that had to be resolved during our stay, so we tried to educate the hospital employees by reporting the problems when a computer or VoIP phone did not work, by hiring the engineer James Alaniz, who is fully trained to fix any of this problems.

The most important objective achieved during the 6 months has been the deployment of a remote desktop technology, NComputing. This allows to struggle with the problem of computer deterioration within the hospital, caused by the severe weather conditions of the region. In addiction, the management of the hospital has seen it as a great initiative because it reduces the cost of the computers and its maintenance. However, we were only able to install 3 devices plus the server, due to a lack of funds, although the first approach was planned to expand the network with more equipment (up to 7) as there are some departments of the hospital with the same needs.

An important part where many effort has been devoted, consisted of testing the connectivity for the radio-link between the community of Monkey Point and the HRESB. To coordinate all parties involved and get all the necessary resources to make the trip to the community was a costly task. But we eventually were able to carry out the test, although the results obtained were not satisfactory since we did not get connectivity between both sides of the link.

Another issue seen as a good initiative was the expansion of the VoIP telephony network out of the hospital range, in order to provide direct communication between the main health centres of Bluefields and facilitate the transfer of patients. But

although we performed the configuration tasks, it could not be conducted due to lack of resources by the centres where were supposed to be installed. The budget for each centre is closed and controlled from Managua, so they have little flexibility to make the purchase of equipment. For this reason, to request the installation of the Internet and buy a brand new VoIP phone were tasks that could not be carried out by the bureaucracy involved.

A critical point in the project has been the lack of involvement by the counter-parties. Nowadays, we reached a point of stagnation where they do not cherish any of the improvements provided for their citizens. It can be seen during the trip that took place in Monkey Point (to test connectivity of the radio-link), and the trip to La Aurora (to restore the communication), as we have encountered with several obstacles just to travel to the communities mentioned. For this reason, it was thought advisable to sign an agreement between the different parties involved in the project to ensure its continuity and that the work done by the TSF will not deteriorate and get lost.

After these 6 months in Nicaragua it is the time to analyse future needs and ways to continue the project. The following list of objectives treats several fields where TSF could continue working. However, it should be outlined that the main objective proposed in the plan of STAS in 2006 is now completely obsolete, since most communities where they wanted to implement radio-links already have Movistar or Claro coverage so, consequently, they can connect to the Internet. For this reason we believe that TSF should assess the possibility of change the area or even the country.

- **Interconnection between conventional and VoIP telephony.** Nowadays, the hospital has an OpenVox card installed on the server that allows to call from VoIP phones to conventional ones, but not vice versa. That is to say, from digital to analogue. The interconnection between both technologies would expand the telephony to any department, no matter which system is used.

- **Incorporation of new VoIP phones.** Mainly, in SILAIS and Juan Manuel Morales health centre, for all the reasons given along this report. Due to a lack of resources and Internet connection over there, it was not possible to do so this phase, but it is expected that in the near future conditions will be favourable.

- **Expansion of the NComputing network.** With the foundations laid for this new technology in the frame of the hospital, it is vital to take advantage of it and keep replacing old conventional computers by these ones; or provide communication to new isolated departments with that system.

- **Structured wiring for JMM.** Since the project involves different institutions (not only the hospital), the aid workers could combine the tasks between the hospital and JMM. Over there, with Internet connection, the work could be focused on implementing a structured wiring infrastructure to cover all the departments of the health centre.

WEBGRAPHY and BIBLIOGRAPHY

[1] TELECOS SENSE FRONTERES. “Plan director del sistema de Telemedicina del Atlántico Sur”, 2008.

[2] FURTET CORDERO, Santi. “Telecos Sense Fronteres: Pla de telecomunicacions per a la regió del Kukra River. Fase V”. Director: Roc Messeguer Pallarès. [Final Thesis]. Universitat Politècnica de Catalunya, Enginyeria tècnica de Telecomunicacions (Especialitat Sistemes), 2010.

[3] PALAU ZAIDÍN, Macarena and BENAVIDES GÓMEZ, Jesús. “Telecos Sense Fronteres: Pla de telecomunicacions per a la regió del Kukra River. Fase VI”. Director: Roc Messeguer Pallarès. [Final Thesis]. Universitat Politècnica de Catalunya, Enginyeria tècnica de Telecomunicacions (Especialitat Sistemes), 2011.

[4] HELLSTRÖM, JOHAN (2005). “Bridging the Digital Divide? Self-Manage IT - A Ugandan Case Study”. School of Economics and Commercial Law. Göteborg University. Department of Informatics.

[5] MAX-NEEF, M. et al. (1986). “Desarrollo a escala humana: Una opción para el futuro” Development Dialogue, Nº. Especial; 9-93.

General Context

- Wikipedia, la enciclopedia libre. Nicaragua. http://es.wikipedia.org/wiki/Nicaragua [Reference date: 15/03/2012]
- The World Bank. World Development Indicators database. http://siteresources.worldbank.org/DATASTATISTICS/Resources/GDP.pdf [Reference date: 15/03/2012]
- Operador Telcor. Datos Estadísticos del Sector de las Telecomunicaciones en Nicaragua. http://www.telcor.gob.ni/Desplegar.asp?PAG_ID=14 [Reference date: 15/03/2012]

Maintenance and Improvements

- Grandstream Networks, Inc. Support of GXP280. http://www.grandstream.com/index.php/products/ip-voice-telephony/enterprise-ip-phones/gxp285 [Reference date: 15/03/2012]

- Health software by MINSA. http://www.minsa.gob.ni:8091/PORTAL/ [Reference date: 20/06/2012]
- Software OCSInventory. http://www.ocsinventory-ng.org/en/ [Reference date: 20/04/2012]

VPN

- Wikipedia, la enciclopedia libre. Virtual Private Network. http://en.wikipedia.org/wiki/Virtual_private_network [Reference date: 30/10/2012]
- IVPN, a personal VPN service. PPTP vs L2TP vs OpenVPN. http://www.ivpn.net/knowledgebase/62/PPTP-vs-L2TP-vs-OpenVPN.html [Reference date: 30/10/2012]
- VYPRVPN, VPN service. Comparación de Protocolos VPN-PPTP vs L2TP vs OpenVPN. http://www.goldenfrog.com/ES/vyprvpn/pptp-vs-l2tp-vs-openvpn [Reference date: 30/10/2012]
- OpenVPN, private tunnel. http://openvpn.net/ [Reference date: 12/02/2012]
- NO-IP. The DNS service provider. http://www.no-ip.com/ [Reference date: 01/05/2012]
- Dyn, Managed DNS, Outsourced DNS & Anycast DNS. http://dyn.com/dns/ [Reference date: 01/05/2012]

Radio-link

- Ubiquiti networks. http://www.ubnt.com/ [Reference date: 12/02/2012]
- Ubiquiti networks (Wiki). AirControl Manual de Usuario. http://wiki.ubnt.com/AirControl_Manual_Usuario [Reference date: 12/02/2012]
- COUDÉ, Roger. Software Radio Mobile. http://www.cplus.org/rmw/english1.html [Reference date: 10/05/2012]

Desktop virtualization

- NComputing. Thin Client L300. http://www.ncomputing.com/ [Reference date: 25/01/2012]
- Fox Networks. Thin client Ncomputing L300. http://www.foxnetwork.ru/index.php/en/component/content/article/77--ncomputing-l300.html [Reference date: 25/01/2012]

- VmWare, Virtualización de escritorios. http://www.vmware.com/products/view/overview.html [Reference date: 25/01/2012]
- Citrix. Xen Desktop, the virtual desktop. http://www.citrix.com/English/ps2/products/product.asp?contentID=163057&ntref=mainxdvanityurl [Reference date: 25/01/2012]

Impact project evaluation

- The Max-Neef Model of Human-Scale Development. http://www.rainforestinfo.org.au/background/maxneef.htm [Reference date: 25/05/2012]
- Bridge. Real Access/Real Impact criteria and 12 Habits of Highly Effective ICT-Enabled Development Initiatives. http://www.bridges.org/ [Reference date: 25/05/2012]

APPENDIX A
TECHNICAL ISSUES

APPENDIX I. Telephony VoIP

I.1 Installation of VoIP telephone Grandstream GXP280 (Internal)

Phone configuration

To install and configure a VoIP telephone within the Hospital frame, via the initial web provided by Grandstream (192.168.1.20) we first assigned one of the IP of the network rang: 192.168.1.63 (for Radiology) and 192.168.1.64 (for Warehouse), as well as the mask, gateway and DNS.

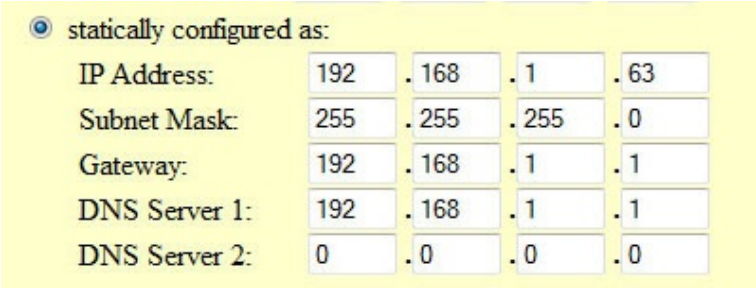


Figure 1. IP table

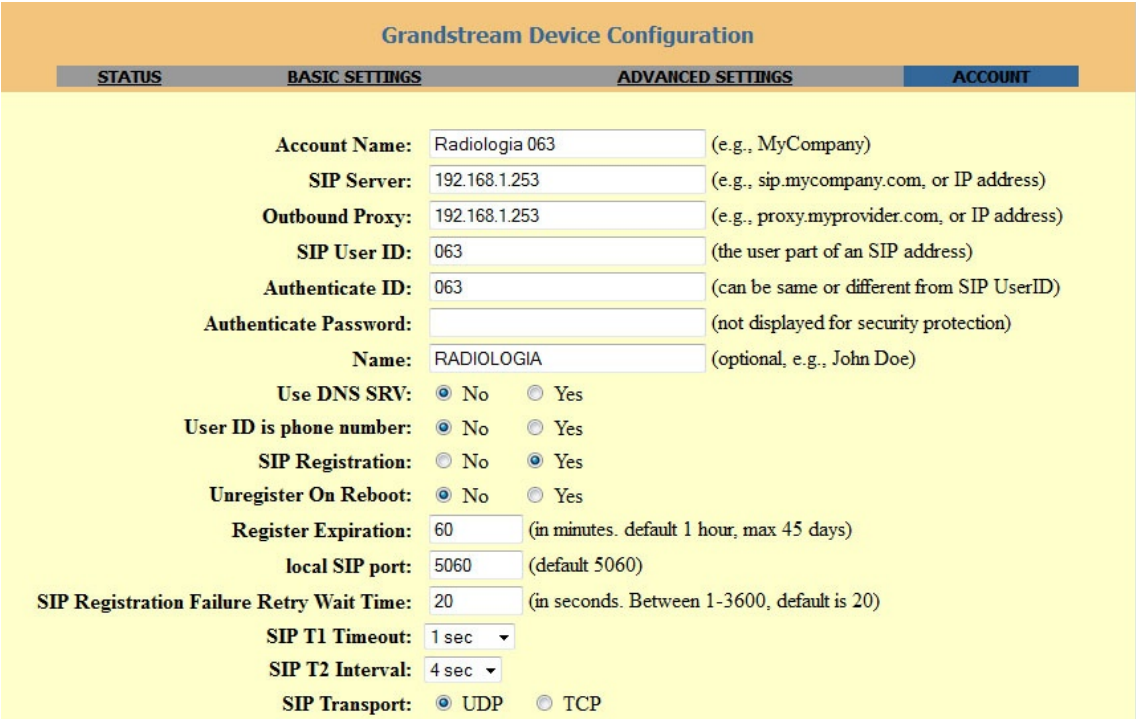


Figure 2. SIP registration for internal phone

Server configuration

Once the telephone was completed, 3 steps needed to be taken into account in the server, where Asterisk is running.

1) *sip.conf*

This file is used to add the SIP register to Asterisk. We added a new user for each department with its features and ID, which matched with the configured IP in order to avoid duplicates or misunderstandings, as follows:

```
;RADIOLOGIA
[063]
type=friend
host=dynamic
username=063
canreinvite=no
callerid=”Radiologia” <63>
qualify=no
nat=no
call-limit=4
```

2) *extensions.conf*

This file is used to monitor the calls between SIP registers and its behaviour among them. That is to say, the dialling, establishment, answering and hang-up of the calls. To define an extension, there must write the word *"exten"* followed by "=>", and then the name of the extension, the priority as well as the application to be executed.

```
[default]
exten=>063,1,Dial(SIP/063)
exten=>063,n,Hangup()
```

3) *General reset*

To end up, both SIP registers and DIALPLAN needed to be reloaded as well as the whole Asterisk system. Afterwards, the telephone was already enabled within the network.

```
asterisk -r
sip reload
dialplan reload
exit
/etc/init.d/asterisk restart
```

I.2 Installation of VoIP telephone Grandstream GXP280 (External)

Phone configuration

To install and configure a VoIP phone external to the Hospital frame, via the initial web provided by Grandstream (192.168.1.20) we assigned one dynamic IP corresponding to the external network rang. The important issue is the usage of the Hospital's public IP as a SIP server (200.62.92.220) so the phone can be identified within our network.

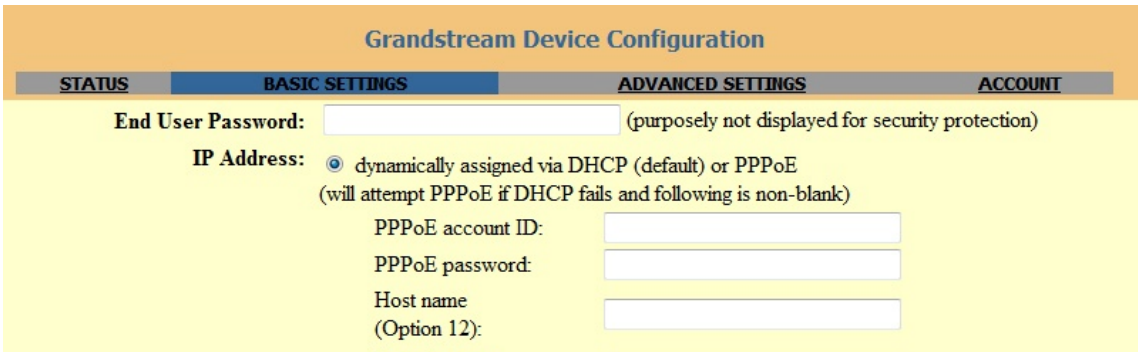


Figure 3. IP dynamically assigned

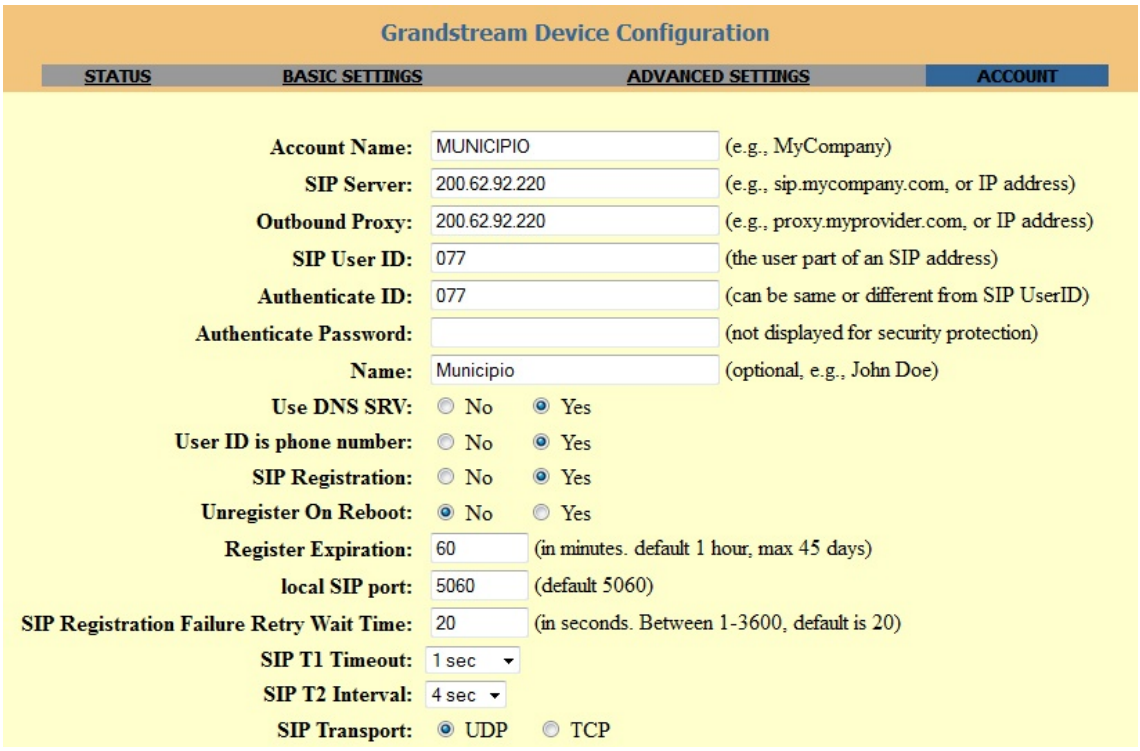


Figure 4. SIP registration for external phone

Server configuration

Once the telephone was completed, 3 steps needed to be taken into account in the server, where Asterisk is running: the configuration of 'sips.conf' and 'extens.conf'

1) *sip.conf*

The 'sip.conf' file specifies the public IP available to the HRESB, although we have the public IP service provider we use DNS discussed above in section 3.5.1 Remote Access.

```
externip = 200.62.92.220
externhost=hresbaccesoremoto.no-ip.org
localnet=192.168.1.0/255.255.255.0
```

There was also added a new user, taking account of putting a password, allowing NAT mechanism and GSM encryption because it is lighter protocol for transmission of audio and, due to having that slow Internet connection the potential problems have to be assessed.

```
[077]
type=friend
username=077
callerid= "municipio" <77>
canreinvite=no
host=dynamic
secret=O9u9PFFK                 ;High security password
nat=yes                         ;Allowing NAT access
qualify=yes
disallow=all
allow=gsm                       ;Allowing GSM protocol
```

Moreover, for the users already in use (those VoIP phones within the HRESB network) is was blocked the access from outside the network with the following commands:

```
[136]
type=friend
secret=136
host=dynamic
canreinvite=no
callerid="Fisioterapia" <136>
qualify=yes
nat=no
call-limit=4
deny=0.0.0.0/0.0.0.0
permit=192.168.1.0/255.255.255.0
```

2) *extensions.conf*

Besides introducing a new phone on the Asterisk PBX, one must specify to what extension and which process will follow when establishing a call. The settings used was:

```
exten=>077,1,Dial(SIP/municipio,30,g)
exten=>077,n,Goto(dailing-options,s-${DIALSTATUS},1)
```

APPENDIX II. IP Network Inventory

Over time, many and many units have been added to the hospital network. Eventually, this has lead to a mess of IP and devices. In order to make things clear, this chapter lists which devices have been configured with static IP and which are running with dynamic ones. The criteria relies on its performance. That is to say, the specific devices which strictly need to be part of the network are set-up with static IP. The rest (all the computers and laptops spread over the departments) just by dynamic IP.

II.1 Static IP

It ranges from “192.168.1.1” to “192.168.1.79” with the exception of the 2 servers.

General			
192.168.1.1	Router Biblioteca	192.168.1.11	Biblioteca Dra Castro
192.168.1.5	VPN Access	192.168.1.12	Biblioteca Dell
192.168.1.6	VPN User	192.168.1.252	Servidor Gestión
192.168.1.7	VPN User	192.168.1.254	Servidor Asterisk
192.168.1.8	VPN User	200.62.64.1	DNS Principal
192.168.1.9	VPN User	200.62.64.65	DNS Alternativo
192.168.1.10	Impresora Canon		
N-Computing		**VoIP Telephony**	
192.168.1.20	Servidor	192.168.1.50	Emergencias
192.168.1.21	Biblioteca 1	192.168.1.51	P/S La Aurora
192.168.1.22	Cirugía	192.168.1.52	Biblioteca
192.168.1.23	Biblioteca 2	192.168.1.53	Pediatría
		192.168.1.54	Gineco/Obstetricia
Radio links		192.168.1.55	Cirugía/Ortopedia
192.168.1.40	AirGrid HRESB	192.168.1.56	Medicina
192.168.1.41	AirGrid Cerro	192.168.1.57	Estadísticas
192.168.1.42	Bullet Cerro-La Aurora	192.168.1.58	Consulta Externa
192.168.1.43	Bullet La Aurora	192.168.1.59	Quirófano

192.168.1.44	Bullet Cerro-MP	192.168.1.60	Neonato
192.168.1.45	Bullet Monkey Point	192.168.1.61	Servicios SSR
192.168.1.46	AirGrid MP-P/S	192.168.1.62	P/S Monkey Point
192.168.1.47	AirGrid P/S MP	192.168.1.63	Radiología
		192.168.1.64	Bodega

Table 21. List of static IP

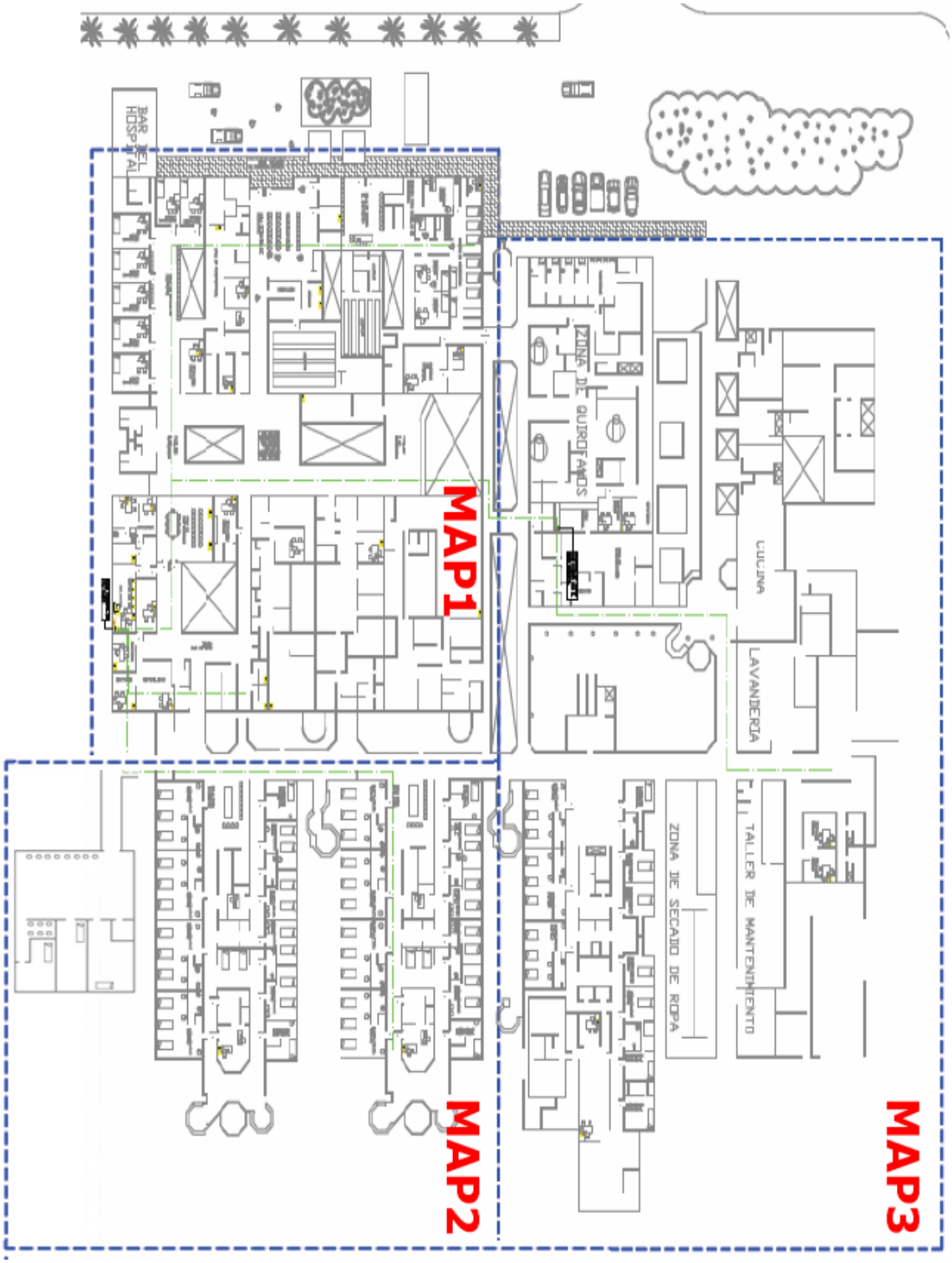
II.2 Dynamic IP

It ranges from “192.168.1.80” to “192.168.1.250”

Department	Nº of units	Department	Nº of units
Administración	1	Nefrología	2
Auditorio	1	Patología	1
Bodega	2	Radiología	1
Colposcopía	1	Recursos Humanos	1
Contabilidad	2	Rosa Rivas	1
Dirección	1	Servicios Generales (Jorge)	1
Epidemiología	1	Subdirección	1
Estadísticas	2	Trabajo Social	1
Farmacia	1	Ultrasonidos	1
Fisioterapia	1		

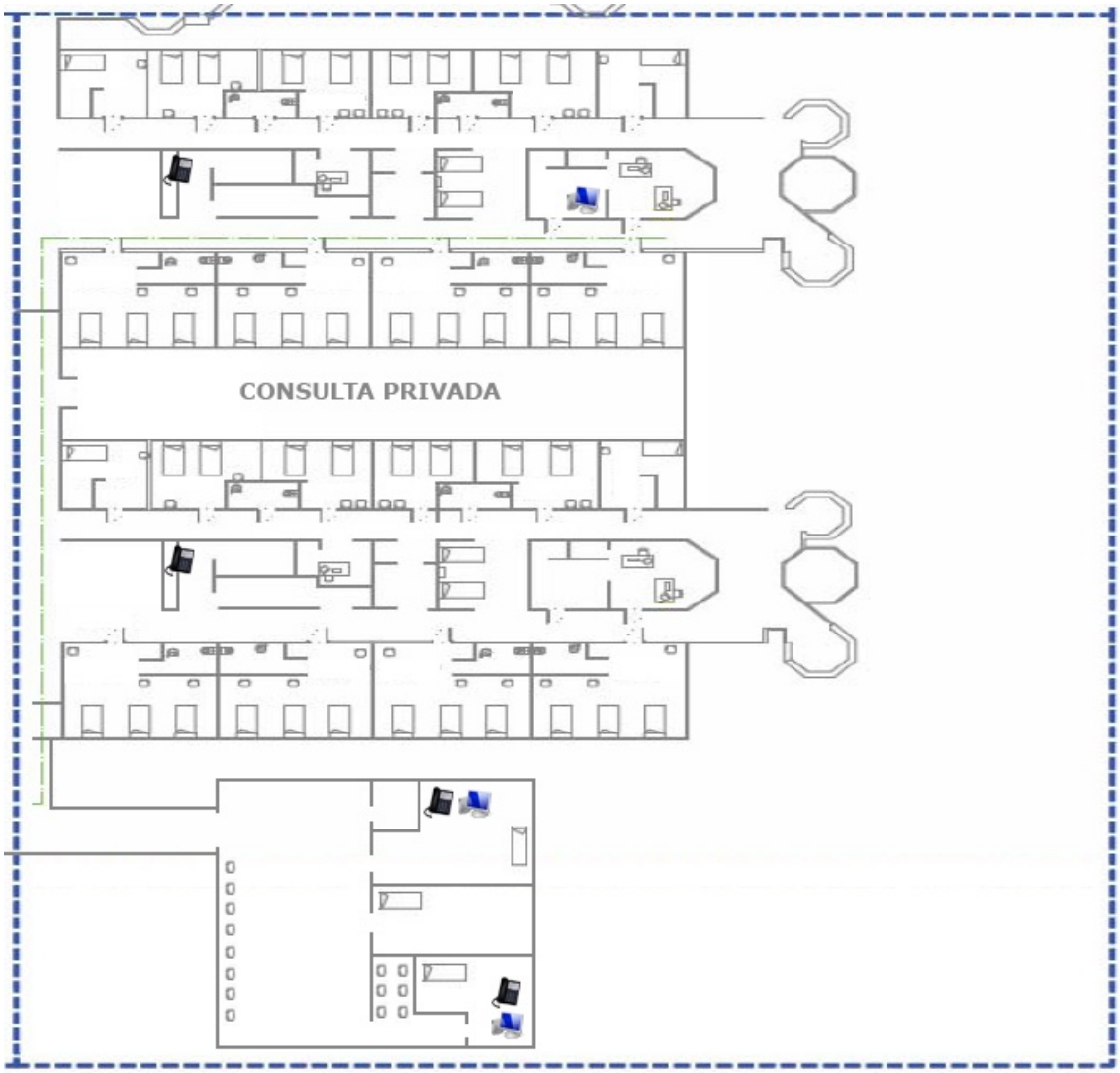
Table 22. List of dynamic IP by departments

II.3 Maps of the hospital with units installed

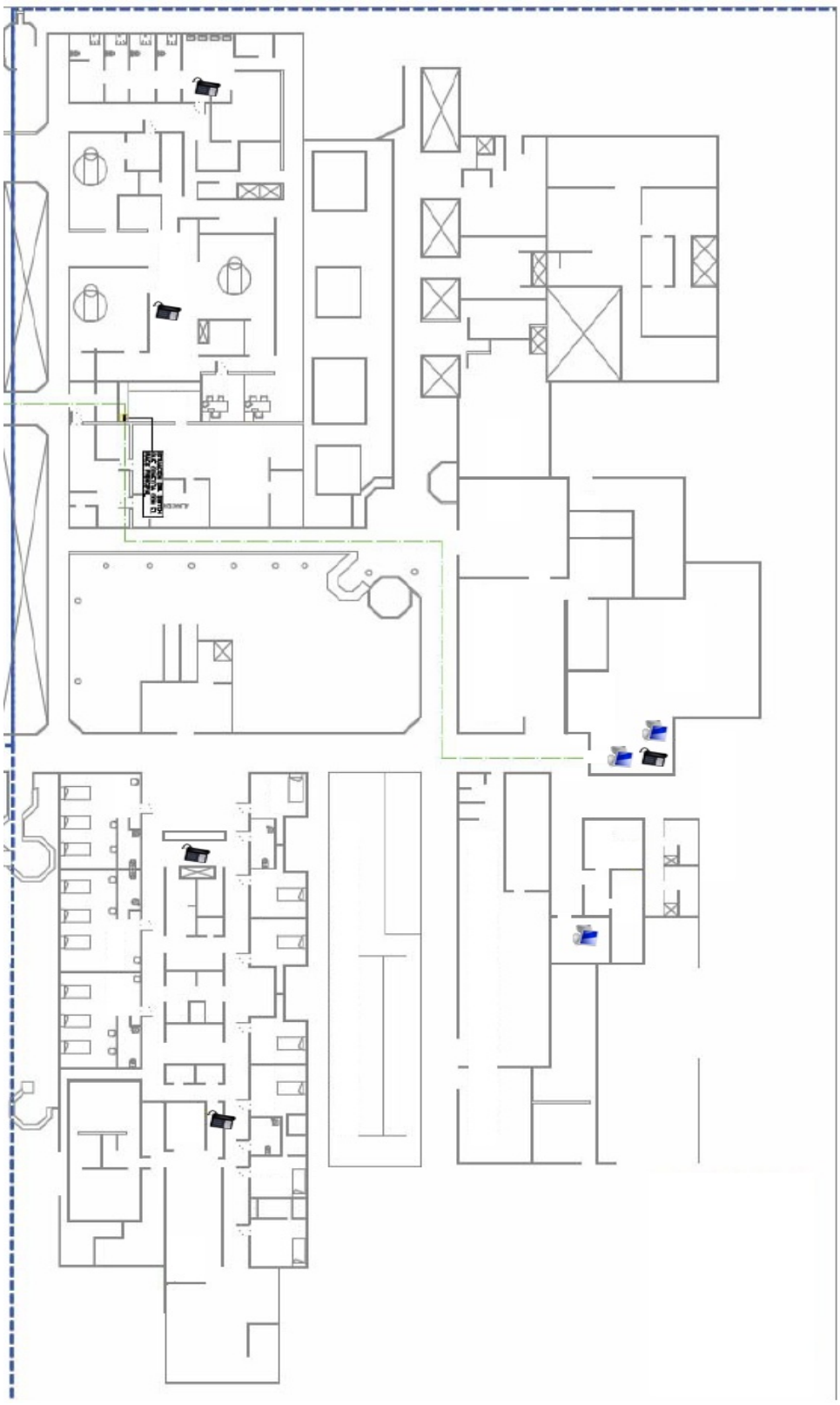


MAP 1

MAP 2



MAP 3



APPENDIX III. OpenVPN Configuration

III.1 Server configuration

First of all, we install both OpenVPN and security OpenSSL packages.

```
sudo apt-get -y install openvpn
sudo apt-get -y install openssl
```

Configure the OpenVPN daemon not to boot the system automatically.

```
sudo nano /etc/default/openvpn
```

Remove the start-up script to not start without configuring it.

```
sudo update-rc.d -f /etc/init.d/openvpn remove
```

openvpn.conf file is created in the /etc/openvpn/

```
sudo nano /etc/openvpn/server.conf
```

There, write the following settings:

```
dev tun
proto udp
port 1194
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
dh /etc/openvpn/keys/dh2048.pem
user nobody
group nogroup
server 10.6.0.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/clients.txt
status /etc/openvpn/status.txt
persist-key
persist-tun
push "redirect-gateway def1"
push "route 192.168.0.0 255.255.255.0"
keepalive 10 120
verb 3
comp-lzo
```

Now create the script to configure and start the vpn server.

```
sudo nano /etc/init.d/vpnserver
```

Paste this code, changing the range of IP's, when necessary.

```
#!/bin/sh
#
vpnserver_start()
{
 echo "VPN Server [OK]"
```

```
 echo 1 > /proc/sys/net/ipv4/ip_forward
 /etc/init.d/networking restart  > /dev/null
  /sbin/iptables -t nat -A POSTROUTING -s 10.6.0.0/24 -o eth0 -j
MASQUERADE
    /usr/sbin/openvpn    --config    /etc/openvpn/server.conf    2>>
/etc/openvpn/error.txt 1>> /etc/openvpn/normal.txt &
}
vpnserver_stop()
{
 echo "VPN Server [NO]"
 /usr/bin/killall "openvpn"
 iptables -F
 iptables -X
 /etc/init.d/networking restart > /dev/null
}
vpnserver_restart()
{
  vpnserver_stop
  sleep 1
  vpnserver_start
}
#
case "$1" in
 'start')
   vpnserver_start
  ;;
 'stop')
   vpnserver_stop
  ;;

 'restart')
   vpnserver_restart
  ;;
 *)
  vpnserver_start
 ;;
esac
```

Assign execute permissions to the script.

```
sudo chmod +x /etc/init.d/vpnserver
```

Configure to auto start with the system.

```
sudo update-rc.d vpnserver defaults
```

Afterwards, OpenVPN is already configured. Now you have to activate the TUN module in the kernel.

```
sudo modprobe tun
sudo echo "tun" >> /etc/modules
```

Create the authentication keys. By copying the example of easy-, we create the entity, certificates, and encryption keys, which use OpenVPN.

```
sudo cp -R /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
```

Now enter the folder where the utilities were copied and create the keys. Be aware that all the keys must be in the same folder to avoid duplicates.

```
sudo cp -R /usr/share/doc/openvpn/examples/easy-rsa/ /etc/openvpn/
cd /etc/openvpn/easy-rsa/2.0
sudo mkdir keys
```

Finally, edit the vars file that is in the folder /etc/openvpn/easy-rsa/2.0

```
sudo nano /etc/openvpn/easy-rsa/2.0/vars
```

There, we must update the following values:

```
export OPENSSL="openssl"
export PKCS11TOOL="pkcs11-tool"
export GREP="grep"
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA`
export KEY_DIR="/etc/openvpn/easy-rsa/2.0/keys"

export PKCS11_MODULE_PATH="dummy"
export PKCS11_PIN="dummy"
export KEY_SIZE=2048
export CA_EXPIRE=3650
export KEY_EXPIRE=3650
export KEY_COUNTRY="NIC"
export KEY_PROVINCE="RAAS"
export KEY_CITY="Bluefields"
export KEY_ORG="HRESB"
export KEY_EMAIL="genismauri@gmail.com"
```

Need to run.

```
source ./vars
```

There must be cleaned in case there are entities, certificates and keys.

```
./clean-all
```

Now we generate Diffie Hellman security 2048 bits.

```
./build-dh
```

Then, we generate the certificate authority.

```
./build-ca
```

At this point, to generate keys and certificates, we first start by the server ones.

```
./build-key-server server
```

Continue with the certificates and keys for the client.

```
./build-key clientehresb
```

This step must be repeated for each customer or user who wants to connect to the VPN. Finally we check out if all the files are in the right place, in the folder

```
/etc/openvpn/keys
```

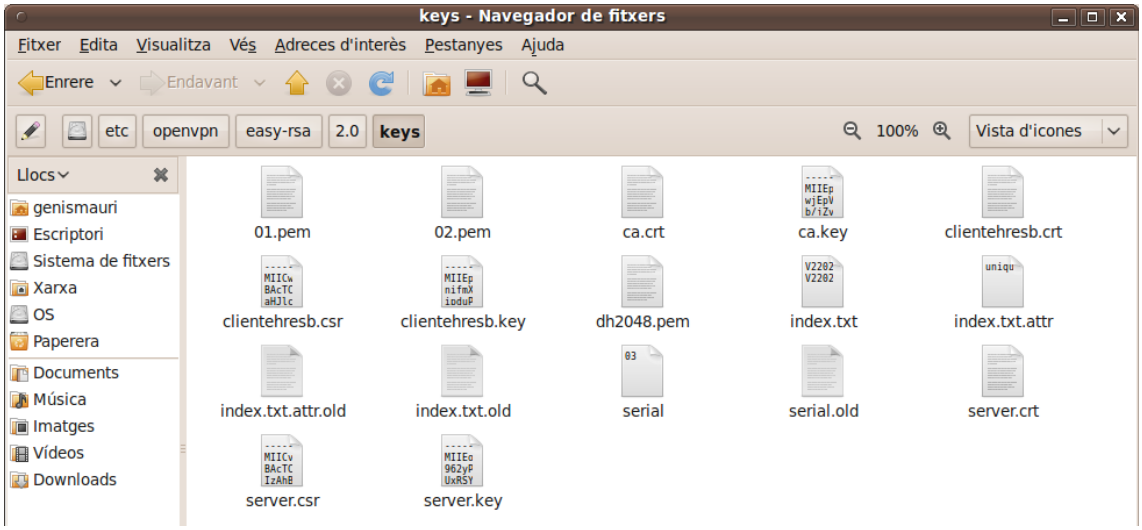


Figure 5. Keys and certificates created, both for server and client

Then, create a file that OpenVPN generates itself.

```
sudo openvpn --genkey --secret ta.key
```

Start the server to verify that everything worked out.

```
sudo /etc/init.d/vpnserver start
```

III.2 Client configuration in Windows

The first step is to download the OpenVPN application written for Windows. All downloads are available on the official website of the software:

http://openvpn.se/download.html

After the installation, the following step is to configure OpenVPN. You must access the folder that was created after the installation.

```
C:\Program Files\OpenVPN\sample-config
```

And take the client configuration file *client.ovpn*, and copy it to:

```
C:\ProgramFiles\OpenVPN\config
```

Which will be modified to connect to the VPN server.

```
client
dev tun
proto udp

remote 192.168.1.28 1194
resolv-retry infinite
nobind
mute-replay-warnings

ca ca.crt
cert clientehresb.crt
```

```
key clientehresb.key

comp-lzo
tun-mtu 1500

keepalive 10 120
verb 4

route-method exe
route-delay 2
```

Also as noted in the previous section after completing the certificates, keys and signatures of the client to the server, we have to copy the same files to the folder where *client.ovpn* is stored. These files are *ca.crt*, *clientehresb.crt* and *clientehresb.key*. As we can see in the configuration script it has to be detailed the names of the security certificates.

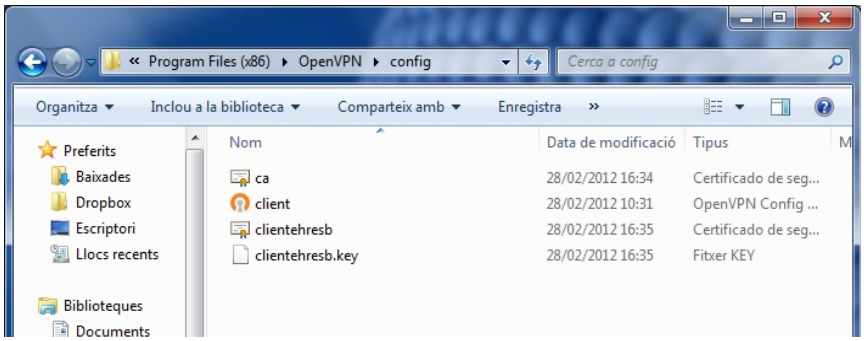


Figure 6. Keys and certificates for windows client

To connect as a client, first of all OpenVPN should be running in the server. Then, we can access and run OpenVPN windows always as administrator. We see an icon in the toolbar of Windows (there are 2 PC's in red with a globe), which represents the GUI of OpenVPN. Right-click should select the option to "Connect."

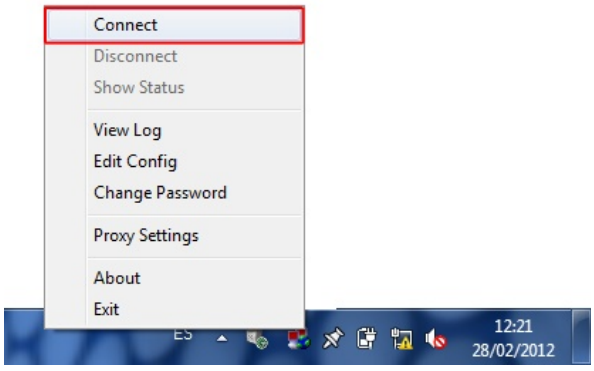


Figure 7. OpenVPN connection in Windows

In the OpenVPN screen it can be seen the steps to confirm and execute the VPN connection.

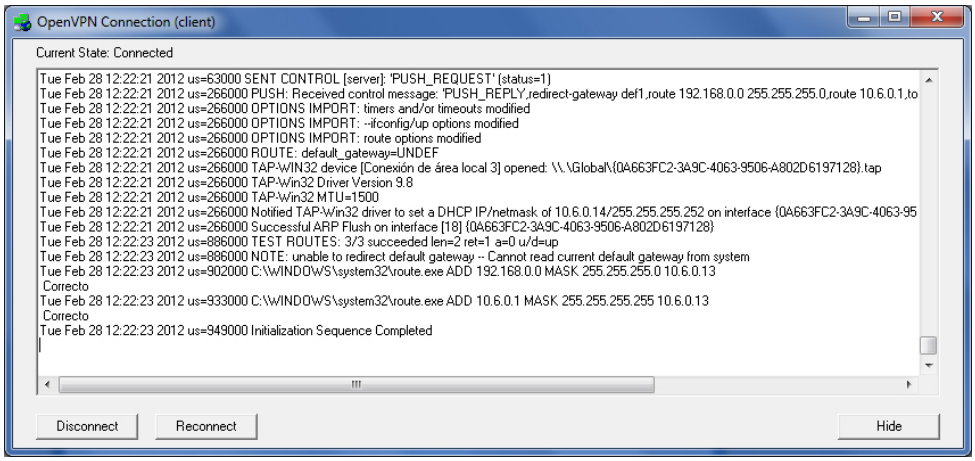


Figure 8. Steps for OpenVPN connection in Windows

Once the connection has been established, the icon with the two PC's in red, changes to green, and if we hover the mouse over it, will shows that the connection is made as a client, as well as the date and connection time and the IP which has been assigned. If the connection is lost at some point, the icon becomes yellow, then red.

Figure 9. Execution of OpenVPN connection

To verify the VPN connection it can be executed the *ipconfig* command in the console.

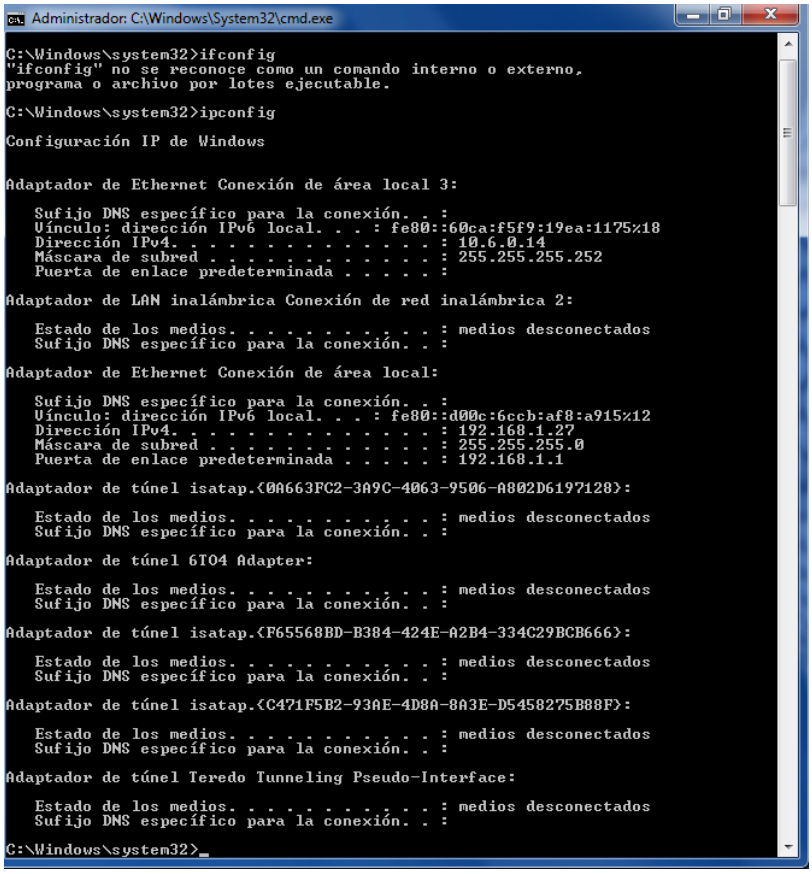


Figure 10. Verification of VPN connected

When the VPN connection is performed a problem with the Internet connection is detected. As it can be seen in the figure below, destination 0.0.0.0 is sent to the eth0 and the tun0 interface at the same time.

Figure 11. Windows routing table without Internet connection

The problem was solved by modifying the routing table, deleting the conflicted destinations and adding the correct. It has to be taken into account that the consola has to be running as a administrator to modify the routing table.

```
route DELETE 0.0.0.0
route ADD 0.0.0.0 MASK 255.255.255.0 192.168.1.1 METRIC 21
```

The final table configuration is detailed in the next figure.

```
===========================================================================
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0    255.255.255.0     192.168.1.1     192.168.1.27     41
         10.6.0.1  255.255.255.255       10.6.0.13       10.6.0.14     31
        10.6.0.12  255.255.255.252       En vínculo      10.6.0.14    286
        10.6.0.14  255.255.255.255       En vínculo      10.6.0.14    286
        10.6.0.15  255.255.255.255       En vínculo      10.6.0.14    286
        127.0.0.0        255.0.0.0       En vínculo      127.0.0.1    306
        127.0.0.1  255.255.255.255       En vínculo      127.0.0.1    306
  127.255.255.255  255.255.255.255       En vínculo      127.0.0.1    306
        128.0.0.0        128.0.0.0         10.6.0.13       10.6.0.14     31
      192.168.0.0    255.255.255.0         10.6.0.13       10.6.0.14     31
      192.168.1.0    255.255.255.0       En vínculo      192.168.1.27    276
     192.168.1.27  255.255.255.255       En vínculo      192.168.1.27    276
     192.168.1.28  255.255.255.255       192.168.1.1     192.168.1.27     21
    192.168.1.255  255.255.255.255       En vínculo      192.168.1.27    276
        224.0.0.0        240.0.0.0       En vínculo      127.0.0.1    306
        224.0.0.0        240.0.0.0       En vínculo      192.168.1.27    276
        224.0.0.0        240.0.0.0       En vínculo      10.6.0.14    286
  255.255.255.255  255.255.255.255       En vínculo      127.0.0.1    306
  255.255.255.255  255.255.255.255       En vínculo      192.168.1.27    276
  255.255.255.255  255.255.255.255       En vínculo      10.6.0.14    286
===========================================================================
```

Figure 12. Windows routing table with Internet connection

III.3 Client configuration in Linux

First of all, we install both OpenVPN and security OpenSSL packages.

```
sudo apt-get -y install openvpn
sudo apt-get -y install openssl
sudo aptitude -y install network-manager-openvpn
```

The next step is to configure the script *cliente.conf*, located in the folder /etc/openvpn/config

```
client
dev tun
proto udp
remote 192.168.1.28 1194
resolv-retry infinite
nobind
mute-replay-warnings
ca ca.crt
cert clientehresb.crt
key clientehresb.key
comp-lzo
tun-mtu 1500
keepalive 10 120
verb 4
route-method exe
route-delay 2
```

Copy the files *ca.crt*, *clientehresb.key* and *clientehresb.crt,* created by the server, in the same folder where the script *cliente.conf* is stored.

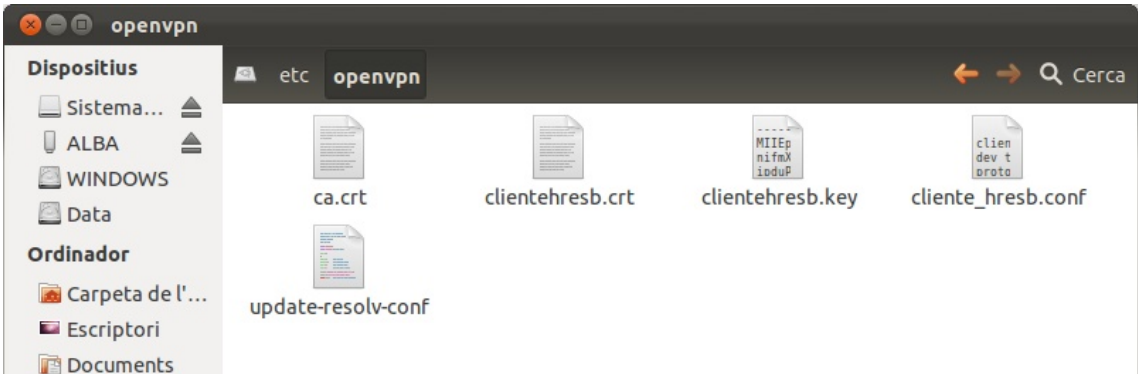


Figure 13. Keys and certificates for Linux client

To run the client just follow the commands:

```
sudo /etc/init.d/openvpn start
```

As explained in the windows client configuration a problem with Internet connection was detected and solved changing the routing table.

```
alba@alba:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.6.0.13       128.0.0.0       UG        0 0          0 tun0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
10.6.0.1        10.6.0.13       255.255.255.255 UGH       0 0          0 tun0
10.6.0.13       0.0.0.0         255.255.255.255 UH        0 0          0 tun0
128.0.0.0       10.6.0.13       128.0.0.0       UG        0 0          0 tun0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
192.168.0.0     10.6.0.13       255.255.255.0   UG        0 0          0 tun0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
192.168.1.28    192.168.1.1     255.255.255.255 UGH       0 0          0 eth0
alba@alba:~$
```

Figure 14. Linux routing table without Internet connection

The command used for the table modification was the following:

```
sudo route del -net 0.0.0.0 netmask 0.0.0.0 dev tun0
sudo route add -net 0.0.0.0 gw 192.168.1.1 netmask 0.0.0.0 dev eth0
```

```
alba@alba:~$
alba@alba:~$ netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
10.6.0.1        10.6.0.13       255.255.255.255 UGH       0 0          0 tun0
10.6.0.13       0.0.0.0         255.255.255.255 UH        0 0          0 tun0
128.0.0.0       10.6.0.13       128.0.0.0       UG        0 0          0 tun0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
192.168.0.0     10.6.0.13       255.255.255.0   UG        0 0          0 tun0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
192.168.1.28    192.168.1.1     255.255.255.255 UGH       0 0          0 eth0
alba@alba:~$
```

Figure 15. Linux routing table with Internet connection

APPENDIX IV. Windows 7 VPN

IV.1 New users in PPTP

The first step **in order to** connect to the VPN HRESB is to create new users in the PPTP with the following command.

```
nano /etc/ppp/chap-secrets
```

Two users were configured for us (albaboj – genis), plus a generic user for the rest of cooperating TSF (tsf). In the following figure it can be seen the script modified.

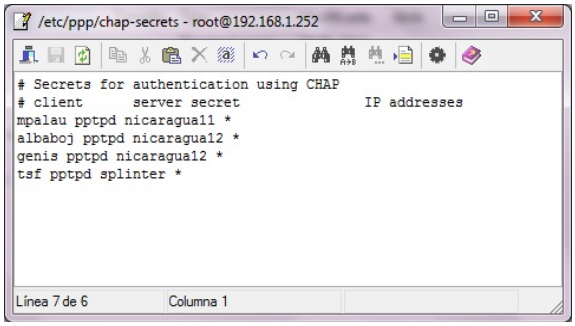


Figure 16. Chap-secrets script

IV.2 Windows 7 VPN configuration

The following figures show the steps to configure a VPN in Windows 7.

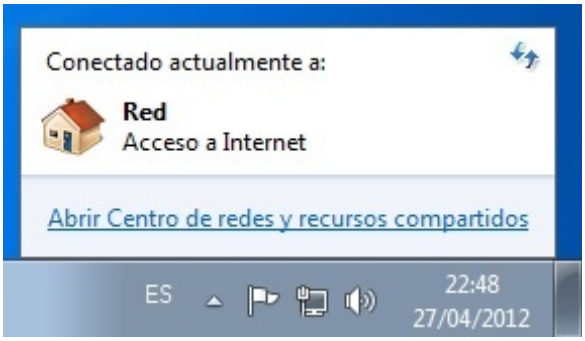


Figure 17. Windows 7 VPN configuration (1)

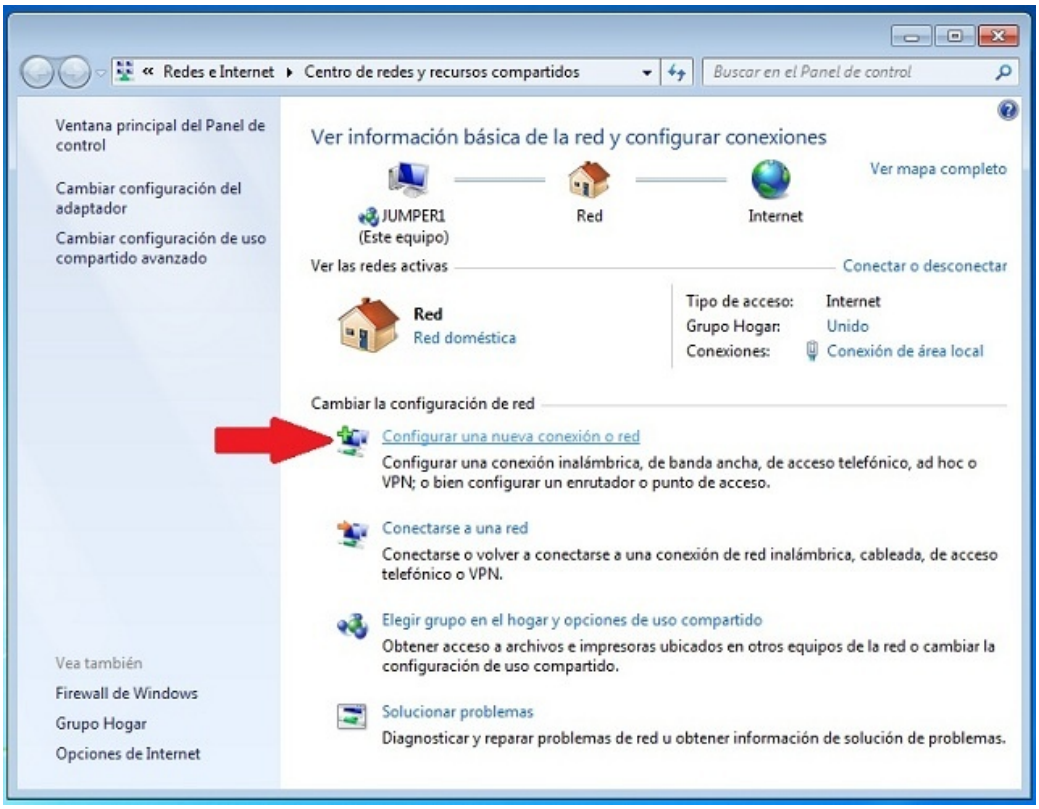


Figure 18. Windows 7 VPN configuration (2)

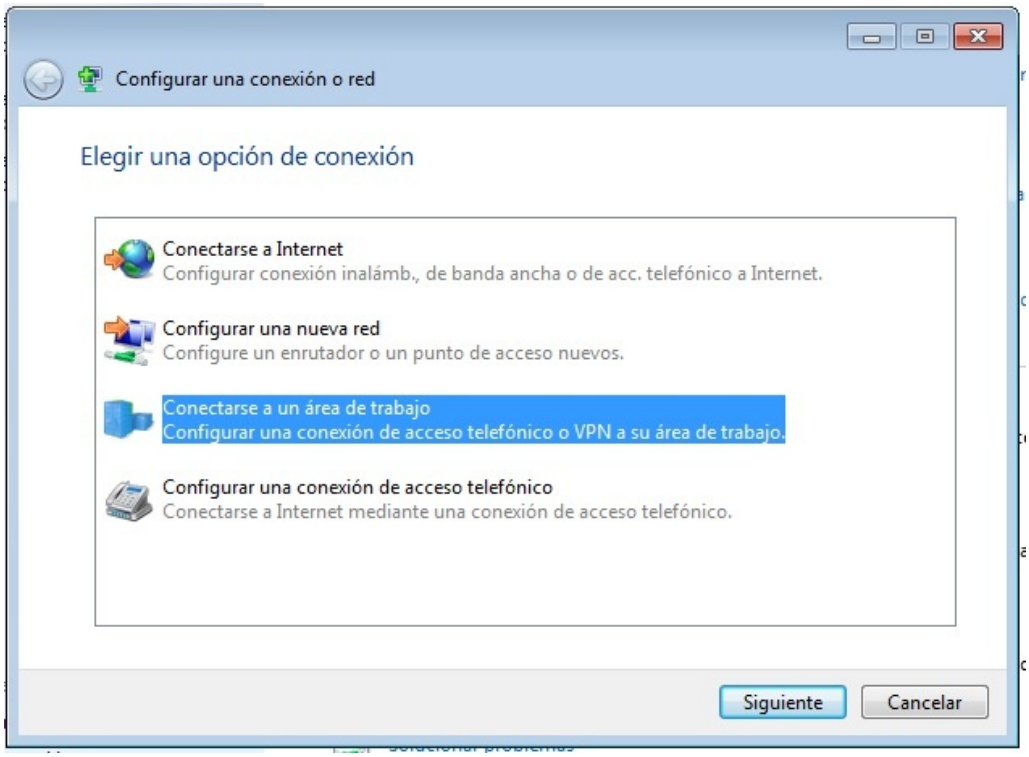


Figure 19. Windows 7 VPN configuration (3)

Figure 20. Windows 7 VPN configuration (4)

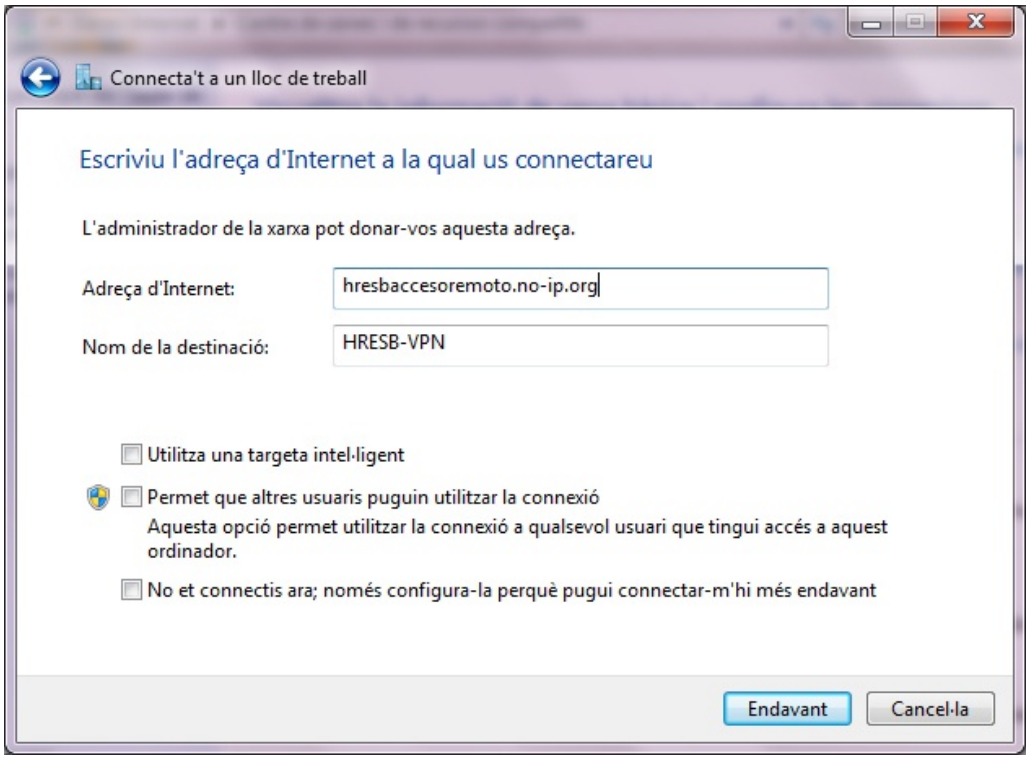


Figure 21. Windows 7 VPN configuration (5)

In order to resolve the Internet access problems when the VPN is connected it has to be configured the following options in the properties of the VPN created.

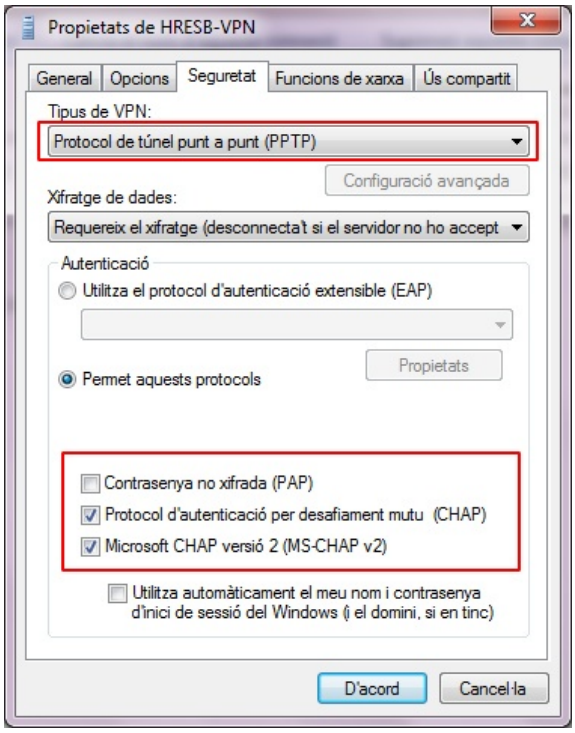


Figure 22. Windows 7 VPN configuration (6)

Also the *Funciones de xarxa> Protocolo de Internet versión 4 (TCP/Ipv4)> Propiedades > Opciones Avanzadas.*

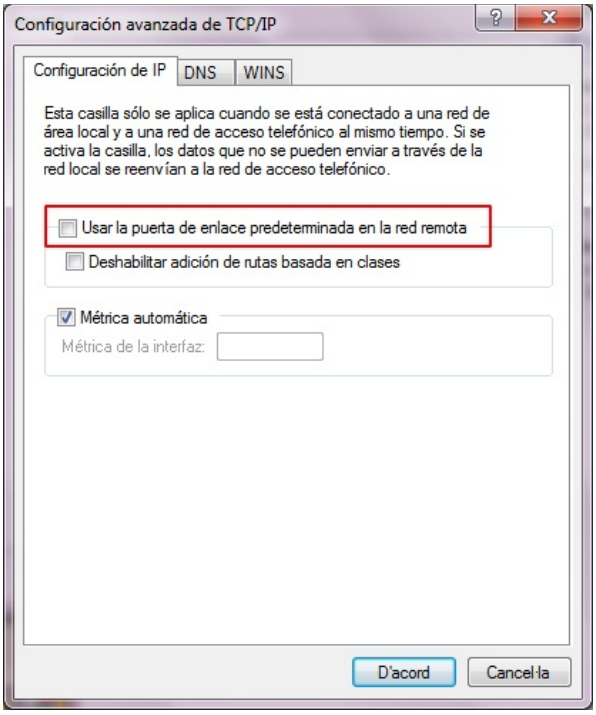


Figure 23. Windows 7 VPN configuration (7)

Finally we can stablish the VPN connection with our user and password.

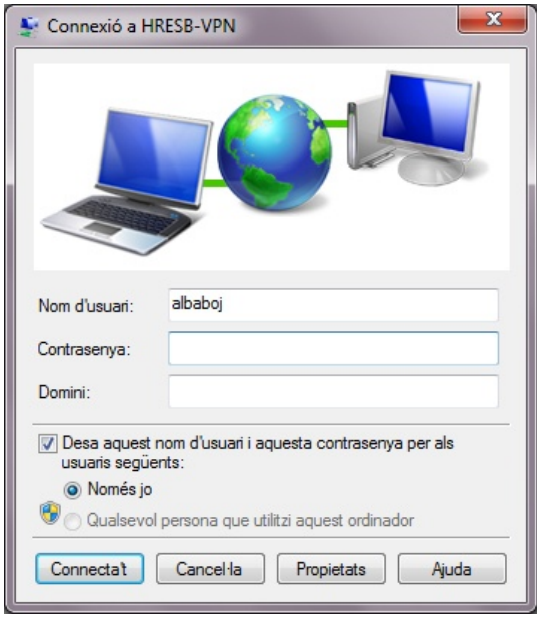


Figure 24. Windows 7 VPN configuration (8)

APPENDIX V. Samba

V.1 Getting Samba configured

The first step is to install samba, then create a new empty file where all the configuration will be done, and finally to open the file inside an editor:

```
sudo apt-get install samba
sudo touch /etc/samba/smb.conf
sudo gedit /etc/samba/smb.conf
```

V.2 'smb.conf' configuration

This is the main file it needs to be configured, located in /etc/samba/smb.conf.
It details the global settings in terms of workgroup or interfaces. Afterwards, *homes*, *netlogon* and *profiles* are referred to the management of users (creation of names and passwords). First of all, it is analysed each parameter, followed by the configuration.

[globals]

workgroup = lab. This line assigns the task force. Clients who want access to their resources must belong to the same work-group. Importantly, should be the same workgroup name than Windows. Otherwise Windows computers will not access samba resources in Linux computers.
netbios name = genismauri. Name that appears on the network server.
server string = Samba Server version %v. This command allows to add a welcome message for the Samba server. Adding %v, displays the version number of Samba.

printcap name = cups
printing = cups
disable spoolss = yes
show and printer wizard = no
These lines allow to share all printers on the remote computer.

hosts allow = 10.6.0.
interfaces = 10.6.0.1/24 10.6.0.
With the above two lines, it is possible to allow access only to certain networks to the server (the end point in “interfaces” is important because it indicates that all the network ranking 10.6.0.X is included).

The following lines explains how to share a folder on your computer:

[MyFiles]. Name that appears in the shared folder.

path = /home/pbruna/dades. Path to the resource. This folder must exist so it must be created beforehand.
read only = no. Defining the resource not just able to be read.
guest ok = yes. Allows access in guest mode.
browseable = no. Permission for reading on the resource.
writable = yes. Permission for writing on the resource.
create mask = 0777. Permissions when creating files.
directory mask = 0777. Defining permissions when creating sub-files.

Finally, there are listed the different items enabled to be shared, such as printers or folders, with the valid users and its privileges for each one.

[printers]

path = /var/lib/samba/printers. Path to the resource.
printable = yes. Important to enable this action in all printer shares (and / or [printers]) so Samba can recognise that it comes to printers.
browseable = no. Permission for reading on the resource.
guest ok = yes. Allows access in guest mode.
write list = root. Defines who is the printer administrator.
create mask = 0664. Permissions when creating files.
directory mask = 0775. Defining permissions when creating sub-files.

The configuration used for our scenario is shown below.

```
[global]
	netbios name = genismauri
	workgroup = lab
	announce version = 5.0
	socket options = TCP_NODELAY IPTOS_LOWDELAY SO_KEEPALIVE
SO_RCVBUF=8192 SO_SNDBUF=8192
	host allow = 10.6.0.
	interfaces = 10.6.0.1/24 10.6.0.
	bind interfaces only = yes

	security = user
	null passwords = true
	usershare owner only = false
	name resolve order = hosts wins bcast

	wins support = yes
	printcap name = CUPS
	syslog only = yes
	server string = &h samba 3.4.0
	username map = /etc/samba/smbusers
```

```
[homes]
       valid users = %S
       create mode = 0600
       browseable = no
       read only = no
       veto files = /*.{*}/.*/mail/bin/

[netlogon]
       path = /var/lib/samba/netlogon
       admin users = Administrator
       valid users = %U
       read only = no
       available = no
       browsable = no

[Profiles]
       path = /var/lib/samba/profiles
       valid users = %U
       create mode = 0600
       directory mode = 0700
       available = no
       browsable = no
       writable = yes

[print$]
       path = /var/lib/samba/printers
       guest ok = yes
       write list = root
       create mask = 0664
       directory mask = 0775

[printers]
       path = /tmp
       printable = yes
       guest ok = yes
       browseable = no


[MyFiles]
       path = /home/samba/
       writeable = yes
       create mask = 0644
       directory mask = 0755
       force user = genismauri
       force group = genismauri
       browseable = yes
       valid users = genismauri, alba
```

V.3 Starting samba and setting up user accounts

Once *smb.conf* is set up, we have to create valid accounts with password for each of the users. It is possible to create as many accounts as necessary, always following these instructions:

```
sudo useradd -s /bin/true genismauri
sudo smbpasswd -L -a genismauri
sudo smbpasswd -L -e genismauri
```

The "-s /bin/true" in the first line prevents the users from being able to access the command-line of our Linux box.

V.4 Security consideration

Finally, we share the folders we are interested in, giving permissions of reading or writing (Figure 23) to the specific users (Figure 24). An overview shows the privileges for each of the directories we are dealing with.

Figure 25. Editing permissions of a shared folder

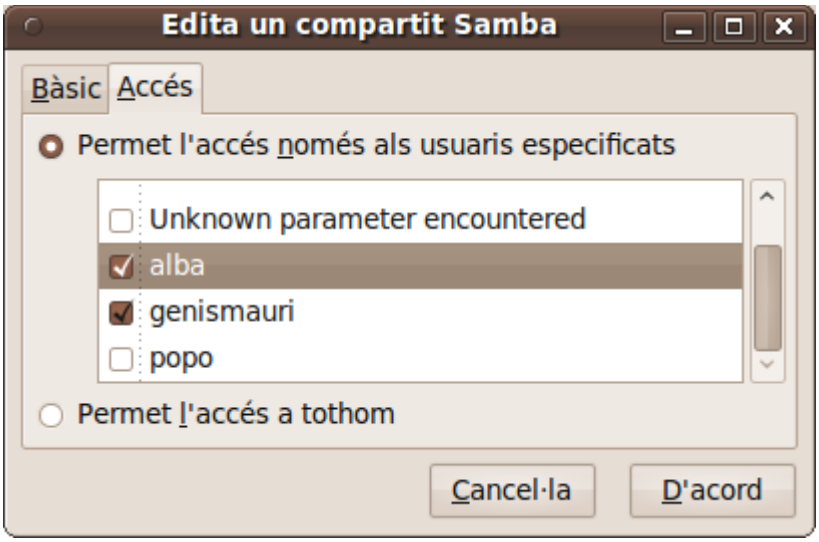


Figure 26. Editing users allowed

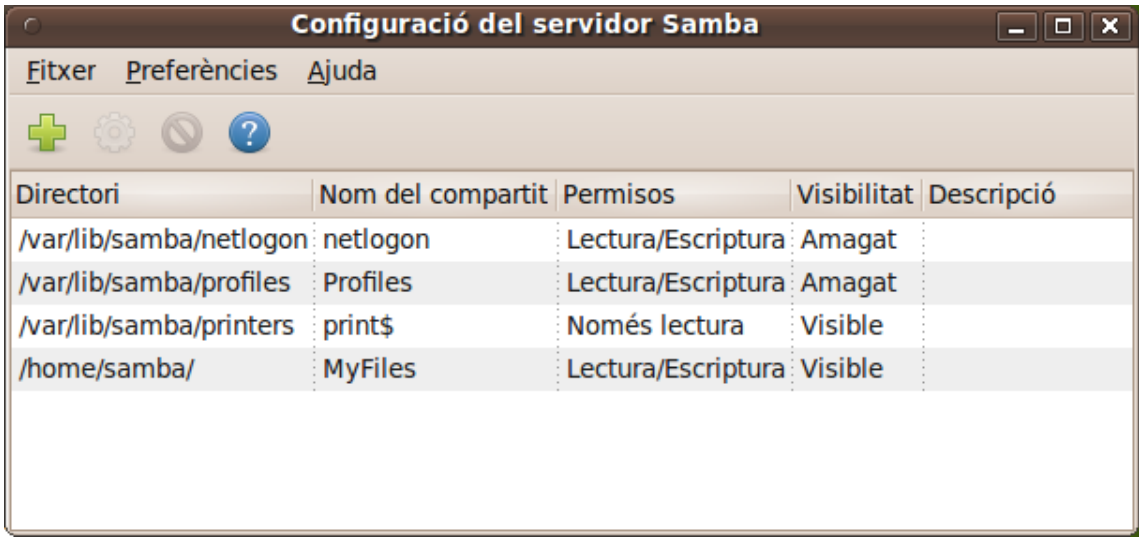


Figure 27. Overview of shared directories

It is also important to enable server's firewall (in our case 'Firestarter') and allow the connections for each IP (or a whole range). Sometimes, even though allowed via *smb.conf* file, the firewall yet blocks the interfaces. The users connected through these IP's can log in and have access to the shared documents:

Figure 28. Firestarter enabled

V.5 Samba installation on Linux client (Ubuntu 9.10)

To install the Ubuntu client you have to install the Samba package with the following command:

```
sudo apt-get install samba samba-client smbfs smbclient
```

In order to access to the shared folders, it has to open a folder and in the address bar we have to enter:

`smb://10.6.0.1`, where IP is the tunneling IP of the server.

Shared folders appear in the network when the access is successful. To access each of them, the system asks user name and password.

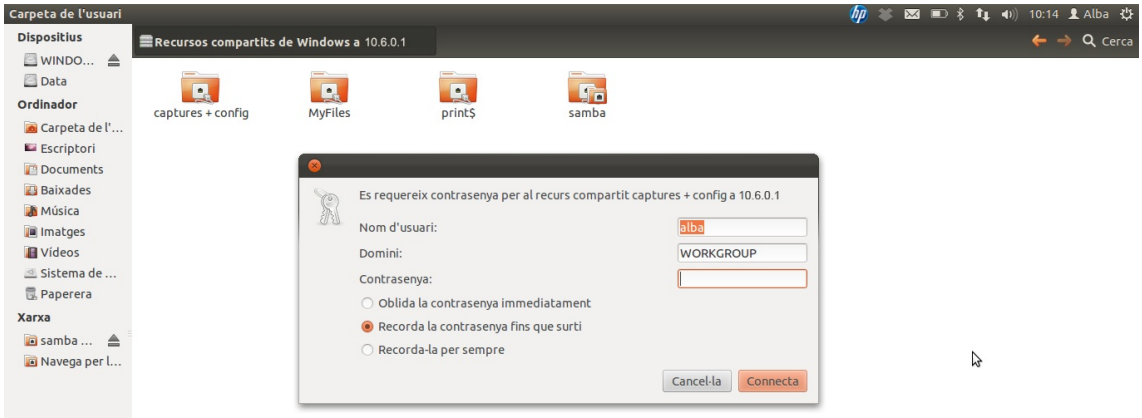


Figure 29. Samba access in Ubuntu client

If the user name and password are correct, we can access to all documents.

Figure 30. Shared folder on Samba

V.6 Samba installation on Windows client (Windows 7)

In order to access to the shared folders created within Linux' server, we have to do the following steps. First of all, the shared network options need to be enabled. Settings can be changed at: *Tauler de control>Xarxa i Internet>Centre de xarxes I de recursos compartits.*

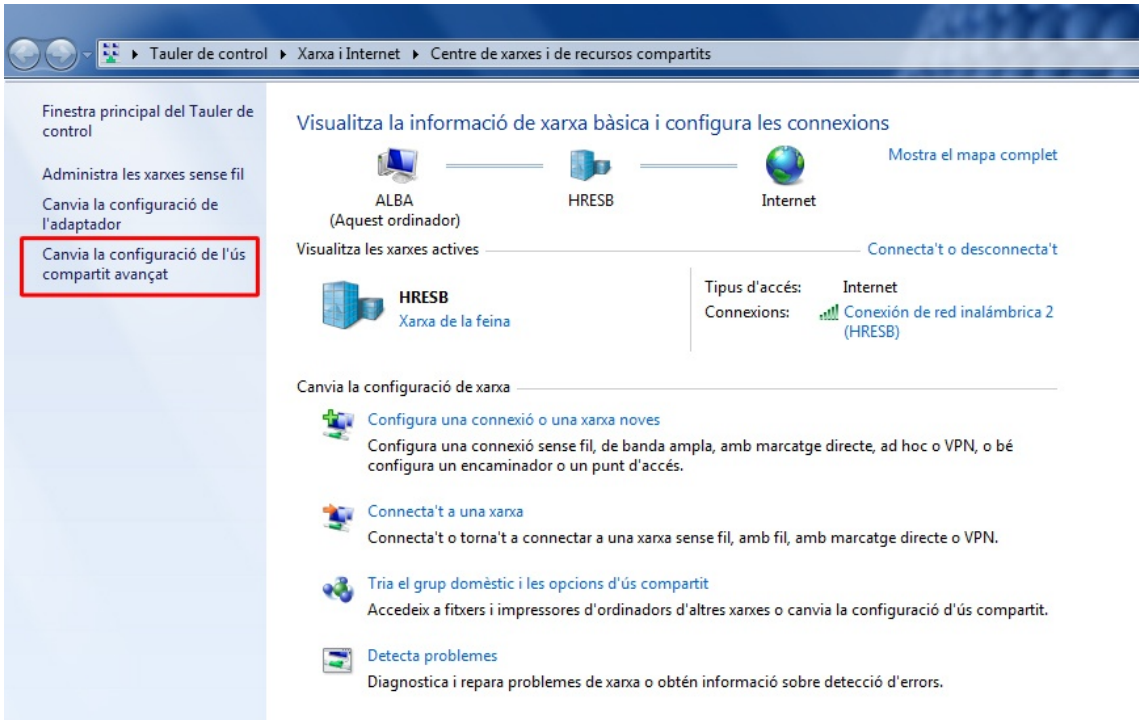


Figure 31. Samba Windows Client configuration (1)

In this menu, we have to enable all the options in order to detect any network shared. Through the following figure the different options changed can be seen. It has be taken into account the option where we can choose the encryption, since Ubuntu only accepts 80 and 56 bits instead of 128 bits (which is the default option).

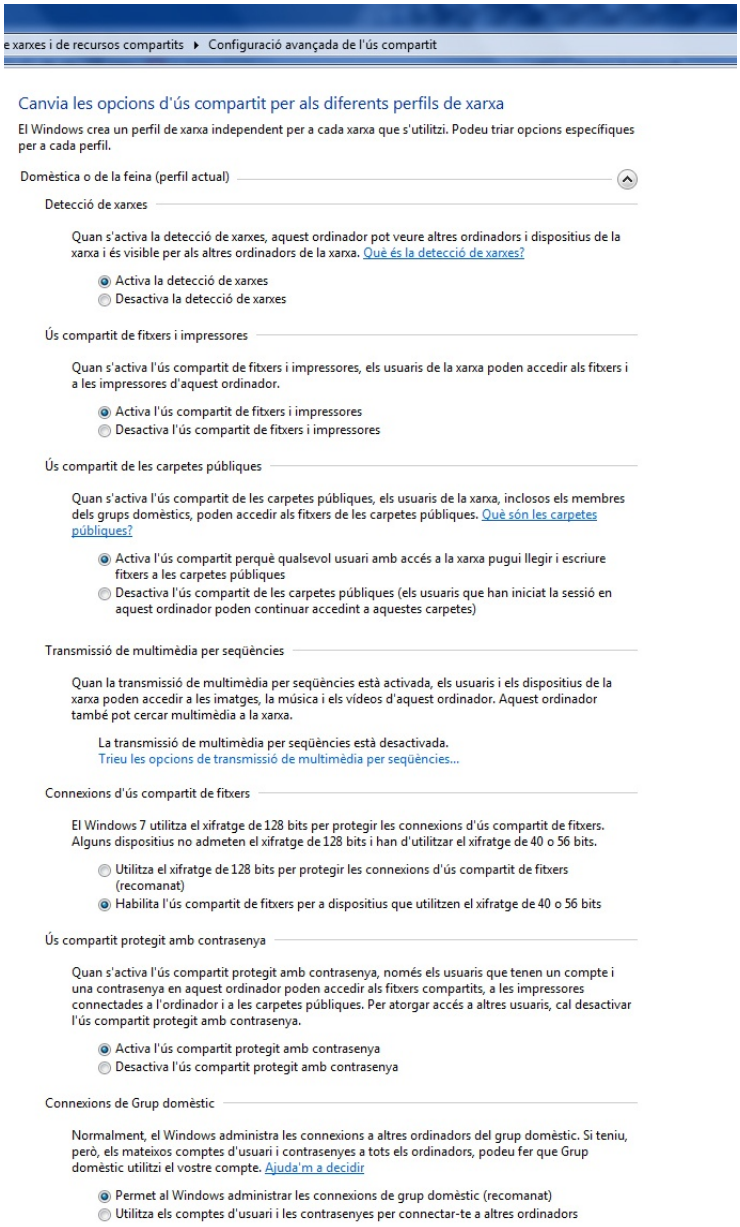


Figure 32. Samba Windows Client configuration (2)

The following step to do is to rename the group which Windows is working, in order to be the same as is configured on the server side, in our case LAB. This requires access to: *Tauler de control>Sistema I seguretat> Sistema. ()*

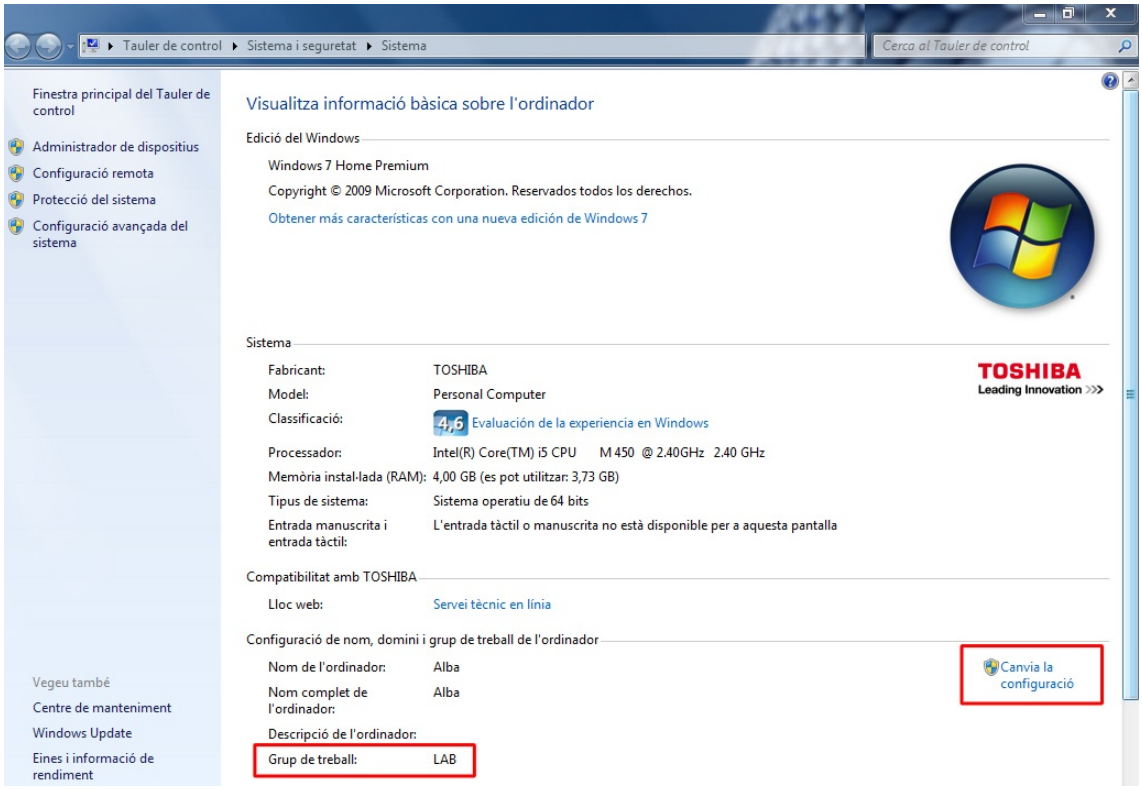


Figure 33. Samba Windows Client configuration (3)

There we have to indicate the new work group:

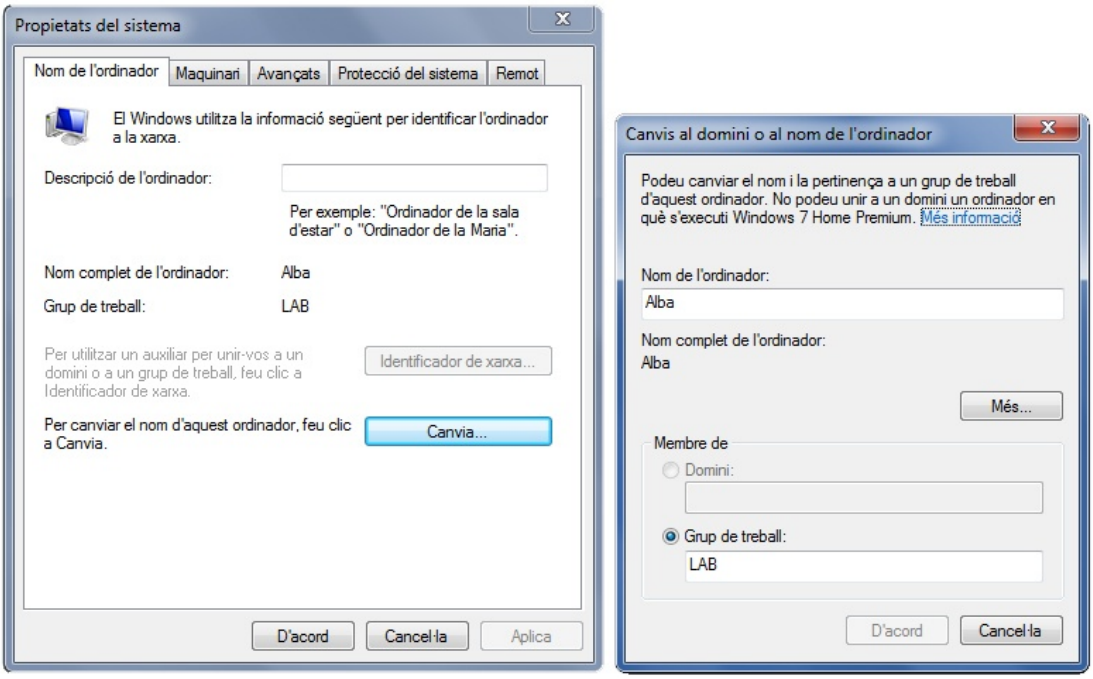


Figure 34. Samba Windows Client configuration (4)

Finally, it is important to disable the Windows firewall in order to permit the access to the shared folders. Otherwise, it will kept blocked.

To get into a folder, in the address bar we have to enter:

`\\10.6.0.1` , where IP is the tunneling IP of the server.

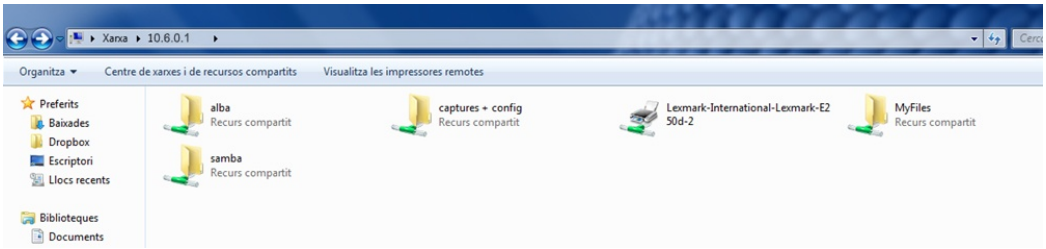


Figure 35. Samba access in Windows client

APPENDIX VI. No-IP

VI.1 Registration

Firstly, to use the No-IP utilities we have to register a new user (http://www.no-ip.com/newUser.php) with the following parameters:

username: *tsf_hresb*
password: *splinter*

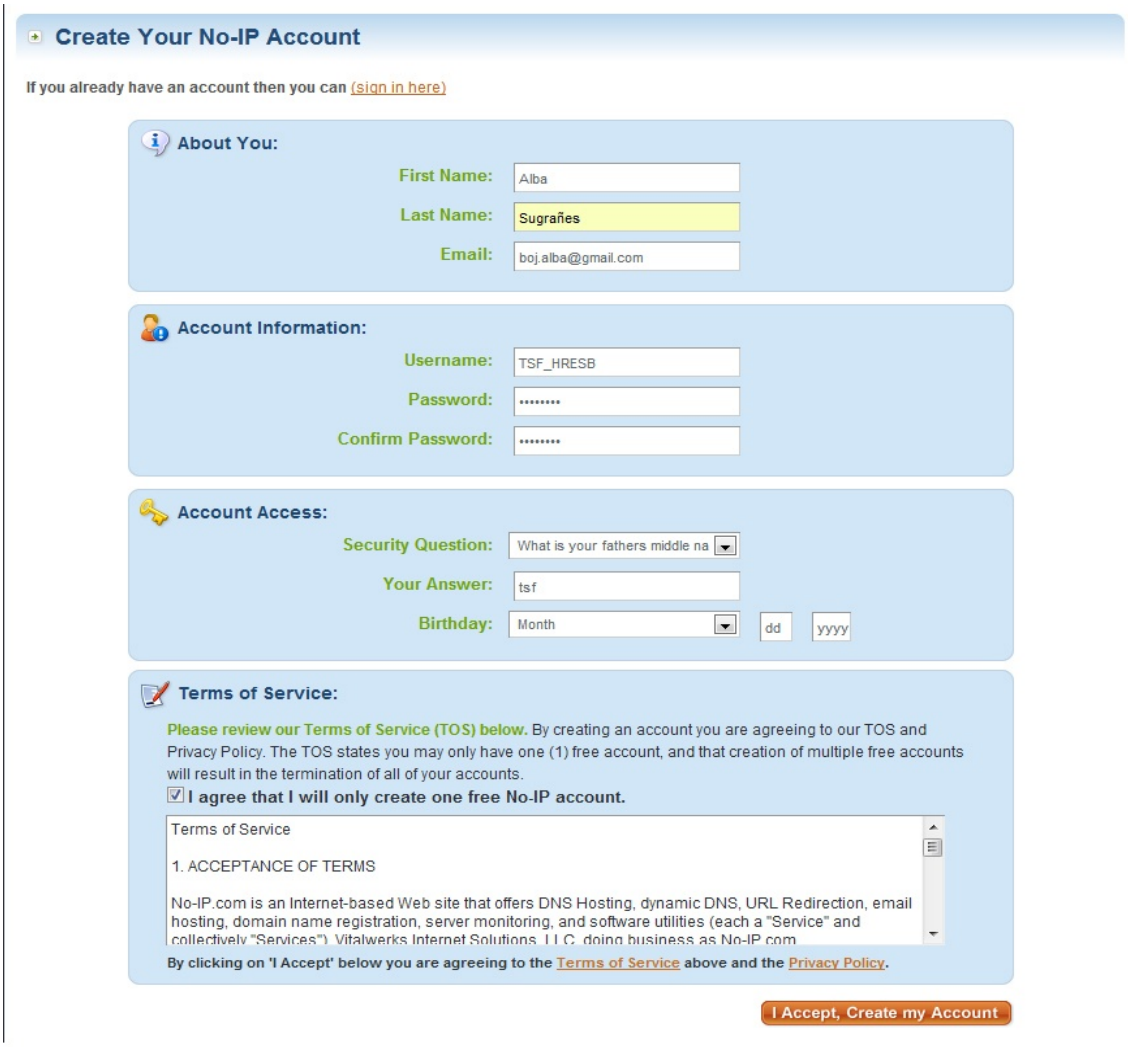


Figure 36. No-IP registration

No-ip will send us a confirmation email. Then, we have to enter our email account that we introduced when we checked, once being in our mail we click the link to activate our account.

VI.2 Add a host

The next step consist of adding a host in our account. In the user panel we have to check hosts/redirects and add a new one. In our case, the configuration implemented is described as follows.

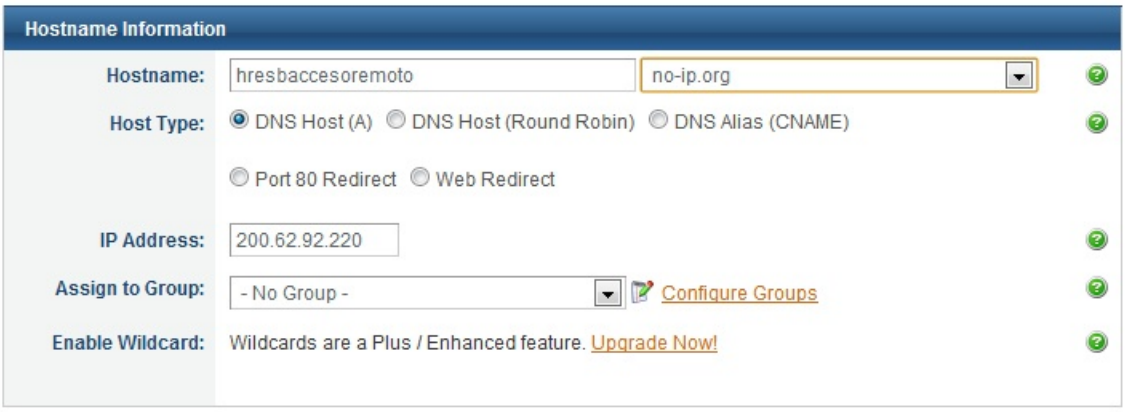


Figure 37. No-IP adding host

When we finish the configuration, we see that in our account the new host is created.

Figure 38. No-IP hresb host

VI.3 Client No-IP installation

In our case, No-IP packages are already installed on the management server. If you have to install new packages, use the following commands.

```
sudo apt-get install noip2
```

For this reason, we only need to reconfigure the no-ip installed with the new host.

Useful command lines for no-ip client. To run the client:

```
sudo /usr/local/bin/noip2
```

In order to configure a client:

```
/usr/local/bin/noip2 -C
```

Firstly it has to select the Internet interface, in our case the ethernet interface. Then we have to enter the login or email which we use in the registration (tsf_hresb or boj.alba@gmail.com) and the password. As we have only one host, automatically choose as default.

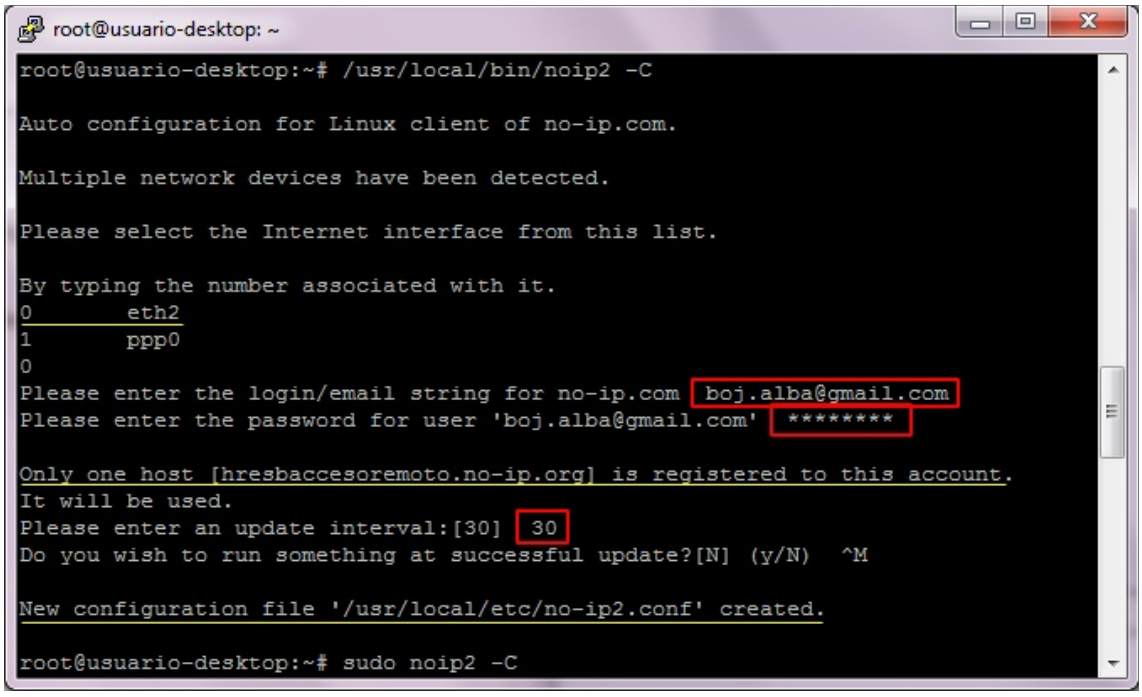


Figure 39. Client No-IP configuration

To display the info about the running client we have to use the following command:

```
/usr/local/bin/noip2 -S
```

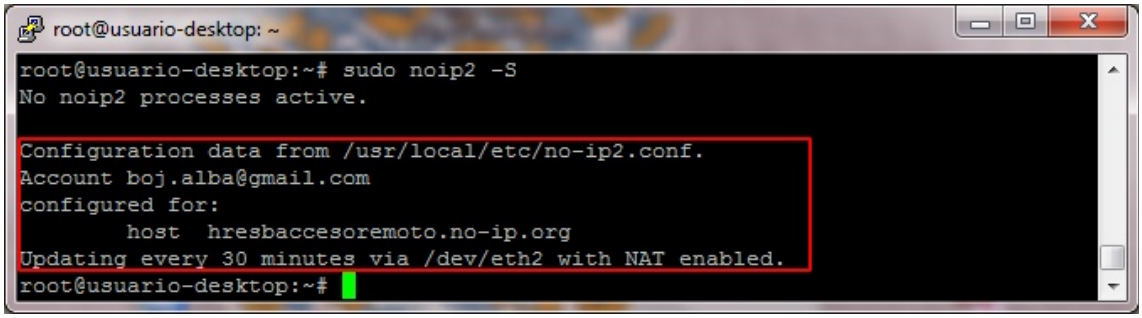


Figure 40. Running Client No-IP

If we want to make it run every system start-up, we need to make a script:

```
sudo nano /etc/init.d/noip2
```

We enter the following:

```
#! /bin/sh
sudo /usr/local/bin/noip2
```

We exit the editor and make it executable:

```
sudo chmod +x /etc/init.d/noip2
```

Now we add it to system start-up:

```
sudo update-rc.d noip2 defaults
```

Finally, we ping our domain (hresbaccesoremoto.no-ip.org) to verify the proper operation and it must return our external IP.

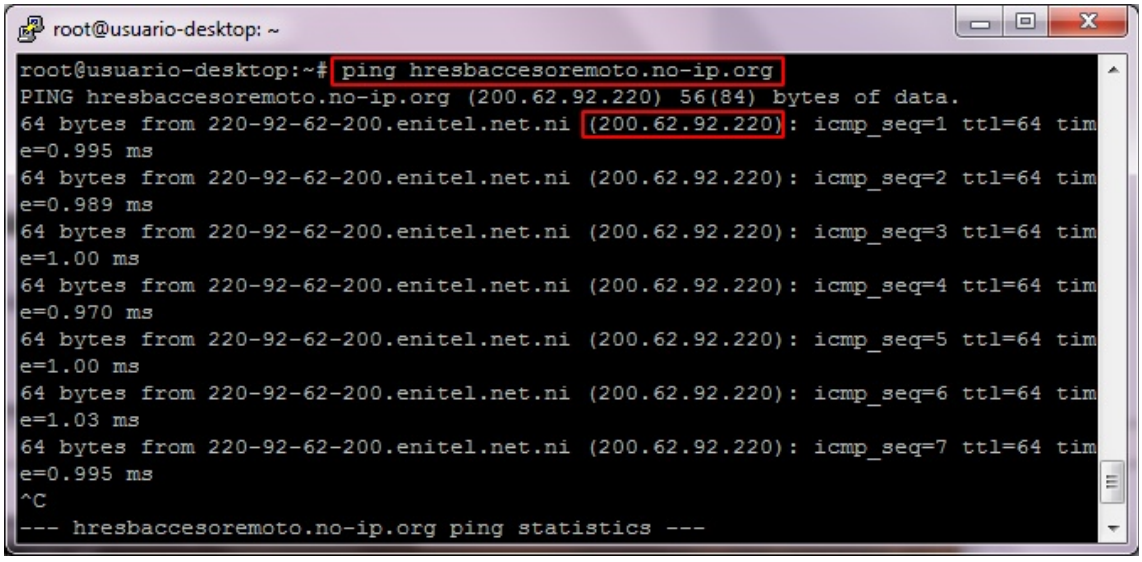


Figure 41. Client No-IP ping

VI.4 Home page No-IP

When entering to *hresbaccesoremoto.no-ip.org,* one can see the following home page:

Figure 42. No-IP home page

We set the home page so that we could directly access to the monitoring revices, inventory, incidents... In the var/www it can be seen the configuration script index.html

```
<html>
<head>
<title>HOSPITAL REGIONAL ERNESTO SEQUEIRA BLANCO - BLUEFIELDS</title>
</head>
<body>
<center><img src="hospital.jpg" alt="HOSPITAL"><p></center>
<p>
<DIV ID=layer1 STYLE="position:absolute; top:100px; left:600px">
    <P><img src="encabezado.gif" alt="Menu Principal"></P>
</DIV>
<p>
<DIV ID=layer2 STYLE="position:absolute; top:150px; left:580px">
<ul>
<li><a                                    href="http://hresbaccesoremoto.no-
ip.org/zabbix">MONITORIZACIÓN</a>
<li><a href="http://hresbaccesoremoto.no-ip.org/mantis">INCIDENCIAS</a>
<li><a                                    href="http://hresbaccesoremoto.no-
ip.org/ocsreports">INVENTARIO</a>
<li><a href="http://hresb-bluefields.wikispaces.com">WIKI</a>
<li><a href="http://hresbaccesoremoto.no-ip.org/correo">CORREO</a>
<li><a href="http://hresbaccesoremoto.no-ip.org/index.php">CARE2X</a>
</ul>
</DIV>
<p>
<DIV ID=layer3 STYLE="position:absolute; top:500px; left:630px">
<a    href="http://www.telecossensefronteres.org/es/"><img    src="tsf.gif"
alt="TSF"></a>
</DIV>
</body>
</html>
```

APPENDIX VII. Radiolink HRESB-Monkey Point

To install and configure the Bullet M2, via the initial URL provided by Ubiquiti (192.168.1.20), it was necessary to set a new static IP according to the IP's of the HRESB network. Moreover, we also configured other parameters such as the central frequency or the transmission speed, as the following figures show the configuration for the large link between the antenna of Cerro Aberdeen (192.168.1.44) and antenna of Cerro Monkey Point (192.168.1.45):

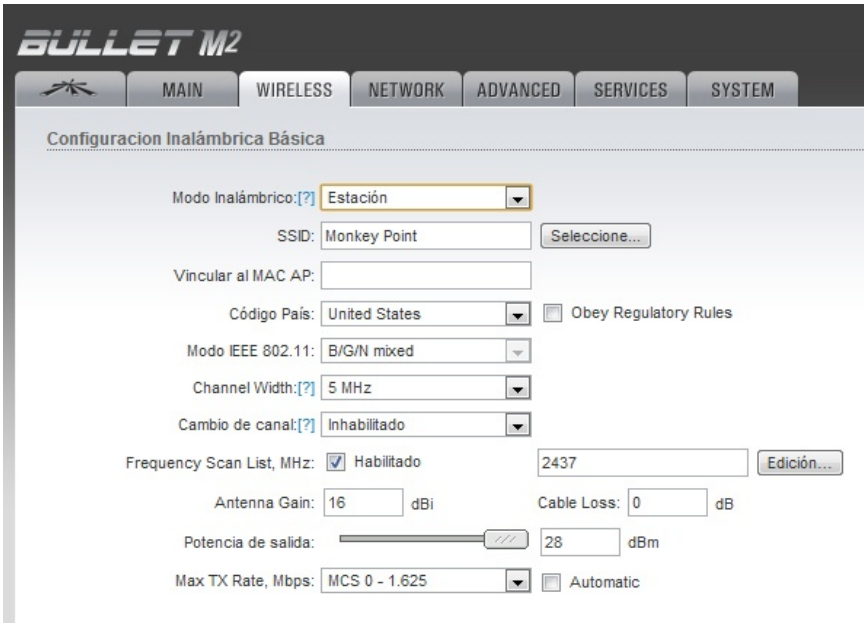


Figure 43. Cerro Aberdeen - Bullet M2 wireless set-up

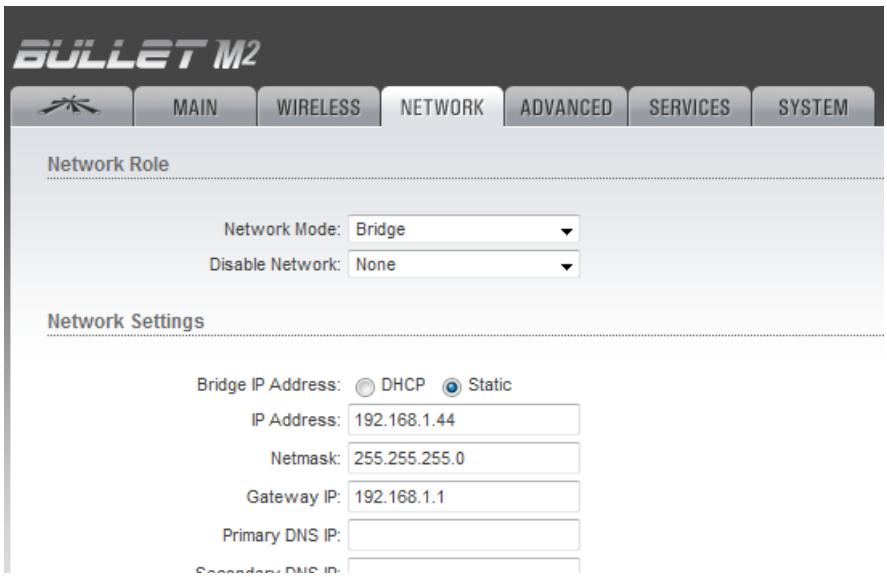


Figure 44. Cerro Aberdeen - Bullet M2 network set-up

Figure 45. Cerro Aberdeen - Bullet M2 advanced set-up

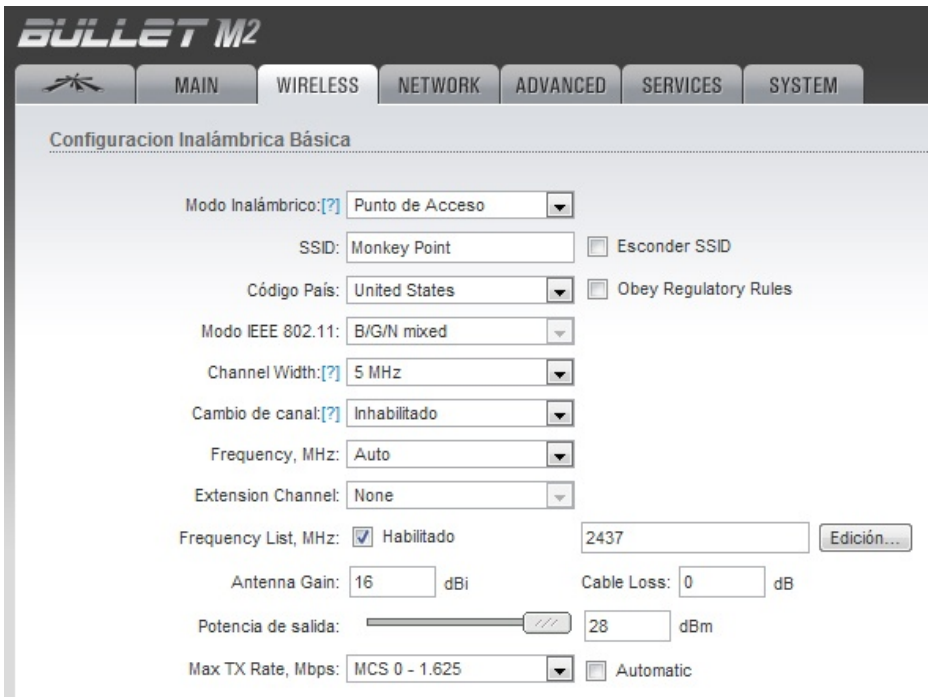


Figure 46. Cerro Monkey Point - Bullet M2 wireless set-up

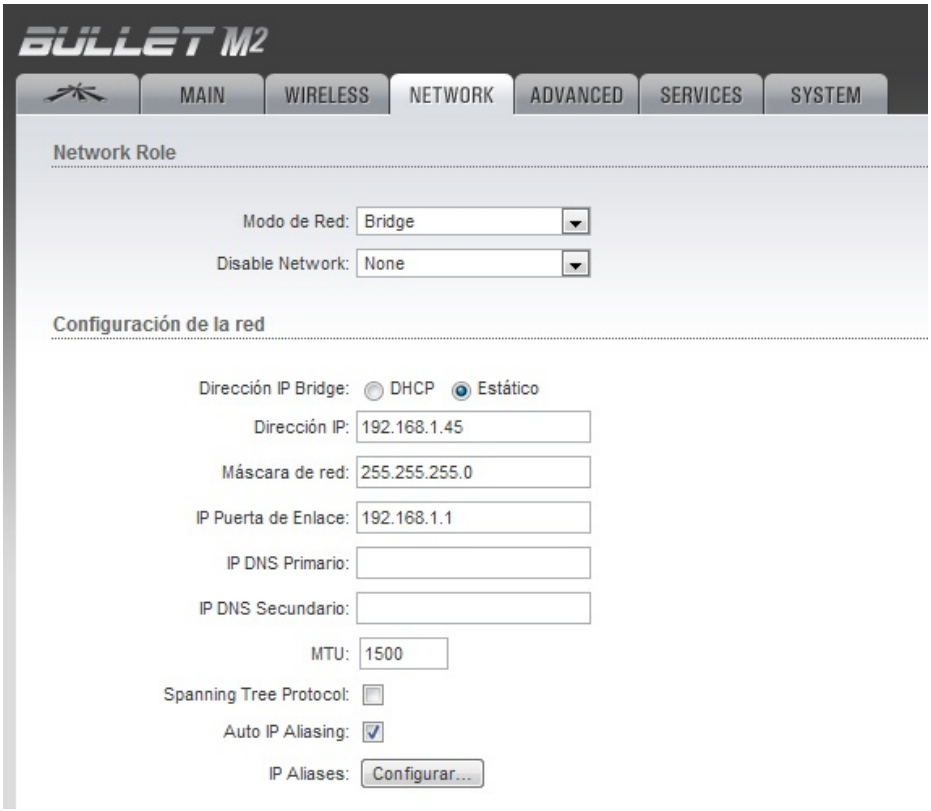


Figure 47. Cerro Monkey Point - Bullet M2 network set-up

Figure 48. Cerro Monkey Point - Bullet M2 advanced set-up

In addition the tool AirControl was installed in order to manage all the antenna in the network. To install the tool we can download the last version in the following link:

http://www.ubnt.com/aircontrol

Run the installation file and follow the instructions until to complete the installation. To access the application, run your web browser and type the URL in the address bar:

http://localhost:9080

It has be taken into account that the user and password for default are ubnt.

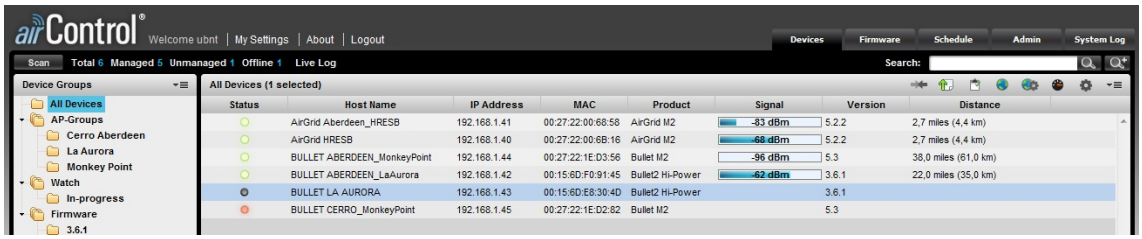


Figure 49. AirControl tool

APPENDIX VIII. NComputing installation

VIII.1 Windows 7 installation

To avoid problems with the vSpace installation it is recommended to do a Windows 7 clean installation, that is to say, from 0. To begin the Windows 7 install process, you will need to boot from the Windows 7 DVD.

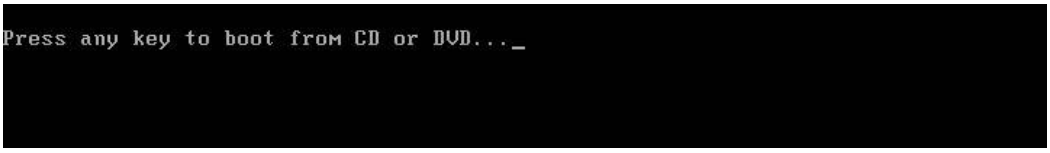


Figure 50. Windows 7 start-up

Choose the *Language to install*, *Time and currency format*, and *Keyboard or input method* that you would like to use in Windows 7.

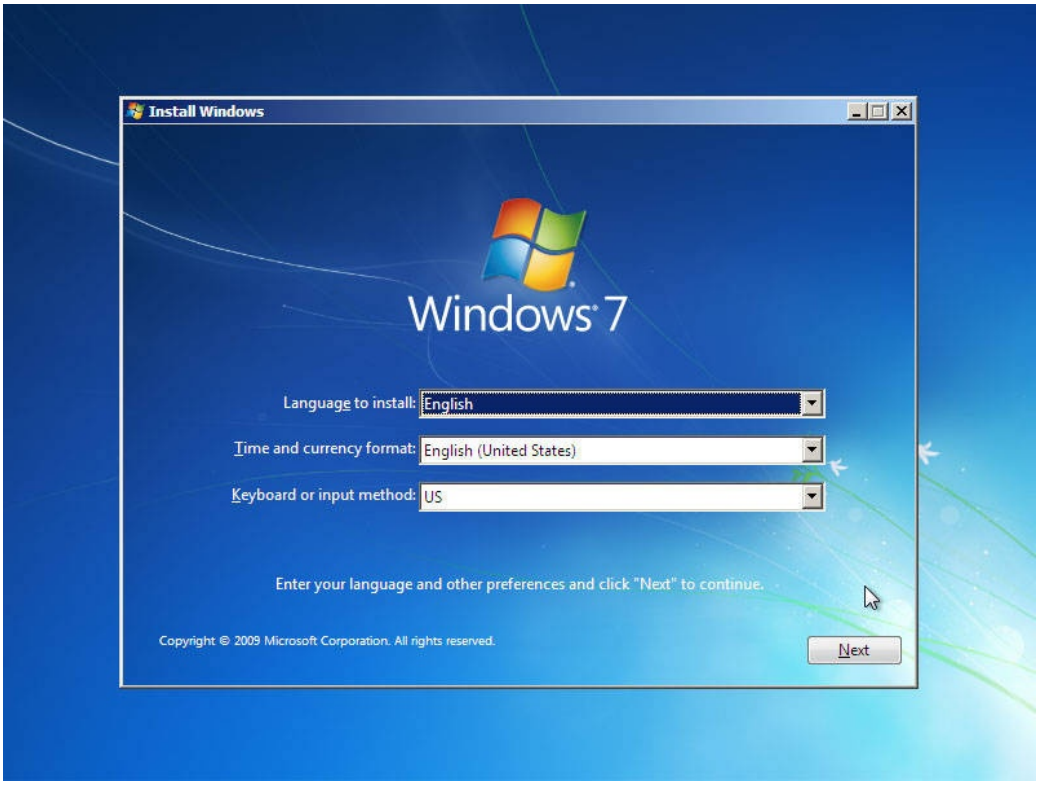


Figure 51. Windows 7 installation (1)

This will officially begin the Windows 7 installation process.

Figure 52. Windows 7 installation (2)

The next screen is a text-box containing the Windows 7 Software License. Read through the agreement, check the *I accept the license terms* checkbox under the agreement text and then click **"Next"** to confirm that you agree with the terms.

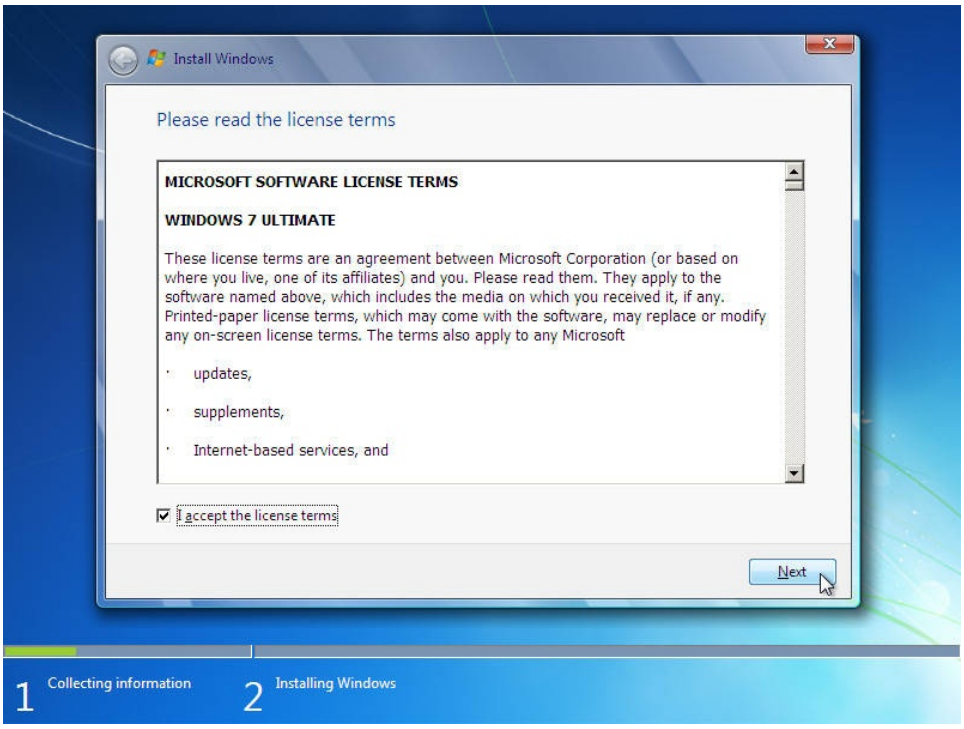


Figure 53. Windows 7 installation (3)

The window that appears next, there is offered the choice of Upgrade and Custom (advanced). Click on the Custom (advanced) button.

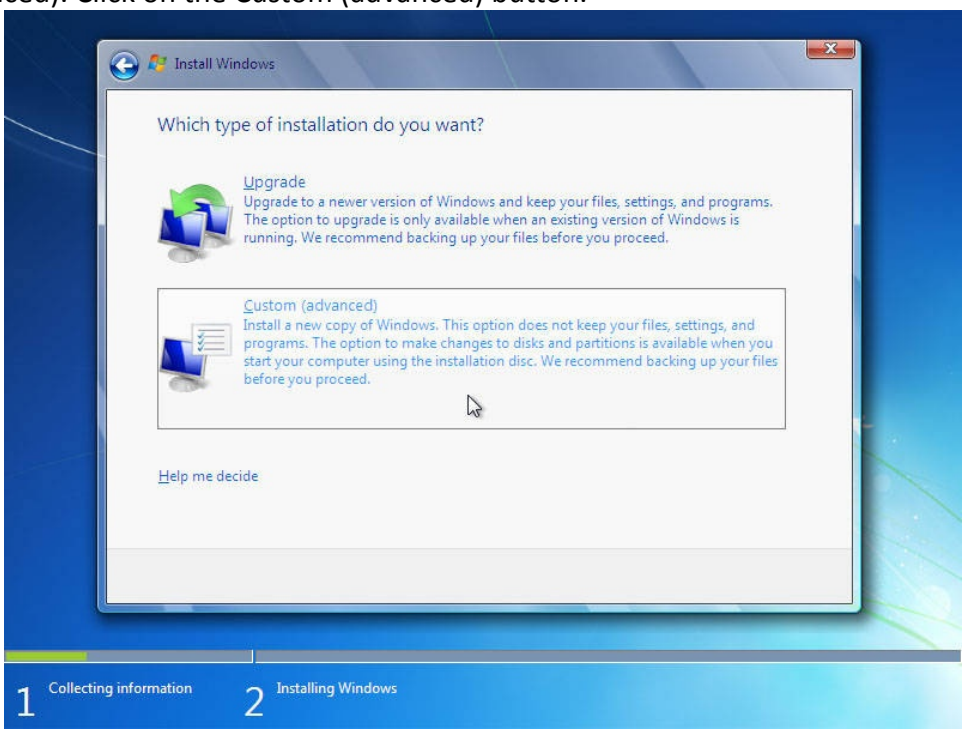


Figure 54. Windows 7 installation (4)

In this step, you will be choosing the physical location to install Windows 7 to. Choose the appropriate unallocated space or previously partitioned space on a hard drive.

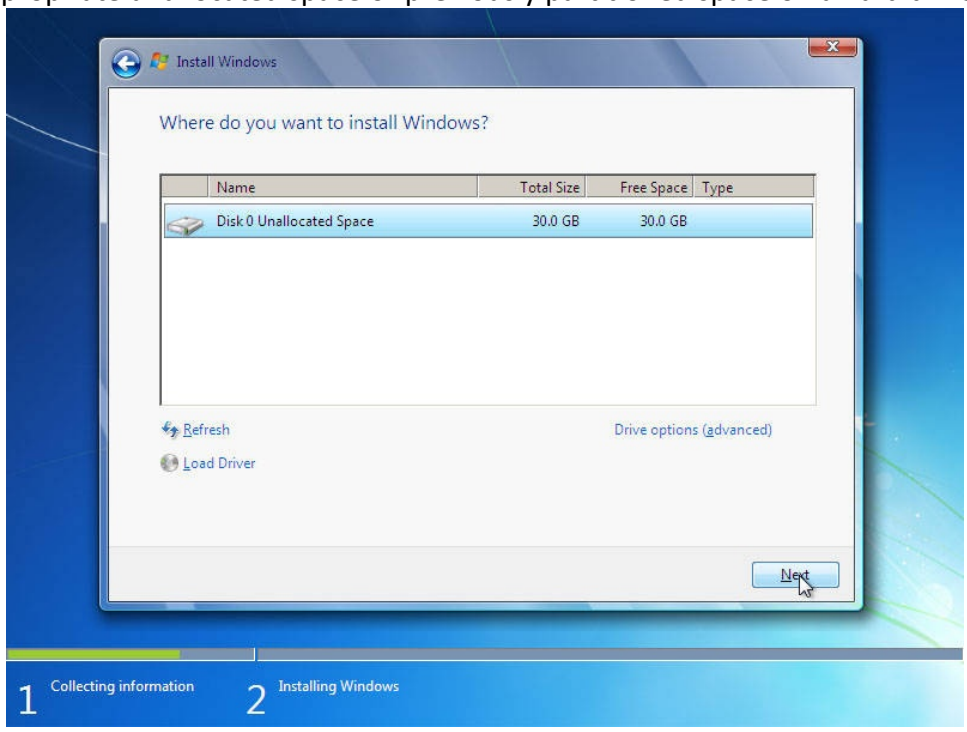


Figure 55. Windows 7 installation (5)

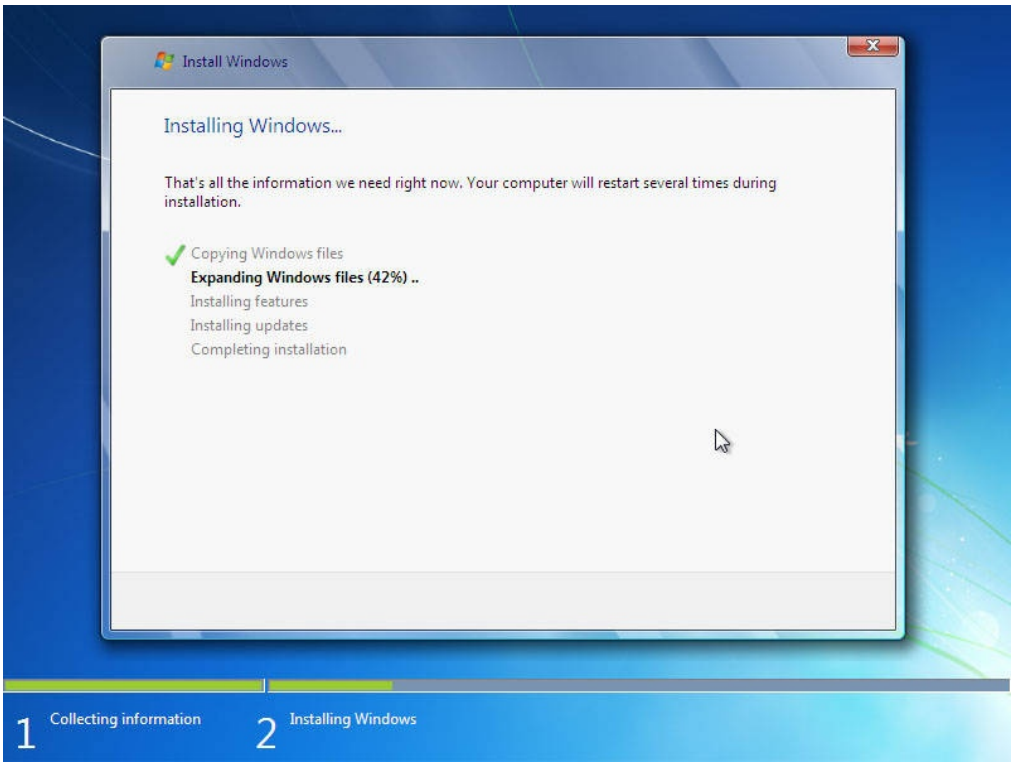


Figure 56. Windows 7 installation (6)

Now that the Windows 7 set-up process is completed, it is necessary to restart the computer so the whole process will be finalized.

VIII.2 Installation of vSpace™ software

The first step is to download the latest version of our vSpace software from the NComputing Software Download Center. Locate and download the correct software based on product model (L300 Virtual Desktop) and operating system (Windows 7 of 64 bits).

http://www.ncomputing.com/softwaredownload

After downloading and extracting the installer files, double click the downloaded ".exe" file to begin the installation process. Just follow the installation steps without any special configuration.

In order to avoid problems with the installation, different statements have been taken into account:

- **Administrative rights** are necessary to install vSpace L-6.5.1.10 onto Windows 7. So, although you may be logged-in as a Windows 7 user that is a member of the Administrators group, you still will not have enough "administrative rights" to install vSpace 6 and the MSI installer will generate an error message saying: "You need administrative rights to install this software. Installation Failed."

  We need to launch the "Administrative Command Prompt" by going to *All Programs > Accessories > Command Prompt* and then right-click and select "Run as administrator."

  Once the "Administrative Command Prompt" console pops up, launch the installer using the following command:

  ```
  msiexec /i setup.msi
  ```

- Anti-virus, firewall, and other types of security software can sometimes **interfere with the installation** of NComputing's vSpace software. For this reason, any Anti-Virus or Firewall software need to be disabled during the installation of the product.

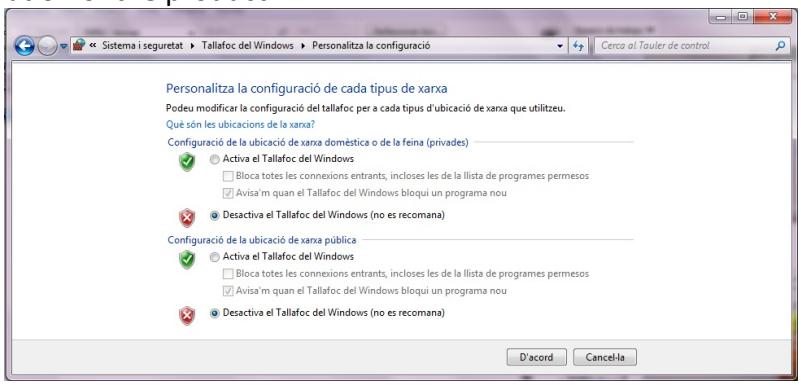


Figure 57. Disable firewall of Windows 7

- It is also important to **disconnect the updates** of windows as some of them can block the vSpace software. It can be disconnected in the *Administración de equipos.*

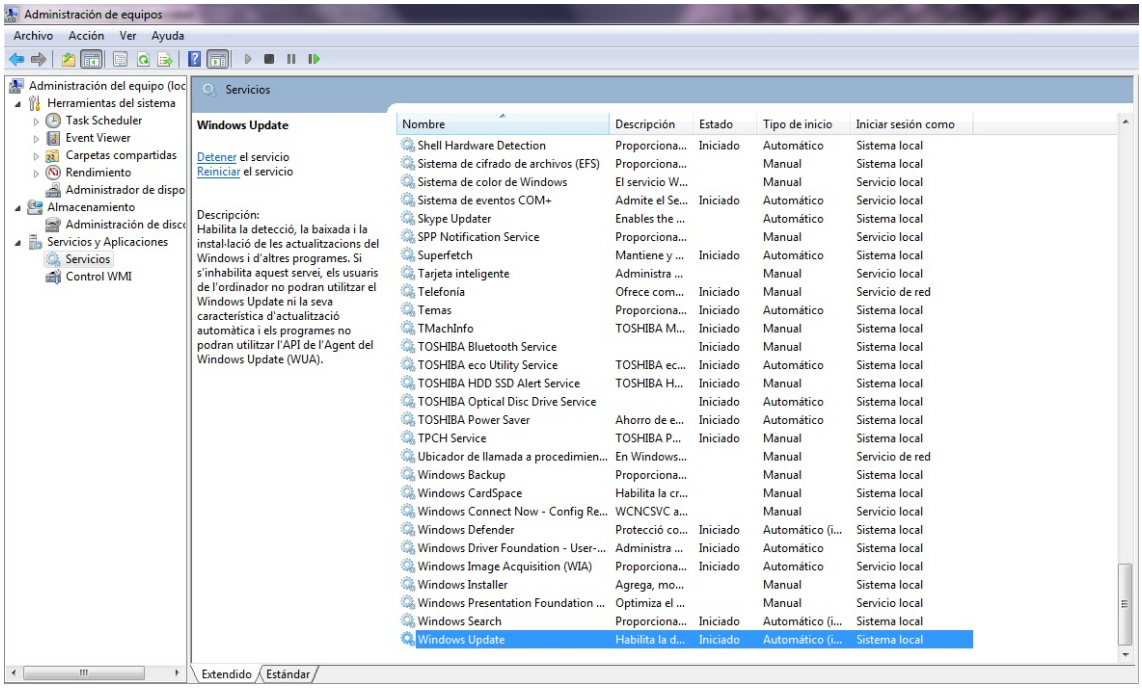


Figure 58. Disable Update Windows 7 (1)

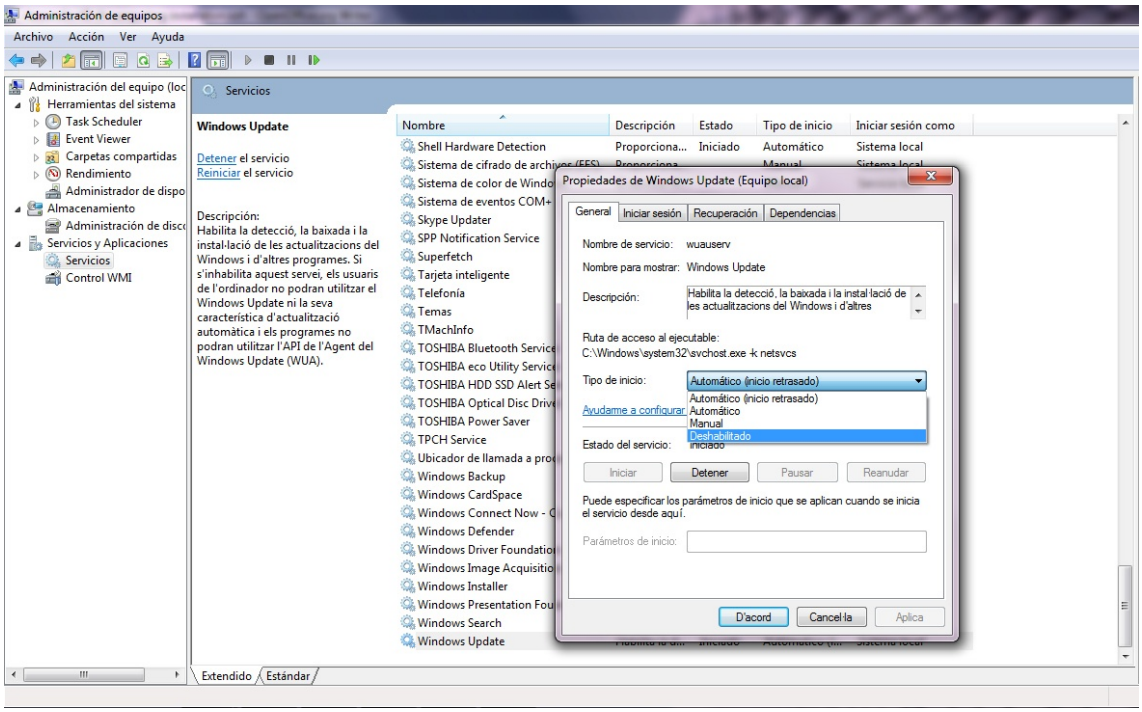


Figure 59. Disable Update Windows 7 (2)

VIII.3 Users setup

First of all, the users have to be created in the computer. To do so, enter into the *Administración de equipos*

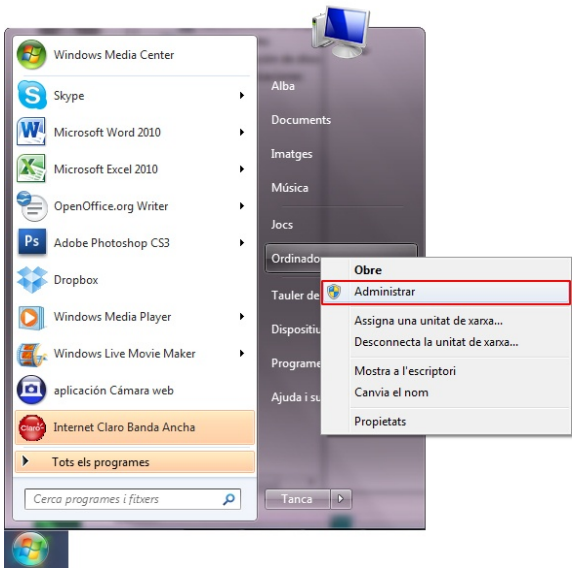


Figure 60. Set up users in Windows 7

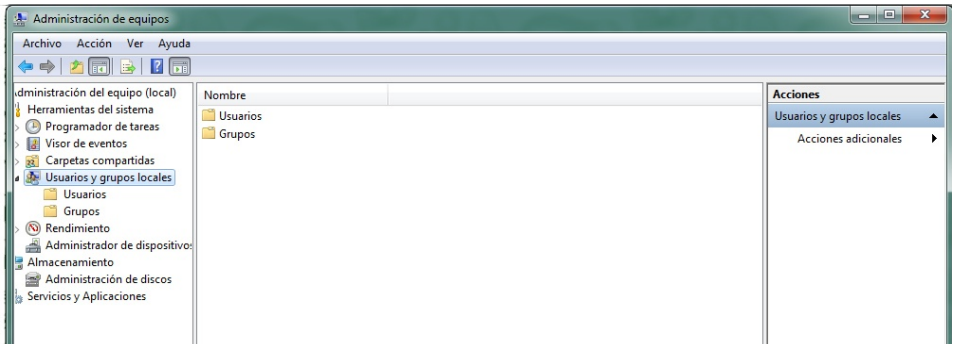


Figure 61. Administración de equipos in Windows 7

Within the folder *Usuarios* we have to create a new user for each N-computing device. For each user, there must be created a name that identifies itself and a password. Also, there must take into account to mark the following options:

- *El usuario no puede cambiar la contraseña*
- *La contraseña nunca expira*

By this, the whole configuration control rests with the administrator.

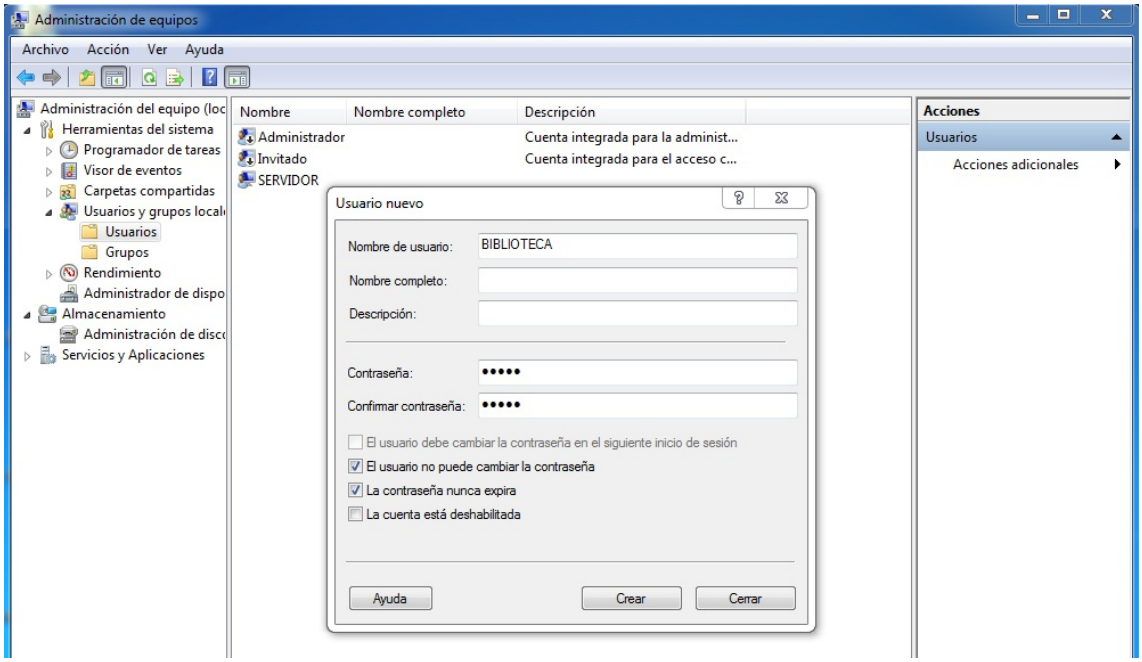


Figure 62. Add users in Windows 7 (1)

In the following picture, the new users created can be seen.

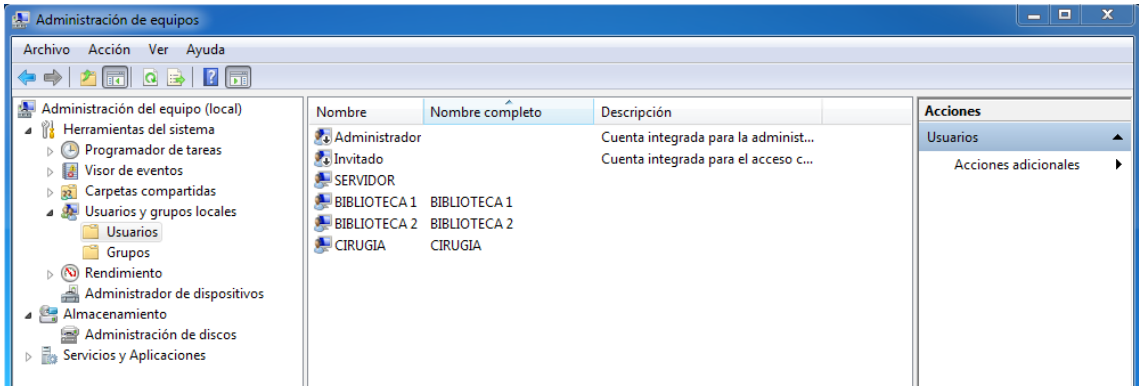


Figure 63. Add users in Windows 7 (2)

Then, add new users to the group of *usuarios de escritorio remoto.*

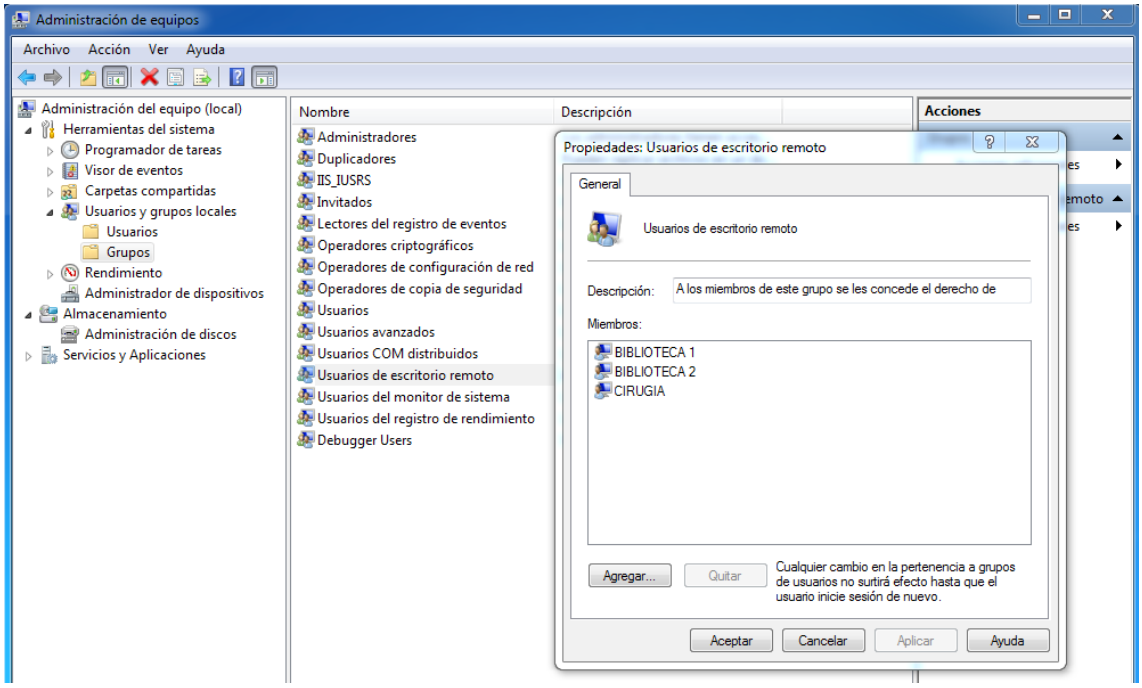


Figure 64. Add users in remote desktop in Windows 7

VIII.4 Connect peripherals

At this point, we are prepared for the next step, connect the NComputing device with its peripherals.

Figure 65. Instructions for connecting peripherals

VIII.5 L300 NComputing configuration

The scenario to implement is the server with 3 NComputing terminals, corresponding each of them to a department within the hospital. Both equipment are integrated into the existing network, with the reservation of an exclusive range of IP for that technology.

In order to have a more accurate control of the devices, it was established to use static IP for the network configuration. Thus, the server started by 192.168.1.20 and the NComputing units continued the sequence by 192.168.1.21 and so on (with the reservation up to 192.168.1.39 for future additions).

The choice of using static (and not dynamic) IP was due to its performance. That is to say, in the case of the Internet connection being down, the system keeps correctly working since all the devices know their address and the server's one (no need of routing), so the network is not damaged and the communication keeps flowing. By using dynamic ones, the system is strictly dependant on the Internet connection and the router.

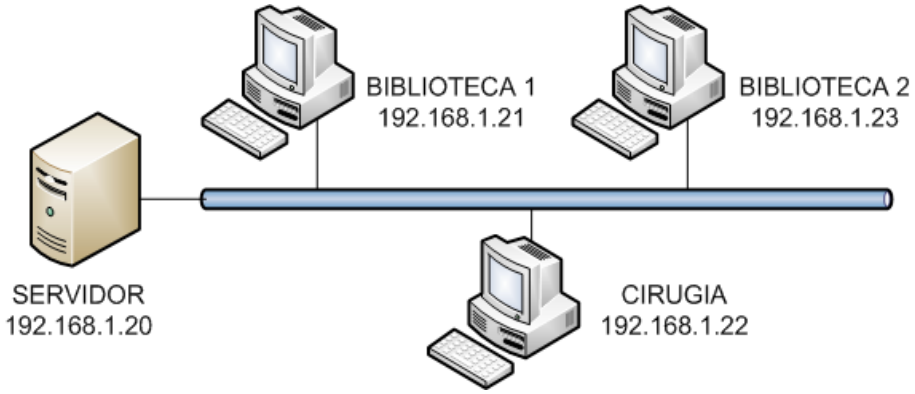


Figure 66. Network configuration

Referring to the server, it is only necessary to put an IP address with its corresponding common parameters of the existing network. Click on *Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Conexiones > Propiedades > Protocolo de Internet versión 4 (IPv4)* and fill the gaps with the information given.

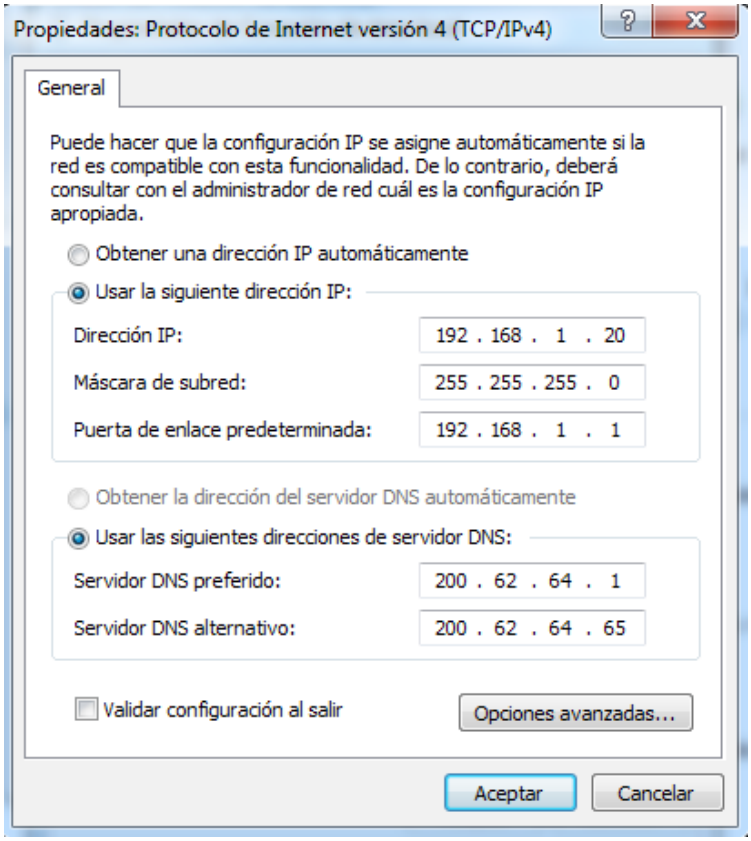


Figure 67. Network configuration

The configuration of the NComputing devices can be done through their respective prompt or via the vSpace management console (placed in the server). It is way easy to monitor from that console, so all the devices can be visualized through it.

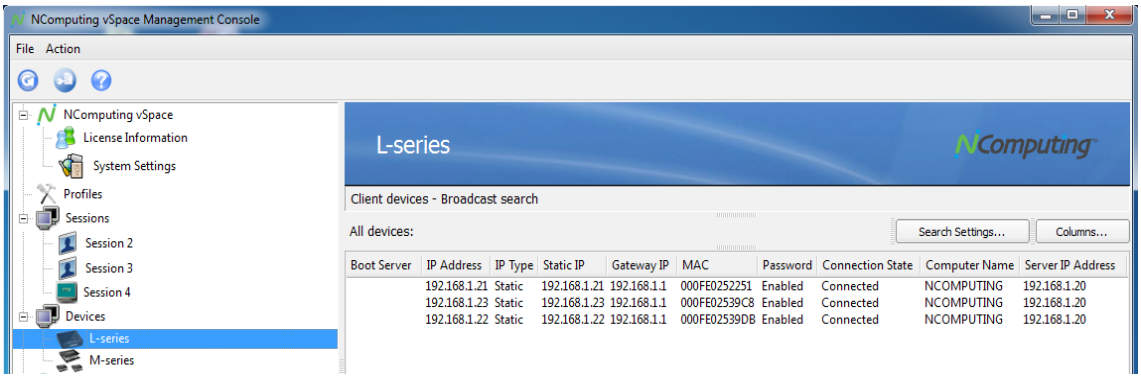


Figure 68. NComputing vSpace management console

First of all, the devices have to be labelled so one can identify them among the rest. Notice that the network eventually will be large so it is recommendable to keep the track of them.

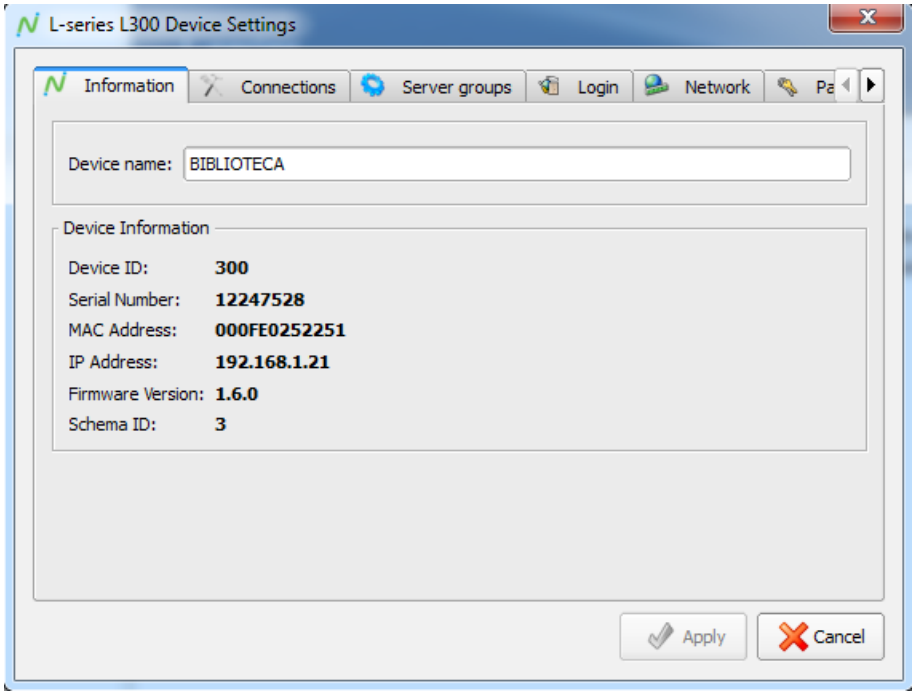


Figure 69. General settings

At this point, the NComputing devices needed to be linked with the server which had vSpace software installed on it. Easily, only one device appeared on the list and was added to the group created.

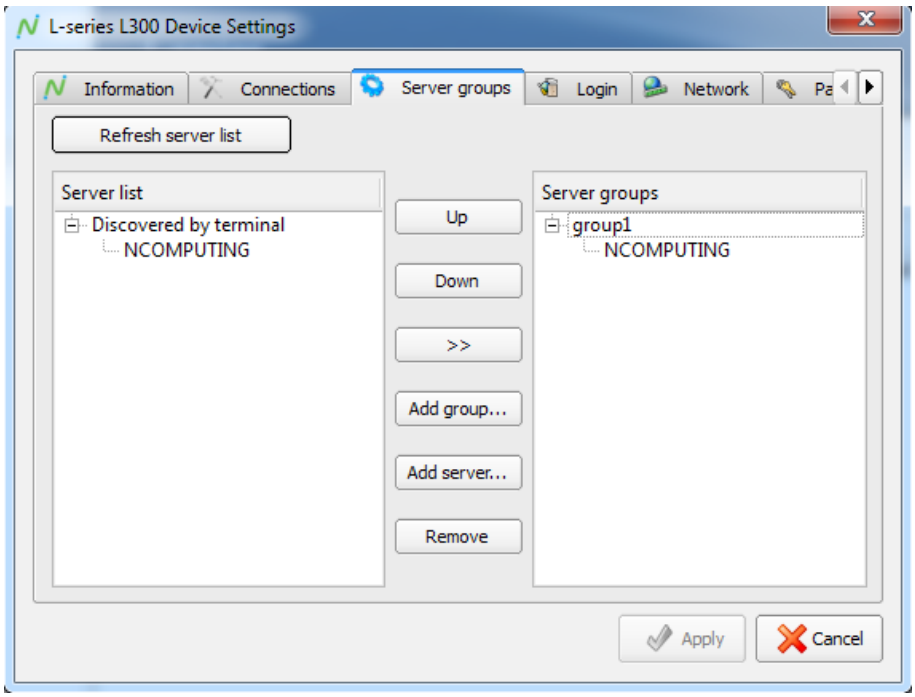


Figure 70. Link to the server

Following the IP network scheme studied above, each device was configured with its parameters. In addiction to the IP, mask, gateway and DNS were also defined.

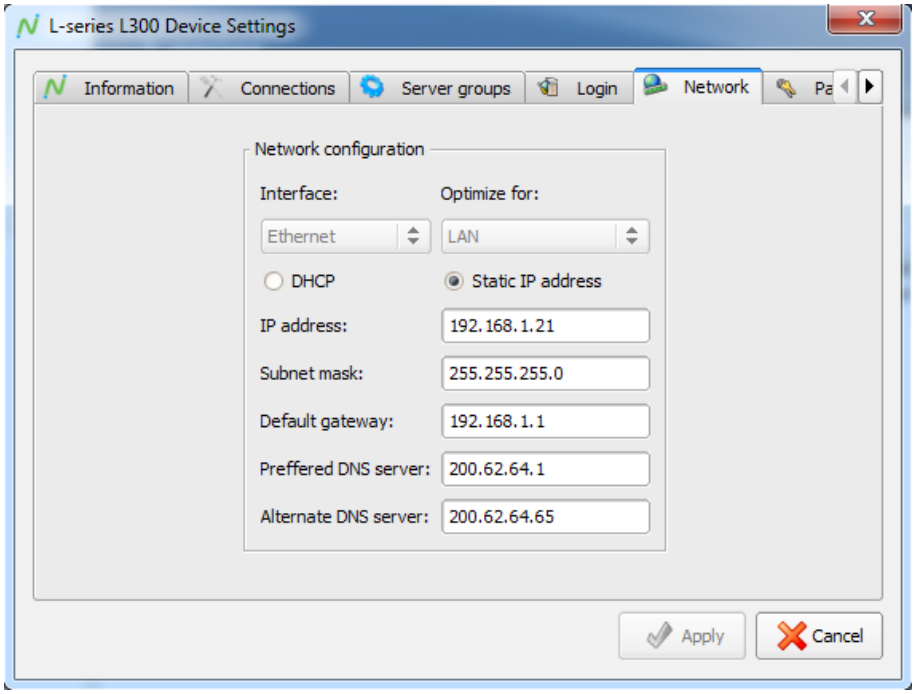


Figure 71. Network configuration

As many people was expected to use the computer, a good practise was to set a password to protect the whole configuration and avoid involuntary changes. That code disabled the option to modify any setting.

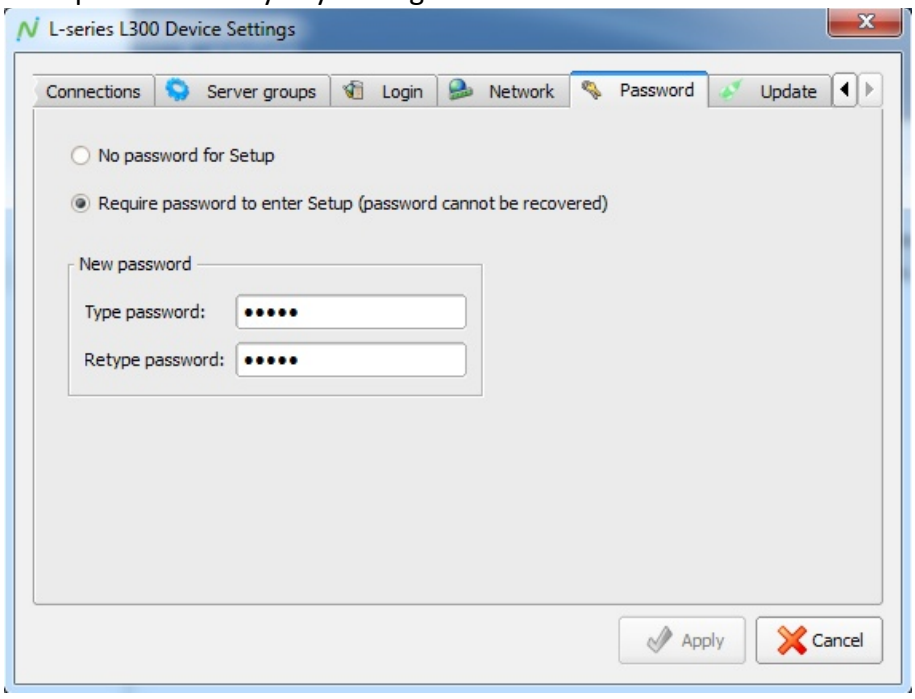


Figure 72. Password configuration

In the same purpose to make things easier, it was possible to enable an *auto-connect* option, so the NComputing devices immediately recognise the server and log in directly to the application, avoiding a set of screens which may mislead the user.

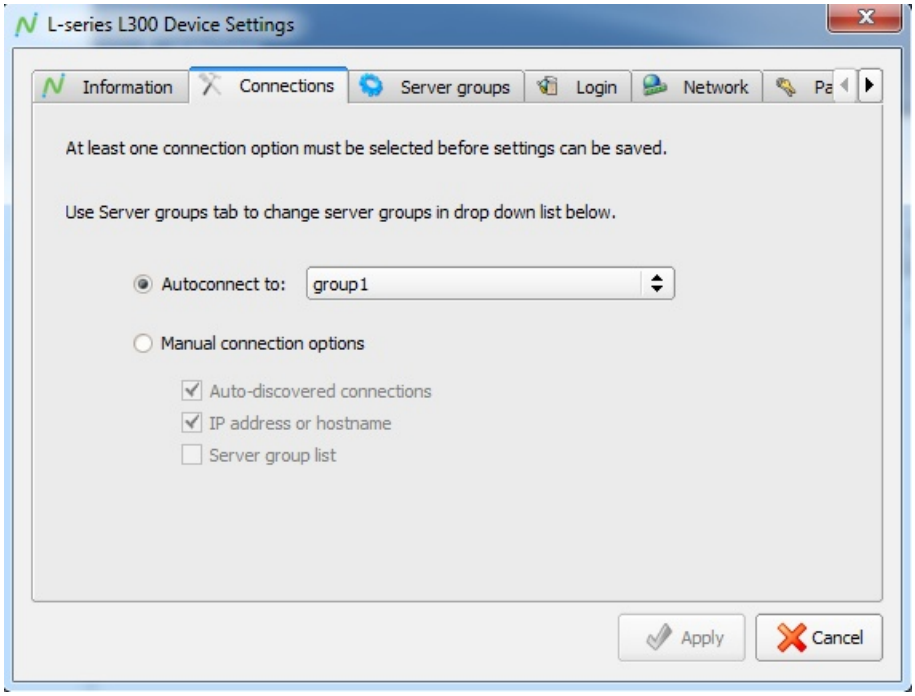


Figure 73. Auto-connect configuration

Afterwards, all the devices should already be registered to the vSpace, so available to use them. From the vSpace management console, one can visualise if that is correct and the rest of the configuration settings. Be aware that the Firmware version can not be updated, so by right clicking to the device, it is possible to update to the last version of it.

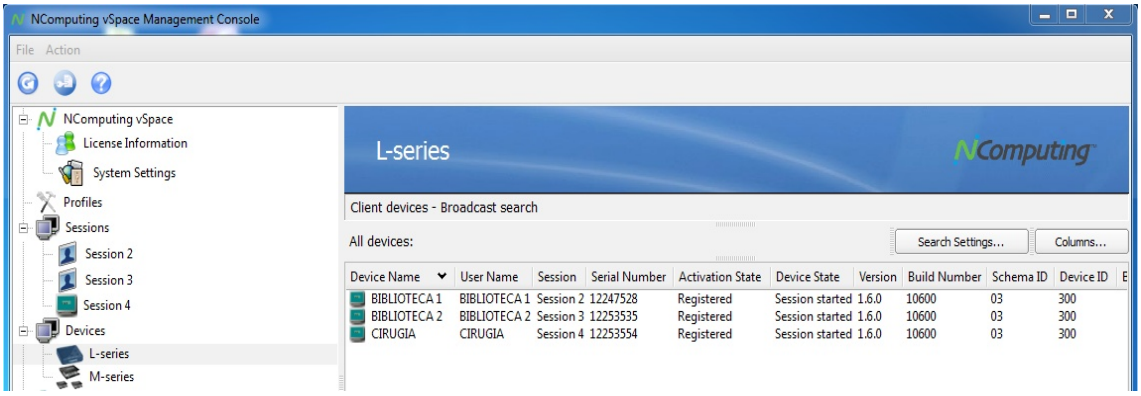


Figure 74. Client devices overview

VIII.6 Register vSpace™

Product registration is required for all L-Series devices and vSpace software to enable normal product use, downloading updates and technical support. Prior to registering, sessions will time out after one hour and devices will not be able to connect after 30 days.

When registering the software, all the access devices must be connected to the host system using Ethernet. Select "vSpace Registration" in the Windows Start menu. In the case of Online Registration, follow the instructions below.

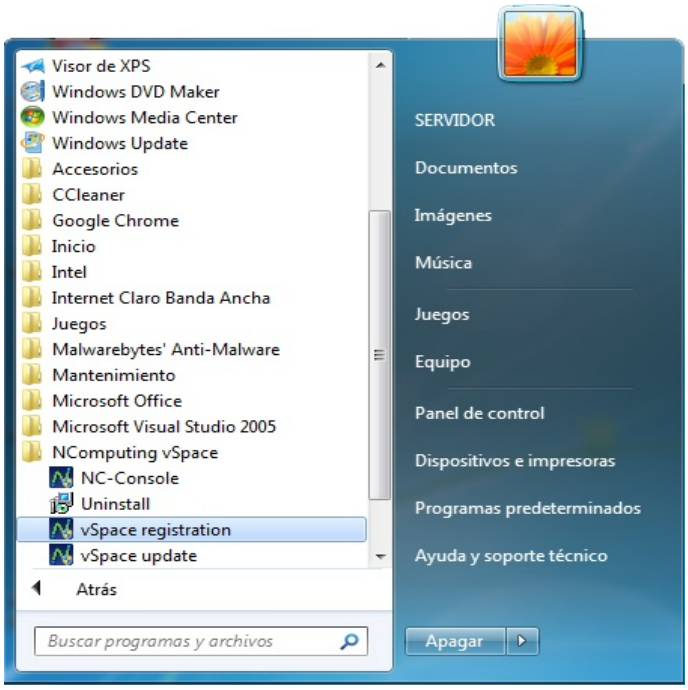


Figure 75. vSpace registration (1)

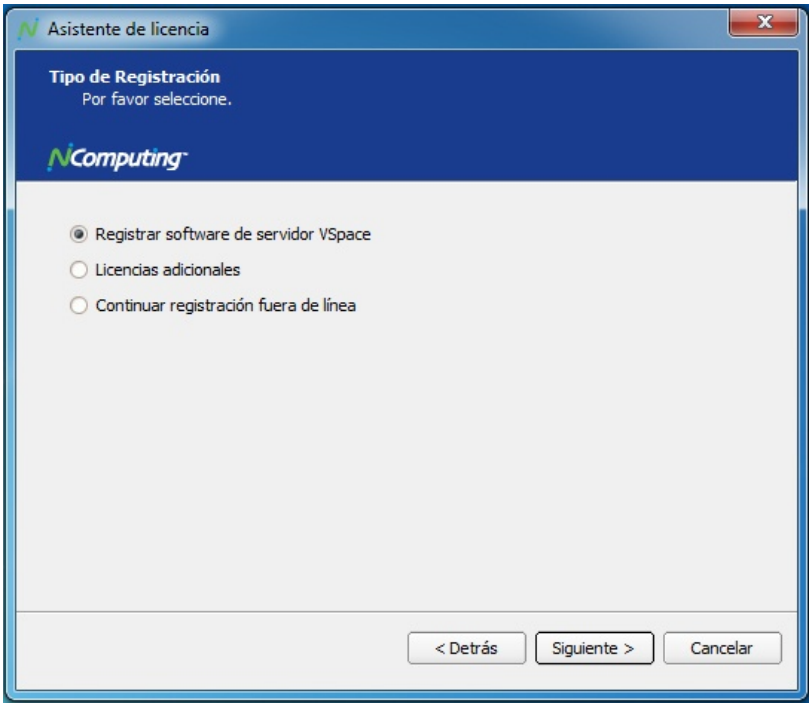


Figure 76. vSpace registration (2)

At the "Customer Data" screen, if the data fields are not already populated, enter the registered user's relevant information. Each field in this window must be filled in. Once all the data is entered, click on the "Next" button.

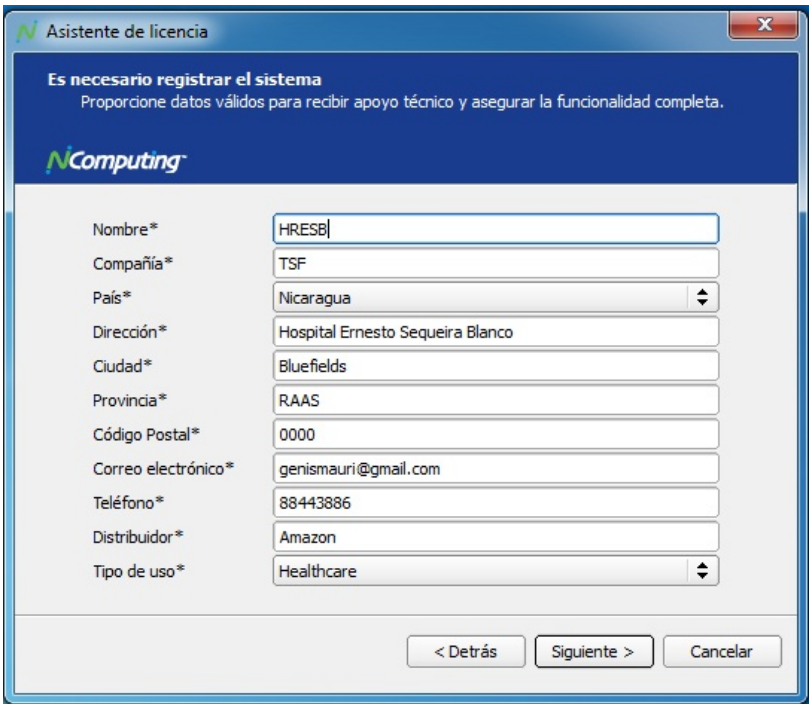


Figure 77. vSpace registration (3)

On the Registration Type screen, select “Register online, using your Internet connection” and click “Next”.

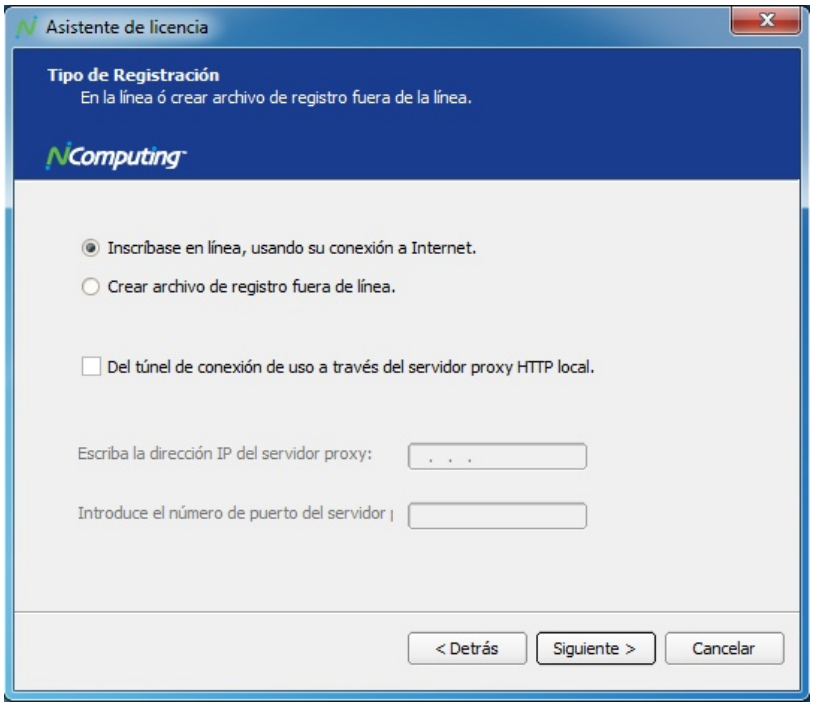


Figure 78. vSpace registration (4)

The registration wizard will then show a list of all unregistered L-series access devices that are currently connected to this vSpace host, that now can be registered. Afterwards, it can be seen through the NComputing console that all the devices appear to be registered and ready to be used.

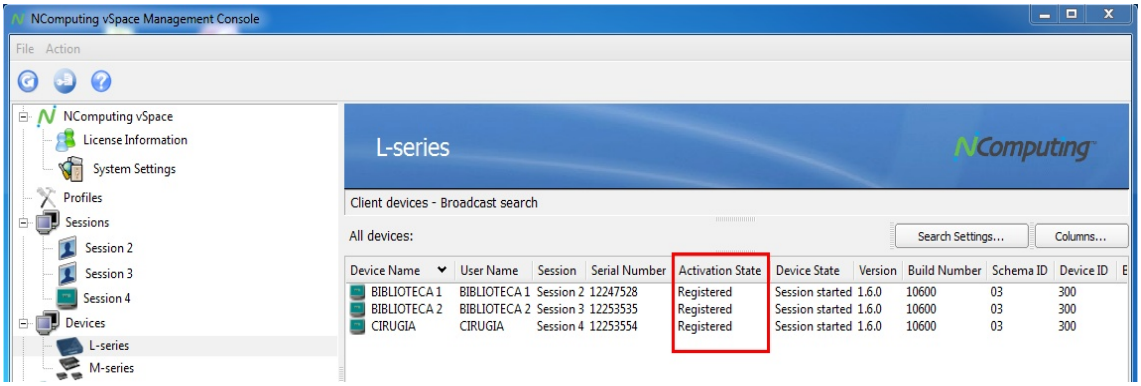


Figure 79. vSpace registration (5)

APPENDIX IX. Deep Freeze

IX.1 Deep Freeze Installation

Deep Freeze requires Windows 2000, Windows XP (32 or 64 Bit), or Windows Vista (32 or 64 Bit), or Windows 7 (32 or 64 Bit), and 10% free hard drive space.

The steps that we have to follow in order to install the software are the following. The Deep Freeze software can be download in:

http://www.faronics.com/es/downloads_es/

After downloading and extracting the installer files, double click the downloaded DFStd.exe to begin the installation process.

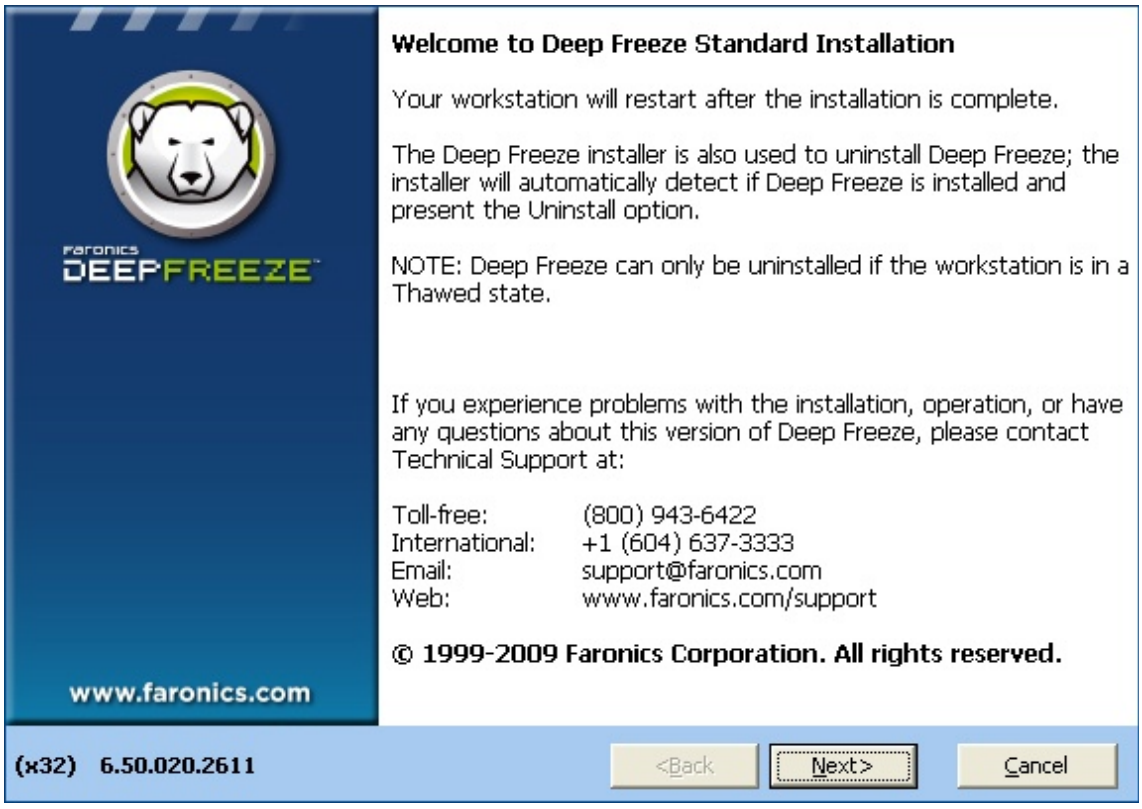


Figure 80. Deep Freeze installation (1)

We have to click I agree to the terms in the License Agreement and continue with the installation.

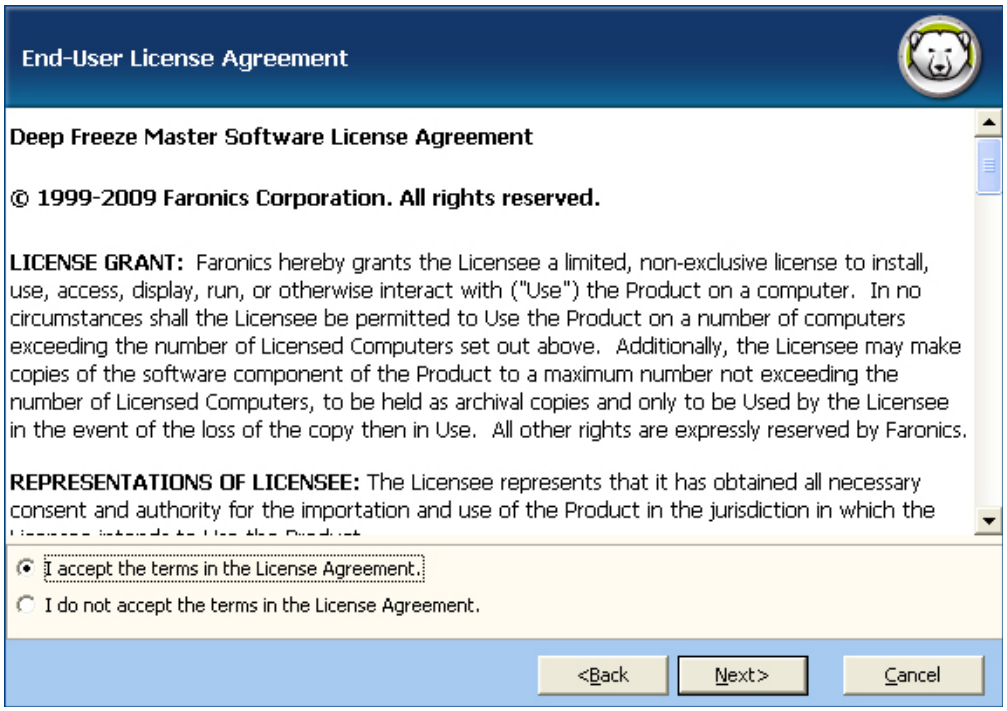


Figure 81. Deep Freeze installation (2)

Enter the License Key or select the Use Evaluation check box to install Deep Freeze in Evaluation mode. The Evaluation period ends 30 days after installation. Contact Faronics to purchase a License Key.

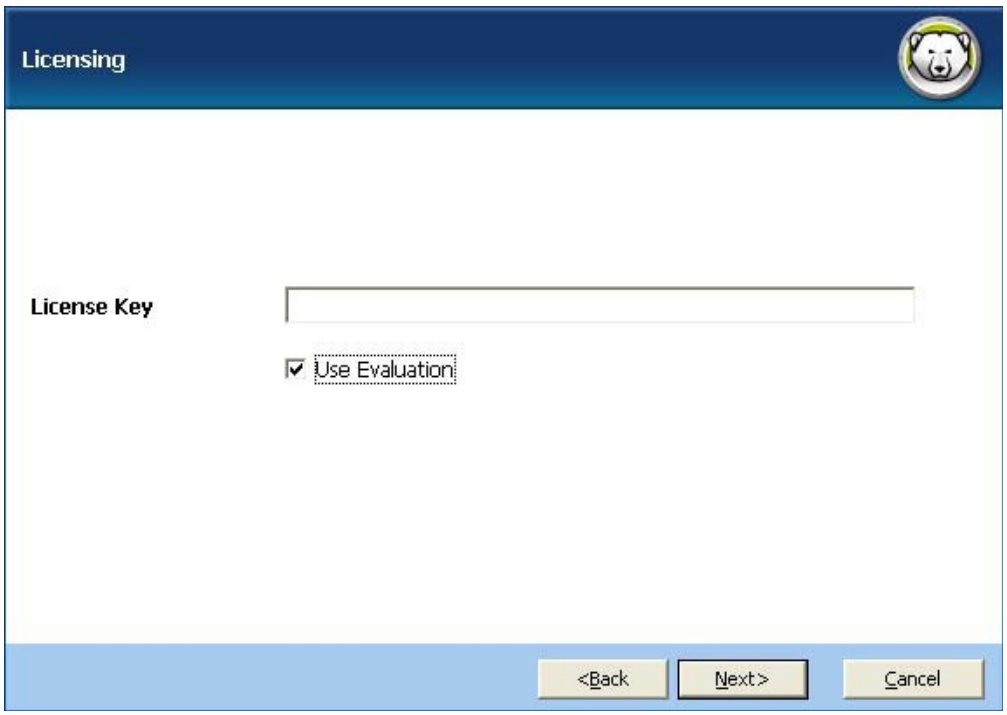


Figure 82. Deep Freeze installation (3)

Choose the drives to Freeze from the displayed list.

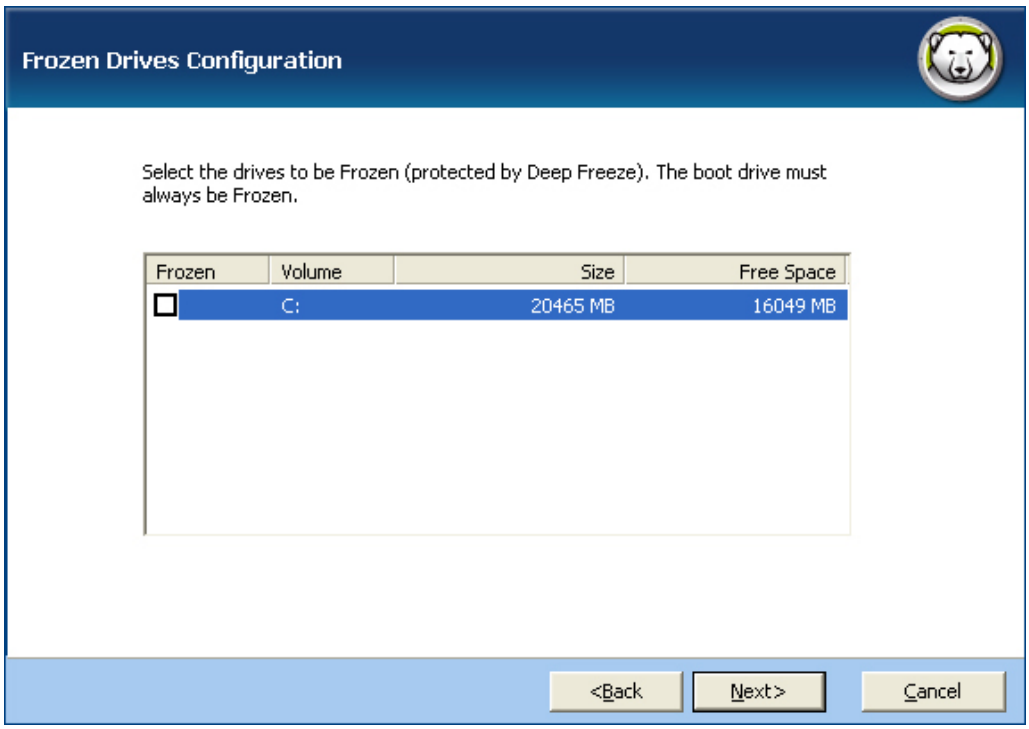


Figure 83. Deep Freeze installation (4)

Finally, click Install to begin the installation. The computer restarts immediately after the installation is complete.

The Frozen or Thawed Deep Freeze icon appears in the System Tray after installation and indicates whether the computer is currently protected by Deep Freeze (Frozen) or unprotected (Thawed). When the computer is Frozen, the following icon is displayed in the System Tray:

Figure 84. Frozen Deep Freeze icon

When the computer is Thawed, the following icon is displayed in the System Tray:

Figure 85. Thawed Deep Freeze icon

IX.2 Deep Freeze Login

To do the login to Deep Freeze we have to press SHIFT and double-click the Deep Freeze icon in the System Tray. The following dialog is displayed below.

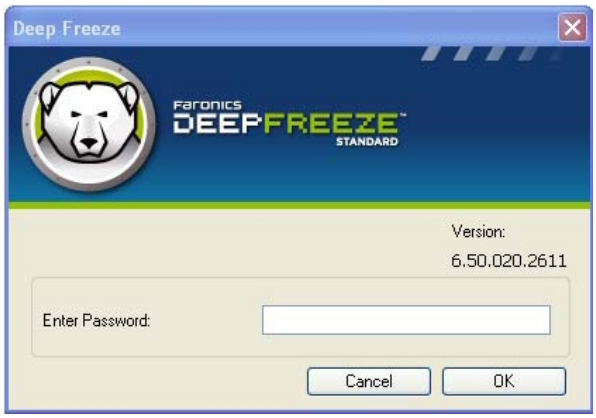


Figure 86. Deep Freeze login

If no password has been set, leave the password field blank and click *OK*.

The *Status* tab is used to set the mode Deep Freeze will be in after the next restart. We have to choose one of the following options:

- *Boot Frozen* to ensure the computer is Frozen the next time it is restarted.
- *Boot Thawed on next* to ensure the computer is Thawed each time it is restarted for the next specified number of restarts.
- *Boot Thawed* to ensure that the computer is Thawed each time it is restarted.

In our environment we decide to implement the option Boot Frozen in order to ensure that every morning when we turn the server we will have the default settings configured.

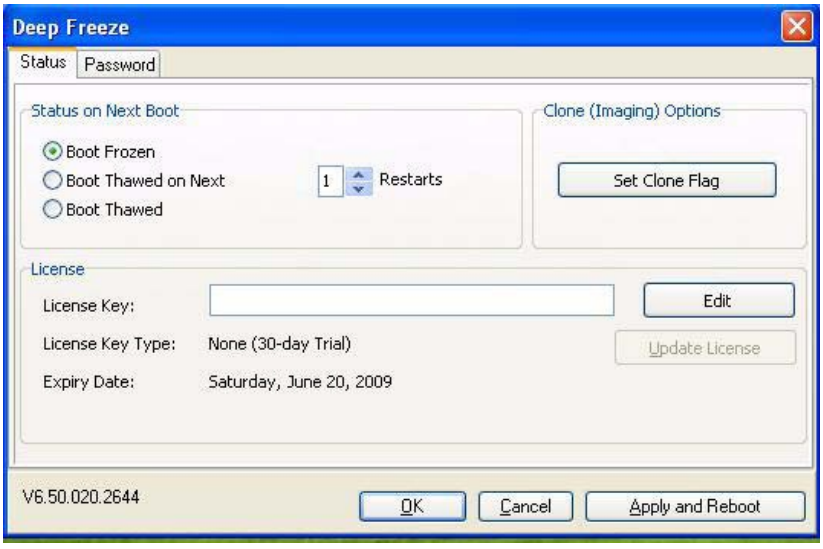


Figure 87. Deep Freeze status tap

APPENDIX X. Digitazion of Reports

X.1 Old Reports

Monthly report of hospitalized patients

Reporte Mensual de Fisioterapia
Pacientes Hospitalizados

SILAIS
Municipio
Unidad
Mes

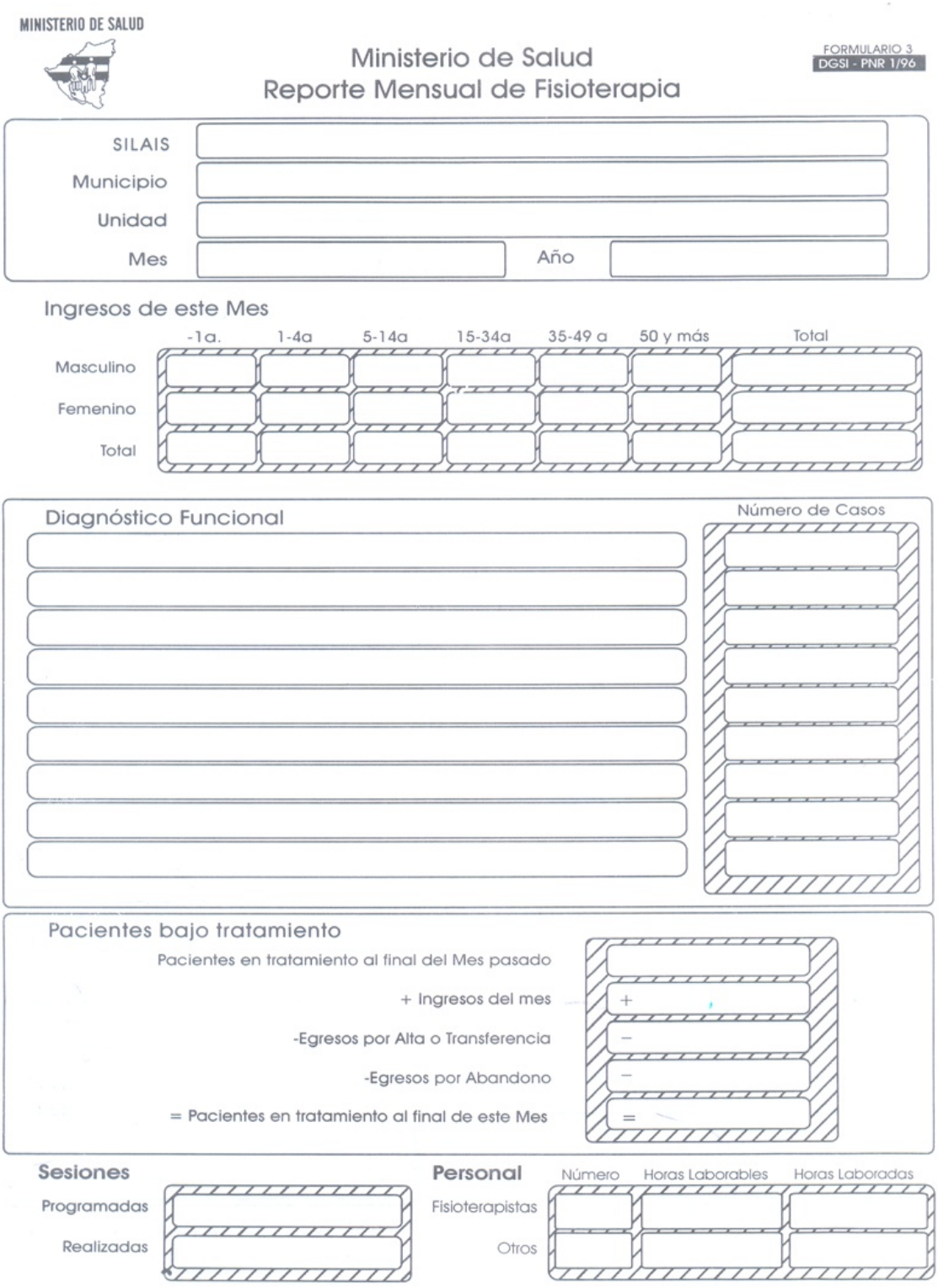
Salas	Amanda				Francis		Guicelly		Iveia		Total
Medicina Interna											
Ortopedia											
UCI											
Pediatría											
Ginecobstetricia											
	M	F	M	F	M	F	M	F	M	F	
-1a											
1-4a											
5-14a											
15-34a											
35-49a											
50 – más											
Tratamientos											
Terap. Resp.											
Reed. Musc.											
Recomendaciones											
Total											

Observaciones:

Monthly Report per treatment

	Amanda				Francis		Guicelly			Total
Total de pte										
Pte repetitivos										
Ingresos Nuevos										
Ptes sig. mes										
Altas										
Abandonos										
Sesiones program										
Sesiones ejecutadas										
Dolor musc.										
Debilidad musc.										
Limitación Func.										
Limitación Art.										
	M	F	M	F	M	F	M	F	M	F	
- 1 año											
1- 4 a											
5 – 14a											
15- 34 a											
35 – 49 a											
50 - más											
Termoterapia										
Masaje										
Electroestimulo										
Reed. Muscular										
Reed. Marcha										
Mecanoterapia										
Tto. Esp.										
Ultrasonido										
Total										

Monthly Report general statics



MINISTERIO DE SALUD

Ministerio de Salud
Reporte Mensual de Fisioterapia

FORMULARIO 3
DGSI - PNR 1/96

SILAIS
Municipio
Unidad
Mes
Año

Ingresos de este Mes

	-1a.	1-4a	5-14a	15-34a	35-49 a	50 y más	Total
Masculino							
Femenino							
Total							

Diagnóstico Funcional	Número de Casos

Pacientes bajo tratamiento

Pacientes en tratamiento al final del Mes pasado	
+ Ingresos del mes	+
-Egresos por Alta o Transferencia	−
-Egresos por Abandono	−
= Pacientes en tratamiento al final de este Mes	=

Sesiones

Programadas	
Realizadas	

Personal

	Número	Horas Laborables	Horas Laboradas
Fisioterapistas			
Otros			

X.2 Excel files

Patients admission

INGRESOS

Nº	Nº exp.	Nombre	Municipio / Comunidad	Fecha Ingreso	Diagnóstico	Hospital/E. Médica	Fecha Egreso
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							

Monthly report

Reporte Mensual de Fisioterapia

	Amanda	Francis	Guicelly	Lucía	Total
Total de pte					0
Pte repetitivos					0
Ingresos Nuevos					0
Ptes sig.mes					0
Altas					0
Abandonos					0
Sesiones program					0
Sesiones ejecutadas					0

Diagnóstico

Dolor muscular					0
Debilidad muscular					0
Limitación Fun.					0
Limitación Articular					0

	M	F	M	F	M	F	M	F	Total
-1 a									0
1 - 4 a									0
5 - 14 a									0
15 - 34 a									0
35 - 49 a									0
50 - más									0
	0		0		0		0		0

Tratamientos

Termoterapia					0
Masaje					0
Electroestimulo					0
Reed.Muscular					0
Reed. Marcha					0
Mecanoterapia					0
Tto. Esp.					0
Ultrasonido					0
Total	0	0	0	0	0

Ministerio de Salud
Reporte Mensual de Fisioterapia

SILAIS	RAAS		
Municipio	Bluefields		
Unidad	HRESB		
Mes	Enero	**Año**	2012

	-1a	1-4a	5-14a	15-34a	35-49a	50 y más	Total
Masculino	0	0	0	0	0	0	**0**
Femenino	0	0	0	0	0	0	**0**
Total	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Diagnóstico Funcional	**Nº de casos**
Dolor Muscular	0
Debilidad Muscular	0
Limitación Funcional	0
Limitación Articular	0
Total	**0**

Actividades Realizadas	**Nº de casos**
Termoterapia	0
Masaje	0
Electroestimula	0
Reed.Muscular	0
Reed. Marcha	0
Mecanoterapia	0
Tto.Esp.	0
Ultrasonido	0
Total	**0**

Pacientes bajo tratamiento

Pacientes en tratamiento al final del Mes pasado	0
+ Ingresos del mes	0
- Egresos por Alta o Transferencia	0
- Egresos por Abandono	0
= Pacientes en tratamiento al final de este Mes	**0**

Sesiones

Programadas	0
Realizadas	0

Personal	**Número**	**Horas Laborables**	**Horas Laboradas**
Fisio.			
Otros			

Resp. de Fisioterapia	Lic. Guicelly	**Fecha**		**Firma**	
Resp. de Estadística	Lic. Gina Gaitán	**Fecha**		**Firma**	
Director de la Unidad		**Fecha**		**Firma**	

Monthly report of hospitalized patients

Reporte Mensual de Fisioterapia
Pacientes Hospitalizados

SILAIS	RAAS		
Municipio	Bluefields		
Unidad	HRESB		
Mes	Marzo	**Año**	2012

Salas	**Amanda**	**Francis**	**Guicelly**	**Lucía**	**Total**
Medicina Interna					**0**
Ortopedia					**Err:501**
UCI					**Err:501**
Pediatría					**Err:501**
Ginecobstetricia					**Err:501**
Total	**0**	**Err:501**	**Err:501**	**Err:501**	**Err:501**

	M	**F**	**M**	**F**	**M**	**F**	**M**	**F**	
-1 a									**0**
1 - 4 a									**Err:501**
5 - 14 a									**Err:501**
15 - 34 a									**Err:501**
35 - 49 a									**Err:501**
50 - más									**Err:501**
	0		**Err:501**		**Err:501**		**Err:501**		**Err:501**

Tratamientos

Terapia Resp.					**0**
Reed. Musc.					**Err:501**
Recomendaciones					**Err:501**
Total	**0**	**Err:501**	**Err:501**	**Err:501**	**Err:501**

Observaciones

APPENDIX XI. Excel User Manual

telecos sense fronteres

Documentos Excel

Formación técnica sobre
la herramienta de Office Excel 2007

6 de marzo de 2012
Departamento de Fisioterapia - HRESB

telecos sense fronteres

Índice

- Motivación
- Objetivos
- Documentos tratados
  - Ingresos de pacientes
  - Reporte mensual de pacientes hospitalizados
  - Reporte mensual de Fisioterapia
- Herramientas básicas
- Propuestas de mejora

Motivación

- Datos diarios y mensuales siempre tratados a mano, sin un control del almacenamiento.
- Interés propio del personal en digitalizar estadísticas e información, así como aprender nuevas tecnologías.
- Computadora en buen estado ubicada en Fisioterapia con escaso uso.

Objetivos

- Llevar un control más concreto del ingreso de pacientes.
- Digitalizar estadísticas diarias y mensuales.
- Facilitar y ahorrar tiempo en el trabajo de las empleadas.
- Dar uso a los equipos instalados en Fisioterapia.

telecos sense fronteres

Documentos tratados

'Ingreso de pacientes'

- Gestión de datos de los nuevos pacientes

Fisioterapia | Enero - 2012 | HRESB

INGRESOS

Nº	Nº expediente	Nombre	Municipio/Comunidad	Fecha de Ingreso	Diagnóstico	Hospital/E. Médica
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

telecos sense fronteres

Documentos tratados

'Reporte mensual de pacientes hospitalizados'

- Estadísticas por especialista

Salas	Amanda	Francis	Guicelly	Lucía	Total
Medicina Interna	1	1		1	3
Ortopedia	1	1		1	3
UCI	1	1		1	3
Pediatría	3	9		9	21
Ginecobstetricia	0	0		0	0
Total	6	12	0	12	30

	M	F	M	F	M	F	M	F	
-1 a	2	1	2	4			2	4	15
1 - 4 a			3	1			1	1	6
5 - 14 a		1							1
15 - 34 a	1						1	1	3
35 - 49 a	1						1	1	3
50 - más			1	1					2
	6		12		0		12		30

Tratamientos

Terapia Resp.	3	9		9	21
Reed. Musc.	1	2		1	4
Recomendaciones	5	4		10	19
Total	9	15	0	20	44

telecos sense fronteres

Documentos tratados

'Reporte mensual de Fisioterapia'

- Estadísticas de diagnósticos y actividades realizadas

	Amanda	Francis	Guicelly	Lucía	Total
Total de pte		3			3
Pte repetitivos		4			4
Ingresos Nuevos					0
Ptes sig.mes					0
Altas					0
Abandonos					0
Sesiones program					0
Sesiones ejecutadas					0

Diagnóstico

Dolor muscular					0
Debilidad muscular					0
Limitación Fun.					0
Limitación Arterial					0

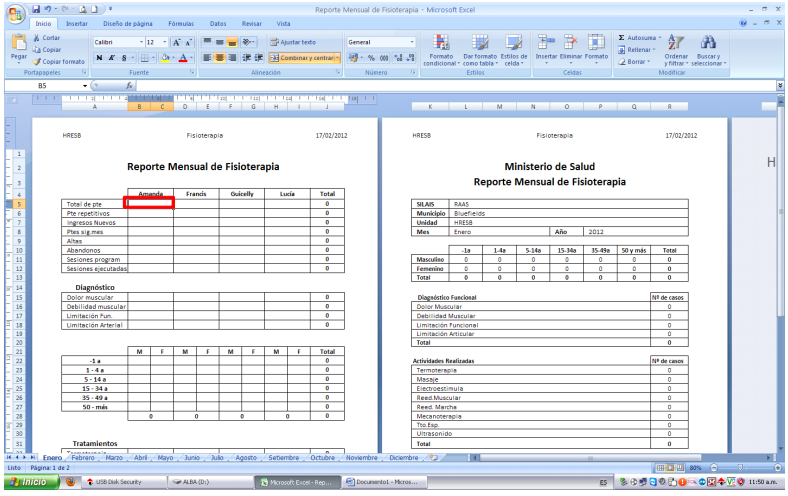
Actividades Realizadas	Nº de casos
Termoterapia	0
Masaje	0
Electroestimula	0
Reed.Muscular	0
Reed. Marcha	0
Mecanoterapia	0
Tto.Esp.	0
Ultrasonido	0
Total	**0**

telecos sense fronteres

Herramientas básicas

Modificar datos

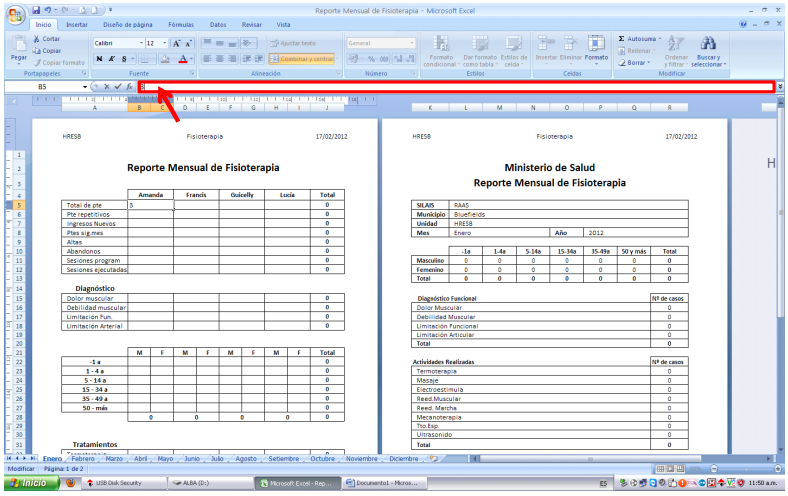
- Seleccionar la casilla que se quiere modificar



Herramientas básicas

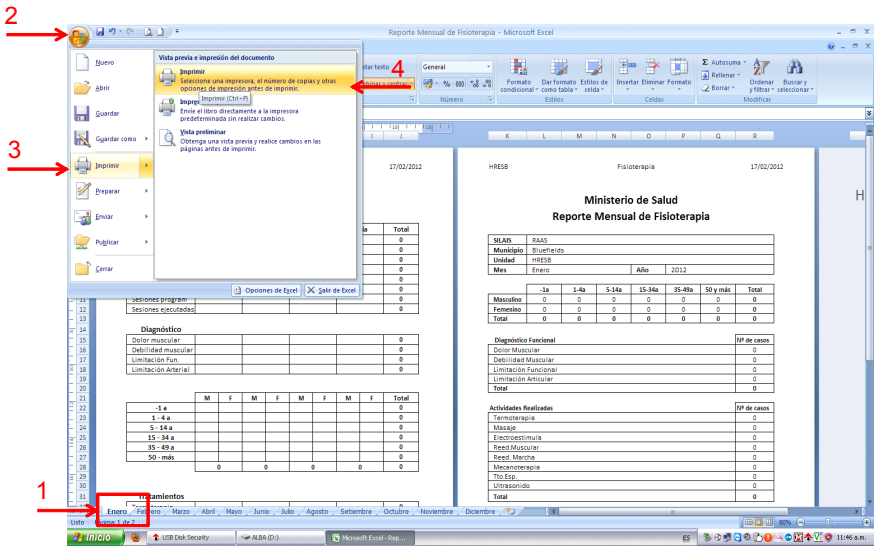
Modificar datos

- Seleccionar la barra en rojo para poder escribir en la casilla.



Herramientas básicas

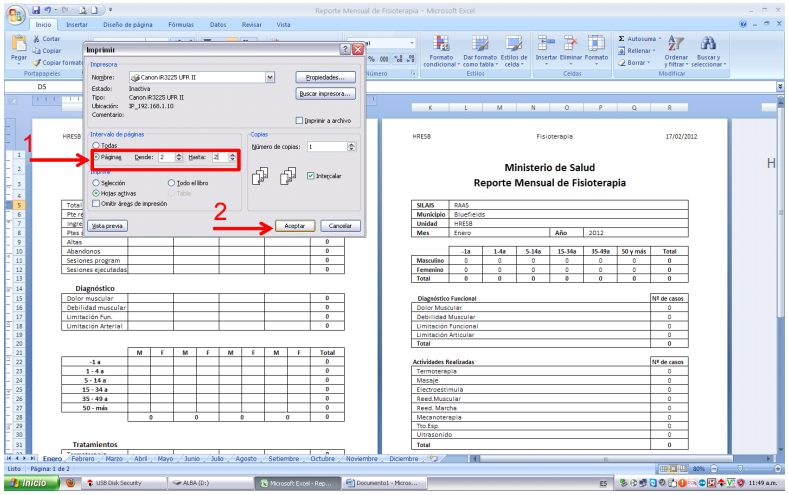
Imprimir documento



Herramientas básicas

Imprimir documento

- Seleccionar la página que se quiere imprimir



Propuestas de mejora

- Digitalizar la hoja de incidencias diarias, donde se muestran los pacientes ingresados y los tratamientos seguidos a cada uno de ellos, por especialista.

- Sería necesario:
  - Tener una infraestructura de computadoras más amplia, una para cada especialista.

APPENDIX XII. Agreement UPC-BICU

Model BILATERAL AGREEMENT for the academic year 2011/2012

between (name and ID code of the institution)	BLUEFIELDS INDIAN & CARIBBEAN UNIVERSITY (BICU)	
Socrates contact person (name, address, phone, fax, E-mail)	Ing. René Cassell Martinez, Secretario General	Email : guabul59@gmail.com phone 505-25721277
and (name and ERASMUS ID code of the institution)	UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC) E BARCELO 03 Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels (EETAC)	
Mobility contact person (name, address, phone, fax, E-mail)	Ms Silvia Ruiz International Office Avda.Canal Olímpic, s/n 08860 Castelldefels, SPAIN	Email: EETAC.relacions.externes@upc.edu Tel: +34 93 413 7030 Fax:+34 93 413 7000
Dept. contact person (name, address, phone, fax, E-mail)	Ms Mª Jesús Melo International Office Avda.Canal Olímpic, s/n 08860 Castelldefels, SPAIN	Email:EETAC.relacions.externes@upc.edu Tel: +34 93 552 3518 Fax:+34 93 413 7020

The above mentioned parties agree to cooperate in the following activities within the mobility programme. Both parties agree to adhere to the principles and conditions as stated in the Socrates Guidelines, the Application Form and, in case of approval, the Contract. Both parties will endeavour to carry out the agreement to the best of their abilities.

Student Mobility

Subject Area		Level		Country		Total number	
Code	Name	Under-graduate	Graduate	from	to	Students	Student months (=sum)
523	Telecommunications Engineering	X X	X X	SP NI	NI SP	2	10x2

Teaching staff mobility of short duration (1-8 weeks)

Subject Area Code	Topic(s) taught	Name of staff member	Home Country	Host Country	Duration in number of weeks	Number of teaching hours per week
523	Telecommunications Engineering					

Signatures of the authorised representatives of both institutions:

Name of institution: BLUEFIELDS INDIAN & CARIBBEAN UNIVERSITY (BICU)	Name of Institution: Universitat Politècnica de Catalunya (UPC) Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels (EETAC)
Name and status representative: Ing. René Cassell Martinez, Secretario General	Name and status of representative: Silvia Ruiz, Mobility Coordinator
Signature:	Signature:
Date: Stamp 13/DIC/2011	Date: Stamp 13/DIC/2011

BLUEFIELDS INDIAN & CARIBBEAN UNIVERSITY (B.I.C.U.) SECRETARIO GENERAL

Campus del Baix Llobregat
UNIVERSITAT POLITÈCNICA DE CATALUNYA
Àrea de Relacions Externes
Edifici D7, planta 0
C/ Esteve Terradas, 10
08860 Castelldefels
Tel. 93 552 35 00
Fax 93 413 70 20

APPENDIX XIII. Agreement TSF-SILAIS RAAS

Bluefields, Junio de 2012
Convenio de Colaboración entre
TSF y SILAIS RAAS

Nosotros, JUDIT RIUS CAMPRUBÍ, mayor de edad, Ingeniera Técnica de Telecomunicación, con documento de identidad 47722829Z y de nacionalidad española, actuando en su calidad de Vocal de la Junta Directiva de la ONG "Telecos Sense Fronteres", en lo sucesivo denominada TSF, en representación de la Junta Directiva con facultad legal para suscribir el presente Convenio, por una parte, Dr. RICARDO TAYLOR ELLIS, mayor de edad, casado, médico y cirujano, portador de Cédula de Residencia Nicaragüense Número 602-311260-0001Q, actuando como director del SILAIS RAAS, con facultad legal para suscribir el presente Convenio.

Considerando:

Primero: Que TSF, es una organización no gubernamental (ONG) sin ánimo de lucro que tiene como finalidad trabajar para reducir la llamada brecha digital en aquellos países menos favorecidos.

Segundo: Que, conscientes de que el acceso a las comunicaciones y la conectividad global tienen un impacto profundo sobre la calidad de vida de las personas, sus posibilidades de formación, el acceso a servicios de salud, la defensa de sus derechos civiles y en general el desarrollo máximo de su potencial como ciudadanos, la asociación tiene como objetivo principal facilitar, en la medida de sus posibilidades y en colaboración con otras asociaciones y entidades, el acceso a los servicios de telecomunicaciones a los núcleos de población más desfavorecidos, y situados en la otra parte de la llamada "fractura digital", a través de proyectos concretos.

Tercero: Que, desde hace ya algunos años, TSF está realizando un proyecto de cooperación en Nicaragua en estrecha colaboración con el Hospital Regional Ernesto Sequeira Blanco de Bluefields. Se han proporcionado herramientas en Telecomunicaciones, para que la región pueda mejorar su nivel sanitario y pueda conocer las ventajas de las TIC en sus procesos, gestiones y vida cotidiana.

Cuarto: Que el SILAIS RAAS es una estructura regional del Ministerio de Salud de Nicaragua, bajo quien se encuentran todas las unidades de salud municipales, como son el Hospital Regional Escuela "Dr. Ernesto Sequeira Blanco, in Memoriam" y el Centro de Salud "Juan Manuel Morales" , ambos de Bluefields, así como el resto de unidades de los siete municipios.

Quinto: Que en ambas organizaciones existen ejes transversales enfocados en el fortalecimiento de capacidades locales, participación comunitaria así

como la implementación de tecnologías amigables al medio ambiente.

Sexto: Que **TSF** y **SILAIS RAAS** consideran indispensable la participación activa de actores locales para el desarrollo de proyectos en beneficio de las comunidades más desposeídas.

Séptimo: Que el intercambio y la colaboración interinstitucional fortalece las bases para la implementación y el mantenimiento de nuevas tecnologías y planes de desarrollo en pro de la población nicaragüense.

Por lo tanto, acordamos:

TSF y el **SILAIS RAAS** acuerdan la celebración de este convenio el cual se regirá por las siguientes cláusulas:

I. Naturaleza y objetivo del convenio:

El presente convenio define la relación general interinstitucional solidaria de intercambio y colaboración cuyo propósito principal es establecer sinergia entre ambas organizaciones, para el desarrollo y mantenimiento de diversos proyectos en beneficio de las comunidades rurales marginalizadas de Nicaragua.

II. Principios de actuación:

TSF y **SILAIS RAAS**, para efectos de regular las relaciones interinstitucionales de trabajo, acuerdan los siguientes principios:

II.1. Implicación directa del **SILAIS RAAS** en el mantenimiento de la infraestructura de telefonía de VoIP y el radioenlace que **TSF** ha brindado durante estos años a la región, localizados en:

a) El Hospital Regional Ernesto Sequeira Blanco, con la infraestructura de telefonía de VoIP, el sistema NComputing y una antena AirGrid para los radioenlaces.

b) La comunidad de San Francisco de Kukra River, con un teléfono de VoIP y una antena Ubiquiti para el radioenlace.

c) El Cerro Aberdeen de Bluefields, con 3 antenas (AirGrid y Ubiquiti) para los radioenlaces.

II.2. Revisión y mantenimiento anual de los equipos y dispositivos instalados en las localizaciones previamente mencionadas para su correcto funcionamiento.

a) El material consiste en: Teléfonos de VoIP Grandstream, equipos Ncomputing, cables coaxiales, conectores, antenas y dispositivos configurables (AirGrid, Bullet), switch, torre de madera.

b) La problemática puede derivar de: desconfiguración de los teléfono o antenas, deterioramiento de los cables coaxiales y/o conectores, oxidación de las antenas, erosión de la madera de la torre, mal funcionamiento del switch.

II.3. La resolución de las posibles anomalías se resolverán, como principal opción, con la contratación temporal del ingeniero en computación James Alaniz, conocedor del proyecto desde sus inicios y totalmente capacitado para realizar las tareas necesarias.

II.4. En el caso que alguno de los equipos mencionados anteriormente no pueda ser reparado, el **SILAIS RAAS** asume el coste de comprar y reemplazar dicho equipo por uno de nuevo del mismo modelo.

II.5. Respeto de la independencia y dinámicas propias de cada organización.

II.6. Promoción de las relaciones respetuosas y cordiales entre los diversos actores involucrados en diferentes procesos definidos en el marco de este convenio.

II.7. Cumplimiento de los compromisos y acuerdos estipulados en este convenio.

III. Operatividad del convenio:

III.1. Para efectos prácticos del convenio, cuando se desarrollen acciones o contratos específicos de colaboración entre ambas instituciones, se requiere de la solicitud expresa de una de las partes y el consenso de ambas.

III.2. En el caso de ejecución de proyectos específicos, se pueden añadir Anexos al presente convenio para la descripción detallada de las responsabilidades respectivas de ambas partes, según el modelo en Anexo.

III.3. Para la ejecución del presente convenio, las partes nombran como contrapartes oficiales a:

a) Por parte de TSF:
Judit Rius Camprubí
e-mail: juditriuscamprubi@gmail.com

b) Por parte del SILAIS RAAS:
Dr. Ricardo Taylor Ellis
Teléfono: (+505) 257 222 20 / (+505) 885 467 93

c) Por parte del Centro de Salud Juan Manuel Morales:
Dr. Mario Méndez
Teléfono: (+505) 257 222 34 / (+505) 891 662 53

d) Por parte del Hospital Regional Ernesto Sequeira Blanco
Dra. Aránzazu Arana
Teléfono: (+505) 257 201 55 / (+505) 891 453 82

III.4. En el caso que alguna de las contrapartes oficiales no forme parte de la organización a la que representan en el momento de la ejecución del proyecto o modificación de alguna de las acciones, se considera que la persona la cual ocupa su cargo es nombrada contraparte oficial, con pleno derecho de ejecución del convenio.

IV. Domicilios oficiales:

a) Telecos Sense Fronteres
C/ Esteve Terrades 7,
CP 08860. Castelldefels, Barcelona, España
Sitio web: www.telecossensefronteres.org
e-mail: info@telecossensefronteres.org

b) SILAIS RAAS
Barrio de Nueva York, Bluefields
RAAS, Nicaragua

c) Centro de Salud Juan Manuel Morales
Barrio de Nueva York, Bluefields
RAAS, Nicaragua

d) Hospital Regional Ernesto Sequeira Blanco
Barrio de San Pedro, Bluefields
RAAS, Nicaragua

V. Resolución de conflictos:

V.1. Cualquier conflicto entre las Partes que no sea resuelto por la vía directa y conciliatoria, deberá dirigirse mediante proceso de arbitraje de equidad, cuyo tribunal estará integrado por tres árbitros: uno nombrado por **TSF**, otro por **SILAIS RAAS** y un tercero designado de común acuerdo por ambas partes.

V.2. En caso de incumplimiento de alguna de las obligaciones por ambas parte o en caso de algún daño causado mutuamente, las

diferencias serán ventiladas ante las autoridades administrativas y judiciales de la República de Nicaragua, debiéndose cubrir el costo de su representación legal en Nicaragua.

VI. Duración del convenio:

El presente convenio tiene una duración limitada a dos años a partir de su firma por cada una de las partes.

Este convenio se prorrogará tácitamente por períodos de 2 años, salvo que alguna de las partes comunique de forma fehaciente la voluntad de finalizarlo, con una antelación mínima de 3 meses antes del vencimiento de cualquiera de sus prórrogas.

VII. Modificación, anexos y disolución:

La modificación de este convenio ó la adición de un anexo requieren del consenso expreso escrito de las partes. La disolución se requiere la voluntad expresa de una de las partes y debe ser negociada conforme lo pactado, quedando claras las razones de la disolución por escrito.

Leído todo lo anterior y encontrándolo conforme lo expresaron las partes correspondientes, procedemos a firmar en dos tantos de un mismo tenor a los_____ días del mes de _____ del año 2012.

Judit Rius Camprubí **Vocal Junta Directiva** **Telecos Sense Fronteres**	**Dr. Ricardo Taylor Ellis** **Director del SILAIS RAAS** **Nicaragua**
Dr. Mario Méndez **Director del Centro de Salud** **Juan Manuel Morales** **Nicaragua**	**Dra. Aránzazu Arana** **Directora del Hospital Regional** **Ernesto Sequeira Blanco** **Nicaragua**

MODELO DE ANEXO N°A COMPLETAR
CONVENIO ESPECÍFICO PARA EJECUCIÓN DEL PROYECTO: A COMPLETAR
entre TSF y SILAIS RRAS

1.1. Objetivo general

1.2. Objetivos específicos

1.2.1. ...

Cláusula Segunda: C*ompromisos de TSF*

2.1 ...

Cláusula Tercera: *Compromisos de SILAIS RAAS*

3.1 ...

Cláusula Cuarta: *Compromisos Comunes*

4.1. Intercambiar información de interés mutuo.

4.2. Velar por el cumplimiento de acciones establecidas en el marco del presente convenio a fin de garantizar los resultados esperados.

Cláusula Quinta: *Duración, ejecución y vigencia del Convenio*

5.1. La duración del presente Convenio será

5.2. El presente convenio finalizará una vez cumplidos todos los compromisos por las partes.

5.3. Para la ejecución del presente convenio las partes nombran como contrapartes oficiales a:

Por parte de TSF:
A COMPLETAR

Por parte de blueEnergy
A COMPLETAR

Cláusula Sexta: Firma

Leído todo lo anterior y encontrándolo conforme lo expresaron las partes correspondientes, procedemos a firmar en dos tantos de un mismo tenor a los_____ días del mes de _____ del año 2012.

Judit Rius Camprubí
Vocal Junta Directiva
Telecos Sense Fronteres

Dr. Ricardo Taylor Ellis
Director del SILAIS RAAS
Nicaragua

Dr. Mario Méndez
Director del Centro de Salud
Juan Manuel Morales
Nicaragua

Dra. Aránzazu Arana
Directora del Hospital Regional
Ernesto Sequeira Blanco
Nicaragua

APPENDIX B
PROJECT CHRONOLOGY

MIÉRCOLES, 23 DE NOVIEMBRE DE 2011

Preparando la nueva fase

A dos semanas de empezar la nueva fase del proyecto, creemos que es el momento de presentarnos. A partir de ahora hasta el verano, Alba y Genís seremos los cooperantes encargados de seguir con el proyecto de telemedicina en Nicaragua.

Principalmente, los objetivos que hemos definido son los siguientes:

- Terminar el radioenlace entre el HRESB y el Puesto de Salud de Monkey Point que Macarena y Jesús empezaron hace unos meses.
- Implementar el software de gestión hospitalario que el Ministerio de Salud de Nicaragua (MINSA) está desarrollando actualmente, para facilitar el día a día del personal del hospital.
- Crear una VPN para interconnectar los diferentes Puestos de Salud de la RAAS.
- Implementar una arquitectura de escritorios remotos (con NComputing) para los principales departamentos del HRESB, con la finalidad de solucionar los problemas climatológicos y de gestión que presentan los ordenadores actuales.

Durante la preparación a lo largo de estas últimas semanas, hemos simulado en un laboratorio de la UPC, la implementación de la VPN y la viabilidad de los escritorios remotos, para tener un conocimiento previo de las tecnologías y facilitar el trabajo *in situ*.

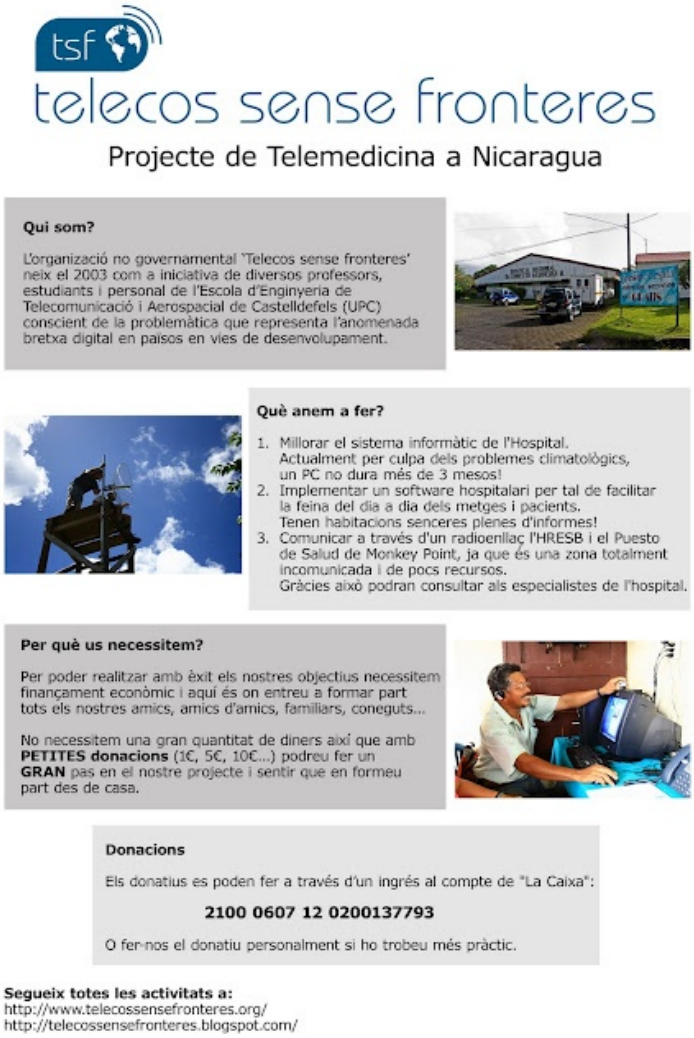
Día de trabajo en el laboratorio

JUEVES, 24 DE NOVIEMBRE DE 2011

Buscando financiación

¡Os necesitamos!
Con la ayuda del Centre de Cooperació per al Desenvolupament de la UPC (CCD), hemos conseguido gran parte del presupuesto necesario para la nueva campaña. Aún así, nos falta un empujón! Hemos realizado una serie de acciones, como este póster, para incentivar a amigos, familiares, conocidos o cualquier persona que tenga afinidad con el tema.

¿Te animas a participar? Puedes hacer donaciones aquí.



JUEVES, 15 DE DICIEMBRE DE 2011

A vueltas con la cooperación

Uno de los pilares básicos de la cooperación trata de implicar directamente las personas a quien vas a ayudar, con la finalidad de que no observen el proyecto desde la distancia, de una manera totalmente ajena, sino que sientan que forman parte de él, que están involucrados y son una pieza clave.

Con el acuerdo que recientemente hemos cerrado entre la Bluefields Indian & Caribbean University (BICU) y la Universitat Politècnica de Catalunya (UPC), se pretende dar continuidad al proyecto de telemedicina de forma ilimitada, ya que este vínculo involucrará a algunos estudiantes de la BICU para que hagan un seguimiento de las acciones que TSF realizará en el futuro. De este modo, cuando no haya la presencia de cooperantes en Bluefields, y gracias a los conocimientos adquiridos, ellos podrán realizar las tareas de mantenimiento que se precisen, acercando el propio proyecto a la comunidad.

La tarea no es sencilla pero promete, veremos como evoluciona!

LUNES, 16 DE ENERO DE 2012

Llegada de Alba en Bluefields

Damos la bienvenida a Alba, que justo acaba de llegar a Bluefields y ya se siente una nica más.

En estos primeros compases después de las vacaciones navideñas, hemos estado trabajando en tareas de mantenimiento del hospital, como la revisión de los teléfonos IP (muchos de los cuales no estaban funcionando correctamente) o la reubicación de algunos ordenadores dentro del recinto con tal que el personal pueda trabajar más tranquilamente. Era inversemblante ver, por ejemplo, que en la sala de neonatos se allara un terminal de uso diario por los doctores (que entraban y salían continuamente), cuando debería ser un espacio de silencio y paz para los bebés.

Hemos detectado que el enlace con La Aurora está dañado y la comunicación está cortada, así que nos ponemos manos a la obra para solucionarlo lo más rápidamente posible. Mientras que en Bluefields, Jimmy nos enseñará como instaló la tecnología NComputing en el seminario del pueblo.

También hemos tenido el placer de conocer a Noris Padilla, estudiante de la BICU que nos ayudará desde mañana mismo con todo lo que sea necesario, mostrando una excelente actitud para aprender.

Árbol navideño delante del Hospital

VIERNES, 20 DE ENERO DE 2012

Actividades de la semana

Durante esta semana hemos tenido la oportunidad de visitar el Seminario Pío X de Bluefields, done Jimmy nos enseñó en detalle el sistema de NComputing que instaló para que los chicos del seminario pudieran trabajar con computadoras. Esta tecnología es ideal en ambientes como este o en el hospital, donde tanto el consumo de energía o el mantenimiento de los equipos es mucho menor que en una configuración estándar.

Sistema del seminario

Por otra parte, Noris Padilla y Carla Hooker son las dos estudiantes de la BICU que están colaborando activamente con TSF. Tienen una muy buena actitud y ganas de aprender todos los conceptos que no han podido adquirir durante sus estudios en la universidad (más enfocados a temática de sistemas). Trabajan con nosotros todas las mañanas. Nos han ayudado, por ejemplo, en bloquear ciertas páginas web (como Facebook o YouTube) con la finalidad de descongestionar un poco la pésima velocidad de la red del hospital.

Carla y Noris en la biblioteca

Paralelamente, hemos configurado y provado el material que Jesús y Macarena nos dejaron aquí. Las antenas Hyperlink que utilizaremos para hacer el radioenlace entre el Cerro Aberdeen y Monkey Point funcionan a la perfección, y estamos resolviendo problemillas que han aparecido con las AirGrid para hacer el enlace corto entre Monkey Point y el Puesto de Salud de esta población.

VIERNES, 27 DE ENERO DE 2012

Pequeños obstáculos

Tal y como os comentamos en el post anterior, tuvimos algunos problemas con una de las antenas AirGrid que comunicará la torre de Monkey Point con el Puesto de Salud de la comunidad. Finalmente, después de hacer toda las pruebas posibles y de ponernos en contacto con la empresa donde se compró el material, se ha llegado a la conclusión que está dañada. Así que esta mañana hemos hecho todos los trámites para devolverla y poder recibir una de nueva. Esperamos que llegue pronto :)

Aun así, con el resto de material ya configurado y listo, hemos realizado una simulación de la comunicación entre ellas y se ha probado de realizar una llamada vía teléfono VoIP. Todo ha salido satisfactoriamente! Así que sólo estamos pendientes de recibir la nueva antena y podernos reunir con el Gobierno comunal para empezar a trabajar.

Simulación de llamada VoIP entre Hospital y Monkey Point

Todos hablan de la brujería de Bluefields y recientemente un virus que oculta las carpetas de los PenDrive está causando quebraderos de cabeza a los ciudadanos de la región. Finalmente con la ayuda de Jimmy hemos podido controlar la situación y solucionar el problema. Esperamos que el virus nos dé una tregua.

VIERNES, 17 DE FEBRERO DE 2012

Al suave

Después de varias semanas sin escribir en el blog os ponemos al día de los trabajos realizados. Principalmente hemos dedicado tiempo en comprar los equipos NComputing y el servidor. Esto nos ha llevado algunos quebraderos de cabeza ya que vienen de Managua y de Miami y teníamos que coordinar toda la compra. Pero finalmente ya está todo en camino y antes que termine el mes esperamos tenerlo todo aquí! :)

Otro trabajo importante de éstas semanas ha sido la digitalización de las fichas que utilizan en el departamento de Fisioterapia. A través de algunas de sus especialistas, nos llegó la petición de poder hacer un uso más amplio de la computadora que tienen instalada en el departamento. Nuestra propuesta fue digitalizar las fichas que utilizan mensualmente para hacer los recuentos de pacientes y tratamientos, con la finalidad de facilitarles la tarea cuando desde Estadísticas se les pidan los resultados. Nuestro trabajo ha sido pasar las fichas que tenían en papel a Excel. Además se les ha hecho una capacitación del programa Excel ya que algunas de ellas no tenían conocimientos.

Y seguimos con la paciencia de que el tiempo mejore y las lluvias cesen, con tal de poder ir a San Pacho a verificar en qué estado andan los equipos, y a Monkey Point para terminar el radioenlace.

Después de ya casi cumplir dos meses de la llegada de Genís y un mes de mi llegada, Alba, podemos decir que nos encontramos muy a gusto con todos nuestros compañeros y Bluefields. Así que nos despedimos con una foto de todos ellos en el día del amor y la amistad.

Día del amor y la amistad

MARTES, 21 DE FEBRERO DE 2012

TSF en Radio Kukra Hill

Este fin de semana tuvimos la oportunidad de visitar Kukra Hill gracias a la invitación de Padre Enrique, un misionero español que está desarrollando varias tareas en esta parte del país, con la gente del pueblo y de todas la comunidades cercanas.

El sábado por la tarde, junto a un par de psicólogas gallegas que trabajan en el CAPS de Bluefields y nos acompañaban, fuimos entrevistados en Radio Kukra Hill por el mismo Padre Enrique, comentando los detalles del proyecto de telemedicina que estamos llevando a cabo en la RAAS, región donde se encuentra este pequeño municipio. La cálida acogida que tuvimos, así como el agradecimiento que recibimos por parte de la comunidad por el trabajo que se está haciendo, fueron motivo de satisfacción y motivan para seguir adelante.

PD: Por cierto, ayer por la mañana nos llegó el servidor y poco a poco se va perfilando el montaje de la virtualización de escritorios en el marco del hospital. Seguiremos informando!

DOMINGO, 25 DE MARZO DE 2012

Unimos esfuerzos

GEDEOM es una asociación sin ánimo de lucro que viene actuando desde el año 2003. Se dedican principalmente en estudiar las enfermedades oncológicas y malformativas en países emergentes. Han elaborado multitud de proyectos, desarrollados en Marruecos, Nicaragua, Sry Lanka y la República Dominicana, y esperando su desarrollo en Mauritania, Camerún y Níger. Actualmente un grupo de 6 cirujanos están intentando implementar el departamento de Oncología del hospital de Bluefields ya que ahora mismo cualquier paciente con cáncer es trasladado a Managua.

Hace unas semanas tuvimos la oportunidad de conocer el Director de la Asociación, el doctor Vicente Muñoz Madero, y nos comentó que necesitaría apoyo técnico para implementar el proyecto en el HRESB. Principalmente nuestro trabajo se basaba en realizar un estudio de viabilidad de los equipos necesarios para poder realizar videoconferencias y transmisión de datos entre Nicaragua y España. Las mejoras que se han propuesto para poder garantizar la correcta implementación del proyecto son las siguientes:

- Mejora de las prestaciones en ancho de banda de Internet (pasando de 256 Kbps a 2 Mbps).
- Compra de un proyector con mejor resolución, luminancia y contraste para poder visualizar las operaciones con detalle.
- Incorporación de un sistema de audio (altavoces y micrófono) para poder realizar videoconferencias grupales.

Además quieren que por parte de TSF se les apoye con la instalación de los equipos y el correcto funcionamiento de Internet. Por nuestra parte estamos dispuestos a colaborar al 100%, siempre pensando en que la infraestructura del hospital vaya mejorando!

LUNES, 26 DE MARZO DE 2012

Novedades

Antes de todo pedir disculpas por estar tantos días sin actualizar el blog pero llevamos 10 días sin Internet en el HRESB. Hoy por hoy aun no nos han restablecido la conexión pero estamos pendientes de que pronto podamos volver a tener servicio, al menos hoy vendrá un técnico a revisar el cableado exterior!

Aun sin tener Internet hemos podido avanzar con el proyecto, os ponemos al día de todo.

Antes que nada informaros que finalmente después de varios problemas con el envío de los equipos NComputing ya los tenemos en nuestras manos!!!

Servidor y Equipos NComputing

Por otra parte la semana pasada estuvimos reunidos con todos los implicados en el radio enlace de la comunidad de Monkey Point. Estamos muy contentos de los resultados porque pudimos organizar el viaje al detalle, ya tenemos el transporte, el andamio para hacer las pruebas, el generador, el combustible necesario para el viaje, y una fecha aproximada de cuando haremos el viaje pero todo dependerá de si la antena que enviamos a reparar llega a tiempo. Además conseguimos los permisos para ir a instalar la antena al Cerro Aberdeen, así que mañana nos vamos al Cerro junto con James Alaniz y las estudiantes de la BICU.

Esquema del enlace con Monkey Point

Otro de los avances que hemos realizado es la coordinación para crear una VPN entre las distintas instituciones de sanidad ubicadas en Bluefields, entre ellas se encuentra el SILAIS, el HRESB y el Centro de Salud Juan Manuel Morales. Con la implementación de una VPN podrán tener conexión directa entre ellos a través de los teléfonos de VoIP y entre los radio enlaces de La Aurora y Monkey Point. De ésta forma se facilita la comunicación y el trabajo.

Finalmente comentar que ya tenemos los papeles entregados para participar en la **XX Convocatòria d'Ajuts del CCD per a Ajuts a Accions de Cooperació.**

Esperamos que la próxima vez que actualicemos sea con la conexión del Internet en pleno funcionamiento!

MIÉRCOLES, 4 DE ABRIL DE 2012

Primera visita al Cerro

Buenas noticias! La semana pasada programamos una visita al Cerro Aberdeen para instalar una de las antenas, la que enlaza Bluefields con Monkey Point, con resultado plenamente satisfactorio. Con la colaboración de Jimmy y las dos estudiantes de la BICU (y alguna dificultad más de lo previsto), conseguimos colocar el dispositivo a 20 metros de altura, encarado al municipio de Monkey Point, tal como teníamos planificado.

Pintamos las piezas metálicas con pintura anticorrosiva y cubrimos las partes delicadas con cinta protectora, siempre pensando en la protección del material.

Después de hacer diversas pruebas, la conectividad entre el Hospital y dicha antena está establecida correctamente y resta terminar el enlace con la instalación de la otra parte, en Monkey Point, la cual llevaremos a cabo durante este mes de abril.

Damos las gracias a un pequeño equipo de operarios de una televisión nica que, altruistamente, nos ayudó con el tema del material pesado y las alturas, las cuales dominaban a la perfección. Que viva la cooperación!

JUEVES, 19 DE ABRIL DE 2012

Visados renovados

Ya estamos al ecuador de nuestra aventura!

Aprovechando las vacaciones de Semana Santa nos fuimos a visitar Costa Rica y así, de paso, renovaríamos el visado ya que al entrar a Nicaragua nos dieron un visado para residir solamente 3 meses en el país.

Frontera Nicaragua - Costa Rica

Así que empezamos la segunda etapa del proyecto. Principalmente tenemos que continuar el trabajo empezado antes de las vacaciones, es decir:

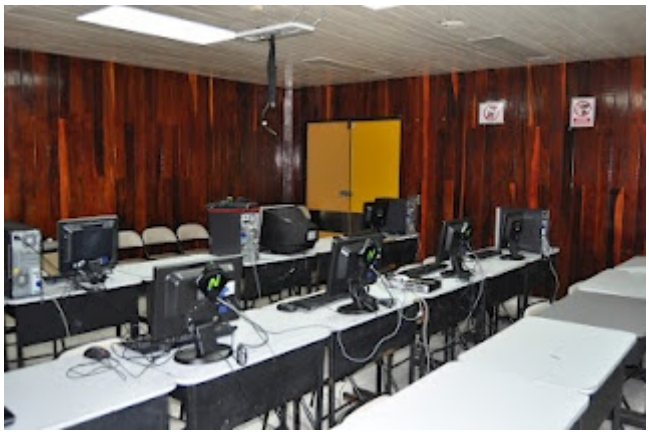
- Terminar el radio enlace con Monkey Point, tal y como os explicamos en la entrada anterior ya tenemos la primera antena instalada! (Primera visita al cerro).
- Instalar los equipos NComputing que justo llegaron antes de irnos de vacaciones.
- Continuar la implementación de la VPN entre los distintos centros de salud de Bluefields. Antes de irnos empezamos la coordinación de la red pero algunos de los centros estaban sin Internet por falta de presupuesto, así que tenemos que organizarnos de nuevo.

MARTES, 24 DE ABRIL DE 2012

NComputing en funcionamiento

¡Primer objetivo del proyecto conseguido y con éxito!

Los dispositivos de escritorios remotos NComputing ya se han instalado. Para probar su correcto funcionamiento se nos pidió que los instaláramos en el auditorio para poder hacer una capacitación sobre búsqueda de información en Internet. Era la prueba de fuego para comprobar si era un buen sistema. Finalmente se visualizó la tecnología como un gran avance para el hospital ya que han ganado nuevas computadoras, han reducido el gasto energético, han reducido el espacio y el mantenimiento de cada equipo.



NComputing

Después de la capacitación se decidirá en que departamento son más imprescindibles las nuevas computadoras.

VIERNES, 27 DE ABRIL DE 2012

Segunda visita al Cerro Aberdeen

Hoy a primera hora hemos ido de nuevo al Cerro Aberdeen para instalar un switch que conectara todos los radioenlaces. Cuando fuimos a instalar la antena direccionada a MonkeyPoint no lo contemplamos y nos olvidamos de traerlo. Así que hoy hemos ido a terminar el trabajo.

Instalación del Switch

Por otra parte, el lunes iremos a la comunidad de La Aurora a revisar el radio enlace que está caído desde que llegamos. Hemos tardado tanto en ir porque el tiempo no nos lo ha permitido. La Aurora es una comunidad que se puede llegar por tierra, a través de trochas (caminos fangosos), o por el río Kukra. La forma más rápida y segura es ir por tierra pero éste año ha llovido mucho y los caminos para llegar están impracticables, así que hemos tenido que esperar el momento apropiado.

A ver si el lunes tenemos suerte y podemos llegar hasta La Aurora!

JUEVES, 10 DE MAYO DE 2012

Intento de restauración del enlace con San Pancho

Este fin de semana, aprovechando una brigada medico-política del Hospital, nos hemos desplazado a La Aurora para intentar restaurar el enlace que tenemos con el Puesto de Salud. Desde hace unos meses, la comunicación se había perdido y hasta la fecha no habíamos tenido la oportunidad de movilizarnos a esta comunidad para verificar qué sucedía.

En primera instancia, detectamos que el Bullet estaba encendido pero la señal no llegaba. Además, el POE estaba dañado y la entrada LAN no funcionaba (con la cual cosa, el teléfono VoIP tampoco). El primer problema era un tema de configuración del propio Bullet. Además, reemplazamos el POE por otro de nuevo. Después de estos cambios la señal llegó otra vez a La Aurora, pero tan debilitada que no era posible establecer una llamada correctamente.

Con la ayuda de Mateu, hemos hecho nuevas hipótesis sobre qué sucede. Aparentemente, la alineación de las antenas es correcta, así como la configuración de las mismas. Se transmiten -65 dBm que deberían garantizar una buena recepción de la señal. El problema podría recaer en el Bullet, el cual se podría haber mojado o medio dañado en su interior. Así pues, esperamos tener la posibilidad de poder volver a San Pancho lo más pronto posible para solucionar el problema y reestablecer la comunicación entre el Hospital y el Puesto de Salud.

JUEVES, 17 DE MAYO DE 2012

Pruebas de conectividad a Monkey Point

Después de varios meses para poder coordinar a todas las partes implicadas y todo el material, fuimos a Monkey Point a hacer las pruebas de conectividad del radio enlace.

Finalmente Genís y yo decidimos que uno de los dos se quedara en el Cerro Aberdeen para poder solucionar cualquier problema que sucediera con la antena instalada allá. El viaje a Monkey Point nos había costado muchos esfuerzos y sólo teníamos una oportunidad, así que teníamos que prever y tener controlados todos los posibles errores que nos pudieran ocurrir con el radio enlace, así que Genís se quedó al Cerro para poder así solucionar los posibles problemas de allí.

A las 6 de la mañana del sábado ya estábamos en el muelle del MINSA preparados para empezar el viaje. Además de la Dra. Castro y yo viajaba con nosotros Allen, alcalde Monkey Point, i Francisco Villavicencio, auxiliar de enfermería pero capacitado en el sistema de radio telecomunicaciones del MINSA.

En una hora y media llegamos a Monkey Point, un viaje movido ya que la luna había cambiado y había alborotado un poco el mar. Cuando llegamos ya teníamos a los hombres de la comunidad esperándonos para ayudarnos a cargar el andamio y el material hasta el cerro donde se iban a realizar las pruebas.

Cerro de la Turbina de Blue Energy

Todo el mundo colaboró al 100% con el montaje del andamio y la antena. Como curiosidad comentar que para proporcionar energía a la antena y a la computadora que traíamos los conectamos a la turbina eólica que tiene instalada la ONG BlueEnergy en

la comunidad.

Andamio y posterior instalación de la antena

Baterías conectadas a la turbina eólica de BlueEnergy

Finalmente llegó el momento de la verdad! Y el resultado no fue satisfactorio ya que las antenas no se veían de ninguna forma… así que empezamos a valorar posibles fallos como: altura de la antena, configuración… La configuración de las dos antenas era correcta y para solucionar la altura de la antena conseguimos un palo para poderla poner más arriba, así que finalmente conseguimos que estuviera a 12,5 metros!! (En las simulaciones se había considerado 10 metros). Pero aun así no conseguíamos recibir señal desde Bluefields.

Para terminar de asegurarnos que todo estaba bien teníamos que hablar con Genís, él estaba al Cerro esperando mi llamada. El problema es que en Monkey Point no hay señal de celular y es imposible comunicarte!! ¡Pero estaba todo planeado! En la

comunidad hay un puesto del ejército naval que tiene una radio con la que se comunican con el puesto de la naval de Bluefields, así que simplemente los de la naval de Bluefields tenían que llamar a Genís con un celular. Muy amablemente nos hicieron el favor y conseguimos hablar. Pero simplemente nos sirvió para llegar a la conclusión que lo teníamos todo tal y como se había planeado en las simulaciones y el radio enlace no funcionaba, podía ser la distancia de 48,8km (las antenas tiene su máximo de cobertura a 50km), la vegetación abundante… Eran consideraciones que se habían tenido en cuenta pero la realidad, es la realidad y a veces hay cosas que no se pueden prever.

Teníamos previsto quedarnos a dormir a Monkey Point y el día siguiente volver a realizar pruebas y volver, pero nos habían alertado que las previsiones del mar eran muy malas y era mejor volver el mismo día. Así que aunque nos pesara porque no habíamos conseguido nuestro objetivo teníamos que recogerlo todo y volver a Bluefields.

Grupo de la expedición a Monkey Point

Realmente el viaje de vuelta fue una odisea, grandes olas que nos mojaron de arriba a bajo! Y como dirían nuestros amigos nicaragüenses, gracias a Dios llegamos a Bluefields!

JUEVES, 24 DE MAYO DE 2012

Instalación NComputing's

Ya hace unas semanas que recibimos los equipos NComputing y que los pusimos en funcionamiento pero no ha sido hasta hoy que se han instalado en su ubicación final. Finalmente se han ubicado 2 NComputing's en la Biblioteca y uno en el departamento de Cirugía. Principalmente se han ubicado en los departamentos donde hay más demanda, sobretodo ahora que el hospital ha pasado a ser hospital universitario y todos los estudiantes de medicina de la región hacen las prácticas en el recinto.

NComputing's instalados en la Biblioteca

Para poder instalar y conectar correctamente los NComputing a la red del hospital, en el departamento de Cirugía se tuvo que pasar cable Ethernet por el falso techo, pero gracias a la ayuda de los chicos de mantenimiento del HRESB fue un momento realizarlo. A diferencia de Cirugía, en la Biblioteca la instalación fue trivial ya que anteriormente ya tenían computadoras instaladas ahí y tenían todos los cables preparados.

NComputing en el Departamento de Cirugía

Además para asegurarnos un correcto funcionamiento de los nuevos equipos diseñamos unos carteles explicativos donde se informaba al usuario como encender el equipo y como conectar su memoria USB.

Cartel informativo

Siguiente objetivo: Instalar un teléfono de VoIP fuera de la red del hospital!

LUNES, 28 DE MAYO DE 2012

Teléfonos de VoIP fuera del HRESB

Tal y como os mencionamos en la anterior entrada del blog, teníamos planeado instalar teléfonos de VoIP fuera de la red del hospital. Se consideró la posibilidad de que se ubicaran teléfonos de VoIP en el SILAIS y en el Municipio, dos instituciones involucradas en el proyecto ya que son las beneficiarios del radio enlace de La Aurora y los que se hagan en un futuro. Con los teléfonos de VoIP tendrán conexión directa con la comunidad de la Aurora y con los distintos departamentos del hospital para coordinar traslados o intercambiar información de pacientes.

¡Así que nos pusimos a trabajar! Teníamos que configurar la centralita Asterisk instalada en fases anteriores del proyecto para permitir las llamadas de teléfonos externos a la red del HRESB.

¡¡Finalmente lo conseguimos!! Ya tenemos el Asterisk configurado para poder instalar teléfonos fuera del recinto, pero el problema es el ancho de banda del hospital. Hicimos llamadas de prueba des del Consorcio (lugar donde vivimos) instalando un teléfono y llamando a la Biblioteca, aunque utilizamos un codec de audio liviano, la llamada tenía pérdidas... así que tenemos que valorar la instalación. La solución ideal sería contratar una conexión de Internet solamente para el servicio de VoIP o reservar un determinado ancho de banda, pero ya no estamos a tiempo de implementarlo así que lo dejaremos para una futura fase del proyecto.