UNIVERSIDADE DA BEIRA INTERIOR
Engineering

CORSmonit: GNSS networks remote monitoring system

Pedro Miguel Henriques Venâncio

A Thesis submitted to require the Degree of Master of
Computer Science Engineering
(2nd study cycle)

Advisor: Prof. Rui Manuel da Silva Fernandes

Covilhã, Portugal
June 2012

To Juliana.

Acknowledgement

I am deeply grateful to my supervisor, Professor Rui Fernandes for his constant support, help and guidance. For receiving me in SEGAL and proposing this challenge. For always being there when needed. For having introduced me to a new and interesting scientific area. And most important of all, for being a good friend!
A special thanks to my parents and brother, for their endless love, support and encouragement.
To all my close friends and colleagues, thank you for the strong words in the difficult moments.
At last, but not least, I would like thank my girlfriend, Juliana, for motivating me to improve my knowledge and move my academic career forward.

Thank you all.

Abstract

The task of monitoring a GNSS (Global Navigation Satellite Systems) network requires time, human resources and a need for automation, which increases proportionally with the number of stations included in the network. The solutions that are actually avaiable in the market have high comercial value and in most of the times this makes it unavailable for an organization. This thesis presents a real time GNSS networks monitoring system that significantly reduces the time and effort needed to execute this task.
Furthermore, an useful front-end, for publication of related network monitoring information, was developed and implemented.

Keywords

SEGAL, GNSS, CORS, MGN, Monitoring, Network, GPS, GLONASS.

Resumo

A tarefa de monitorizar redes GNSS (Global Navigation Satellite Systems) exige recursos temporais e humanos e necessidade de automatização, os quais aumentam proporcionalmente com o número de estações incluídas na rede. As soluções disponiveis no mercado têm um custo elevado estando muitas das vezes fora do alcance de uma qualquer organização. Apresenta-se nesta dissertação um sistema de monitorização em tempo real de redes GNSS, que reduz significativamente o tempo e esforço necessários para executar a referida tarefa.
Além disso, desenvolveu-se e implementou-se um front-end útil para publicar informação directamente relacionada com as redes a monitorizar.

Palavras-chave

SEGAL, GNSS, CORS, MGN, Monitorização, Rede, GPS, GLONASS.

Contents

List of Figures

List of Tables

List of Acronyms

UBI	Universidade da Beira Interior
GNSS	Global Navigation Satellite System
SEGAL	Space & Earth Geodetic Research Laboratory
MGN	Monitoring GNSS Networks
CORS	Continuously Operating GNSS Reference Stations
NAT	Network Address Translation
ISP	Internet service provider
NAPT	Network Address and Port Translation
RAM	Random Access Memory
GIPSY-OASIS	GNSS-Inferred Positioning System and Orbit Analysis Simulation Software
RINEX	Receiver Independent Exchange Format
DI	Departamento de Informática
CI	Centro de Informática
RAID	Redundant Array of Independent Disks
VLANS	Virtual Local Area Network
ILO	Integrated Lights-Out
PHP	Hypertext Preprocessor
HTTP	HyperText Transfer Protocol Secure
CSS	Cascading Style Sheets
ICMP	Internet Control Message Protocol
DOY	Day of Year
AFRL	US Air Force Research Laboratory

Chapter 1

Introduction

This dissertation, entitled "CORSmonit: System for remote monitoring of GNSS networks", follows the work and research I've done over past year in SEGAL (Earth & Space Geodetic Analysis Laboratory), a laboratory that it is a scientific collaboration between UBI (University of Beira Interior) and IDL (Instituto D. Luíz - University of Lisbon). I'm presenting and defending this dissertation with the goal of acquiring a Master's degree on Computer Engineering - branch of Networks and Multimedia.

The dissertation is divided into four chapters, Introduction, Monitoring Support Structure, MGN - GNSS Networks Monitoring, and Concluding Remarks.
First, I introduce the context of the dissertation and the work done. I do some considerations concerning the various GNSS (Global Navigation Satellite Systems) networks managed by SEGAL (five specific networks were the subject of study and development in this dissertation). I define the objectives originally outlined and the main contributions.
The second chapter deals with the structures supporting the monitoring, i.e., structures that support the work of the laboratory and the performance of the monitoring of the GNSS networks. Two areas were defined: SEGALnet and SEGALweb. The first one relates to the servers and internet connections between them and the various GNSS stations, the second concerns the SEGAL Web portal and the available online services.
In the third chapter I analyze the two versions of the application developed in this project: MGN - GNSS Networks Monitoring, server and client, and the features related to the automatic alert system and the data handling.
In the last chapter I present some general considerations and the conclusions.

1.1 Project Background

In the next sub-chapters I contextualize the project concerning the predefined objectives, the daily basis work on the laboratory and the problems that were necessary to solve. I present some considerations on the networks operated by the laboratory and discuss five of them, that were considered relevant and targeted for research in the course of this dissertation.

1.1.1 Considerations about the various GNSS networks managed by SEGAL

A "GNSS Network" is a term applied to a network of permanent GNSS stations, usually also defined as CORS (Continuously Operating Reference Stations). Each station is composed by one GNSS system (receiver, antenna, and ancillary systems, which can include a computer) has shown in figure 1.1. Such computer stores and sends the acquired data over the internet, depending on the configuration of each one. The data generated are used to serve multi-disciplinary scientific applications. [1]
SEGAL currently receives and processes data from more than four hundred permanent stations

throughout the World. This generates a high complexity level of management and maintenance tasks in addition to a high data traffic.

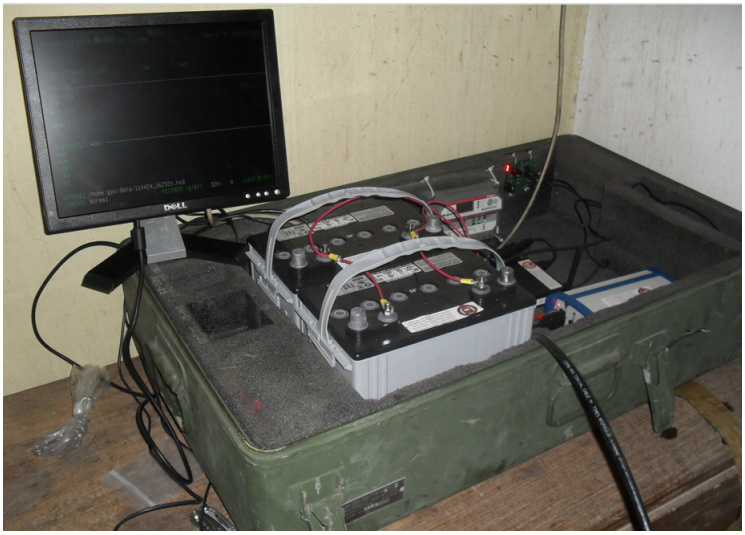

Figure 1.1: Permanent station installed in Kisangani, DR Congo

1.1.2 Monitored Networks: NIGNET, REPANGOL, SCINDA and SEGAL

Among the various networks managed by SEGAL, there are four that stand out for their importance and need for constant monitoring. These have been targeted for development and testing of the system, which will be described in Chapter 3. Namely, we have:
a) NIGNET (Nigerian GNSS Permanent Network). This network is currently composed by eleven GNSS stations distributed throughout the territory of Nigeria (represented on figure 1.2).
b) REPANGOL (Angolan GNSS Permanent Network), which is distributed throughout the territory of Angola and it's composed by eighteen permanent stations.
c) SCINDA, which is diferent from the above, since it's composed by fourteen permanent stations located in several countries, among them, Cape Verde, Sao Tome and Principe, Nigeria, Democratic Republic of Congo, Uganda, Kenya, Tanzania and Thailand. This network is managed in colloration with US Air Force in the framework of the SOGRA (Supporting Optimized Geodetic Research in Africa) project.
d) SEGAL, composed by twelve permanent stations located in Cape Verde, Sao Tome and Principe, Niger, Democratic Republic of Congo, Botswana, Tanzania, Malawi, Mozambique and the Republic of Mauritius. This network is formed by the stations directly installed and/or monitored by SEGAL.

This main goal of the work done in this dissertation was to develop and implement an automatic system to monitor any permanent CORS network [2]. It is already in place for the abovementioned networks.

1.1.3 Problem analysis

The main issue that this dissertation is looking at is: how to manage and analyze the connection status and the upload of the data from each station in real-time?

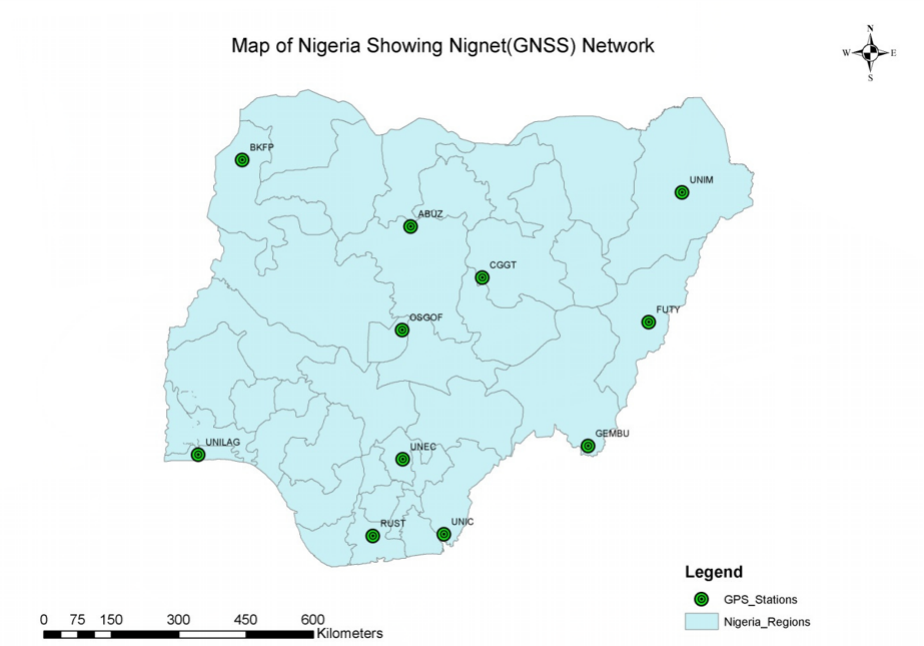

Figure 1.2: NIGNET map

Previously to the development of this project the task of analyzing the Internet connection and data upload, without having to pay expensive software licenses of comercial software, consumed a lot of time at SEGAL. Additionally, it was not optimized. The GNSS network administrator would have to input several commands in the terminal server to verify the current status of each station and then analyze the received information. This process multiplied by tens of stations and performed on a daily basis would reduce time that the administrator could apply performing other tasks.

There are some proprietary applications, for example GPSNet from Trimble [3], that offers similar solutions, some even more developed, but they are expensive and therefore not available to all existing GNSS network administrators.

So, the main problems identified early were:

a) Low-level intuitive processes, time consuming and not very user-friendly - the user needs to possess certain advanced competencies in the area of UNIX based operating systems management.

b) Limited access - only users with existing accounts in the server could perform monitoring actions.

1.2 Objective definition

After a brief analysis of the problem, I have identifyed the objectives to be developed:

a) Creation of an application for remote monitoring of GNSS stations able to analyze and recognize the various states of the Internet connection and data upload to the server. The application should have an intuitive and user-fiendly interface as well as provide access over the Internet (web-based) to any authorized user by the network administrator.

b) Access by the user to the station data - The user should have access, in a quick and simple way, to each network station data.

c) In order to further facilitate the administrator tasks, the application should possess an simplified module for the management of monitored stations (inclusion/exclusion) and enable the creation of

email alerts. Thus the network administrator and the local technicians responsible for the stations maintenance could obtain real-time information and act quickly in order to significantly reduce the stations downtime and data loss.
In addition to these objectives, it was important to prepare the support basis for the application, namely the requirements in terms of computational resources. For this, I have defined the fundamental needs in terms of the Control Center (Hardware and Software).

1.3 Communications suport

The core of the MGN network in terms of network status evaluation is the comunication layer between each CORS station and the server.
Due to the shortage of global IP addresses [4], many ISPs began to sell connections in which the client already is behind a NAT.
NATs are mechanisms that allow some kind of an Internet expansion, making use of non-global IP addresses [5].
The most common type of NAT is the NAPT which is commonly used in domestic network equipment, such as routers (which although are commonly called this way but usually meet many more functions that simple routing function and are sometimes also defined as "home gateway"). This type of NAT maintains a table of connections where it is added an input whenever a call is made to the Internet. This table is consulted when there is a connection from outside to determine which internal machine corresponds to this connection [6].
In this case it is obvious that connections initiated from outside can not succeed. The selected solution is to use a technique known as TCP hole-punching [7]. A daemon is initiated and an active connection to a Internet server is permanently ensured. In this way there's always an open door in the NAPT translation tables, allowing external connections.
In order to solve this issue, we have developed and implemented an alternative solutions: the Reverse OpenSSH Tunneling. This is a free and open source solution, available for any Linux distribution.
An example: The machine A (inside the NAT) creates a connection to Server B (through the Internet) and asks him to forward any connection on a port K on the server B K to an IP address Y, port Z, on machine A.

1.4 Major contributions

This dissertation presents itself as a valid contribution for the management and maintenance of CORS. Through a simple and intuitive interface, network administrators and users can carry out their work in a faster and more intuitive way. Thus, the major contribution is the simplification of various monitoring tasks associated with the maintenance of such networks.

Chapter 2

Monitoring support structure

In this chapter I discuss the structure that supports the entire system: acquisition, storage and processing data from SEGAL CORS networks. Inside this structure is the developed project: monitoring system and community Web portal (information and data release).
I defined two distinct sub-structures: SEGALnet and SEGALweb. The first one relates to the network servers, comunication links with the CORS and data storage. The second concerns the whole Web structure, i.e. laboratory front end and its web-based applications.

2.1 SEGALnet - Network servers

Initially the lab was composed by four servers. Desktop type machines equipped with Intel Pentium Dual CPU E2200 processors and four GB of RAM named: SEGAL, GEODAC, FANGIO and OASIS. The first three servers ran Ubuntu Desktop version 9.10 distribution and OASIS was running Scientific Linux version 5.3, yet another Linux operating system distribution.
SEGAL was the server used to process data from GEODAC. GEODAC had the function of receiving data from the CORS (establishing the necessary Internet connections). OASIS and Fangio fulfilled the purpose of storing data (already processed or not).

2.1.1 Scenario

All the servers are connected to the DI network, which is inside the University general network and is managed by CI (shown in figure 2.1). The laboratory communicates directly with two different networks defined as 0.1 (teachers network) and 1.1 (students network). It is important to take this into account since it influences the data flow.

As I mentioned earlier, GEODAC receives data generated by the GPS receivers (about fifty) when executing observations on a pre-defined (usually 1 Hz or 30 sec, depending on the quality of the connection internet) daily basis. The data is converted (to RINEX format) and stored in the server until processing. The processing stage is carried out in the SEGAL server after the data has been copied from GEODAC. After this task, the original files remain in GEODAC (RAW format, depending on the manufacturer). The solutions of interest that results from the processing (positions and water vapour parameters) are stored in SEGAL.
In order that these solutions can be quickly generated, SEGAL makes use of thirty computers installed in a classroom next to the laboratory (room 6.19). SEGAL server, which communicates with both networks (0.1 and 1.1) sends the data for processing through the network 1.1. The processing is performed in parallel mode (carrying out multiple jobs simultaneously in each computer) using shell scripts developed by SEGAL laboratory and making use of the application GIPSY-OASIS II [8]. Each machine in the room 19.6 is equipped with four processors and four GB of RAM and is running the Linux operating system distribution Fedora, version 15 (Gnome).

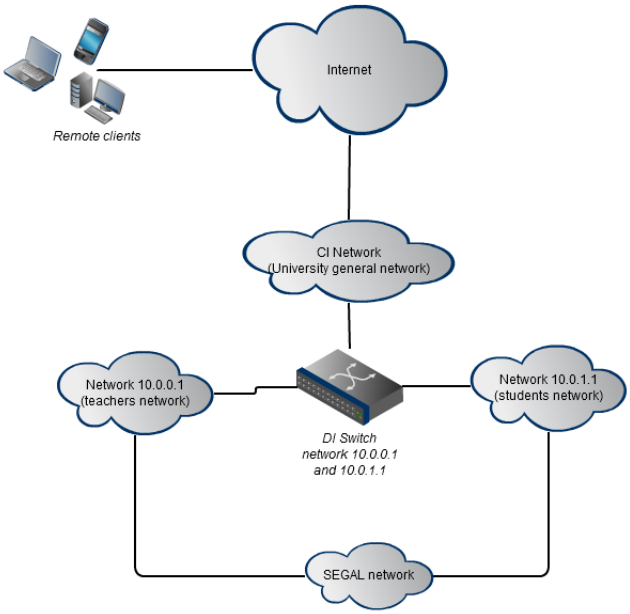

Figure 2.1: CI and DI network

The other two servers, OASIS and FANGIO, fulfill the tasks of storing multiple backup data and performing some auxiliary processings.
Figure 2.2 represents the network structure described above.

2.1.2 Installation and configuration

There was a need to upgrade the network, improving the performance and storage capacity. Due to this optimization the machines and network architecture referred in the previous sub-chapter have been changed. The new network has only two servers: SEGAL and GEODAC.
The four desktops were replaced by two high-performance servers, an HP ProLiant DL 380 G7 in Figure 2.3, with 12Gb of RAM and an HP ProLiant DL 380 G6 8Gb, both with Intel Xeon processors 5600 series family each containing eight 500GB hard drives, resulting on 4TB of storage capacity for each server.
Following this upgrade there was the selection and installation of an operating system that would guarantee a good performance - the Ubuntu Server version 10.10. I installed and configured the selected operating system in RAID 5 level, creating a single logical hard drive.
RAID5 was selected instead of other RAID level because the parity data in the array is distributed across all hard drives and it is not stores in a specific location which results in improved perfomance and better fault tolerance.

These servers were placed together in a rack on the DI systems room with a network switch model D-LINK DGS-1210-24, which is inexpensive and has twenty-four ports with support for VLANs and fiber optic facilities.

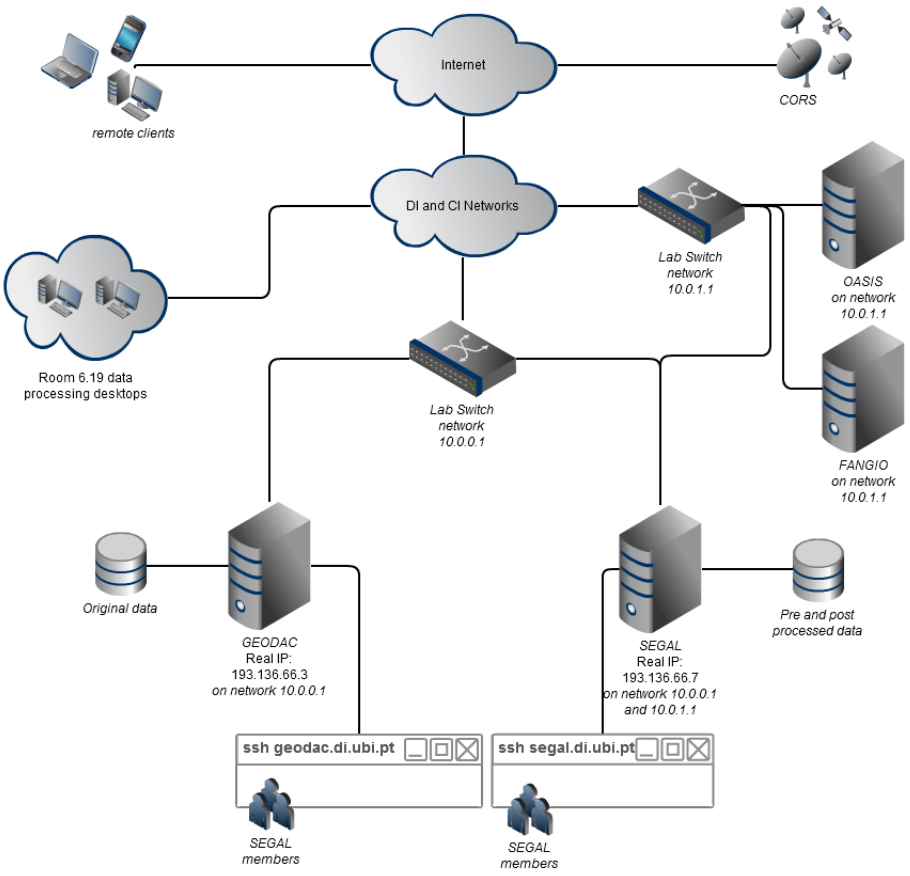

Figure 2.2: Old network structure

2.1.3 Network description

Presently the lab network can be described with the following elements: rack in the systems room with two servers and a network switch. The switch communicates with the DI switch which establishes comunication with all the other rooms of the department and with the CI. The CI communicates with the outside world - the Internet - in other words, it is the laboratory gateway. Both servers have real IP addresses, being directly accessible from outside the network. SEGAL server has an active network interface dedicated to comunications (throw network 1.1) with the room 6.19 that contains the desktops for parallel processing, referred in sub-chapter 2.1.1.
SEGAL continues to be the dedicated server for data storage and processing. GEODAC server is still receiving data from CORS, storing the originals, and hosting the Web portal front end and the web-based applications.
The old desktop servers still remain in the network but with secondary tasks. The former GEODAC changed its name to GEO and is now a test server running the Ubuntu Desktop operating system version 10.10. The former SEGAL is now called SAT and it is also a test machine but running the Microsoft Windows operating system Server 2008 R2 and the old OASIS is now used for applications development, running the Microsoft operating system, Windows 7.
Figure 2.4 shows the described network.

Figure 2.3: HP ProLiant DL 380 G7

2.1.4 Maintenance

Regarding maintenance tasks, there is the need of ensuring permanent communications and the service availability. This depends on the availability of the networks managed by the CI and DI. But apart from that certain aspects need to be guaranteed, such as permanent physical access to servers in case of operating system crash or even the availability of services as the Web portal and Web-based applications.
For security reasons only the DI network administrator can give authorization for physical access to the systems room, where the SEGAL servers rack are installed. And if during one weekend a crash occurs on a server? The answer lies in the third version of iLO (Integrated Lights-Out) provided by HP [9]. After the proper configuration, it provides permanent remote access to the servers compared with physical access. This is an advanced and powerful management tool providing performance reports and constant monitoring, as seen in figure 2.5.

The remote access is done through a ssh tunnel (ports 22, 23, 80, 443 and 3389) established between the user computer, a systems room server and the destination server (SEGAL or GEODAC), since the iLO network interface has a local IP.

2.2 SEGALweb - Laboratory front end

In the next section it is described in detail the Laboratory front end needs, objectives and further development.

2.2.1 Needs

Like in any other laboratory it is very important to possess means of communicating information and results on the Web. SEGAL front end emerges as a mean to fulfill this mission. In addition, the front end also becomes a tool for the SEGAL users (sixty-four currently registered) providing access to stored data and to web-based applications such as the MGN (GNSS Monitoring Networks), described in detail in the following chapter.

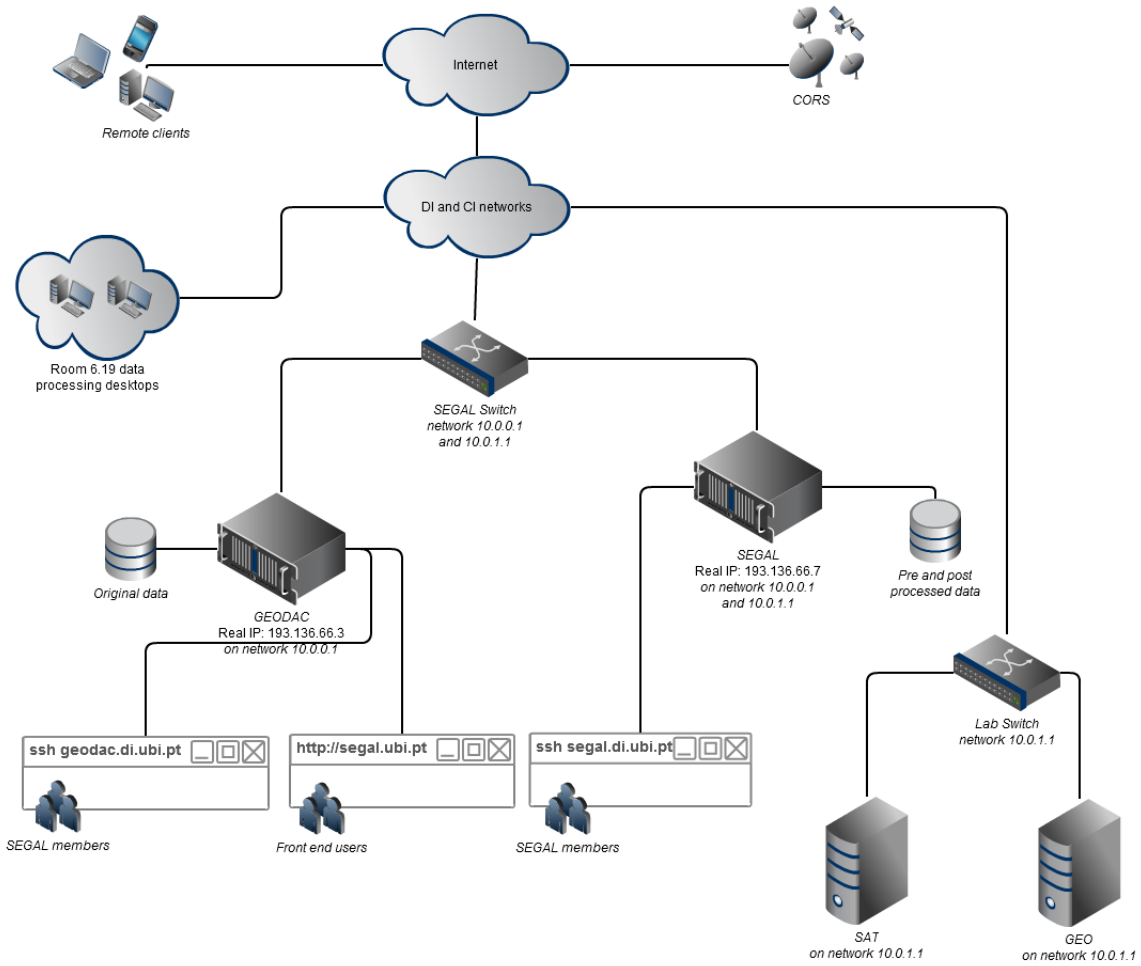

Figure 2.4: New network structure

2.2.2 Development

The laboratory front end - previously defined as Web Portal and - was developed using Joomla! (free and open source content management system) version 1.5 [10].
The server that hosts the Web Portal, as previously mentioned, is GEODAC. So this machine was previously prepared to receive an installation of Joomla!, meeting all the technical requirements. They are: PHP version 4.30.10 or later, MySQL version 3.23 or higher and Apache HTTP Server version 1.3 or higher [11]. The database "segal_site_db" was created to support the Web Portal. This database currently has fifty-one tables containing the most diverse data such as menus, users, sessions, news articles, etc.. This structure was created following the CMS installation.
The programing languages used in the development and maintenance of the front end are HTML, CSS and PHP. Edited using the well-known tool Notepad++. All images were edited with Corel PHOTO-PAINT version 11.
An integration between the Web Portal and SEGALs Facebook [12] page was recently developed.

2.2.3 Contents

In terms of information availability , the Web Portal provides the user with a menu where you can access recently published news or files, lab members information, currently active projects, past

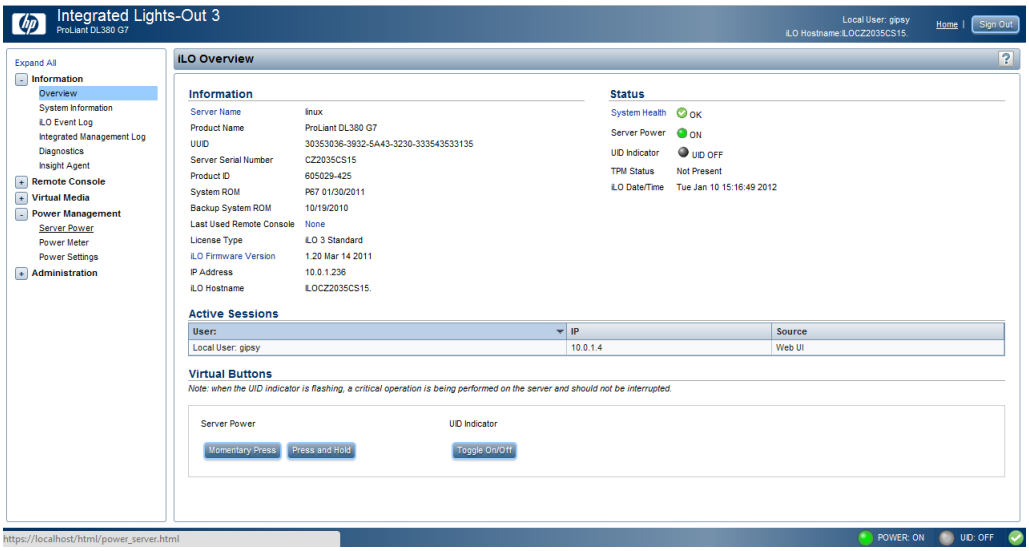

Figure 2.5: GEODAC iLO UI Screen

publications (undergraduate projects, MsC and PhD dissertations), scientific articles, publications in scientific books and a list of collaborations with other institutions.
There are some locked contents that can only be accessed through previous login, i.e. scientific articles, and access to the CORS data.

2.2.4 Functionality and usability

The language of the Web Portal is English. This is the working language at SEGAL and it makes perfect sense. Moreover seventy-seven percent (forty-nine in a universe of sixty-four) of the registered users, to the date of this dissertation, are foreigners that do not speak Portuguese.
The layout development followed after the installation and proper configuration of the Web Portal. A template was developed taking into account several aspects of SEGAL. It was later installed on the CMS, creating the appearance that is now visible to all users. A main objective was: to have a simple and intuitive interface with a good appearance, which we believe has been achieved! The user can notice a connection between the layout main colors and SEGAL logo. The pages have white color background that contrasts with the text colors gray, blue and green providing a light reading. Figure 2.6 shows the Web Portal main page.

One of the aspects taken into account on the MGN development was the usability. In my opinion it is essential that the user can execute any task in a simple and efficient way.
The Web-based application interface must be simple and easy to use. That way accomplished in the MGN development, i.e. the user with a maximum of three clicks can reach any part of the site. And the navigation through the web site is simple, as it was confirmed by several user feedbacks received over the time since initial activity.
To assist the user finding any topic or item of the Web Portal,a search engine has been installed and it is always visible on the upper right corner. Below this search module there are links to the three institutions that are directly connected to the laboratory: the Universidade da Beira Interior, DI and Instituto Dom Luiz, Universidade de Lisboa in which SEGAL is an associated laboratory. In addition the main menu on the left is easily identifiable and navigable as well as the section of

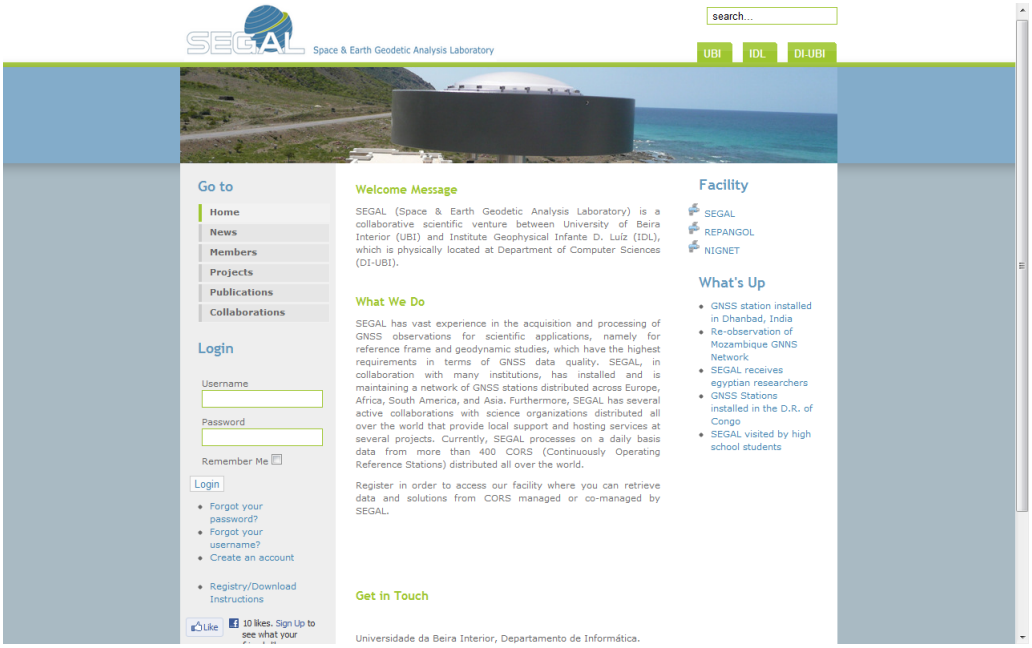

Figure 2.6: SEGAL Web Portal main page screen

the laboratory facilities on the opposite side. Beneath this you can always navigate to one of the last five published news on the Web Portal. In order to access some of the facilities the user needs to register first. After it, all restricted areas can be accessed once logged in. A manual is available for download to help the user to perform the registry, which contains instructions how to perform the registry and make use of the facilities.

An element that I found crucial for any visitor of the Web Portal to notice, was the lab contact data. It remains always visible at the footer. I chose this method in favor of creating one more main menu option.

Chapter 3

MGN - Monitoring GNSS Networks

This chapter addresses the main subject of this dissertation: the MGN application.
I selected for the examples the NIGNET network. This network has all three connection types suported by MGN and it is already in use since some months ago.
This web-based application is divided into two different versions: MGN Main and MGN Lite. The first one handles all the administrative aspects of the network monitoring, in other words, this is a tool to be used by the administrator of the GNSS network. The second one, called lite version, only provides information that is available to the user concerning the status of the stations and the downloaded date. It does not provide permissions to execute any change to the existing configuration.
In chapter 3.2 a functional description of the application is done in which I discuss its development.
In sub-chapter 3.3 I discuss the four different modules of the developed application, MGN Main: Network Status, Stations Configuration, Alerts Configuration and Data Handling.
Finally, the Lite version of the application is demonstrated.

3.1 Description

This tool allows the user, if logged in as administrator, to manage the GNSS network.
After the initial configuration a simplified but intitive view of the network is generated, as shown in figure 3.1.

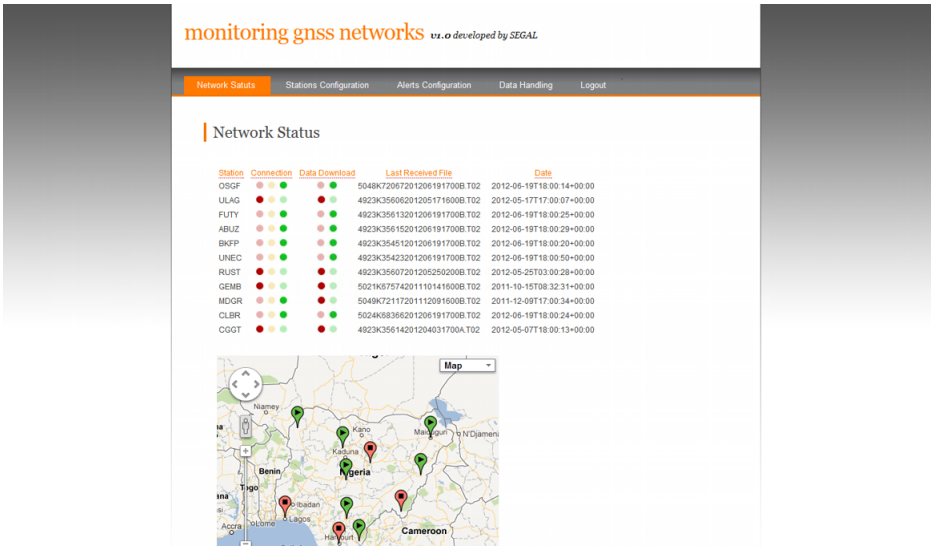

Figure 3.1: MGN administration main page

3.2 Development

The MGN was developed for a Linux based environment running Apache Web Server version 2.2.16 and PHP version 5.3.3.. The application was developed mostly in PHP programing language. But HTML, CSS and JavaScript are also used.
The application has an integration with Google Maps (through the use of Google Maps PHP API version 3 [13]), displaying the geolocation of the network stations.
In order to create a more secure development process, I implemented a three layer system: Development (DEV), Quality (QUA) and Production (PRO). The main objective of this system is to ensure that no change to the application is released before being tested and approved by the project manager.
After changing the application in DEV, the new version is exported to QUA in which exhaustive tests to the performance and the results are made. The changes are then examined by the project manager that verifies if the objectives have been achieved and whether the new version is ready to be published. If approved, the new version is exported to PRO and the users are informed of the update.

MGN is currently being used by staff of the different organizations that are collaborating with SEGAL. In the case of Nigeria, the Office of the Surveyor General of the Federation (OSGoF) [14], the national mapping agency of Nigeria.

3.3 Modules

MGN Main version includes four modules that interact with each other: Network Status, Stations Configuration, Alerts Configuration and Data Handling, which are described in detail in the following sub-chapters.

3.3.1 Network Status

The main page displays the current network status through several indicators, as show in the next figure, 3.2. The status of each connection and data download is displayed by two color systems in each line (red,orange and green like traffic lights). The last two indicators list the file name and transfer date of the last received data from the station.

In order that the desired information will be displayed in real time to the task manager, several tasks are performed: during the installation process, the MGN server creates a job in the operating system crontab. This job will execute, every minute, a shell script that updates a specific file that contains all the tcp6 type connections of the ssh daemon running on the server and it is called "status file".
Next, the MGN system analyzes them (discussed in the following sub-chapter) and analyzes the type of connection that each station has with the server. The connection can be of three types: IP, VPN or FILE. This means that data from a station can:
a) IP - the remote system has a real IP which status can be checked. A direct connection is established between the server and the station.
b) VPN - arrive through a ssh tunnel (discussed earlier in sub-chapter 1.3);

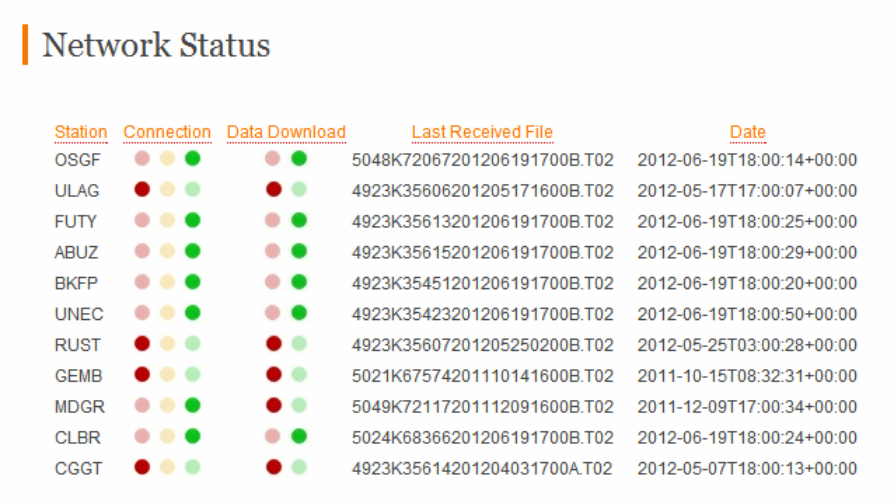

Figure 3.2: Network Status

c) FILE - be uploaded directly to a directory on the server via FTP push;
The best solution is a) but unfortunately is not a always possible to configure this type of connection due to local network restrictions. To bypass some connection problems, type b) is normally applied. In worst cases, when we have almost no control regarding the local network administration, type c) is configured.
For cases of direct IP connection, MGN uses the fping tool (fast ping). It uses a ICMP echo request to determine if a target host is responding. The usual ping tool would take a longer reponse time and unlike ping, fping is meant to be used in scripts, so its output is designed to be easy to parse [15].

Table 3.1 contains the eleven stations added to MGN in order to test their performance. These stations belong to the NIGNET network mentioned in Chapter 1 (cf. Figure 1.2).

Table 3.1: NIGNET configured stations.

Station ID	Locality	Dada connection type
OSGF	Abuja	FILE
ULAG	Lagos	VPN
FUTY	Yola	VPN
ABUZ	Zaria	VPN
BKFP	Birnin Kebbi	VPN
UNEC	Enugu	VPN
RUST	Port Harcourt	VPN
GEMB	Gembu	VPN
MDGR	Maiduguri	VPN
CLBR	Calabar	VPN
CGGT	Toro	IP

Like I mentioned earlier, MGN has two diferent color systems: one for the Internet connection status between the server and the station and the other to indicate the data download status, depending on the type of connection, as shown earlier in Figure 3.2.

For VPN connection:
Green connection - the ssh tunnel is established;
Orange connection - the ssh tunnel is not established but the latest data file was recently downloaded (time $<$ variable defined by the network administrator);
Red connection - the ssh tunnel is not established and the latest data file downloaded exceeds the

predefined time limit.

For VPN data download:
Green data download - if the latest downloaded data file was created within the last twenty-four hours;
Red data download - if the latest downloaded data file was created past the last twenty-four hours;

For FILE connection:
Green connection - if the latest data file was downloaded within the last twenty-four hours;
Orange connection - not applicable;
Red connection - if the latest data file was downloaded past the last twenty-four hours;

For FILE data download:
Green data download - if the latest downloaded data file was created within the last twenty-four hours;
Red data download - if the latest downloaded data file was created past the last twenty-four hours;

For IP connection:
Green connection - connection between the server and the IP is established;
Orange connection - connection between the server and the IP is not established but latest data file was recently downloaded (time $<$ variable defined by the network administrator);
Red connection - connection between the server and the IP is not established and recently there is been no data file downloaded (time $>$ variable defined by the network administrator).

For IP data download:
Green data download - if the latest downloaded data file was created within the last twenty-four hours;
Red data download - if the latest downloaded data file was created past the last twenty-four hours;

It should be noticed that the creation date of a file might not be the same as the downloaded date. This situation is can be exemplified with three case studies:
- The internet connection of a station is fully functional and the data file was uploaded to the server immediately after its creation (daily/hourly).
- The station has been for several days without internet connection and when it finally could upload the data files to the server, the creation date has a delay when compared to the server clock;
- The internet connection of a station is fully functional but there is a problem with the GPS receiver and it is not generating data.
These cases were considered and can be quickly identified by using this MGN module.

For a quick and easy station identification MGN generates a network map, through an integration with Google Maps (based on the coordinates defined in the configuration file for each station). The icons that indicate the geolocation of each station can vary (depending on the connection status), as shown in Figure 3.3. The green icons with the symbol "start" (for a better perception) indicate that the communication between the server and the station is established. The red icons with the symbol "stop "indicate that the communication between the server and the station is not

Figure 3.3: MGN generated map

established.

Another feature present in this module is the data availability analysis. This is a simple and intuitive way of making the data available for download, to the user. Listing all the avaiable data by days and months, in a table, separeted by year tabs. The green table cells represent the existence of data for that specific day and the possibility of download, by clicking on it. The red table cells are shown when there are no data available for the referred day.
The user just by looking to each year table can have the perception of the station reliability, as shown in figure 3.4.

3.3.2 Stations Configuration

In this module, the network administrator can manage the network monitoring: add, remove and check the settings for each station.
When adding a station, several fields must be filled: station name, location, connection type (VPN, FILE or IP), IP or ssh tunnel number (if applicable), file extension of the data generated by the GPS receiver, connection time limit, station coordinates (latitude and longitude), the server directory to where the data is uploaded, unique identifier in the data file name, characters sequence present in the file name and related to the original creation date and finally, a brief description.
It is important to analyze when the file was actually created by the receiver. Depending on the receiver manufacture i.e. Trimble, Topcon and Navatel. Trimble files have T02 extension and the name is composed by a six caracteres ID followed by the creation date (i.e. 4923K3560620120517160 0B.T02). Topcon files have TPS extension and the name is composed by the four caracteres station ID followed by the creation date (i.e. IGCA20120604i.TPS). Novatel files have rng.gz extension and the name is composed by the six caracteres refering the creation date followed by the creation hour (i.e. 120619130000.rng.gz).

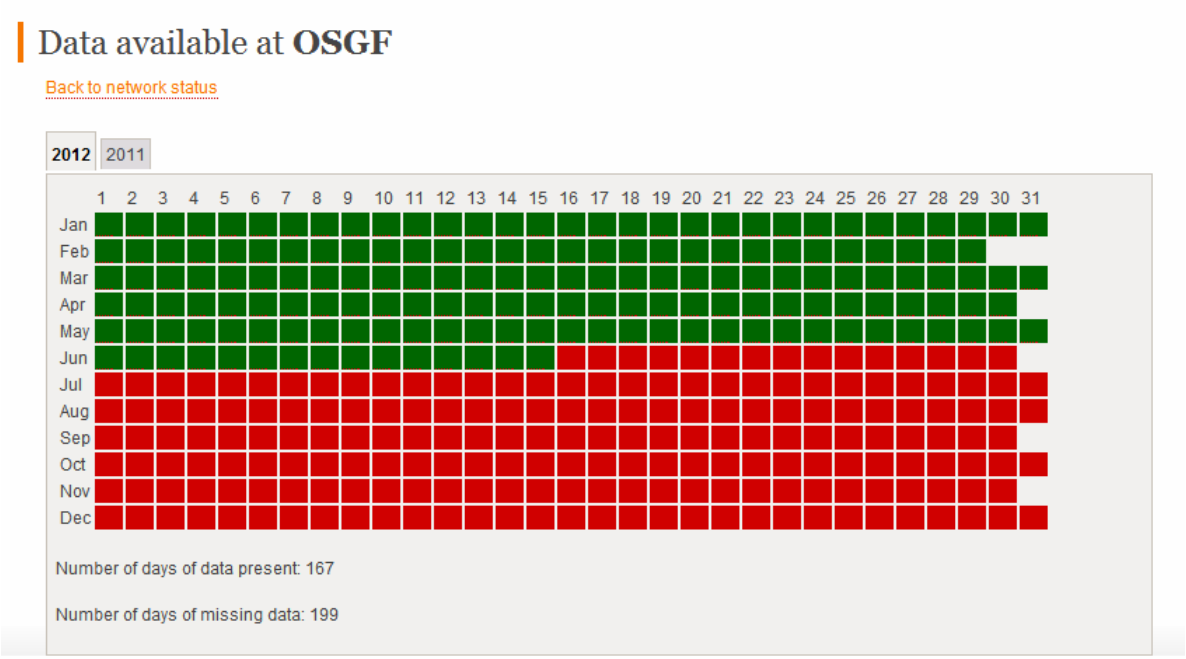

Figure 3.4: Data available at OSGF

It is necessary to get the date inserted in the file name and comparing it with the metadata date, independently of the receiver manufacture.
After the input of the described data the station is added to the network and it starts being monitored by MGN, as shown in Figure 3.5. The added station can now be identified on the map. To facilitate the identification each station is given a number.

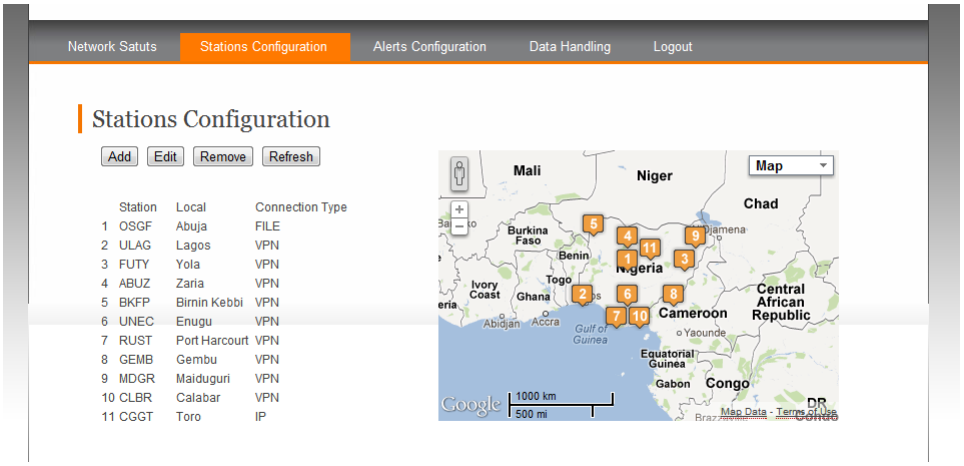

Figure 3.5: Stations Configuration page

3.3.3 Alerts Configuration

It is essential that communication downtime of a station is as short as possible. For this matter a tool that can automatically alert all involved personnel in case of any communication failure is considered very useful. MGN Alerts Configuration module implements this functionality.

This module allows real-time notifications of any communication failure between the station and the server. The network administrator and each station technician is immediately informed, enabling them to act quickly and resolve the problem that caused the failure. The notifications are automatically sent via email.
Before the administrator would have to perform periodic manual reviews of the several station connections status. And there was the possibility of forgetting some, that would result in considerable data loss.
By cliking on the station icon representated on the map, as shown in Figure 3.6, a balloon pops up with the information from existing alerts and options to remove or add new ones. When adding a new alert, the administrator is prompted to enter the recipient email and configure the notification dispatch parameters:
- Number of hours after being offline;
- Number of hours after returning online.
According to the specificity of each station these parameters can vary i.e. if a station often changes its connection status before stabilizing the administrator simply wants to receive one alert and not several.

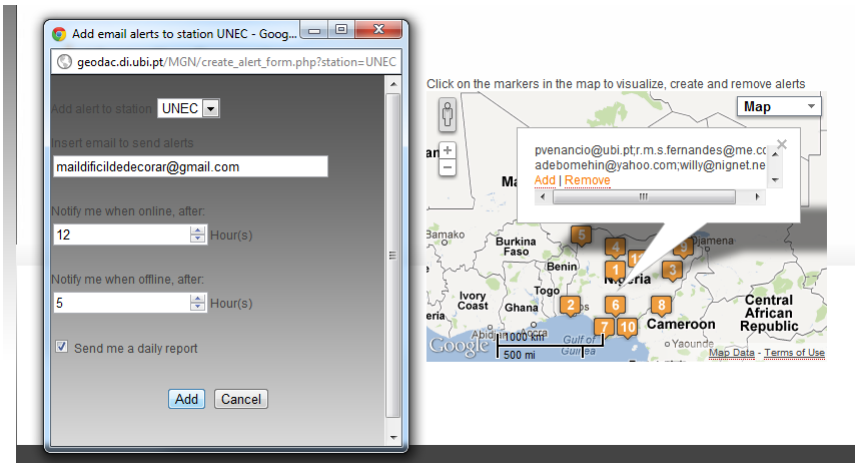

Figure 3.6: New alert creation

After this task, the configuration file alerts are updated and taken into account in the hourly task that runs continuously on the server and sends alerts when necessary.
The contents of the e-mail alerts (as shown in figure 3.7) are the following: the subject is described which owns the station network and alert, the body of the message is an indication of the number of hours that have passed since the station changed its status to offline / online and when the last file was received regarding this station.

Apart from these two alert types, MGN sends a daily report of all network stations that are offline. This report indicates the total downtime and when was the last data file downloaded.

3.3.4 Data Handling

The last module to be analyzed is the Data Handling. This tool provides a search engine for the data files of the network stored on the server.

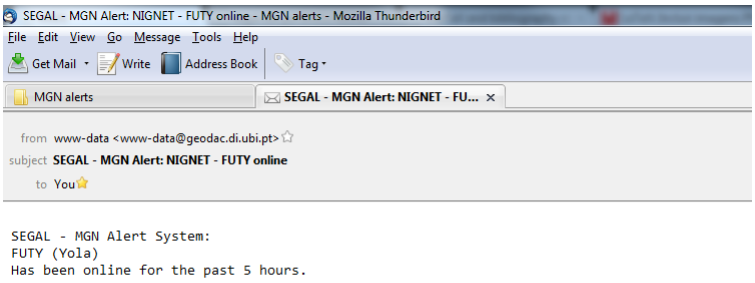

Figure 3.7: NIGNET Alert: Station FUTY has returned online

This module presents itself as an essential element in the daily life of professionals for whom MGN is a important working tool. It allows access to the data. Through a easy and obvious interface the user can select a time interval of a particular station data for further processing and storage. The process begins by inserting the four characters station identifier (for one or more stations simultaneously) and the DOY interval, as shown in Figure 3.8. The result is a list of data files available for download, by just cliking on each one.

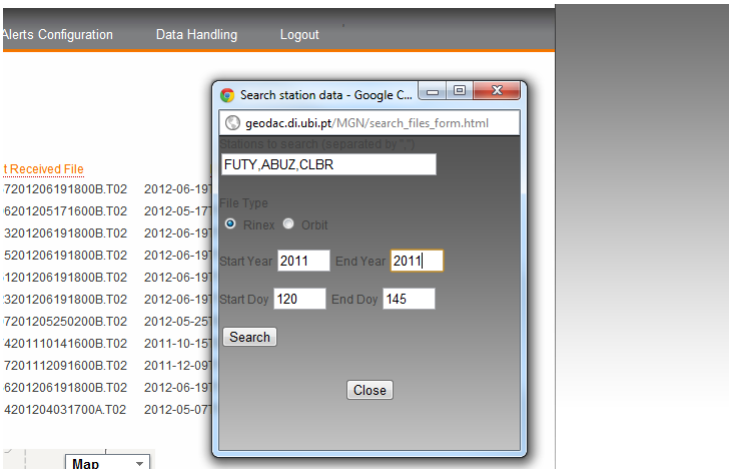

Figure 3.8: Rinex search for stations:FUTY, ABUZ and CLBR

3.4 MGN Lite

In case the user does not login as administrator, it can only have access to some features of MGN. Having said that, MGN Lite is basically a limited version of MGN Main. This version only includes the Network Status module (referred to in subsection 3.3). At the moment this version is being applied to five networks worldwide. In figure 3.9 is shown its application on SCINDA.

In addition to the network stations configuration file, the Lite version has one more configuration file defined as "interface file". In this file all the configuration regarding the application interface are present: network name, location of the data files repository and the map zoom level.

Figure 3.9: MGN Lite: SCINDA

By simply configuring both configuration files, MGN automatically generates new monitoring status and interface display.
It can adapt to any CORS network (independently of the connection type).

Chapter 4

Final Remarks

4.1 Conclusion

In my point of view the work developed and demonstrated in this thesis is an asset for the field of GNSS, for SEGAL in particular. The laboratory now has new tools to support present and future researches.
The possibility of monitoring a CORS network in real time through an not expensive solution constitutes, in my opinion, an improvement. Several tasks have been successfully simplified.

In personal terms this experience was enriching since it was necessary to research topics related to Geodesy and GNSS, which were relevant to the subsequent problems analysis and comprehension. Along with Computer Science these are now fiedls of interest for me, in which I will certainly develop new solutions in a near future.
I would like to point out that this thesis addresses two of the main computer science topics: multimedia and networks.

Glossary

NIGNET	Nigerian Permanent GNSS Network.
REPANGOL	Angolan Permanent GNSS Network.
SCIDA	AFRL, Boston College and SEGAL GNSS Network.
Crontab	Time-based job schedule table.

Bibliography

[1] National Aeronautics Ruth E. Neilan and Space Administration Jet Propulsion Laboratory, 2008. Position, Navigation and Timing: GPS Scientific Applications. 1

[2] Chris Rizos, 2008. The Contribution of GNSS CORS infrastructure to the mission on modern Geodesy. 2

[3] Trimble, 2005. Trimble GPSNet Software. 3

[4] Ipv4 address depletion, online. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_addr-dep.html. 4

[5] How nat works, online. http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a 0080094831.shtml. 4

[6] Overview of napt, online. http://rfc-ref.org/RFC-TEXTS/3022/chapter2.html#d4e440538. 4

[7] Peer-to-peer communication across network address translators, online. http://www.brynosaurus.com/pub/net/p2pnat/. 4

[8] Gipsy-oasis ii, online. https://gipsy-oasis.jpl.nasa.gov/. 5

[9] Hp ilo - overview, online. http://h18013.www1.hp.com/products/servers/management/iloadv3/index.html. 8

[10] What is joomla?, online. http://www.joomla.org/about-joomla.html. 9

[11] Joomla! technical requirements, online. http://www.joomla.org/technical-requirements.htm. 9

[12] Segal facebook page, online. http://www.facebook.com/SEGAL.Lab. 9

[13] Google maps javascript api v3, online. https://developers.google.com/maps/documentation/javascript/. 14

[14] Osgof geoportal, online. http://www.osgof.com/. 14

[15] Fping manual, online. http://linux.die.net/man/8/fping. 15

Appendix A

Web Portal Registry/Download Instructions Manual