Université Catholique de Louvain
Louvain School of Engineering
Department of Computer Engineering

Master thesis

Analysis and performance monitoring of a large WiFi network

Authors:
Adrian Healey
Clément Wayembergh

Thesis Supervisor:
Olivier Bonaventure

A thesis submitted to obtain the degree of *Master 120* in *computer science* with option in *networking and security*.

Louvain-la-Neuve
June 2014

We would like to specially thanks Olivier Bonaventure, Dominique Margot and Quentin Hunin from the UCL SRI team for their availability, support and help during the realization of this project.

Contents

Chapter 1

Introduction

With nearly 30.000 students and 10.000 staff members (including teachers and researchers), the Catholic University of Louvain (UCL) is the largest french speaking university in Belgium. The university has several campuses based in Brussels, Tournai, Mons, Charleroi and Louvain-la-Neuve, the latter being the widest and the one we focus on throughout this study. On this campus, a wireless internet connection is provided by the university and is available for all the students and staff members for free. To be more precise, there is a total of four wireless networks available in Louvain-la-Neuve. Three of them are developed and maintained by the university itself and are reserved either for the students (with the SSID `"student.UCLouvain"`), for the staff (with the SSID `"UCLouvain"`) or only to have a limited Internet access in order to consult the UCL's wireless configuration web page or to download required programs for Windows XP and Vista (with the SSID `"UCLouvain-prive"`). The fourth network with SSID `"eduoram"` is for education roaming. Eduroam is the secure, world-wide roaming access service developed for the international research and education community[4]. Basically it allows students, researchers and staff members from other universities to get a wireless connectivity within the UCL's campus without being enrolled to the Catholic University of Louvain.

Providing those wireless accesses for such a large community of users and all over the campus is a real struggle for the UCL's SRI (*Infrastructure des réseaux du Système d'information*) team which is in charge of keeping the networks up and running whatever troubles may happen. Indeed, in order to deliver and ensure, at any time, a quality connectivity with high performances for everyone, it is vital to develop and maintain those networks everyday so that they remain reliable and efficient.

In this study we focus on analyzing and implementing a monitoring tool for the wireless network infrastructure of the Louvain-la-Neuve campus that will help the SRI

team identify, in real-time, the possible problems that might occur on that infrastructure, allowing them to react and be able to fix them as quickly as possible.

1.1 State of the art

Here we present the state of the art of network monitoring and performance analysis tools.

1.2 Towards a custom WiFi monitoring tool

From the state of the art described above, we can see that there is room for research in the wireless network monitoring and performance analysis area.
Since the UCL infrastructure is rather complex and uses technologies such as Cisco controllers, Cisco WiSMs, RADIUS, LDAP and DHCP servers it can be quite difficult to track down all the processes that are executed during an authentication request issued by a user who wants to connect to the UCL's wireless network and it is even more difficult to track down a problem that has occured on that network.

Indeed, the log files produced by the controllers are highly verbose inducing an arduous and tricky work of decryption whenever the SRI team wants to trace down a particular network problem. Moreover, another issue the SRI team faces everyday on the Louvain-la-Neuve area is the fact that there are more and more users trying to get a wireless connection on the campus today than before. This can be explained by the fact that nowadays, a significant part of students (as well as staff members) does not only come and attend to courses with their own laptop but also bring smartphones and tablets. The problem those new devices arises is that they can be inadvertently configured to automatically connect to a WiFi network (in our case one of the UCL's wireless networks), whenever one is reachable, even if the user is not currently using those devices to surf the web. These unused connections, added to the one already made by all the laptops, can lead to an overload on an access point resulting into bad performances behaviors and lower signal strengh, since the user's connection request might be redirected to a farther access point, inducing connectivity or network access problems.

Our implementation and vision for this monitoring tool is based on three milestones. First of all, we gather on our private server all the information about what is happening and has happened on the wireless network. Once we have collected these two

kind of raw data, that we qualify as *active logs* and *passive logs*, we analyze and store them into our custom database aggregating them and removing useless data. Finally, we have developed an online platform on which we present the relevant data about the network's state in real time and in a way that is more convenient and understandable for the SRI team users than the overly verbose log files.

Throughout this thesis, we discuss the implementation of a custom WiFi monitoring tool for the UCL's network infrastructure that will help network administrators from the SRI team managing the wireless network and identifying possible problems in order to fix them and avoid further disturbances for the end users. In a first chapter, we present the working environment and more specifically, the UCL's Internet infrastructure. We also give a further detailled discussion about the data our system needs to gather and analyze in order to work properly. In another chapter, we present all the network key components and protocols that are used inside the university's network and where connectivity problems might occur. Finally we provide and describe an implementation of our monitoring tool and we discuss the gathered results and feedbacks after having deployed it on the Catholic University of Louvain's wireless network.

The following subsections give a quick overview of the two first milestones.

1.2.1 Data gathering

The first important step in our implementation is the network's raw data gathering process. Indeed, to work properly our monitoring tool needs to gather all the information available about what is happening and has happened on the UCL's wireless network. These data come from several heterogenous sources. For the *active logs* (i.e. real time information), we have developed and implemented a C script that runs on an OpenWRT router. This script uses the `wpa_supplicant` control interface to make a never ending connection loop to each of the four available SSIDs on the campus in order to make a complete authentication chain and to see if each of those networks is reachable or not. The script inserts every process' event response it receives from wpa_supplicant into a log file that it then sends after a specified amount of time to our server. The routers equiped with this script are thus able to send real time information of the different networks' status.

The second kind of information we gather are the *passive logs*. For those data we collect log files directly from the Cisco controllers. These files contain all the details about the key elements of the network infrastructure which are the RADIUS, LDAP and DHCP servers as well as information about all the different WiSMs (Wireless Services

Modules). As for the active logs, those files are also received and stored into our private server.

1.2.2 Data analysis

Once information either from the controllers or the routers is gathered and stored into the server, the analyzing phase begins.
We have designed and implemented in Python a parser that goes through all the files we have on the server and that parses all piece of information from them. It then inserts the valuable information into our custom database and rejects all the unecessary and useless one. By doing so, our monitoring tool now has all the UCL wireless infrastructure status and details in hands and we can start aggregating them in order to produce a readable and relevant output that we show on our online platform.

Chapter 2

Working Environment

2.1 UCL's wireless infrastructure

2.1.1 Overview

On its Louvain-la-Neuve's campus area, the Catholic University of Louvain offers 4 different networks, with different SSIDs, that are reserved to certain parts of users according to their category. Those available networks are the following:

- `student.UCLouvain`: Available for the students enrolled at UCL.
- `UCLouvain`: Reserved for university's professors and the researchers.
- `UCLouvain-prive`: Limited access to check the UCL's wireless configuration page or to download required program for Windows XP and Vista.
- `visiteurs.UCLouvain`: Accessible for guests invited by the university.
- `eduroam`: Internation education roaming access.

Security is an important issue at the university and several measures are regularly taken by the SRI team in order to keep the integrity and the consistency of the UCL's network untouched. As an example, Windows has decided on the 8th of April 2014 to end the XP's support and updates leaving all the remaining laptops running this operating system unprotected to possible external threats[8]. The problem with that Windows' decision is that those computers might become more vulnerable to security risks and viruses and if a contaminated host connects to the UCL's network it can cause serious damages to the overall infrastructure depending on what the virus is programmed

to do. This is why the SRI team took the decision to block the wireless access to any device that still uses Windows XP after the 8th of April.

The main way of protecting the network infrastructure from possible threats that has been installed and configured by the SRI team is the use of the IEEE 802.1X standard providing an authentication mechanism for the devices that want to connect to a UCL's network.
Basically, every student, professor or researcher needs a special WiFi username and a password to connect to one of the networks. The username is composed of two parts, on one side the general login the user has received from the university's administrative system when he had enrolled himself, and on the other side the following part `@wifi.uclouvain.be`. With that username, the user also needs a password, which is the same has the password he uses to connect to the university's web site. Without those credentials or if the user misspell he's username or password, it is impossible for him to connect to the UCL's wireless network.

This kind of authentication mechanism is only possible if the infrastructure has several key entities that are going to handle all of this security process.

2.1.2 Design

Using the network monitoring software InterMapper[6] we see that the UCL network is composed of seven neighborhood routers (CtPythagore, CtHalles, CtLew, CtStevin, CtCarnoy, CtMichotte and CtSH1C). Six of them are present on the Louvain-la-Neuve campus and only CtLew is on the Wolluwé Campus. Those routers task is only routing.

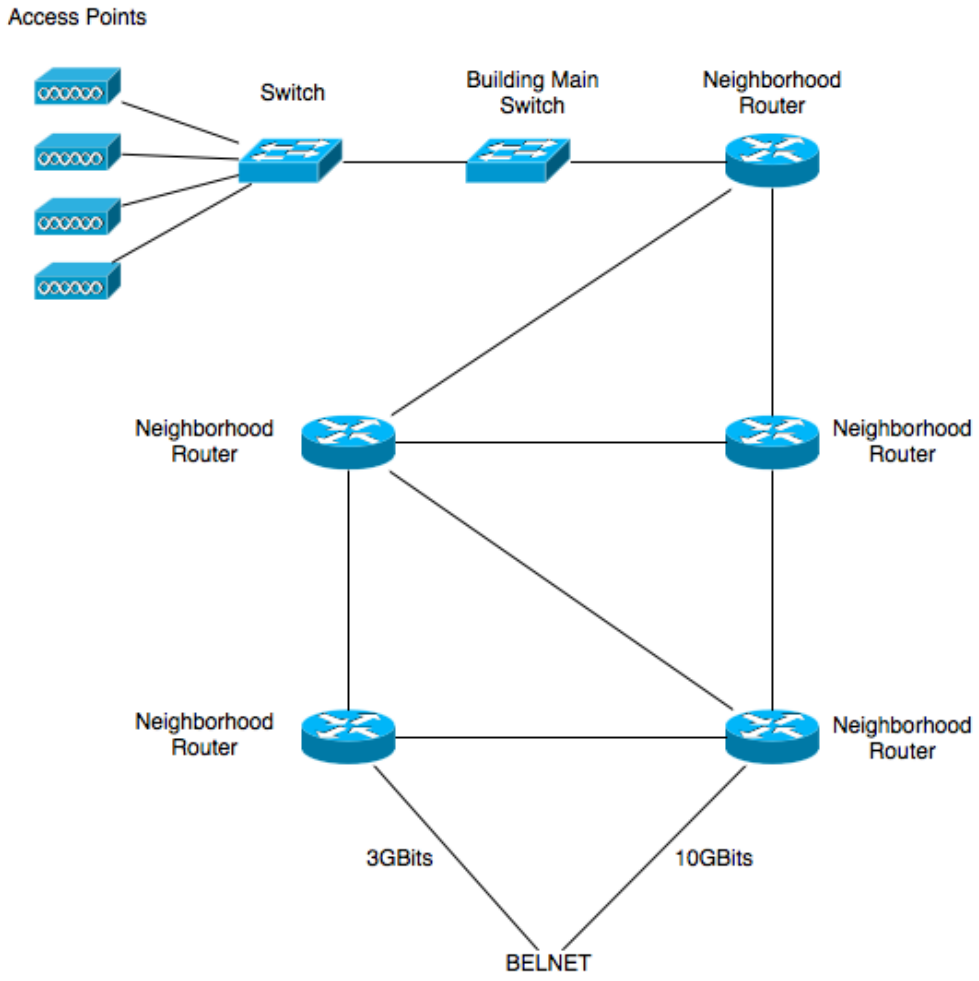
Internet access is provided by Belnet via a 10GBit ethernet link directly connected to the CtPythagore. There is also a second 3GBit ethernet link connected to the CtHalles router but this link is never used. It is only a backup link in case of failure of the main one.

The infrastrucutre also has two main servers which are CtTier2 and CtAquarium. Those main servers are datacentres that contain the RADIUS servers as well as the LDAP servers.

Then for each building there is a switch and this switch is directly connected to one of the seven routers. Each of those switches has 48 ports that are connected to the access points inside the concerned building.

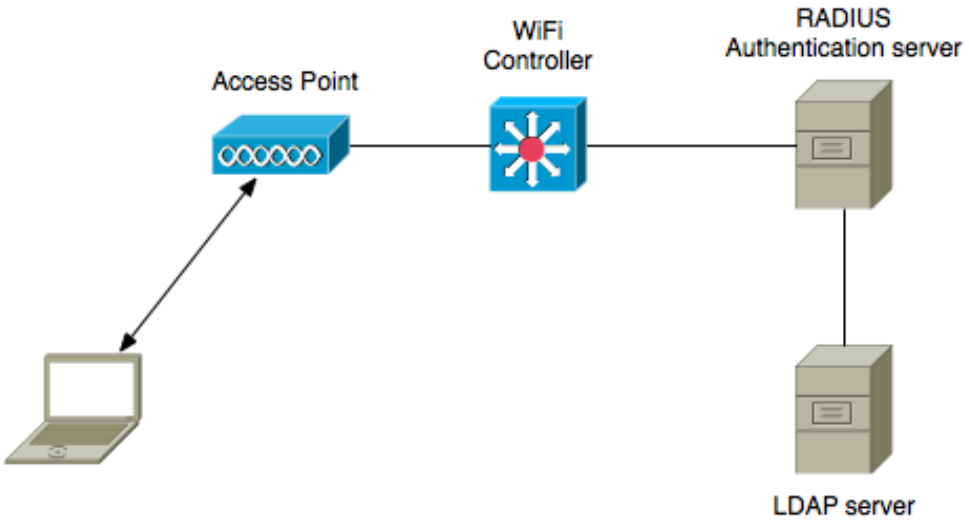
Concretely, in each building we find ethernet plugs that are connected to what we call concentration points. Those points contain commutators that is connected to the building switch that is connected to one of the main routers.
An important point to mention is that the network is not a full mesh.

Here is a simplified representation of the UCL network infrastructure:



2.2 Network Topology

Here is the representation of the network topology:



The Catholic University of Louvain has chosen to use the IEEE 802.1X protocol for user authentication. Thus when a user wants to connect to the WiFi, the access point will realize an EAP negociation with the supplicant. It transmits this EAP information to the controller who is going to interact with the RADIUS authentication server who, in turn, is going to asks information to the LDAP server. Once the RADIUS server authenticate the requesting user, the connection is established.

2.3 Understanding the passive and active logs

Chapter 3

Network Components and Protocols

3.1 802.1X

3.2 RADIUS

3.3 WiSM

3.4 DHCP

3.5 SNMP

The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices [7]. It is part of the TCP/IP protocol suite and it is mainly used by network administrators to get information about devices on the network and the network performances. These information help the administrators to resolve problems on the network or simply to manage it.
A SNMP network has three main components:

- `Network-management system (NMS)`: A NMS is the main component of an SNMP-managed network. It is the management entity that controls the managed devices. It uses the SNMP protocol and can interact with the managed devices to get information using special commands and messages.

- `Managed devices`: It is a network device that contains an SNMP agent. They collect and store information to make them available for the network-management systems. Those devices can be routers, servers, switches,etc. They also run the SNMP protocols to be able to respond to the requests made by the NMS.
- `Agents`: An agent is the thinking part of a managed device. It is a software module that understands the management information and translates them into a SNMP compatible form.

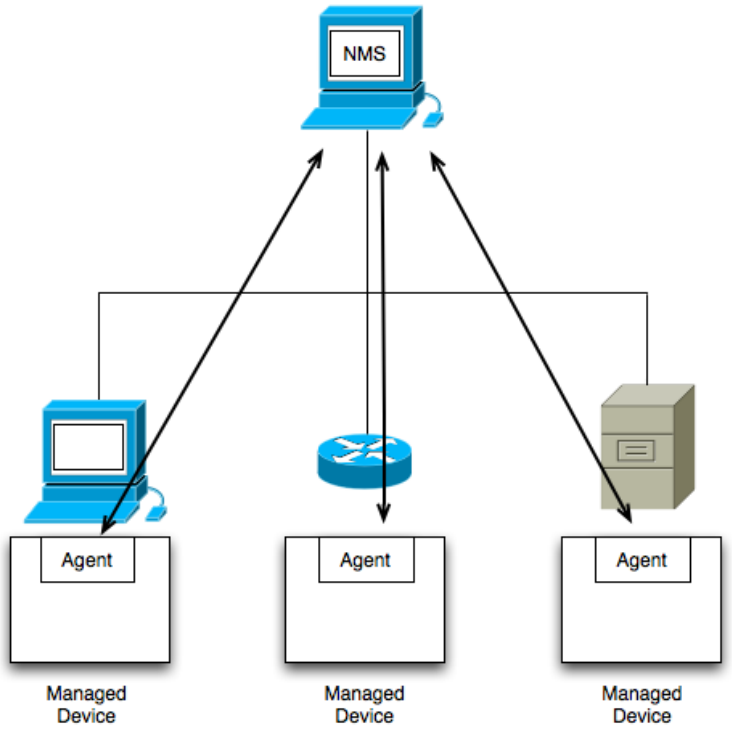


FIGURE 3.1: A typical SNMP managed network

All the network objects are described and organized hierarchically in a Management Information Base (MIB). There are MIBs for each set of related network entites that can be managed. These MIBs are accessed using a network-management protocol such as SNMP.

3.6 Problems encountered

Chapter 4

Monitoring Tool - Architecture

4.1 Architecture

The system have two very distinct entities. The first part is the one responsible for gathering information. This component handles the responsibility to keep the operational database up to date and in a consistent state. The other side of the application is the one managing the analysis made with the information gathered.

4.1.1 Gatherer

This part of the application is constituted of several modules that allow it to communicate with the various sources of information. Each module is responsible of a distinct kind of information and each of them have to transform the piece of information in a coherent entry in the database. As the information come from heterogeneous origins, each information have to be understood and transform into an entity that can be related to others. Without such transformation, the possible analysis would be really limited and not really interesting.

4.1.1.1 Logs

The first kind of information we managed to analyse was the logs files. There is one file per infrastructure component:

- Radius
- DHCP

- Wism

These elements generate several log each seconds and the first difficulty was to make a first sorting. A part of them are just informational and don't bring useful information about the state of the network. Such information will never be used during the analysis and then they don't have to be store in the database. Another part of the log are repetition of others. In fact, as each element produces its logs independently, some logs can overlap and represent the same information. Redundant information are useless and the same information don't need to be in the database twice. This can seems to be a unimportant issue but in consideration of the quantity of information proceed by the application, an overloading of the database can cause severe performance issue during the analysis phase.

4.1.1.2 SNMP

The SNMP protocol allows us to retrieve information on the controller in real-time. The module handling the SNMP request can update the information about the situation of each access point or any client. This bring a lot of interesting data regarding the users of the network but the main drawback is that the request are heavy. We can't make them at any time because it requires resources from the controller. In consequence, we have to find the right balance between keeping the database update and not overloading the controller with SNMP request. The main information extracted are the status of every access points (AP). We can see what access point are actually associated with the controller. A lot of statistics (e.g the load of the AP) are available. The same holds for the client associated to an access point. Each mobile station is indexed by the controller and statistics about it are hold.

4.1.1.3 Active Monitoring

[OpenWRT]

4.1.1.4 Database

The database have to be capable of representing each kind of information and manage the links between them. It isn't hard to create entries for a log but the difficulties appear when we make link with other entities and have to keep them in a coherent state. Several questions raised when we try to designed our database. For example, if a client is no

more associated with an access point, do we have to remove it from the database? Such questions can seem futile but have deep implication on the database.

4.1.2 Analyser

As the gatherer only put available information together, it doesn't bring anything new. In the other side, the analyse component will use the data and the links between them to extract useful information about the network. For example, the SNMP shows the people associated with an access point but only an analysis through time will allow us to detect and even forecast overload in the network. This component will manage the analyse on the database and storing the result over the time.

4.1.2.1 Utilization Statistics

4.1.2.2 Event Statistics

Chapter 5

Monitoring Tool - Implementation and Deployment

5.1 Equipment used

5.2 Testbed conditions

Chapter 6

Results and Analyzis

6.1 Results

6.2 Feedback

6.3 Modification proposed by the test users

Chapter 7

Conclusion and Future Talks

7.1 Conclusion

Appendix A

Source Code

Write your Appendix content here.

Bibliography

[1] Serge Bordères and Nat Makarévitch. *Authentification réseau avec Radius : 802.1x, EAP, FreeRadius*. Eyrolles, Paris, 2006. ISBN 2-212-12007-9. URL `http://opac.inria.fr/record=b1128764`. Les protocoles étudiés dans cet ouvrage peuvent être trouvés sur le site http://www.rfc-editor.org.

[2] Jeff Smith, Jake Woodhams, and Robert Marg. *Controller-Based Wireless LAN Fundamentals: An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks*. WebEx Communications, 1st edition, 2010. ISBN 1587058251, 9781587058257.

[3] M.L. Gress and L. Johnson. *Deploying and Troubleshooting Cisco Wireless LAN Controllers*. Cisco Technology Series. Pearson Education, 2009. ISBN 9781587140501. URL `http://books.google.be/books?id=YLHvHGGx5AEC`.

[4] Terena. What is eduroam?, June 2012. URL `http://www.eduroam.org`.

[5] Belnet. Belnet eduroam service, 2011. URL `http://www.eduroam.be`.

[6] InterMapper. Intermapper web server. URL `http://micronoc.sri.ucl.ac.be/~admin/map_screen.html`.

[7] Cisco. Simple network management protocol. URL `http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol`.

[8] Windows. Windows xp support has ended. URL `http://windows.microsoft.com/en-us/windows/end-support-help`.