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

February 2014

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

Contents

Chapter 1

Introduction

1.1 Towards a WiFi Monitoring Tool

As for other universities around the world, the Catholic Univeristy of Louvain offers a large wireless network throughout its different campus. This network provides a direct and reliable connection to all of the students, staff, teachers and researchers of the university at all time. The problem with the UCL infrastructure is that it is quite huge and it is always changing. The UCL/SRI team, which is responsible for the effective development of that infrastructure and its connection with the outside world, is always trying to improve the connectivity on the site by adding access point or upgrading the Cisco controllers for instance.

Because of that complexity, the management and the efficiency of that network has become quite difficult and buggy. Indeed, the logfiles produced by the controllers are very verbosed which induce an arduous and tricky work of decryption when the team wants to find and trace a problem that occured before on the system. Furthermore, there are more and more users trying to get a connection on the campus (laptops, smartphones,...). This might causes some disturbance on the network that leads to connectivity problems for the direct user.

In this thesis, we discuss the implementation of a WiFi monitoring tool that will help the network administrators managing the wireless infrastructure. To achieve that, we proceed in two steps. First of all, we collect all the information that travels over the network. Those information come from heterogeneous sources (from controllers logfiles to active monitoring logs through customized routers). Second, we have to analyze and process that raw data in a way that is understandable and readable for the end users.

1.1.1 Data Gathering

To work properly, our monitoring tool needs to gather data from the UCL wireless network. These data comes from various places and are quite heterogeneous. Indeed, our system implementation gathers, and stores into our private server, the logfiles containing all the information about the RADIUS, LDAP and DHCP servers as well as the information about the different WiSMs (Wireless Services Modules). Thanks to those logfiles we have a complete overview of the network status and the components at all time.

Moreover, we have designed a custom OpenWRT router that authenticate itself on the UCL network to check if there is a problem during the authentication phase. All the information that the router gathers are also stored into our server. This gives active network status information compared to the passive one collected with the different logfiles.

1.1.2 Data Analysis

The next step is the data analysis. In that phase, our system examines all the logfiles of the server and [TODO]

Throughout this thesis we explain what are the main issues encountered today on the university wireless network and how our monitoring tool is helping the network administrators managing this system. In a first chapter, we present the working environment, and more specifically, the UCL Internet infrastructure. We also discuss the different types of logs we use in our tool. In the following chapter, we present all the network components and protocols used inside the network and where connectivity problems can occur. Finally we provide and describe an implementation of our monitoring tool and we deploy it on the network to gather results and feedback.

1.2 State of the art

Here we present the state of the art of wireless network monitoring.

Chapter 2

Working Environment Overview

2.1 UCL Internet Infrastructure

The Catholic University of Louvain (UCL) is one of the biggest universities in Belgium. It gathers almost 30.000 students and about 10.000 other members from staff to teachers and researchers.

The university also owns several student campus. The headquarters of the UCL is located in the city of Louvain-la-Neuve. The campus gathering the health sciences is located in Woluwe-Saint-Lambert and more recently the cities of Tournai and Mons as well as Charleroi were added to the list.

Faced with such a scale, it is vital for the Catholic Univeristy of Louvain to develop a reliable and efficient Internet connection and wireless network able to deliver a connectivity throughout its campus and all users at all time.

The purpose the University enrolled in is to provide an Internet access and a connectivity according to the type of user who wants to connect. To do this, there are 3 main networks at the Catholic University of Louvain, each with a different SSID.

The univeristy also participates in the projet `eduroam` (which stands for education roaming). Eduroam is the secure, world-wide roaming access service developed for the international research and education community[4].

The eduroam system is a RADIUS-based infrastructure that uses the 802.1X security technology to allow for inter-institutional roaming. It allows the users visiting another institution connected to eduroam to log on to the WLAN using the same credentials the user would use if he were at his home institution[5].
The Catholic University of Louvain thus has a fourth network available with the SSID `eduroam` allowing the foreign students to be able to get an Internet connection at any time on the university locations.
The available networks at UCL are the following:

- `student.UCLouvain`: Only for the students enrolled for the current year at UCL.
- `UCLouvain`: Only for university staff as well as for the researchers.
- `visiteurs.UCLouvain`: Accessible for guests invited by the university.
- `eduroam`: Education Roaming access.

2.2 Hardware infrastructure

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.

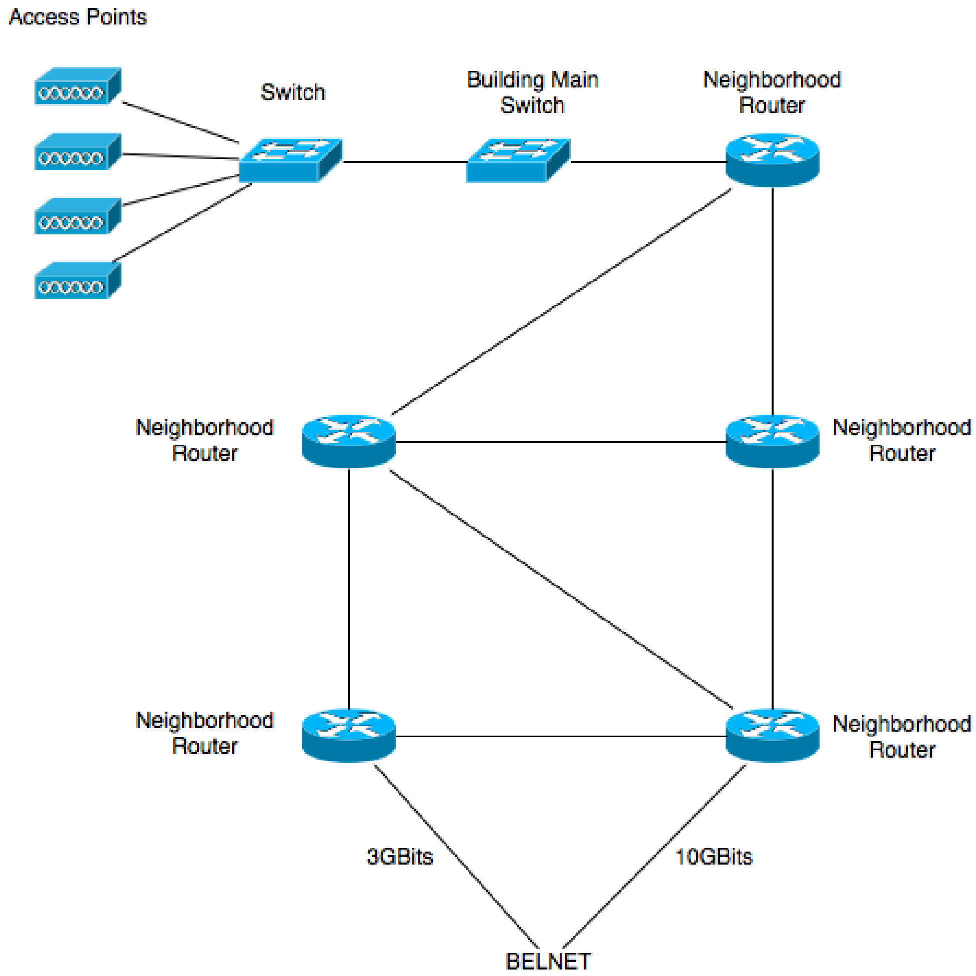
Internet access is provided by Belnet via a 10GBit ethernet link directly connected to the CtPythagore. There is also a second 3GBit ethernet link connected to the CtHalles router but this link is never used. It is only a backup link in case of failure of the main one.

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

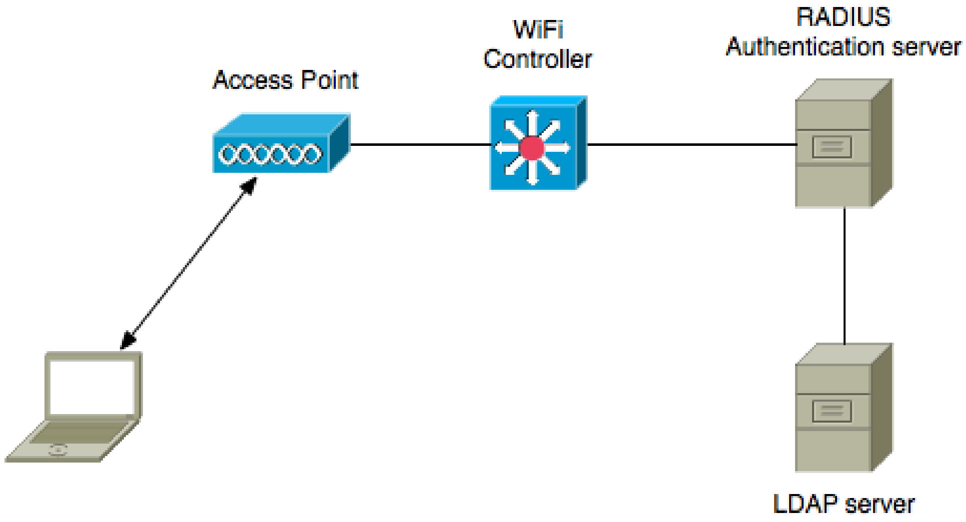
concentration points. Those points contain commutators that is connected to the building switch that is connected to one of the main routers.
An important point to mention is that the network is not a full mesh.

Here is a simplified representation of the UCL network infrastructure:



2.2.1 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

3.6 Problems encountered

Chapter 4

Monitoring tool implementation

4.1 Monitoring tool modeling

Chapter 5

Monitoring Tool 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`.