

## Communication System Design



**Fall 2008**

**OpenCASE**

**“connects world to you”**

**04-01-2009**



### **Team Members:**

Thomas Carlyle Minetto Vilarinho

Md. Safiqul Islam

Abdur Rauf Khan Jadoon

Martin Johansson

Zhang Li

Alper Celik

**TS Lab champion:** Björn Pehrson

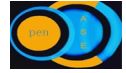
**TSLab coach:** Anders Sjögren

**TSLab co-coach:** Dan Kopparhed

**Principal:** Björn Pehrson

**Company/Organization:** KTH/ICT/TSLab

OpenCASE - Connects world to you



# OpenCASE | Final Report



## Acknowledgment

This project could not have been done without the invaluable help of following people, who have helped us to achieve our final results. That's why we would like to thank to a large number of individuals and previous CSD course teams.

- Professor Björn Perhson, our TS Lab champion, for his encouragement, patience and expert advices. Without him, we could not have been reached up to this point.
- Mr. Anders Sjögren, our project coach, for his project management skills and encouraging comments about our team.
- Ms. Ulla Skidén, one of our teachers at KTH, for helping us about effective communication and marketing skills.
- Mr. Robert Olsson, one of the core developers of Bifrost at Uppsala University, for advising our team about technical subjects and community building.
- Previous CSD teams; OpCon, OSREN-MAREN, OSREN-MoRENet and OSiAN for supplying so much invaluable information for further development of our project.
- Mr. Samuel Ndaula, a former CSD student, for his time and patience to answer all of our questions about business development in Africa.
- Khizer Jalal, Lum Osmani and Santha Kumar for helping us to prepare execution plan for Malawi.
- Daryoush Ali Shokrgozar, Elnaz Shayesteh, Pamela Vicelja and Samuel Ndaula for helping us to prepare execution plan for Mozambique.
- Mr. Voravit Tanyingyong, for his helps about the equipments that we needed.
- Mr. Dan Kopparhed, for his comments and assistance.

Finally, special thanks go to our friends, couples and families who have supported us throughout the project development and being with us even if we could not spend that much time with them during the project period.



## Summary

OpenCASE is an Open Source project. This project outcome is a whole network solution completely based in open source software. Using OpenCASE solution, regular PCs can be turned into routers. But not only that, they can also run networking services like Network Administration, Traffic Monitoring, DNS, Web Server and so on.

OpenCASE project is based on a previous teams (OSiAN) work. They have provided a manual for setting up a whole network. But some services were complex to understand, even for a more advanced user, because all the services needs to be installed and configured in the command line terminal.

We and other OSN users and administrators needed to go through a steep learning curve in order to establish a purely open source network. There was a clear need of having a user-friendly interface so that it was not needed to have an expert to install and configure the OSN. That is why we moved away from the Command Line Interface (CLI) that OSiAN team made, into the Graphical User Interface (GUI) that is provided mainly through Webmin [16]. With Webmin, we can install and configure almost all OSN services with a GUI driven manual. By using our manual, even a user that is not familiar with a service can install and configure it. It is very useful for people who don't have much experience in Linux. Since the Webmin did not support all the networking services we have developed some modules for it, like one for Nagios, WonderShaper and Connection Security (ConSec).

The current Dodowa network needed a redesign to implement authentication, monitoring and connection tracking. We used the GUI-driven approach in a pilot test to redesign most of those aspects. For the authentication, we provide two methods to authorize an user. One is port based authentication, which means that the switch will authenticate the user by using the 802.1x protocol. The other way to authenticate is web based authentication. So, if the user doesn't have 802.1x client installed, he can use the web based authentication, typing username and password in an authentication page. These two methods are using same database, so the user information is synchronized. The monitoring services Nagios and Connection Security are responsible for network monitoring and security. Some basic services such as link DHCP, DNS, Web Server (Apache), Firewall (Netfilters) are also provided in the redesigned network.

OpenCASE - Connects world to you



Due to the open source networking experience acquired during the project, we have also acted as backstoppers for the MAREN and MoRENet teams. When these two teams have finished their project, the networks in Malawi and Mozambique have not been fully implemented. Therefore, we remained responsible for answering their questions and doubts concerning OSN implementation. At last, we also worked on backstopping the OpCon team, in enhancing the business analysis and working to find entrepreneurs interested in OSN.



## Table of Contents

Acknowledgment.....	3
Summary.....	4
1 Introduction.....	8
2 Background.....	8
3 Goals.....	9
3.1 Improving and Enhancing the OSiAN toolbox.....	9
3.2 Redesign of Dodowa Networks.....	10
3.3 Backstopping MAREN and MoRENet Projects (Secondary Goal).....	10
3.4 Business Opportunities of the OSN and the toolbox .....	10
4 Methodology.....	11
4.1 Project Management.....	12
4.2 Iterative Deliverables.....	13
4.3 Time Management.....	13
4.4 Meetings with Teaching Teams & Peer Review.....	13
5 Project Specific Deliverables.....	14
5.1 OSiAN Improvements.....	14
5.1.1 Web-interface OSN approach.....	14
5.1.2 OSN White Paper.....	15
5.1.3 ConSec.....	18
5.1.3.1 Background.....	18
5.1.3.2 Purpose of continued developing.....	19
5.1.3.3 Lab environment setup and description of ConSec basics.....	19
5.1.3.4 Listed features of ConSec.....	21
5.1.3.5 Testing.....	21
5.1.3.6 Integration with Dodowa.....	22
5.1.3.7 Conclusion.....	22
5.2 Dodowa Redesign.....	22
5.2.1 Server 1.....	24
5.2.2 Server 2.....	25
5.2.3 Server 3.....	25
5.2.4 HP2524 Switch.....	25
5.2.5 Easy configuration tool and Packaging.....	26
5.2.6 Monitoring Connection.....	26
5.2.7 User authentication.....	26
5.2.7.1 Services and Scripts.....	26
5.2.7.1.1 Dodowa case.....	26
5.2.7.1.2 Automation Scripts.....	27
5.2.7.1.3 Web server.....	27
5.2.7.2 User Authentication Mechanism.....	27
5.3 Backstopping MoRENet and Maren Projects .....	29



5.4 Improvements of the Business Analysis .....	30
6 Future Work.....	33
6.1 ConSec.....	33
6.2 Dodowa redesign.....	33
6.3 OSN Improvements.....	33
6.4 Buiseness.....	34
7 Conclusions.....	35
8 References.....	36



## 1 Introduction

The OpenCase project started in early September 2008 and ended in early January 2009. During this time, the team have been working on making Open Source software for networks more easy to use. They have all the time had user-friendly in their minds throughout the project. In this document you can find what this project is and how we achieved our goals. In **Goals** section you can find detailed information about what this projects goals is to achieve. How we worked achieving our goals in the project can be be read in **Methodology**. The **Project Specific Deliverables** is described in detailed what OpenCase project have delivered. If some other project wants to continue our work we have provided some proposals of **Future Work**. The outcome of the project is finally discussed in the **Conclusions** section.

## 2 Background

The contemporary communication networks are ruled by proprietary companies like Cisco and Juniper because of their well establishment and long time availability. Open source based network is an alternative solution to the proprietary based solution, where ordinary computers can be used as router and to run other network services, resulting in lower prices, flexibility and possibility of developing applications and features without caring about the proprietary encapsulation of the router or networking tools.

Network services in most of African countries are provided by private companies, thus charging high prices. A Research and Education Network is necessary for those countries to improve and spread education and research. The OSN (open source network) is an alternative to the costs of networking. It is a whole set of open source softwares that can be integrated to provide a network solution as good as the proprietary ones, with the advantage of being open source.

KTH, represented by the TSLab[4], have started several projects for deploying Open Source Networking project all around the world, but having Africa as the main target. The latest projects were implementing the networks in Malawi, by the MAREN team [6], Mozambique , by the MoRENet team [11], and evaluating the business opportunities of the OSN, by the OpCon team [12].

The Open Source Networking includes not only the open source routers (implemented by an open source software running the routing protocol over a open source operational system), but also the open source tools necessary to ensure security, monitoring and administration capabilities to the network.



A previous group of the KTH CSD course, the OSiAN team[14], has worked with the OSN covering an analysis in the Bifrost Linux Distribution[15], a operational system highly optimized for routing developed in the Uppsala University, and the design of some softwares and scripts to enable an easier installation, configuration and integration of the other OSN Services, such as traffic monitoring, package filtering, authentication control and etc.

This project has focused on the OSN services, and, therefore, it has explored several Open Source tools such as Netfilter[16] for package filtering, Squid [17] for Proxy Server, FreeRadius[19] for Authentication, SNORT[18] for intrusion detection system, Webmin[20] for web-based system administration, ConSec[21] for connection tracking, Nagios[22] for network monitoring, MRTG[23] for traffic monitoring, besides other services such as DNS, FTP, Web-server, Database server, DHCP and Mail server.

## 3 Goals

### 3.1 Improving and Enhancing the OSiAN toolbox

To evaluate the OSiAN toolbox from the user perspective, we examined their documents, softwares, scripts involved in the toolbox, and documented bugs and problems. Based on these experiences and the different requirements important for the OSN users in (Dodowa[13], MoRENet[11], MAREN[6] and SSVL-OSN[7] projects). we have defined the scope of the OSiAN improvements.

Some of the requirements which were considered the most important and also the ones feasible to do in the time frame of this project were the following.

- To write a blue print for the OSN solution. A document showing all the modules inside the OSN, their relationship and architecture. This is something that was missing in the current OSiAN toolbox. The document should have the ability to enhance the documentation and presentation of the OSN solutions.
- The second important aspect of the toolbox is the ConSec tool which needed to be improved. We worked to improve the ConSec tool by adding new and advanced features. Improve its graphical user interface to be more user friendly and easy. Besides its integration with Firewall and email server.
- Another important aspect of the OSiAN toolbox is its packaging. We worked on a graphical interface that will act as both manual, trigger of the installation scripts, making the packaging more easy to use. We focused our development in the Webmin software tool, which is a very powerful, fast and user friendly web based interface for system administration of Unix. We had



to add some tools to Webmin which are used by OSN teams but that were not yet supported by Webmin such as ConSec and Nagios. We have also documented on how to customize this packaging into a user-friendly DVD or CD.

- We added some other tools and services that have been used by the summer teams but currently not part of the OSiAN. e.g Squid Proxy Server, Intrusion Detection System, FTP server, mail server.

### ***3.2 Redesign of Dodowa Networks***

We had to redesign the Dodowa network by implementing a port based and web based user authentication mechanism. Our user authentication mechanism should be based on RADIUS and SQL server. The web solution needed the implementation of Firewall rules, Web server, DHCP, DNS servers and MD5 hashing algorithm to encrypt the password and the whole solution needed to implement 802.1x. The redesign also included the ConSec and Nagios tools. We have also to go through, producing a customizable installation CD and show that it can be used for installing and configuring a machine and its services without much user interaction.

### ***3.3 Backstopping MAREN and MoRENet Projects (Secondary Goal)***

The CSD team MAREN ( Research and Education Network in Malawi) and MoRENet (Mozambique Research and Education Network) worked on OSN designs during the middle-end of 2008. For backstopping their projects, we provides support for implementation work on both Malawi and Mozambique. In order to be ready to the backstopping and to understand better the OSN itself and its needs, our team members has joined several meetings with both CSD Projects in Malawi and Mozambique, attended their presentations and demos. The support was restricted to topics covered by the OSiAN improvements.

### ***3.4 Business Opportunities of the OSN and the toolbox***

We had to enhance the business plan based on the Open Source Networking business case, developed by the OpCon team. This included revising the business plan, producing white papers on the business development of the OSN solutions. We have also to Study and analyze the OSN opportunities in Africa based on the continent situation and Open Source market.



Even if there were already established work from previous teams, we targeted to make it more concrete and obvious. One of the most important things was taking previous works to the execution level. Deciding the best business models to make money out of open source technology and helping to the entrepreneurial people were another goals of this project. But, the biggest goal was to make deeper analysis and plans about business around the Open Source PC-Based networking solution in the African market.

On the other hand, as Björn[1] the main stakeholder for this goal, sees the importance of having a discussion forum about open source technology, we decided to create a community around our solution. Even if this idea came so late, we tried our best to achieve a good result. Since open source is much depended on community both from professionals and users, we wanted to create a web discussions forum to encourage people to share their knowledge and experiences. In addition to this, we had close relationship with Afren[25] and Bifrost user forum to invite African and Swedish people to our newly installed web forum.

To sum up, points below were the main goals for business part of our team;

- Deepen the analysis from the OpCon[12] team.
- Create a business plan template, which can be used any African countries.
- Prepare specific documents about Malawi and Mozambique.
- Consult African people and encourage them to take actions about Bifrost/OSiAN.
- Create a community around our whole product.

## 4 Methodology

The OSN open case project can be divided into four sections. These are the following as mentioned above.

- Improvements to the OSiAN toolbox
- Redesigning of the Dodowa network
- Backstopping MAREN and MoRENet projects
- Business opportunities of the OSN and the toolbox.



All of these sections of the project is related to each other, e.g ConSec tool will be improved in the toolbox and will also be implemented in the Dodowa redesign Networks. Similarly we have to use a very powerful, user friendly web based interface tool Webmin for the implementation of different services and tools in OSiAN toolbox as well as in the redesigning of the Dodowa network. Some other tools and services which are used by the MAREN and MoRENet teams, such as FTP server, Squid Server, Intrusion Detection System and mail server, we are going to add these all tools in the OSiAN toolbox. Business opportunities of the OSN and the toolbox were already analyzed by the OpCon team, so we could backstopp them to enhance and improve it.

Working and managing all those tasks was a great challenge for the OpenCase team and also to clear the goals and finalizing the project plan. But the team has worked together by sharing their experiences to achieve all tasks. The team has worked in this project as team of professionals conducting the project in accord to constant feedback given by teaching team, regular meetings, and discussions with coaches (which represented our closer stakeholders). The team improved their skills by attending different trainings, reading, demonstrating, working as a team within the same place, discussing, and sharing their experiences.

The team has divided the tasks among different members in order to achieve excellent results and to meet the exact project goals. Two members lead the work to improve the OSiAN toolbox with a easy OSN approach, by implementing different tools and services with help of powerful and user friendly tool Webmin. One member have assigned the task to work on the ConSec tool. Then another member have worked on the redesigning of the Dodowa networks. During working on these tasks another member has joined the OSN OpenCase team, to analyze the business approaches based on the Open Source Networking business case. Then in the end the Webmin team work together with Dodowa redesigning networks task to implement the user authentication mechanism.

The following are the some approaches we have adopted during our work on the project.

#### **4.1 Project Management**

One member of the group was responsible for managing the project, having another member as a backup in case of absence. The project manager worked really close to the group as technical leader, leading several evaluations of the



state of the deliverables and progress of the project, to them review the next tasks. The approach taken was based on the spiral life-cycle and the iterative and incremental development models. The process consisted on setting a group of iterative sub-tasks, then approaching to first iterations, analyzing and implementing them, to evaluate and start the next iterations (and possible adjustment of previous tasks) converging to the final deliverables.

## **4.2 Iterative Deliverables**

The group has worked creating iterative deliverables and adding them to its websites as internal deliverables so the progress and status of the project could be followed by our coach, teaching team and the group itself. After the coach change, the group also moved to a strategy of documenting the iterative deliverables (the ones done and the ones to be done) in the project plan. This iterative approach is very good in the way that it offers the possibility for the customer to review the work and give feedback or propose changes before the end of the project.

## **4.3 Time Management**

During the whole project all the team members had worked on different tasks. Some of the team members had worked together in a group for some tasks. Each member of the team is maintained an accurate weekly time sheet that was compiled together with weekly progress report. Each member mentioned the time in the weekly time sheet he spend on the individual task. Each member mentioned the deliverables output from the specific task in the time sheet and put the document on the internal deliverables section on project website. Every member of the team has mentioned the problems, possible solutions he faced during the specific tasks. Every one was individually responsible to maintain his time sheet. The project manager also reviewed all the weekly time sheets in order to see how a team member spent the time on the specific task, review the timing for the following tasks and to correct further time estimations also based on the responsible for each goal.

## **4.4 Meetings with Teaching Teams & Peer Review**

We have attended the regular meetings with teaching teams, Coaches and Co-Coaches. With teaching team only the project manager and assistant project manager attended the meetings in order to discuss the phases, goals and status of the project. Each team members have attended the meetings with coach and



Co-Coach to discussed different tasks, issues, discussed the progress of the team and some problems we have faced during the project. The weekly report and the Internal deliverables were a way for the coaches and teaching team to follow the work of the group.

Team review was a very important part of the project, we have reviewed two other CSD teams, reviewed their project plan, technical documents, progress reports, mid term presentation, project website and specific topics on their projects. We have given our comments and feedback on their work. Similarly our work has also been reviewed by the two another CSD teams and we have acted on our project based on that feedback.

For business part of our assignment, we used following methods to achieve our goals.

- Case studies of Open Source Business Models
- Interviews with people such as; previous CSD students, Bifrost developers, African professors and network professionals from NRENs, Entrepreneurs, PHD students from Handelshögskolan, other CSD team members and managers.
- Information gathering from Internet, magazines and previous works of ex-CSD teams.
- Scientific frameworks like TALC and Gartner’s Hype Cycle.
- Video conferences and phone calls with NRENs.
- Outsourcing.
- Effective media usage, like forum, podcasts, video and mailing lists.

## **5 Project Specific Deliverables**

### **5.1 OSiAN Improvements**

#### **5.1.1 Web-interface OSN approach**

In order to describe the Webmin, we will paraphrase the description given at its website:

“Webmin is a web-based interface for system administration for Unix. Using any modern web browser, you can setup user accounts, Apache, DNS, file sharing and much more. Webmin removes the need to manually edit Unix configuration files



like `/etc/passwd`, and lets you manage a system from the console or remotely.”

The system administration capabilities provided by Webmin are quite broad. It also enables the user to verify packages installed on the computer and install new packages by using the native package administrator from the Linux distribution (`apt-get` for Ubuntu and `yum` for Fedora). The Webmin is available to be compiled for any Linux distribution and is packaged in rpm and deb packages. Besides that, it has a version for Solaris and for Windows.

The Webmin comes already with modules for some servers like Sendmail, SSH and Apache. But for the other services, you can create your own native Webmin module, use a third-party native module or you can even add some web-based application (PHP for example) as a module to the Webmin menu.

Since Webmin is based on modules, it is more flexible. For example for the firewall, Webmin has two modules. One is “Simple Firewall”, which is just for basic user. It has very simple and user-friendly GUI. User can easily add basic rules for firewall. Another module is “Shoreline Firewall”, which has all features of firewall and also user-friendly GUI. It could be used by advanced administrator who has more experience and wants to implement more advanced feature in firewall. So, with Webmin, the users can select modules depending on their experience.

Currently, the Webmin posses modules that can be used for Squid Proxy Server, BIND DNS server (and those modules can download the service itself if it is not yet installed), DHCP server, ProFTPD server, both Postfix and Dovecot mail server, Firewall (which there are several modules available, including less sophisticated to very complex ones), and so on.

But some modules of services are not provided by Webmin or third-party modules, like Nagios and ConSec. We developed Nagios and ConSec modules for Webmin, in order to keep a unique web graphical user interface.

For some of the services we haven't developed any module for Webmin, like FreeRadius and RT due to the project time frame. We configured them manually, but a module for those is something that could be done in future.

We provided a GUI-oriented manual for all services using Webmin. It is easier for people who don't have enough Linux experience than the previous manual from the OSIAN team.



### 5.1.2 OSN White Paper

This project dedicated some of its time to write a White Paper about Open Source networking with the aim to provide a brief but comprehensive description of OSN, in a white paper format, including some components added during this project.

The whole white paper can be found at [8], and here we present a small summary of it. We started by dividing the Open Source Networking in layers based on the final usage of the services at each layer and on the intercommunication between the layers, as it is described in the picture below.

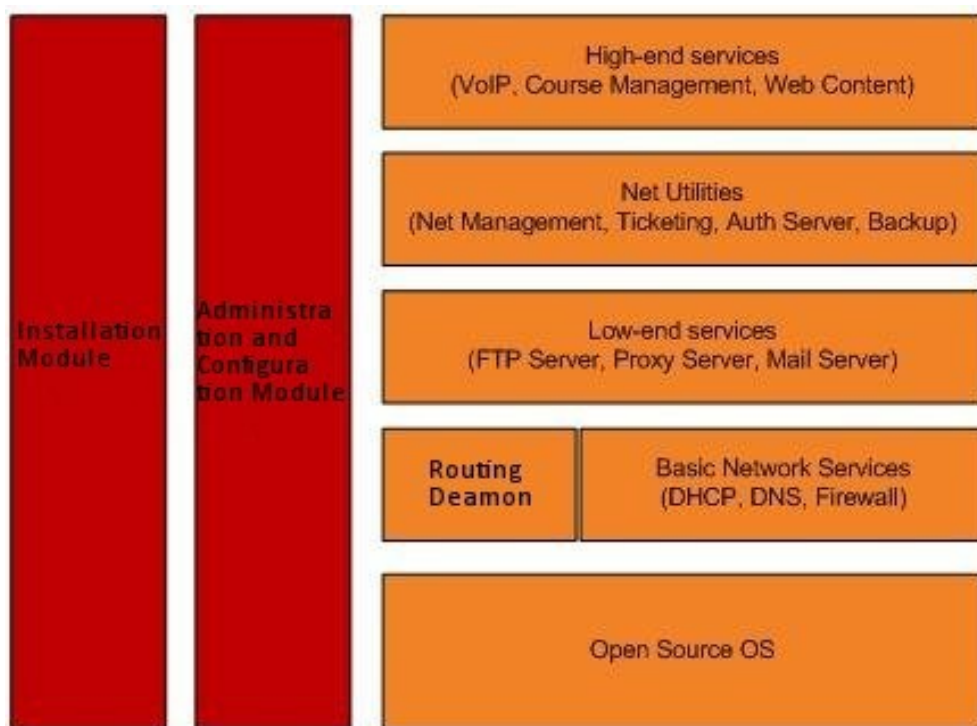


Illustration 1: OSN Component Diagram

That is a general diagram that can be applied for the OSN itself, where the open source routers would generally have only the Open Source OS module and the routing daemon. Whereas, the net utilities and low-end services could be installed in a single machine or distributed in several ones and the high-end services does not even need to be present. The Administration/Configuration Module and the Installation module are used to support the others. The security aspects should also be taken into account, even though they are intrinsic part of all the modules and their integrations.



The Open Source Operational System corresponds to the underlying Operational System to be installed in the machines that will act as routers or to provide network services. The OSN project may use several distributions, taking the advantages of each one of them for each need. In this document we will go very briefly through the configuration of the Operational System, because most of the Linux Distributions either auto-detect the machines configurations or offer the user the possibility to insert it during the installation.

The Routing Daemon module is represented by the software layer providing dynamic routing functionalities for the machine, which could be a software that communicates one of the routing protocol such as RIP, OSPF and or BGP. In the same level, we have some basic network services which are fundamental to provide simple connectivity functionalities and control such as domain name resolution, IP assignment and the packet traffic controlling.

Then, we have the low-end services, which are the ones that offer some application service that could be used by the end user, but are generally used by another application or by the network administrators. Those services include database servers, web servers, ftp servers, proxy servers, ssh servers and mail servers.

The next layer, the Net Utilities, includes the services that are used for network administration and management and are not targeted to the end-user. While the High-end services are several open-source services that can be provided to the end-users once the network has been deployed such as Content Manager, Learning Management System, VoIP server and others. We have not tried to cover those High-end services because they include various services that can be handled by various open-source softwares and we considered as something up to each project to explore by its own.

The white paper asses the security aspects of the OSN as well, even though it does not define it as module in the diagram. Instead of that, we present those as an intrinsic aspect of each service provided (in each layer) and of the relationship in between the services.

At last, there is a configuration/administration which is one of the main developments in this project as a lot of work was done in providing and exploring a tool for configuring and administrating the OSN services and testing this tool in the specific task of redesigning the Dodowa Network.



## 5.1.3 ConSec

### 5.1.3.1 Background

ConSec (Connection Security) was started by OSiAN (Open Source in African Networks) team in Spring 2008. OpenCASE team has the fall of 2008 improved this tool to be more user-friendly and easier to manage. The tool can now display the in- and outgoing connections on a router in both graphs and tables for an easier and faster overview of the network. It is important when running a large network to keep track of the connections, if any suspicious behaviour will occur, ConSec will help the administrator to locate the problem. It can be installed on any Linux-machine and it is using a GUI that is easy accessed in a browser from any computer and place.

### 5.1.3.2 Purpose of continued developing

The purpose of the further development with ConSec was that the OSiAN's version had a vague user-interface that was not that user-friendly. The old interface required the administrator to actively interact with ConSec to get updates of how many connections the network had. The presentation of the connections was also very difficult to understand for a network administrator. One of the main purposes to the further development is because there is no other tool like ConSec out on the market today.

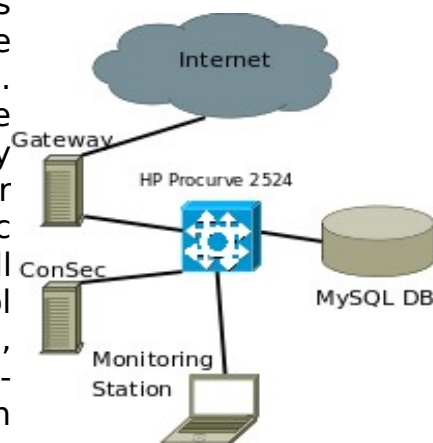
ConSec is in this way very unique and a good contribution to the OSN toolbox. The new ConSec module was developed with Dan Kopparded[2] and the Dodowa[13] project as a customer. As ConSec was developed in iterations, it was revised after each iteration was done.

ConSec is mainly written in PHP/HTML. But it also have some parts written in Perl and Expect. PHP is especially suited for Web development and it can be embedded into HTML. For storing data ConSec is using MySQL as a database.



### 5.1.3.3 Lab environment setup and description of ConSec basics

ConSec was run on a Mac Mini machine and it was monitoring the gateway. This machine and all the others had either Ubuntu Server or Desktop installed. We had another computer setup acting as a database server in this case. Everything could be monitored by browsing to the ConSec web page from one of our laptops connected to the switch. When ConSec updates the current state of connections, it will connect to the gateway machine via SSH protocol and first it will copy the current connection state, which is TCP connections generated by `conntrack-tools`[5], to a file and then download it. It will then parse this file, arranging and counting how many connections there is in total both in- and outgoing and it will do the same for each IP. Both the updating of connections and the parsing is activated each five minutes by Cron, which is a time-base scheduling service. With Cron there will be an automatic update of connections regularly, which is why the graphs can be built in such a easy way and this also decreases the user interaction a lot.



When the parsing of the connection file is done, the results will be uploaded to the MySQL server and also to the RRDTool[9] database file located on the same machine as ConSec. The MySQL Server doesn't have to be on the same computer as ConSec, it can be located on another machine as we have set it up in our lab. The RRDTool database file is only needed for creating the network graphs of the connections.



#### **5.1.3.4 Listed features of ConSec**

- Fetches connections automatically from managed machine.
- List every IP in the network.
- For listed IPs, number of connections and what ports can be shown.
- If a port is known, not only dangerous, it will tell you what it is.
- Ban (Block access to network) can be done to a specific IP.
- Ban can be made with auto-removal of the ban after a set of time.
- All bans can be viewed by the administrator.
- History pages that tells when and what IPs that where over the threshold.
- Graphs of the connections in the network.
- Graphs displaying data up to one year back in time.
- Receive mail of all IPs that had connections over the threshold.

#### **5.1.3.5 Testing**

The final testing of ConSec was done with our lab equipment for the Dodowa project. There have been continually tests done during the development of ConSec. But during this time there was only one developing computer to test every part separately on. They were not tested all together at once as could be done in our lab. So up to the moment we got all the lab equipment ConSec had not been tested in a real environment.

ConSec was in our lab installed by using the Webmin module. This was done because there was a need also to be able to test that the module worked as it should so it actually downloaded all the required packages needed for ConSec.

After that it was time to test the installation progress. The installation progress is an important part because this will setup the databases and create the configuration file. When it was installed and ready to use, we now had to ensure that it was actually getting the newest updates of connections from the gateway machine and also that it was updating all the tables and graphs correctly. Since this progress could be tested during the development phase, there were not many problems found here. All this steps mentioned here was done more than once to ensure that everything was working.



### **5.1.3.6 Integration with Dodowa**

ConSec was integrated with the Dodowa so that there could be an option in ConSec to ban an user from the network. Since Dodowa is using FreeRadius to authenticate users in the network, the banning of users in ConSec had to be able to communicate with the radius. Without the integration, ConSec will just ban the user by adding firewall rules. But with the integration of ConSec and the authentication part of Dodowa, the banning procedure will ban an user from the firewall and at the same time disable the user from logging in again. To be able to disable an user from logging in to the network, ConSec will connect to the radius MySQL table and then add a row saying the reply message to be “Reject” instead of “Accept” for this specific user. The usernames and the corresponding IP address is saved in the radius table so that the correct username will be blocked.

### **5.1.3.7 Conclusion**

With the final version of ConSec done, It is a fully working connections tracking graphical user interface. The ConSec can with the help of contrack-tools[5] display the connections in a way that can help the administrator understand what is going on in the network. Giving the administrator a better view over the connections in the network and also each IP, will help administrator to take decisions if any user should not be allowed in the network. The graphs in ConSec can also help getting an overview of the network, in the way that you can expect when the connections are gonna be high or low. With the help of Webmin ConSec can easily be installed by just using GUI.

## **5.2 Dodowa Redesign**

Network design of Dodowa[13] is an African project for Dodowa Health Research Center(DHRC). KTH has already worked with the designing of the Dodowa network and they have suggested some improvements. The Dodowa network consists of three server machines and one HP pro curve 2524 switch. Following picture illustrates the network infrastructure of Dodowa.

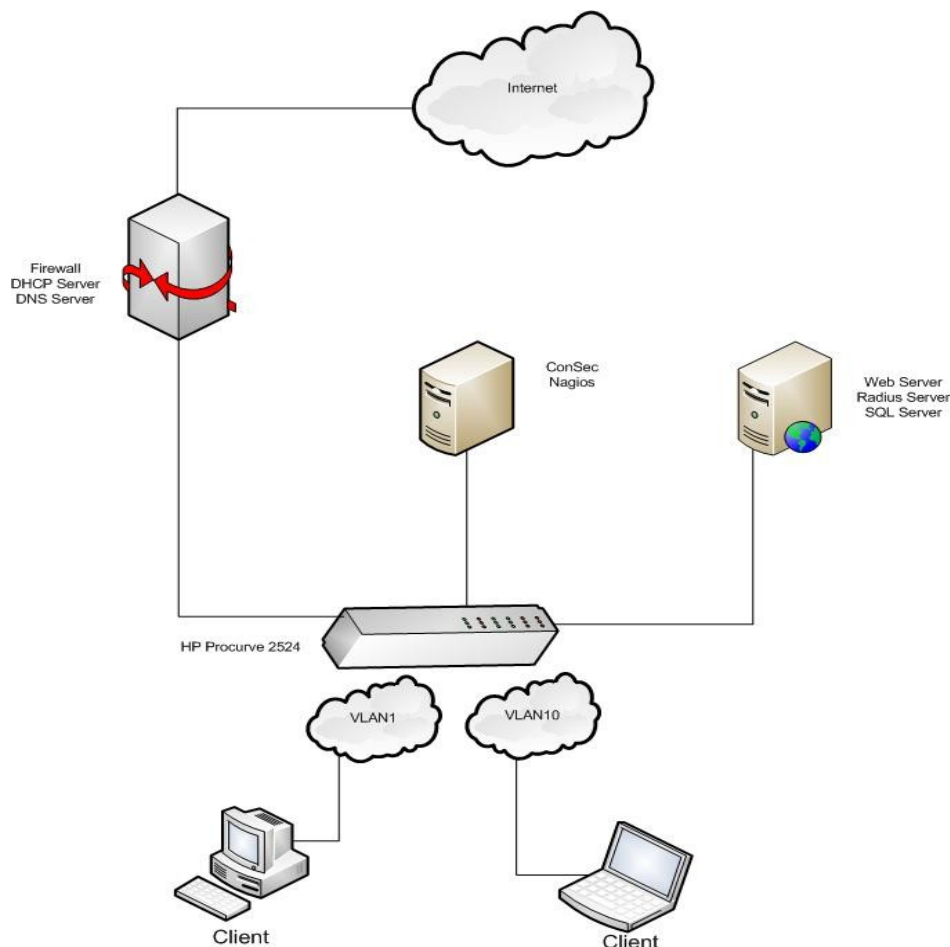


Figure 1: Network Topology

### 5.2.1 Server 1

Server 1 is used as a gateway having two ethernet interfaces. One of them is connected to the dodowa local network and other one is connected to the internet.

Gateway machine is providing the following services:

1. IP tables based firewall.
2. Network Address Translation(NAT) for translating the private address to public address.
3. DHCP server to provide the dynamic private IP addresses to the client.
4. Bind9/named DNS services serving the local network..
5. Routing functionalists for the NAT services.



### 5.2.2 Server 2

Server 2 is used for providing the network monitoring facility. Services used in server 2 are:

1. ConSec - TCP connection tracking
2. Nagios - Network monitoring

### 5.2.3 Server 3

Server 3 is used for the radius server, database and for providing the web page to the unauthenticated users. Following services are installed in server 3:

1. Freeradius- Authenticating the clients.
2. MYSQL - SQL database for storing username and password.
3. PHPmyadmin - Database administration
4. Webserver- Serving the web page

### 5.2.4 HP2524 Switch

HP2524 switch is used to interconnect all the servers and also used for support port based authentication. There are two VLAN configured in the switch - VLAN1 and VLAN10. VLAN is for all unauthenticated clients where they can use both the port based and web based authentication. VLAN10 is for the authenticated client by port based authentication.

Figure 2 shows the blueprint of the Dodowa network:

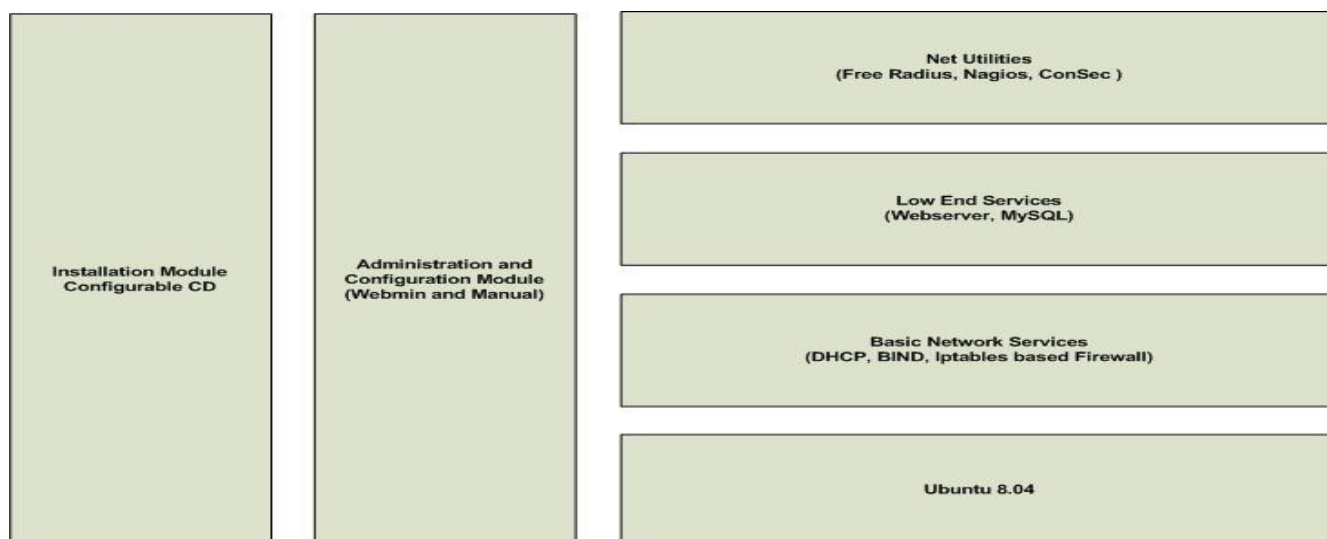


Figure 2: Blueprint



## 5.2.5 Easy configuration tool and Packaging

## 5.2.6 Monitoring Connection

The monitoring of connections is done by using Connection Security (ConSec). In Dodowa we can secure the connections by tracking them on the gateway-machine.

## 5.2.7 User authentication

To provide the user authentication to the user both 802.1X port based solution and web based authentication solution are supported. 802.1X solution is the primary solution and web based authentication is the alternative solution for the users having no 802.1X client. The following sub chapters will discuss about the services used in the Dodowa user authentication case and also describe about the user authentication mechanism.

### 5.2.7.1 Services and Scripts

The installation and configuration of all the services and the automation scripts are available in the following location[3]. Following services are used in the

#### 5.2.7.1.1 Dodowa case

- **DNS** server in Dodowa is used to translate domain name to IP address. When a user connects to the switch, any traffic of this user will be redirected to <https://www.dodowakth.com>. So the main task of DNS server is to translate domain [www.dodowakth.com](https://www.dodowakth.com) for internal network.
- **DHCP** server is used to assign IP addresses to users. Since we have 2 VLAN in the switch, so we need have 2 subnet in configuration file. One for VLAN 1 and another for VLAN 10.
- **Free radius** is the most widely used radius server in the world. FreeRadius server is fast, rich-feature, modular and scalable. It supplies the AAA ( Authentication, Authorization and Accounting) needs.
- **MySQL** is used to store the user name and password where radius server will check MySQL for the authenticating of the user.
- **Firewall** rules are specially for the web based authentication where unauthenticated users will be redirected to the login page and provide their user name and password for authentication. If the authentication is successful then the firewall rule will allow the user. And we have also set firewall rules for the authenticated users via port based authentication and they are always allowed by the firewall.



### 5.2.7.1.2 Automation Scripts

We have created several scripts to automate the process. Specially, scripts are basically created for the web based login. Following scripts are used in our case:

- **Startup Script :** It is a shell script for starting the services and setting up the IP addresses for the web server and gateway.
- **Firewall Script:** Firewall script is created to allow the user when he is authenticated and delete the user when the user is disconnected. One script is executed in the shell of gateway from PHP via SSH.
- **Logout Script:** Logout script is created using perl. That will detect the disconnection of the user and delete them from the Iptables rules.
- **Login Script:** Login script add the the authorized user in the firewall.

### 5.2.7.1.3 Web server

Apache web server with SSL support was used to provide the login page to the user. Since, gateway will listen to the HTTP and HTTPS traffic for the user and redirect the user to the HTTPS page.

### 5.2.7.2 User Authentication Mechanism

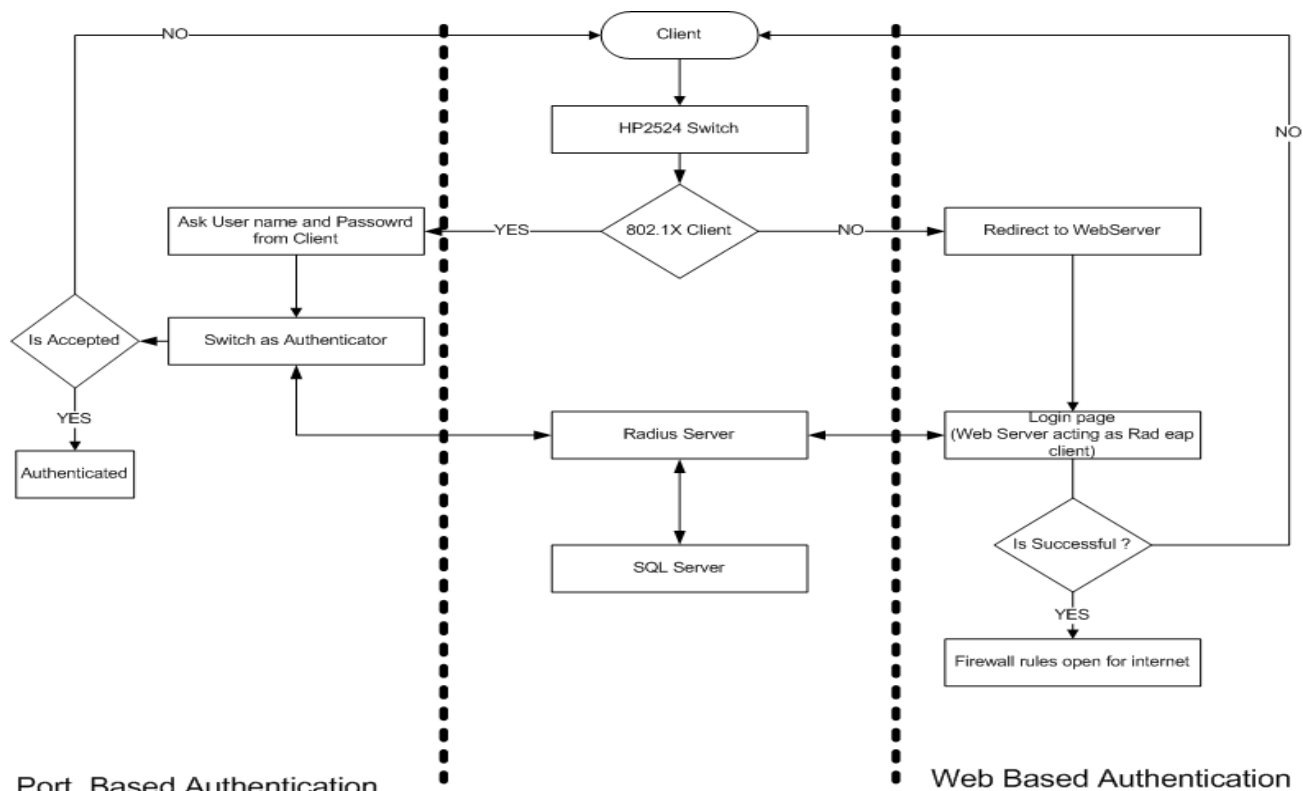
Both the user authentication mechanism works based on the same authentication server. When the client, having 802.1x, is connected to the switch he will be asked for providing user name and password. Then, after providing the user name and password, the authenticator, HP switch, will forward the request to the radius server and radius server will query the MySQL database to check whether the provided information is correct or not. If he is authenticated then the VLAN membership will be changed and he will be allowed to access the Internet, else he will be asked for the user name and password again.

If the client has no 802.1x client than it will follow the web based login. Then, whatever the user will type in the browser then he will be redirected to the login page provided by the web server. The web-server will act as radeapclient for all the users. When the user provide the user name and password then web server will act as the radeapclient and send the request to the web server and if the information is correct then he will authenticated and a script from the web server will SSH the gateway machine and change the firewall rules to allow the users.

The following diagram (Figure 3: User Authentication) illustrates how the user



authentication for the both case works :



Port Based Authentication  
Figure 3: User Authentication

### 5.3 Backstopping MoRENet and Maren Projects

The group also worked on understanding the deployment of the Open Source Networks performed by the MoRENet[11] and Maren[6] CSD Project, as this enabled the team to extend its research in the OSN area and also to backstop the implementation of those projects after they were done.

The projects were at different phases of deployment and the support activities offered to them were quite different from each other and always based on the customer request. The whole report can be found at [10] and here we just briefly describe it.

The implementation of the network in Malawi was at a pending state, and at the moment in which this report was written, they have not yet applied for the IPs or



ASN addresses. The support given was mainly by answering some e-mails regarding question arisen about establishment of a GRE Tunnel, VoIP Integration with PABX network and Learn Management Systems.

In the other hand, the project in Mozambique was just entering the implementation level as they had just received the machines that will act as routers and in the management of the network. They were working on configuring and installing those machines and they faced a few issues:

- The original packaging of the services was targeted to a installation using the Internet.
- They end up using HP Proliant Machines and there was the need of checking the compatibility of the HP Proliant with the MoRENet solution.

After all, the OpenCase team migrated the on-line steps of the OSN installation to a off-line installation based on a customized Fedora package repository and scripts for switching between the on-line repository to the off-line repository. Besides that, we also added a few packages that could be needed for some HP Proliant drivers and provided a guide for the off-line installation, which can be found here [10].

#### **5.4 Improvements of the Business Analysis**

To achieve our goals in the business part, we prepared very specific documents about our initial target markets[26], Malawi and Mozambique. In addition to these, we developed a business plan template to help entrepreneurs to easily understand the concept of the project and write their own business plans according to their target market conditions.

To deepening the previous analysis we used TALC[28] and Gartner's Hype Cycle[28] model to discover the details of our technology and marketing plans for future.

We positioned open source networking at TALC model and showed the potential of our technology by using the Gartner's Hype Cycle model. The reason why we selected these two frameworks was that, they are very famous and well proved models to position our technology on the market and see if this technology worth investing.

Secondly, we outsourced some parts of our execution plans to a group of ICT



Entrepreneurship students. Because of the fact that, our team had only one business consultant it was the best way for us to achieve our goals by outsourcing some part of our work load. Since Prof. Björn[1] also suggested us to use this chance, it was a good option to achieve our goals. For outsourcing, we prepared two different assignments and control the process. Main focus of our outsourcing project was that, business models for Malawi[29] and Mozambique[30], are separately. Naturally, outsourcing was a little problematic but we managed to control the work and helped students to produce high quality works. Our business consultant worked with them quite a lot and he ensured the quality of their business model reports. At the end, we got the document from sub-teams and mixing with our work, we delivered two different execution plans, one for Malawi[31] and other for Mozambique[32].

On the other hand, we continuously provided consultancy services for community from Africa. For example people from Association of African Universities[33] (AAU), Rwanda Education and Research Network (RwEdNet[34]), Malawi Education and Research Network (MAREN[35]), Mozambique research and educational network (MoRENet[36]), ICT Association (ICTAM[37]), South African Education and Research Network (TENET[38]) and Ministry of Science and Technology of Mozambique. Also, we had good communication with the core development team of Bifrost in Uppsala University and they are also in our discussion forum to share their knowledge and experience with our community.

Referring to the table below, we can divide NRENs into two groups as operating NRENs and emerging NRENs. In our discussion forum, we have members from some of these African NRENs. It was difficult to convince people to come and participate but we still tried our best to have active conversations going on in the web forum[39].



Important NRENs			
Operational NRENs		Emerging NRENs	
Country	Name	Country	Name
Malawi	MAREN	Mozambique	MoRENet
Egypt	EUN	Cameroon	RIC
Kenya	KENET	Ghana	GARNET
Algeria	ARN	Nigeria	ngNOG
Morocco	MARWAN	Burkina Faso	RENER
South Africa	TENET	Uganda	RENU
Tunisia	RNRST	Congo	

We have also examined the African market in general to understand if our technology worth investing money or not. We have showed the outcomes of these researches in our documents and white papers. In addition to these, we have spent some time to deepening the business model analysis. We outsourced some parts of this work and it helped us a lot to find the best business practices based on our solution.

In our business plan template[40], we helped entrepreneurs to write their own business plans easily, without making any crucial mistakes about our technology or their target markets. To achieve this, we provided information about industry overview, channels analysis, business models, operation strategies, marketing strategies, sales strategies, promotional strategies, competition strategies, challenges and risks and finally the financial. We added some important appendixes to help entrepreneurs how to write their plans successfully. Since our team had only one business consultant, we generally used well know highly recommended resources to create most parts of these appendixes and the references can be found in those documents.

As a complementary document, we created a tools paper[41] to show consequent CSD students and entrepreneurs what kind of frameworks they can use. We added this paper as appendix to our generic business plan to help entrepreneurs to create better, scientifically approved models for their businesses.



Last but not least, we created podcasts[42] of our business deliverables and any one can download and listen them while on the go. In addition to this, we had a youtube channel[43] where we stream our videos for the project stake holders, coming CSD students and teaching team. The reason why we did, is that it takes lots of time for new CSD students or new project stake holders to read all the documents on the contrary, media is an important tool in these days. So, podcasts and videos can help project stake holders to learn faster about the researches and improvements of our team.

## **6 Future Work**

### **6.1 ConSec**

For the ConSec it could be possible to extend it to also save data of each IP. So that it is possible to view a history over a specific IP in a graph or table.

There could also be more work done with the High/Middle/Low level of displaying the number of connections and also in the details of the IP there could be more “artificial intelligence” in the way that telling the user what type of risk that this IP have.

### **6.2 Dodowa redesign**

In the logout script, we have used a low DHCP lease time around 10 sec so that no one can use the IP address when an authenticated user got disconnected from the network. The future work can be to avoid the unauthentication based on the DHCP lease time and use of advanced script to detect the disconnection from the network at the user interface.

Another point could be to offer the flexibility to configure how many simultaneous connections with the same user name should be allowed.

At last, the design of a configuration CD that can install not only the services and configure them in Dodowa network, but also configure the switch at any moment it is run and without user interaction. In this project we have shown how to create the custom installation CD with preconfigured services, but it still needs to be able to configure the switch at any time and it would be better if this method could be

OpenCASE – Connects world to you



Linux distribution independent.

### **6.3 OSN Improvements**

Some of the High-End services are present in the OSIAN toolbox but we hadn't focused on these High-End services such as RT (Present only in the MAREN and MoRENet projects), VOIP, E-Learning Environment, Website Administration and Telemedicine due to the time constraints. Adapting them (and the Free Radius) to the Webmin GUI based approach would be a great enhancement to the OSN community.

The webmin and its modules also haven't been tested in Bifrost, since our testcase was the Dodowa network which didn't run Bifrost. This is a work that could be performed either by a next CSD team or the Bifrost community in conjunction with the Webmin community.

Some tests could be performed with users to analyze the current user friendliness of the Webmin based OSN approach and detect what could be improved and then those improvements could be applied on the Open Source modules in order to achieve an even more user-friendly environment.

The OSN blueprint was done in a diagram block format, but it could be extended to a UML based format where the components of the OSN could be clearly described.

One late good idea towards the OSN improvements was to move its documentation to a wiki format. This was not done in this case due to time constraints (even though it was done for the specific Dodowa Network documentation), but could be an interesting task for a next group, where the OSN could be presented with both the GUI based and the CLI based approaches in the same wiki.

### **6.4 Business**

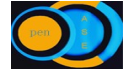
We as a team had only one business consultant and it was difficult to allocate lots of time for every thing related with the business aspects. For consequent CSD teams we suggest to focus on community creation. So far, we already started a



user forum but it needs to have more work done. Since creation of a discussion forum idea comes so late from Björn, we could only install and configure the forum, reached out our already established contacts and tried to encourage them to interact with each other. Because of the lack of time and resources we could only do these but we hope coming CSD teams will continue to work on community building.

Secondly, from the beginning of the course we tried to find some entrepreneurs or African students at KTH, who will return their country, to encourage them to start up a company based on open source networking idea. We have talked with Bruce Zamere, Tumwesige Mujwauzi and Kalkidan Alemayehu, they are all African students at KTH and took CSD course previously, but none of them were thinking, neither to start up a company now nor in 1 year time. So, one of the other future work can be finding an entrepreneur and helping her/him to start up her/his own company. In this process new students can act like business consultants for them.

Thirdly, updating our reports and documents with up to date information and reviewing them can be another future work. Since the data and statistics are always changing may be it will be good to update documents continuously.



## 7 Conclusions

The scope of the project was not so much defined at the beginning of the course. It included several deliverables and customers, with different ideas and requirements. We took some implementation decisions in order to narrow the scope down and to set achievable measurable objectives that would comply with the main requirements from all the stakeholders.

Our solution takes advantages of a lot work already performed by the Open Source community, as we integrate several Open Source softwares in a new context, the one of the OSN, and focusing on providing a graphical interface to the responsible for the OSN project. Furthermore, we have used this new GUI-driven approach in a real case network design by using to redesign the Dodowa network. And we can say that the experience of deploying the network was greatly enhanced by the usage of the graphical user interface.

The team has worked successfully and achieved all the goals and aspects of this project within the specified time period of this project. The two main primary goals have been reached, one was the improvements of the OSiAN toolbox and the other one was the redesigning of the Dodowa network providing the new authentication scheme. The secondary goals of the project were also completed successfully by giving Backstopping to the MAREN and MoRENet teams and providing an enhanced and excellent business analysis plan based on the Open Source Networking business.



## 8 References

- [1] Björn Pehrson, Professor, Principal, TS Lab Champion
- [2] Dan Kopparhed, Co-Coach
- [3] Dodowa documentation, Project team OpenCase, <http://serv.dakit.se/~osn/index.php5/Dodowa>, last visited 3 January 2009
- [4] TS Lab, <http://www.tslab.ssvl.kth.se/>, last visited 3 January 2009
- [5] Contrack-tools, <http://contrack-tools.netfilter.org/>
- [6] OSREN-MAREN, Project homepage, <http://www.tslab.ssvl.kth.se/csd/projects/0831011/>, last visited 3 January 2009
- [7] SSVL-OSN, Project homepage, <http://www.tslab.ssvl.kth.se/csd/projects/0821113/>, last visited 3 January 2009
- [8] OSN GUI-Driven Manual, OpenCase, <http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/OSN-GUI-drivenManual.pdf>, last visited 3 January 2009
- [9] RRDTool, <http://oss.oetiker.ch/rrdtool/>, last visited 3 January 2009
- [10] Offline Installation Mozambique, OpenCase, <http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Offline%20Installtion%20MozambiqueV2.pdf>, last visited 3 January 2009
- [11] OSREN-MoRENet, Project homepage, <http://www.tslab.ssvl.kth.se/csd/projects/0831072/>, last visited 3 January 2009
- [12] OpCon, Project homepage, <http://www.tslab.ssvl.kth.se/csd/projects/0831014/>, last visited 3 January 2009
- [13] Dodowa <http://dodowa.ssvl.kth.se/>, last visited 3 January 2009
- [14] OSiAN, Project homepage, [http://www.tslab.ssvl.kth.se/csd/projects/0811/?q=front\\_page](http://www.tslab.ssvl.kth.se/csd/projects/0811/?q=front_page), last visited 3 January 2009
- [15] Bifrost, <http://bifrost.slu.se/index.en.html>, last visited 3 January 2009
- [16] Netfiler, <http://www.netfilter.org/>, last visited 3 January 2009
- [17] Squid-Cache, <http://www.squid-cache.org/>, last visited 3 January 2009
- [18] Snort, <http://www.snort.org/>, last visited 3 January 2009
- [19] Free Radius, <http://freeradius.org/>, last visited 3 January 2009
- [20] Webmin, <http://webmin.com/>, last visited 3 January 2009
- [21] ConSec Webmin Module, [http://serv.dakit.se/~osn/index.php5/ConSec\\_Webmin](http://serv.dakit.se/~osn/index.php5/ConSec_Webmin), last visited 3 January 2009



- [22] Nagios, <http://www.nagios.org>, last visited 3 January 2009
- [23] MRTG, <http://oss.oetiker.ch/mrtg/>, last visited 3 January 2009
- [24] <http://www.tslab.ssvl.kth.se/csd/projects/0831014/> last visited 17 December 2008
- [25] afren, <http://www.afnog.org/mailman/listinfo/afren> last visited 16 December 2008
- [26] Malawi vs Mozambique, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Malawi\\_Vs\\_Mozambique.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Malawi_Vs_Mozambique.pdf) last visited 15 December 2008
- [27] TALC Open Source Networking, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/TALC\\_OpenSourceNetworking2.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/TALC_OpenSourceNetworking2.pdf) last visited 15 December 2008
- [28] Open Source and Gartners Hype Cycle, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Open\\_Source\\_and\\_Gartners\\_Hype\\_Cycle.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Open_Source_and_Gartners_Hype_Cycle.pdf) last visited 15 December 2008
- [29] OpenCASE Malawi, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/OpenCase\\_Malawi.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/OpenCase_Malawi.pdf) last visited 15 December 2008
- [30] OpenCASE Mozambique, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/OpenCase\\_Mozambique.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/OpenCase_Mozambique.pdf) last visited 15 December 2008
- [31] Execution Plan For Malawi, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Execution\\_Plan\\_For\\_Malawi.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Execution_Plan_For_Malawi.pdf) last visited 16 December 2008
- [32] Execution Plan For Mozambique, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Execution\\_Plan\\_For\\_Mozambique.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Execution_Plan_For_Mozambique.pdf) last visited 16 December 2008
- [33] Association of African Universities, <https://www.aau.org/index.htm> last accessed 15 December 2008
- [34] Rwanda Education and Research Network, [http://www.idrc.ca/fr/ev-83061-201\\_104745-1-IDRC\\_ADM\\_INFO.html](http://www.idrc.ca/fr/ev-83061-201_104745-1-IDRC_ADM_INFO.html) last visited 16 December 2008
- [35] Malawi Research and Education Network, <http://www.malico.mw/maren/> last visited 15 December 2008
- [36] Mozambique Research and Education Network, <http://morenet.mct.gov.mz/en/index.htm> last visited 15 December 2008
- [37] IT Malawi, <http://www.itmalawi.org/site/> last visited 15 December 2008
- [38] Tertiary Education Network, <http://www.tenet.ac.za/> last visited 15 December 2008
- [39] OSN Forum, <http://www.s8.createphpbb.com/osn/> last visited 15 December 2008
- [40] Generic Business Plan, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Generic\\_Business\\_Plan\\_V2.0.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/Generic_Business_Plan_V2.0.pdf) last visited 15 December 2008



- [41] Tools for entrepreneurs, OpenCASE, [http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/tools\\_for\\_entrepreneurs.pdf](http://www.tslab.ssvl.kth.se/csd/projects/0821116/sites/default/files/tools_for_entrepreneurs.pdf) last visited 16 December 2008
- [42] Podcast, <http://podcasts.odiogo.com/csd-fall-2008-osn-team/podcasts-html.php> last visited 16 December 2008
- [43] OpenCASE youtube channel, <http://www.youtube.com/user/kthopen> last accessed 17 December 2008