LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

NETWORK-ATTACHED STORAGE FOR SMALL COMPANIES

Case: Design Foundation Finland

LAHTI UNIVERSITY OF APPLIED SCIENCES
Degree Programme in
Business Information Technology
Bachelor Thesis
Autumn 2012
Jari-Pekka Koivisto

Lahti University of Applied Sciences
Degree Programme in Business Information Technology

KOIVISTO, JARI-PEKKA: Network-attached storage for small companies
Case: Design Foundation Finland

Thesis in Degree Programme in Business Information Technology, 56 pages, 11 pages of appendices

Autumn 2012

ABSTRACT

This study focuses on finding the proper solution to create Network-attached storage (NAS) for a small company. This study was commissioned by Design Foundation Finland, aiming to improve the security and the management of the information. This research will be aiming to find the proper way to design and implement a network storage, which will be used as the main data storage within the company for creating an ideal solution for data maintenance, security and ease of access to all the data of the foundation. The outcome of the thesis is a solution, which is created from scratch, offering a design and implementation of an NAS in a small company with a relatively small budget.

The case foundation is located in Lahti. The foundation was established in 2009, aimed to improve and support the education (of design), as well as research and development of design. Design Foundation Finland also has an own R&D group to improve the design of Finnish products in several industrial fields.

The method used in this study is qualitative, based on the author's own observation within the subject, interviews among the employees of the Design Foundation Finland and it is done by utilizing Design Science research methodology to develop an artifact.

The study result offers a solution to implement and utilize an NAS device in a small company without huge investments on equipment. The study result can be applied to create an NAS for a small company or it can be used as a basis to create an NAS for relatively big companies.

Keywords: NAS, Backup, Security, VPN, File-Server

Lahden Ammattikorkeakoulu
Degree Programme in Business Information Technology

KOIVISTO, JARI-PEKKA:

Network-attached storage for small companies
Case: Design Foundation Finland

Degree Programme in Business Information Technology opinnäytetyö, 56 sivua, 11 liitesivua

Syksy 2012

TIIVISTELMÄ

Tämä tutkimus käsittelee NAS-laitteen käyttöönottoa pienyrityksessä. Tutkimuksen hankkeisti Suomen Muotoilusäätiö, tarkoituksena kehittää säätiön sisäistä tietoturvaa, sekä informaation hallintaa. Tämä tutkimus pyrkii löytämään optimaalisen tavan implementoida ja käyttää NAS-laitetta säätiössä, tai pienyrityksessä. NAS:ia tullaan käyttämään pääasiallisena tiedostojen tallennuspaikkana, tarkoituksena parantaa säätiön informaationhallintaa, tietoturvaa, sekä helpottaa säätiön työntekijöiden pääsyä säätiön sisäiseen informaatioon. Tutkimuksen lopputuloksena on NAS-laitteen käyttöönotto, sekä sen maksimaalinen hyödyntäminen kohdesäätiössä suhteellisen pienellä budjetilla.

Kohdesäätiö sijaitsee Lahdessa. Säätiö on perustettu 2009; tarkoituksena edistää ja tukea muotoilun tieteellistä tutkimusta, koulutusta, sekä kehittämistyötä. Suomen Muotoilusäätiöllä on myös oma ryhmä, jonka tarkoituksena on edistää Suomalaista teollisuusmuotoilua lukuisilla teollisuuden alahaaroilla.

Opinnäytetyö on laadullinen tapaustutkimus, joka perustuu kirjoittajan omiin havaintoihin kohdesäätiössä, toimeksiantajayrityksen henkilöstön haastatteluihin ja se pohjautuu Design Science – tyyppiseen metodologiaan, jossa lopputuloksena on artefakti.

Tutkimuksen lopputulos on ratkaisu NAS-laitteen käyttöönotolle, sekä sen hyödyntämiselle pienyrityksessä ilman suuria investointeja laitteistoon. Tutkimustulosta voidaan hyödyntää sellaisenaan NAS-laitteen käyttöönotolle pienyrityksessä, taikka sitä voidaan käyttää alustavana pohjana NAS-laitteen hyödyntämiselle suuryrityksessä.

Asiasanat: NAS, Varmuuskopiointi, Tietoturva, VPN, Tiedostopalvelin

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

IT	Information Technology
NAS	Network-Attached Storage
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
VPN	Virtual Private Network
LAN	Local Area Network
CPU	Central Processing Unit
PC	Personal Computer
RAID	Redundant Array of Independent Disks
SSD	Solid-state Drive
PSU	Power supply
MoSCoW	Prioritization technique
IDPS	Intrusion Detection and Prevention Systems
DMZ	Demilitarized Zone
SAMBA	File & Printer Server software
Artifact	Built and configured server for Design Foundation Finland
EU	European Union

1 INTRODUCTION

1.1 Background

IT is an essential part of today's business. IT-technology is, among others, in key role for storing business knowledge into a stored format for later use. While IT gives clear advantages over previously used methods for storing knowledge, it also generates various new threats which are discussed in this research. However, these threats can be identified and minimized with the proper combination of hardware and software. This study focuses on utilizing various hardware and software to overcome the previously mentioned threats and it is based on design science.

NAS (Network-attached storage) is a data storage, which is connected to a computer network. NAS acts as a file-server in a network, offering data storage to be located in a stand-alone unit, which client computers can be connected. NAS can be seen as a network drive (via Ethernet) and as such, it can be used to save documents and files as well as read them. Fundamentally, a NAS is a computer, optimized in hardware and software, to be a file server. (Choubey, 2012, p. 134.)

The benefits from using NAS are clear; firstly it will improve the security of the data since it will be located in one place only, rather than divided into several PC's of the company's personnel. That greatly decreases the chances of information leaks due to thefts, mistakes and accidents. Secondly, it will improve the maintenance of the data, allowing the local administrator to locate the data from one place and because of that, it can be managed easier than if the data would be located in several different places. Thirdly, it allows backing up the data frequently with an efficient way, so that the valuable data will not be destroyed in an accident or a single system failure. Fourthly, it improves the accessibility greatly by allowing users to connect to the device via web from practically anywhere. That allows employees to gain access to their documents from home and practically anywhere which has an internet connection. (Iomega, 2010.)

In this case study, NAS will be designed, configured and finally implemented into existing local network of Design Foundation Finland to act as a file-server for the employees of the foundation. The research tries to solve and find out the proper way to implement it, as well as how to utilize it correctly. However, a significant focus will be on finding the most affordable solution without losing on features and fault-tolerance. The budget in this case research is limited to 500 euros. The aim is to support ten simultaneous users. The impact from a significant increase of users will not be studied in this research.

The outcome of this research will be a proper implementation of a NAS in Design Foundation Finland and as such it can be applied to any existing local network in a small-sized company.

1.2 Statement of the Problem

Design Foundation Finland and the employees manage their own data by storing it into their own hard drives. This generates a threat of a data loss in multiple ways: user may accidentally remove his/her own data and while there are no constant backups made, the data may not be recoverable. Another threat is that any of the used laptops may get stolen with the data, which may even generate a risk of mis-use of the information which is located in the hard drive. One more threat is the hard drive failure which may lead to a complete data loss of that specific hard drive content.

1.3 Research Objective and Methodology

The aim of this research is to create a data storage system for the case company which utilizes and fulfills the following requirements:

- Data backups
- External access over Internet
- Access from LAN
- Optimized data security

- Maintainability
- Future expansions
- System health monitoring

This research allows Design Foundation Finland to increase their data security in multiple ways as well as increases their mobility as their centralized data storage can be accessed over Internet. This research can also be used as a guide in the implementation stage of a NAS-system in most scenarios. The research is applicable to be utilized in either home use, or in small offices.

1.4 Overview of Thesis

This thesis is constructed to contain seven main chapters: the first chapters are for the introduction to the subject, followed by the chapters which will lead the reader to find and understand the decisions made in this research. The whole structure is visualized in Figure 1.

Chapter one is the introduction part of this research, containing the background information of the system to be created as well as the reasons why this research is conducted.

Chapter two contains the research approaches for this study. It begins by defining the research approaches utilized in this study. Next the chapter introduces the research framework which includes the necessary concepts for the study. Chapter ends by describing the process of the research methods which includes approaches for research, data collection and the data analysis.

Chapter three contains Literature Review for the study. This includes the background theories and practices to implement external data storage in local area network.

Chapter four presents the implementation process of the NAS for the Case Company: Design Foundation Finland. Firstly, this chapter introduces the Case Com-

pany, their area of expertise and the current IT-infrastructure. Secondly, the background knowledge of the current and the future need is collected by observation during the internship in 2011-2012. Thirdly, by utilizing the theories and the practices of chapter three, the decisions of the needed hardware and the software are done and described. Fourthly, the implementation stage is covered step by step, generating a guide for System Administrators.

Chapter five contains the practical data to be analyzed. The description of the analysis process by using coding analysis method is also part of this chapter.

Chapter six includes and concludes the findings and the results of this research. It also summarizes the overall process of this thesis.

Chapter seven concludes this research by giving it its boundaries, describing the limitations and the validity and finally giving some suggestions for future study of this subject.

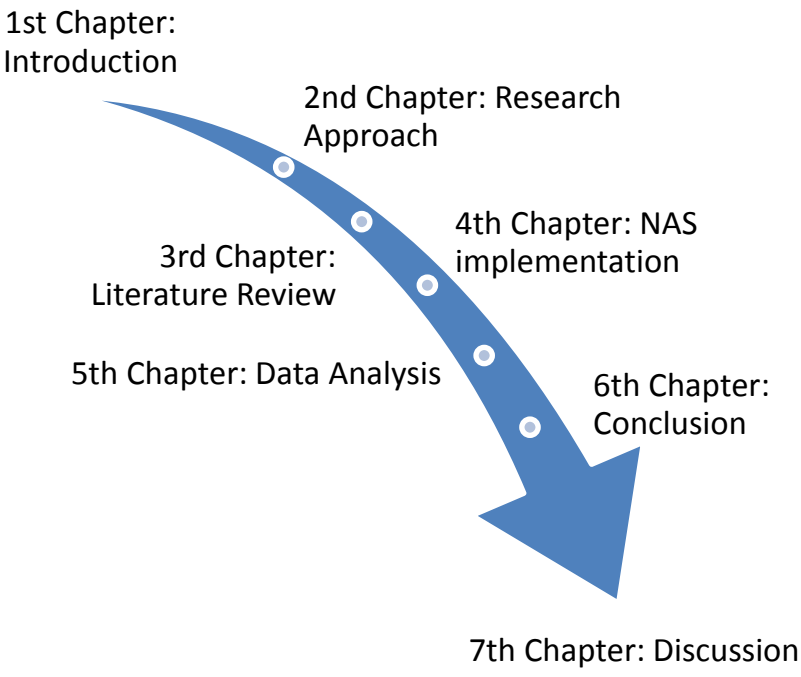


FIGURE 1: Thesis structure

2 RESEARCH APPROACH

2.1 Research Problem

The objective for this study is to research the usage of NAS for small-sized companies and also cover the implementation stage step by step. The final objective is to create a general guide of how to utilize NAS properly in a company environment. This thesis is created to support Design Foundation Finland's IT-environment and is created to lower the risk for a data loss. The following research questions were identified to support this research and the objectives:

1. How to implement a NAS-server in a small-sized company?
2. How to avoid any kind of data loss?
3. What are the system requirements?

2.2 Research Framework

The research framework of this study applies the following concepts which are discovered in the literature review and they are the main topics which are analyzed, discussed and finally transformed and utilized in the case research in Design Foundation Finland.

- Data Security
- Data Accessibility (Mobility)
- Maintainability
- Data Storage

Based on the above concepts a new concept is being created: Data storage which is highly secure, highly accessible and is highly maintainable: The Artifact (see Figure 2).

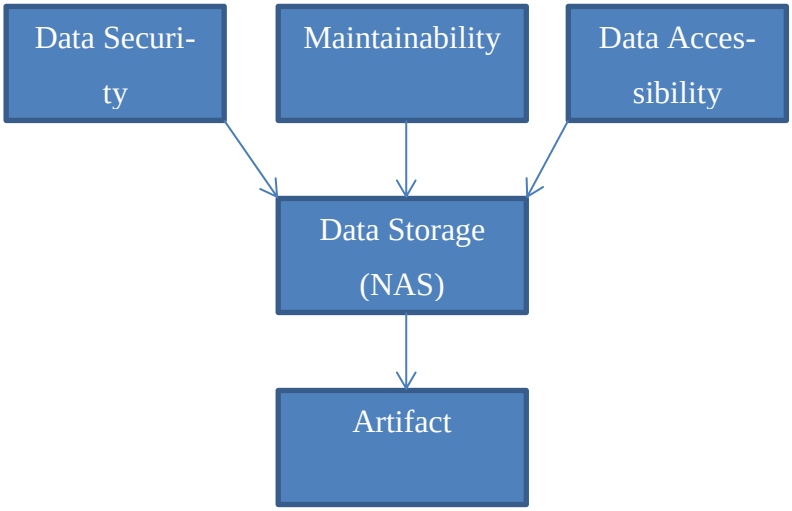


FIGURE 2: Research Framework

The final concept (Artifact) is the result of this study, a NAS which is based on a HP ProLiant DL380 G5 server with two 72 gigabyte and two 146 gigabyte SAS-drives (see Figure 3).

FIGURE 3: HP ProLiant DL380 G5

2.3 Research Method

Deductive research works from general to the more specific and it's also called a "top-down" approach. Inductive research works in the opposite way: having specific observations or facts and generating a general theory based on those observations or/and facts. (Trochim, 2006.)

This study is based on deductive research; the research is done from already defined theories and concepts of network-attached storages and devices. This study seeks to find a proper devices and ways to implement such device in a small-sized company environment.

This research is based on qualitative research method as the solution is for the Design Foundation Finland and the findings are mostly done by observation and also in-depth analysis from the interviews.

2.3.1 Data Collection

The data for this research was gathered during the internship in the case company in 2011-2012. Most of the data is based on the observations and also from the interviews of the employees of Design Foundation Finland.

TABLE 1: Research methodology

RESEARCH METHOD	RESEARCH APPROACH	DATA COLLECTION METHOD
Qualitative	Deductive	Observation and Interviews

2.3.2 Data analysis

The data was analyzed by utilizing the coding analysis methods. In qualitative data analysis coding analyzing has a key role and it's the reason why the decision was made to use it.

Coding is categorizing the text into a more meaningful format without losing the relations between each part (Miles, 1994, p. 56). It's vital to find the key facts and notes from the data to fully understand the phenomenon behind the research.

The interviews in this study were audio-recorded. After the interview, the audio-data was turned into a written text by the author. This text was then analyzed and the contents which were significant were highlighted from the text. These significant findings were categorized and listed to make a map of all the relevant usage scenarios and features what would be needed to be included in the NAS-system. This analysis is needed to fully discover the ways how to utilize the NAS in Design Foundation Finland.

3 LITERATURE REVIEW

This chapter contains the theories and the background to justify the usage of NAS-based solutions in business. When implemented properly, it lowers the risk for a data loss as well as greatly improves the mobility of the work thus allowing employees to work abroad. This chapter contains the basic knowledge of the NAS-based solutions as well as different ways to implement them.

3.1 The Basics of Data Storages

Data storage in information technology is a technology which allows of retaining information. There are different data storage types in the industry, but the concept is very similar. For example, practically almost every computer has at least one hard drive, where all the information is stored. Such information can be for example the operating system or the files created by user. This information can be stored and accessed later on. Hard drives are called to be secondary storages as they're not directly accessed by the CPU of the computer. In computer the primary storage handles the information directly from the CPU, but this study doesn't cover this type of storage. NAS is also one type of a secondary storage. (Choubey, 2012, pp. 133-134.)

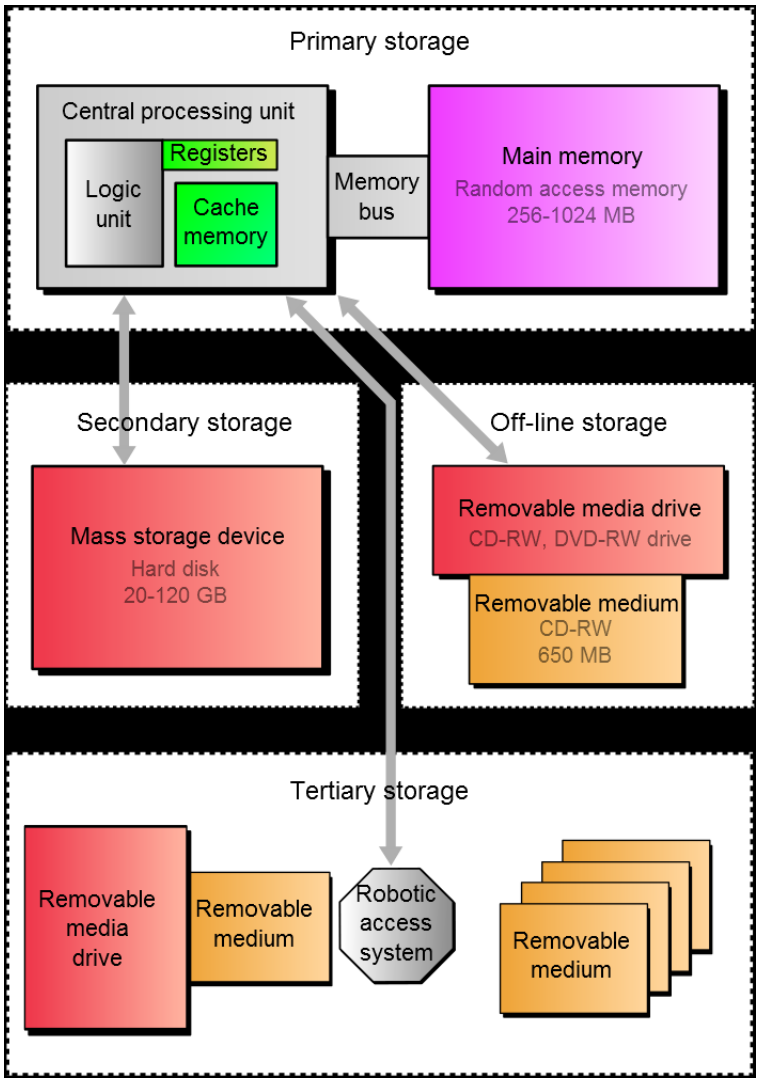


FIGURE 4: Various forms of storage types (Choubey, 2012)

Above figure represents the different types of storages in the computer world. NAS is considered to be in the "Secondary storage" which also includes all types of hard disks.

3.2 Secondary Data Storage Possibilities

There are various types of secondary data storages available today. Most common is the magnetic disk, which can found practically from every PC and server. This type of a disk uses magnetic coating which allows the data to be "written" as magnetic particles. The problem with this type of storage is that it is a mechanical

device and it may stay healthy for a long period of time but there's no guarantee of that to happen. There is, however, a way to avoid data loss from a magnetic disk failure and it's called RAID. There are several different RAID types available and the most commons in home use are RAID 0 and RAID 1. (Stair & Reynolds, 2012, pp. 99-100.)

One of the Secondary Data Storage types is the Solid State Device. It's not an optical drive, like CD-ROM drive, nor it's not a magnetic drive either, but it's a drive which utilizes memory chips. As the drive is not mechanical and it doesn't have any moving parts, it can be considered to be less fragile than typical hard drives are. SSD's are coming to home use and in server environments as well, but since the technology is still new, it's not as trusted as magnetic drives in environments where there is no room for errors. The gain from SSD is clear; it's very fast and it consumes only a fracture of power compared to a magnetic drive. (Stair & Reynolds, 2012, p. 101.)

Network-attached storage (NAS) is also hard disk storage but it's rather an external server, with its own hardware and network connectivity. Usually NAS is configured to act only as a file server which contains tools to manage the network shares, users and user rights. (Stair & Reynolds, 2012, p. 101.)

3.3 RAID for Secondary Data Storage

RAID 0, or striping, utilizes two physical hard drives. Every other block is written to the hard drive which, in theory, could double the performance of a single hard drive. However, this type of RAID increases the risk of a data loss, since all the data is practically lost if one hard drive fails. This is also a reason why this is not so widely used in homes and especially in production use in companies. (Thompson & Thompson, 2011, p. 143.)

RAID 1, or mirroring, utilizes two physical hard drives. Everything is written to both hard drives, which decreases significantly the risks of data loss. However, the capacity is only half of the actual capacity, which makes this type of RAID to be

quite expensive. RAID 1 is a commonly used in home environment. (Thompson & Thompson, 2011, p. 142.)

RAID 5 utilizes three or more physical hard drives. Practically it lowers the risk of data loss, since in three disks RAID it is possible to have a single hard disk failure without losing any data. For example, in RAID 5 with six disks, the capacity is the sum from five disks and one of the disks contains the necessary data to rebuild the data after a single hard disk failure. This setup is quite common in server environment. (Thompson & Thompson, 2011, p. 142.)

RAID 10 is a stacked RAID which can be said to be RAID 0+1, RAID 1+0 or RAID 10. It uses four hard drives which are arranged so that there are two separate RAID 1 setups, which are emerged into one RAID 0 setup, so basically it utilizes two different RAID layers. This setup is fairly common in server environment. (Thompson & Thompson, 2011, p. 143.)

3.4 Operating Systems

> *"So work the honey-bees, creatures that by a rule in nature teach the act of order to a peopled kingdom." (Shakespeare)*

Even though there are various different OS's available, they all act more or less similarly as they utilize and manage the hardware (memory, devices etc.) and form an UI which can be designed to, for example, more powerful or simple (Course Technology, Cengage Technology, 2011, pp. 3-11). Different OS's are designed for different purposes and this research is interested especially in server OS's as the NAS is a server platform.

The options are either Microsoft Windows or Linux, which both offers practically same abilities when implementing a NAS. In literature the findings are mostly based on the author's own views but they do support the fact that Linux should be considered a very stable OS in this kind of use. For example the author of "Linux

in a Windows World" (Smith, 2005) states that Linux has its strength especially in server use and its strengths outweigh its weaknesses.

3.5 The Importance of Data Security

There are several aspects to be considered when improving and creating a highly secure IT-infrastructure for a company. No matter how sophisticated the equipment is being used, the final impact comes from how they're applied and used. This chapter discusses about these aspects and most of them are applied to the final solution, the artefact of this thesis for Design Foundation Finland. As the NAS has to be connected to the Internet and it has to be accessible from outside also, the following aspects has to be thought and changed if necessary. An unsecure network and an unsecure NAS-server can lead for a total disaster, which is essential to understand when applying this type of service in a corporation.

3.5.1 Security Technology: Firewall and VPN

A sophisticated network in a company applies different procedures to protect their LAN from unauthorized usage. Both firewall and VPN are designed to prevent this type of use.

A firewall is a piece of hardware, or a subnet, which either blocks or allows connections from inside of LAN to Internet or vice versa (Whitman & Mattord, 2012, p. 207). Surely they can offer different services but a rule-based firewall is the most common one. They're used to protect the inner subnet from attacks by blocking the connection so that the specified computers cannot be used for something which they're not designed. For example, a firewall can be configured to allow connections to the company's server but at the same to block connection attempts to PCs.

Router is a device which is designed to connect two or more networks together so that the networks can see each other (Whitman & Mattord, 2012, p. 207). The

main idea of a router is to allow a LAN to be connected to Internet, or into a another LAN.

DMZ (see Figure 5) is an demilitarized zone which is located between the outside and the inside networks which is practically used and designed for servers, which doesn't have to be seen inside the LAN but should be seen in the Internet (Whitman & Mattord, 2012, p. 207).

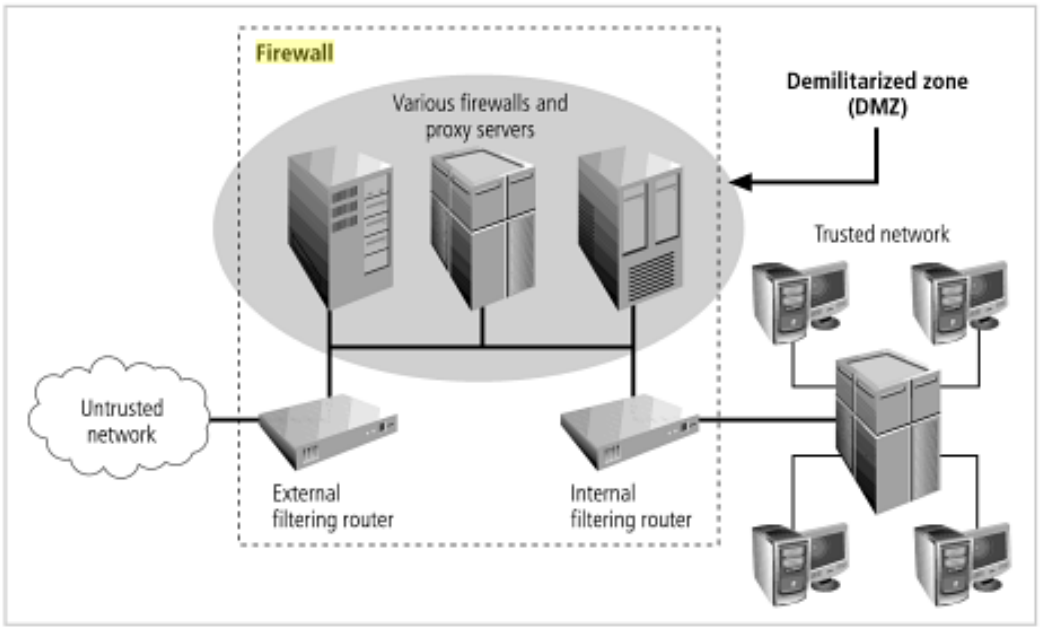


FIGURE 5: Firewall subnet example with DMZ (Whitman & Mattord, 2012)

The above figure shows an example from a local network, which has a sophisticated firewall subnet and two separate routers and a DMZ for the servers.

VPN is a non-direct network connection between multiple communication entities, which is virtualized with VPN software over the Internet (Fellner & Graf, 2009, pp. 4-6). The idea behind VPN is to offer secure communications between two physically different places and extend the LAN into more than one place. This can be, for example, utilized to create a LAN between two offices, which belongs to one company (see Figure 6).

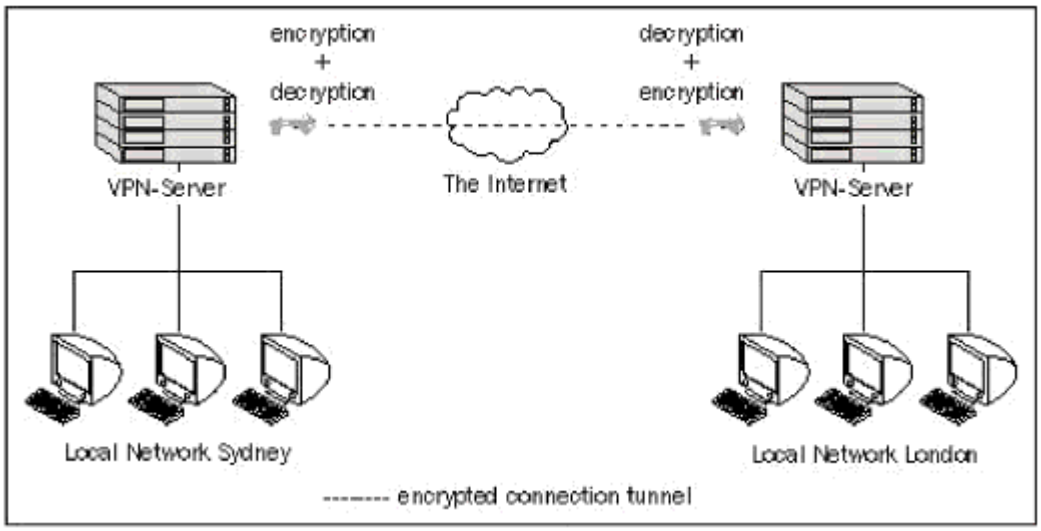


FIGURE 6: VPN between offices in Sydney and London (Fellner & Graf, 2009)

The above figure shows an example of a VPN which connects two LANs together with encrypted tunnel over the Internet.

3.5.2 Security Technology: Intrusion Detection and Access Control

Intrusion Detection and Prevention Systems (so called IDPSs) are designed to detect any unauthorized use either in the inner network or in a single computer. There are two types of IDPS –systems. First is the host-based IDPS, which is a single host version. It monitors the status of the files located in the hard drive(s). Second is the network-based IDPS which monitors the network usage and tries to find any suspicious network traffic. (Whitman & Mattord, 2012, p. 208.) The artifact for Design Foundation Finland will utilize a host-based IDPS since it can be created by utilizing open source software. The reasons why author decided to utilize open source software (software based IDPS) over the network-based IDPS are as follows:

- Open source (free)
- Easy to configure
- Scope on preventing unauthorized access to NAS only
- Network-based IDPS hardware goes over the budget
- No need for extra hardware installations

As the above list shows, there are several reasons why software-based IDPS is capable of delivering the needed security and is, in this case, the better choice.

3.5.3 Cryptography

Cryptography is an essential aspect when creating a NAS which should be accessible from the Internet. If the communication would happen without any type of encryption, the data could be compromised and it could lead into a severe damage for the company. For example a VPN-connection can be encrypted to allow fairly secure connections to the corporation LAN. (Kahate, 2003, pp. 2-42.)

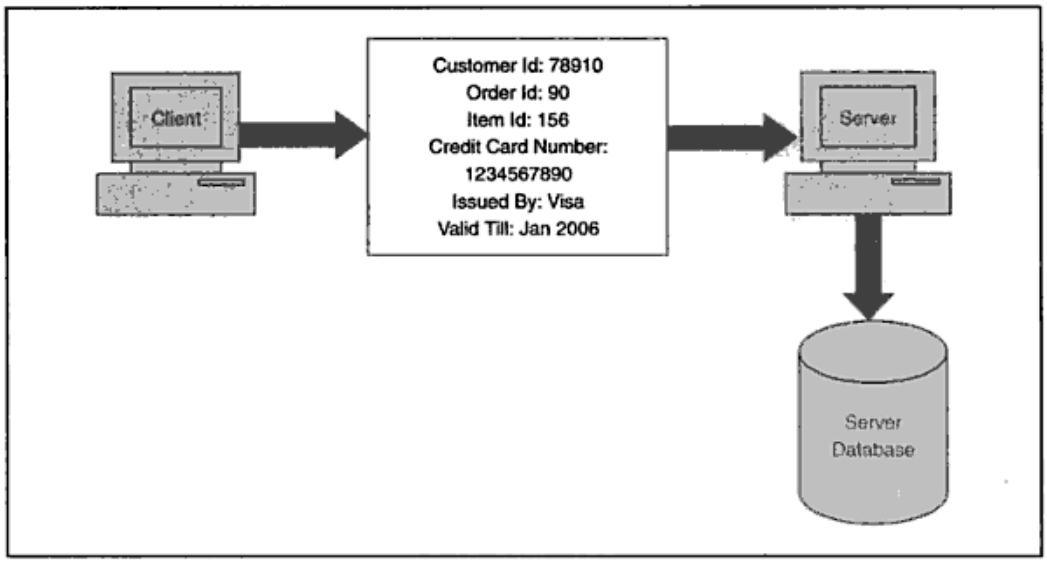


FIGURE 7: Plain (non-encrypted) communication between two hosts (Kahate, 2003)

The above figure shows an example of a plain communication between two separate hosts. The data is relatively easy to capture which makes the connection to be unsecure.

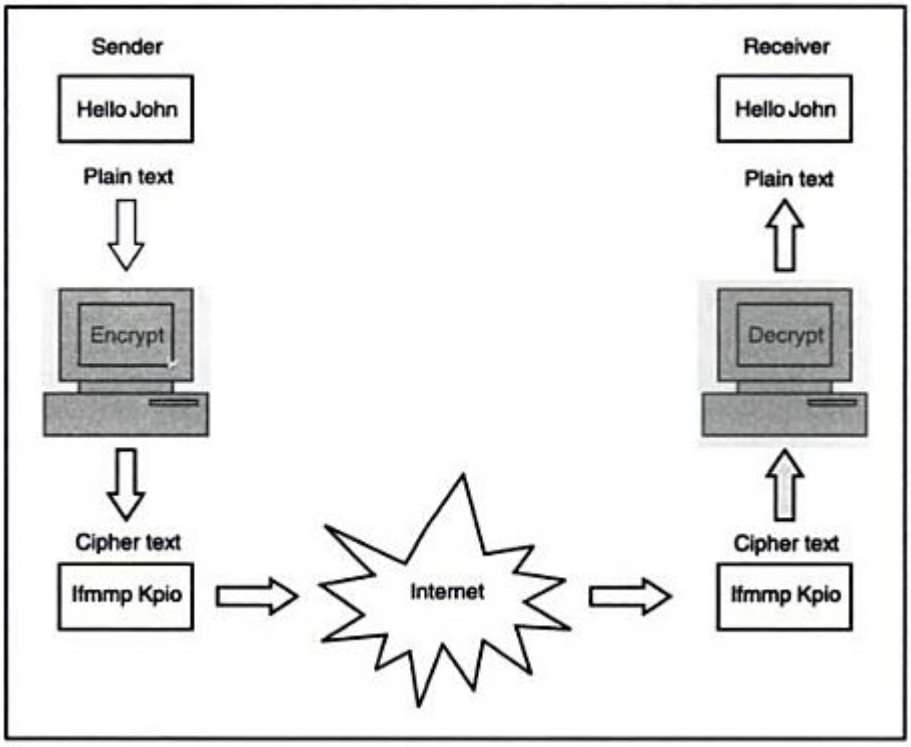


FIGURE 8: Encrypted communication between two hosts (Kahate, 2003)

The figure above shows an example of a communication between two hosts which is first encrypted by the sender host and then encrypted by the receiver host.

3.5.4 Physical Security

Physical security is indeed very important security type since by the lack of physical security there are possibilities for damages or data loss. The whole security of the information is as weak as the weakest link in the whole security. (Erbschloe, 2005, pp. 2-15.)

From a damage occurred by a weak physical security can be very costly (see Figure 9).

Variable	Description	Quantity
A	Number of employees who do work that requires access to computers & communications equipment	100
B	Average cost of employee hour including salaries, benefits, facilities, and overhead	$50.00
C	Potential lost productivity for one day of system outages (A * B * 8)	$40,000
D	Cost to restore or replace damaged equipment	???
	Total cost of outage	C + D

FIGURE 9: An example of a financial damage from a weak physical security (Erbschloe, 2005)

The above figure shows an example where the company's IT-infrastructure is in blackout for one day. This might occur when an important service or hardware is taken down by a physical damage.

3.6 The Importance of Data Backup

Backing up the data is important since whenever we're dealing with essential data, we have to have a disaster recovery plan and backups are a very important side of it. There are different ways how this can be done. A full copy of a system, which holds the data, might be the best choice but it's also the solution which costs most. It depends how tolerant system should it be on how big impact it would generate if a specific data would not be accessible for a period of time. In some cases it is relatively meaningless if a specific data would not be accessible for couple of days. Yet, there are cases and systems where the data should be accessible no matter what happens. These aspects should be thought when building a backup plan and a system which utilizes backups. (Doyle, 2000, pp. 129-132.)

In this research, the case company should use the NAS-server for storing all the documents which are made. Therefore, constant backups should be made and they should be relatively easy and fast to recover to an existing system or a new one. RAID technologies are utilized and can be thought to utilize constant backup. This

alone isn’t enough to offer a needed security, since all the data is still located physically in the same place. Therefore, a service outside of the premises of Design Foundation Finland should be utilized for backups. What is a very important to notice is that these backups are never to be considered as a working solution if the backups are never tested to recover the data.

4 NAS IMPLEMENTATION

4.1 Introduction to Case Company: Design Foundation Finland

Design Foundation Finland is established in 2009. Their mission is to promote and support the development of scientific research and education in the field of design. The Foundation grants scholarships and stipends, runs a design center, and carries out research and development operations.

The Foundation co-operates with universities, universities of applied sciences, various other partners in the field of design and with business partners at both national and international level.

The Foundation receives funding from various private and public sources. The Foundation is governed by a board of trustees.

4.2 Existing IT-Infrastructure

Before my internship in 2011, the Design Foundation Finland moved into their new premises in Lahti. They hired a local networking company (LAN& WAN) to build a LAN to their new premises and it was done by utilizing 10/100 switched Ethernet network with one HP ProCurve switch which has 48 ports to be used (see Figure 10). One of the ports (UPLINK) is connected into a router (see Figure 11), which connects the LAN to the Internet. The uplink speed was decided to be 10/10 (downstream/upstream). This network can be considered to be stable and modern enough to be used with external data storage such as NAS. The whole network infrastructure in Design Foundation Finland can be seen from Appendix 4.

FIGURE 10: HP ProCurve 2610 48-port 10/100 switch

The above figure shows the main switch which is used to connect all the computers and devices into a LAN.

FIGURE 11: NETGEAR router with NAT

The above figure shows the router which is used to connect the LAN into the Internet. The router in Design Foundation Finland premises acts also creates a NAT between the Internet and the LAN to allow all of the clients to be connected to the Internet simultaneously.

4.3 The Implementation of NAS

4.3.1 NAS to act as an Secondary Data Storage

While there are specific NAS devices in the market which utilize RAID technologies, the author decided to utilize a hardware, which is considered to be one of the industry's most stable server platforms, HP ProLiant. This is done to gain the extra fault-tolerance, which is one of the important aspects when building a data storage system. Most NAS-devices in the market aren't able to operate when severe faults occur. One of the most common cases is the PSU fault and since HP ProLiant supports power supply redundancy, it is far more suitable in this type of use. HP ProLiant is a server, which can run different types of OS's. There were two considerable options for the OS:

- Microsoft Windows Server 2008 R2
- Debian GNU /Linux

The decision was easy. Author decided to utilize Debian GNU/Linux in this setup since it is open source, thus free. Why to utilize Linux over Windows? The list is not short but here are the main reasons:

- Free
- Only choice to stay within the budget
- More secure
- More configurable
- Free software

Linux is based on open source. Open source software's main idea is that its source code is free and in this context it means that it is open, public and non-proprietary (Weber, 2004, p. 5). As the foundation needs to operate within a specific budget, there's not much room for extra costs. Therefore it was vital to find a solution which doesn't only meet the requirements, but meets them in inexpensive way. It is also vital to understand that in some use scenarios the better choice, as an OS, would be Microsoft Windows Server. However, in this implementation there were no specific requirements which would have required Windows.

4.3.2 HP ProLiant DL380 G5 as a platform for NAS

The platform for a NAS was decided to be from HP's industry leading server-series, DL380 G5. There are out-of-the-box ready NAS devices (see Figure 12) available and most of them are designed to be located in home environments. However, there are also NAS devices which are rack-mountable (see Figure 13) and which are capable of serving huge amount of data effectively. However, these devices were not an option in this implementation, since they are very expensive compared to the author's decision and solution.

FIGURE 12: D-Link DNS-323 NAS

The above figure shows an example of a NAS which is designed to be located in homes or in small office. It offers RAID capabilities but it doesn't offer the needed performance or the ability to duplicate its power supply which are both required in this implementation.

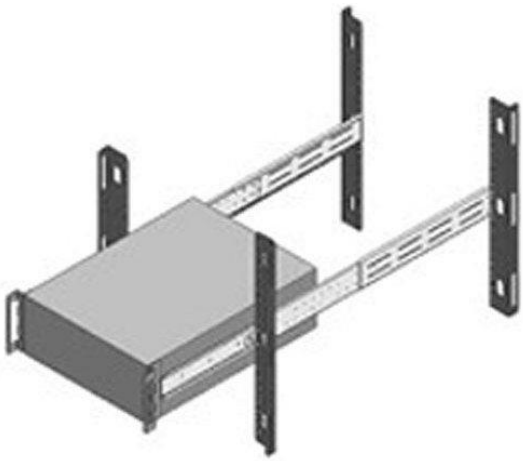


FIGURE 13: Rack-mountable hardware

The above figure shows a rack-mountable hardware which allows devices to be easily installed and maintained. HP ProLiant DL380 G5 has this capability.

4.3.3 Samba file-sharing

There is a wide range of free open source software available to build a NAS-server with Linux OS. For the file sharing, Linux offers Samba which enables the file sharing for Unix-based systems and which communicates with also Windows-based systems (see Figure 14). (Carter, Ts, & Eckstein, 2007, pp. 1-8.)

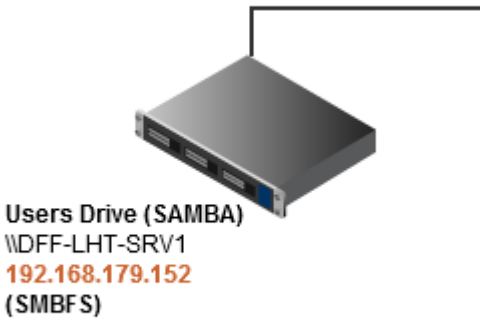


FIGURE 14: Linux (NAS) server with Samba in LAN

Above figure shows a Linux-based computer named DFF-LHT-SRV1 which is the NAS for Design Foundation Finland.

4.3.4 OpenVPN as a VPN-service

VPN is essential in this implementation since it allows secure connection to the case company's premises. With this software the local services, like file-sharing, are not needed to be available to the Internet. This greatly improves the data security.

OpenVPN is open source software which can be utilized to create a VPN between the clients and the server (Keijser, 2011, pp. 1-3). The OpenVPN server is relatively easy to configure and the client software is very simple to use. OpenVPN

uses keys which are installed into the client-side and to the server-side. This key is needed to be the same in both sides; otherwise the server will not establish the connection. A password can be used as an option, or alone without the keys. However, to maximize the security, the implementation solution uses both.

5 DATA ANALYSIS

This research is conducted to find the most suitable way to implement a NAS-server which will utilize VPN-services and which will be reachable from the Internet. The data analysis utilizes coding analysis method to seek the important aspects of the system, for example how the system should work and how it should be used. The discussions, observations and interviews are coded with the following MoSCoW-prioritization (see table 2).

The following table shows the use cases of the NAS-system as well as important aspects of the system features. These aspects are categorized and prioritized by utilizing the MoSCoW –prioritization technique. The reason why MoSCoW-prioritization is used is to find the essential features as well as prioritize them. This is done to utilize the timeframe effectively and to make sure that the most essential features will be delivered with this case study. The prioritization points are generated from the literature review and they represent the functional impact on the system. The coded data is generated from the discussions, interviews and the literature review. The priorities are as follows:

- 1 = Want to have
- 2 = Could have
- 3 = Should have
- 4 = Must have

TABLE 2: Coded data for NAS

Category	**Coded data**	**Priority**
Use cases	Reachable from home	4
	Reachable from LAN	4

	Reachable abroad	3
	Can be used from “My Computer” as a network drive	4
	Able to grant access for specific external clients	2
	Able to access NAS from public computers	3
Features	Constant backups from NAS to external device / location	4
	Able to have an own space in NAS	4
	Able to add users via web browser	2
	Able to remove users via web browser	2
	Able to share files in a common network drive	4

The use cases and features are given grades from one to four. The prioritization is applied with the MoSCoW –technique which is especially designed to reach common understanding between the stakeholders (Cadle, Paul, & Turner, 2010, pp. 176-179). This will generate a mutual understanding between the author and the case company’s representatives.

MoSCoW prioritization is generally used in software developing but it can be used in different projects where a prioritization is important. As the budget and the timeframe are limited in this research, some prioritization is needed to get the most business value out of from the project. MoSCoW –prioritization is generated from different priorities and they’re as follows:

- M = Must have
- S = Should have
- C = Could have
- W = Want to have

According to the coded data, there are several demands which are graded as priority 4. These aspects are taken care of when designing the NAS-system for Design Foundation Finland as "Must have".

Priority 3 features and use cases are considered to be "Should have". These aspects of the system are considered to be quite essential and should be implemented to the final product if there are no good reasons why they should be left out.

Priority 2 features and use cases are considered as "Could have" meaning they're not important aspects and can easily be left out from the final product. These aspects can be implemented if the budget and the time-frame allows.

Priority 1 features and use cases are considered as "Want to have" and they are aspects that are not important at all and only if budget and time-frame allows, they can be implemented.

5.1 Use cases –analysis

The main aspect in use cases –analysis is that a functional NAS has to allow external connections to users. It is very essential for today's business that the company's data storage is reachable around the globe due to globalization. In this specific case, the employees of Design Foundation Finland are also doing distance work and they will benefit from a system which will grant the access to all the needed files, no matter where they are.

It is also mentioned in the discussions chapter that while observing there were clients who liked to have an access to specific documents. This has been done by utilizing a 3rd party system called Dropbox. These 3rd party systems usually deliv-

er the functionality but they also involve risks as they are administrated by their own rules. There's no guarantee of the data security either. These are the main reasons, why an own system is a better choice than relying on external services.

As the usability is always a concern, this system should allow the users to see data storage folders (and drives) as their network drives. There should be at least one network drive which is user-specific, meaning that only the user has the rights to read and write to the folder and one network drive which is for all the employees of Design Foundation Finland. There is also an option to make group-specific folders but as the size of the company is relatively small, there is no need for group rights.

5.2 Features –analysis

As the coded data in features show, the greatest priority is given to user-specific network drives. This is relatively easy to configure with appropriate software. The common folder is also one of the key features and is as easy to configure as user-specific network drives.

Backups from the NAS to external location is an essential part of the fault-tolerance as it will give the needed security for any type of data loss in the primary device (NAS). This feature will be implemented in the near future, but due to the budget, it was withdrawn from this artifact. The optional way to overcome this problem will be constant backups to external storage drive, which will be stored in an external location after the backup operations.

One of the hoped-for features was a web-based user management, which would be rather easy to implement but very hard to manage. This type of management might lead to accidental user removals which might lead to severe data loss. The author declined to implement this type of web-based service as it might cause more trouble than what is the gain.

6 CONCLUSION

Information Technology is an essential part of day-to-day business. Even a small company generates a lot of valuable data which is then stored locally to PC's or into centralized storages. Centralized storage is a far more advanced solution and when implemented and maintained properly, it offers the needed safety for the valuable data.

NAS offers centralized storage which is easy to maintain, it's a very valuable option and it doesn't need huge investments to be established. As discussed in this research, there is however possibly more than one suitable solution. In this research, the artifact is based on an industry leading server technology which allows more services than just file sharing.

NAS can be built on a server or it can be built on a ready-made NAS which is designed for only file sharing. However, it's highly important to notice that with the same budget and by utilizing industry leading server technology, the fault tolerance is highly increased. The author of this thesis recommends investigating the fault tolerance of the equipment, especially when the target is to create business-critical IT-services.

The implementation of an NAS for Design Foundation Finland can be considered a successful project and it shows that an NAS can be implemented and taken in use in a short timeframe (less than two months). However it also depends on the IT-infrastructure, which gives it some restrictions as it relies greatly on how the network is created and what hardware it utilizes. The LAN of the target company should be built to meet the network traffic which this type of a service generates.

All in all, when implemented and designed properly, an NAS is a much better solution than using the local hard drives as data storages.

7 DISCUSSION

7.1 Scope and Limitations

This study focuses on finding the proper way to implement an NAS for the needs of the case company and as such to improve their data security. Since the case company is relatively small and it operates under the regulations of European Union as it's a foundation supported by the EU, it doesn't have the required budget to create IT-solutions which utilize the industry's best policies and practices. This also gives the study some of its limitations; the best solution might not be suitable in this case as the budget for the system to be built is only approximately 500 euros.

This study is narrowed down to discuss the NAS-system; not the equipment around it, such as the network and the client computers. These aspects should be discovered before the actual implementation stage of the NAS. The case company in this study has the needed network infrastructure created beforehand by Nordic Lan & Wan Communication Oy.

7.2 Reliability and Validity

Reliability means a statistical measurement of data about how reproducible it is (Litwin, 1995, p. 6). Therefore it is essential that these findings and decisions are found reliable. However, since this research is narrowed down to create only one type of an NAS, the reliability should be considered to be practically unknown. Considering the given timeframe and the budget, it would have been impossible to make a real-life comparison between different hardware. The facts to support the decision in this thesis are, however, taken from reliable sources. Depending on the area of usage, the created artifact should generate the same testing results in various scenarios.

Validity is a key to a successful study. Invalid data, facts and assumptions can critically change the result of the study, thus providing false knowledge. There-

fore, an invalid research can be considered worthless. (Cohen, Manion, & Morrison, 2007, pp. 133-164.) The validity in this research is confirmed by researching the findings in literature and by comparing the findings between the results in this study and the findings in literature. The validity is also confirmed by inspecting the results after the implementation in Design Foundation Finland.

7.3 Suggestions for Further Studies

As this research is done only to cover situations where the number of users is no more than 10, this cannot be applied to scenarios where the number of users is significantly higher. However, further study of this subject might reveal if this research could be applicable in enterprise-level, where there's significantly more stress towards the data storage system. As the artifact made in this study is expandable, it allows the creator to decide the performance and the size of the NAS by adding different hard drive setup.

One option for further study is discussed in the "Reliability and Validity" – section, the optional ways for the NAS-implementation. Currently there are NAS-devices available, which are typically to be used in home-environment. However, with a higher price tag, there are also NAS-devices which are usually rack-mountable and decently fault-tolerant. It would be a good idea to conduct a further study about the differences between pure NAS-devices and servers like in this research.

PUBLISHED REFERENCES

Cadle, J., Paul, D., & Turner, P. (2010). *Business Analysis Techniques.* Chippenham: British Informatics Society Limited.

Carter, G., Ts, J., & Eckstein, R. (2007). *Using Samba.* Sebastopol: O'Reilly Media Inc.

Choubey, M. K. (2012). *IT Infrastructure and Management.* New Delhi: Dorling Kindersley (India) Pvt. Ltd.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods In Education.* Oxon: Routledge.

Course Technology, Cengage Technology. (2011). *Understanding Operating Systems, Sixth Edition.* Boston: Course Technology.

Doyle, S. (2000). *Understanding Information & Communication Technology.* Cheltenham: Stanley Thornes (Publishers) Ltd.

Erbschloe, M. (2005). *Physical Security for IT.* Burlington: Elsevier Inc.

Fellner, M., & Graf, N. (2009). *Beginning OpenVPN 2.0.9.* Birmingham: Packt Publishing Ltd.

Kahate, A. (2003). *Cryptography and Network Security.* New Delhi: Tata McGraw-Hill Publishing Company Limited.

Keijser, J. J. (2011). *OpenVPN 2 Cookbook.* Birmingham: Packt Publishing Ltd.

Litwin, M. S. (1995). *How To Measure Survey Realiability and Validity.* Thousand Oaks: SAGE Publications Inc.

Miles, M. B. (1994). *Qualitative Data Analysis: an expanded sourcebook.* Thounsands Oaks: SAGE Publications Inc.

Shakespeare, W. (n.d.). The life of King Henry the Fifth. *Act1, Scene II*.

Smith, R. W. (2005). *Linux in a Windows World.* Sebastopol: O'Reilly Media, Inc.

Stair, R., & Reynolds, G. (2012). *Principles of Information Systems.* Joe Sabatino.

Thompson, R. B., & Thompson, B. F. (2011). *Building the Perfect PC.* Sebastopol: O'Reilly Media Inc.

Weber, S. (2004). *The success of open source.* Harvard College.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security.* Boston: Course Technology, Cengage Learning.

ELECTRONIC REFERENCES

Iomega. (2010). *Network Storage From A to Z.* Retrieved November 16, 2011, from Iomega Corporation Web site: http://www.iomeganetworks.com/eBook.pdf

Trochim, W. M. (2006, October 20). *Deduction & Induction*. Retrieved September 21, 2012, from Research Methods Knowledge Base: http://www.socialresearchmethods.net/kb/dedind.php

APPENDICES

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.0.7 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun
```

```
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
key client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

APPENDIX 1: Client-side OpenVPN configuration

```
################################################
# Sample OpenVPN 2.0 config file for           #
# multi-client server.                         #
#                                              #
# This file is for the server side             #
# of a many-clients <-> one-server             #
# OpenVPN configuration.                       #
#                                              #
# OpenVPN also supports                        #
# single-machine <-> single-machine            #
# configurations (See the Examples page        #
# on the web site for more info).              #
#                                              #
# This config should work on Windows           #
# or Linux/BSD systems.  Remember on           #
# Windows to quote pathnames and use           #
# double backslashes, e.g.:                    #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                              #
# Comments are preceded with '#' or ';'        #
################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
```

```
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh1024.pem

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100
```

```
# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
```

```
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
;client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names.  This is recommended
# only for testing purposes.  For production use,
# each client should have its own certificate/key
# pair.
#
# IF YOU HAVE NOT GENERATED INDIVIDUAL
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",
# UNCOMMENT THIS LINE OUT.
;duplicate-cn

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
```

```
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 10

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
```

```
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

APPENDIX 2: Server-side OpenVPN configuration

```
# Samba config file created using SWAT
# from UNKNOWN (192.168.0.4)
# Date: 2012/01/26 00:35:25

[global]
          server string = %h server
          obey pam restrictions = Yes
          pam password change = Yes
          passwd program = /usr/bin/passwd %u
          passwd chat = *Enter\snew\s*\spassword:* %n\n
          *Retype\snew\s*\spassword:* %n\n
          *password\supdated\ssuccessfully* .
          unix password sync = Yes
          syslog = 0
          log file = /var/log/samba/log.%m
          max log size = 1000
          dns proxy = No
          panic action = /usr/share/samba/panic-action %d
          invalid users = nobody root
          locking = Yes
          hide dot files = Yes
          lock dir = /var/cache/samba
          pid directory = /var/run/samba
          load printers = No
          null passwords = No
          security = USER
          hosts allow = 127.0.0.1 192.168.179.0/24 10.8.0.0/24
          hosts deny = 0.0.0.0/0

[homes]
          comment = Käyttäjän kotikansio
          writable = yes
          valid users = %S
          create mask = 0700
          directory mask = 0700
          browseable = No

[hallinto]
          comment = Hallinto
          browsable = yes
          path = /nas/hallinto
          public = yes
```

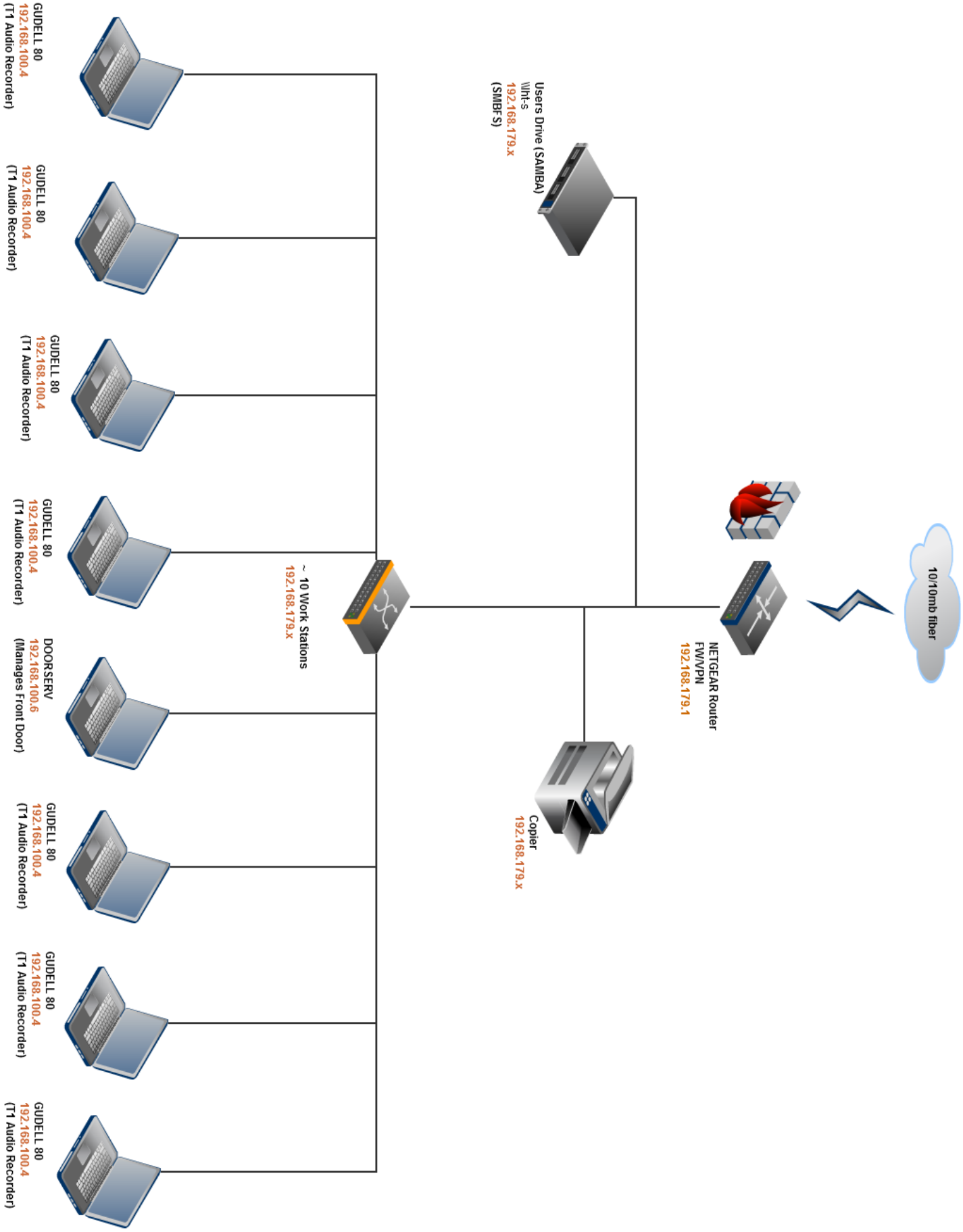
```
          writeable = no
          valid users = pekka, jari-pekka
          admin users = jari-pekka
          write list = pekka, jari-pekka

[yleinen]
          comment = Yleinen jako
          browsable = yes
          path = /nas/yleinen
          public = yes
          writable = no
          valid users = @users
          write list = @users
          admin users = jari-pekka
          guest ok = no

# This one is useful for people to share files

[väliaikainen]
          comment = Väliaikainen tallennustila
          path = /nas/valiaikainen
          read only = no
          valid users = @users
          admin users = jari-pekka
          public = yes
```

APPENDIX 3: Server-side Samba configuration



APPENDIX 4: Network Diagram in Design Foundation Finland network

INTERVIEWS

Pekka Koivisto	17.1.2012
Ville Korhonen	8.2.2012
Ville Korhonen	23.2.2012