LAN and WLAN planning, deployment, and evaluation

MARIA MAGNUSSON

KTH Information and
Communication Technology

Degree project in
Communication Systems
First level, 15.0 HEC
Stockholm, Sweden

Bachelor of Science Thesis

LAN and WLAN planning, deployment, and evaluation

Maria Magnusson

Communication Systems
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden

and
Switch Nordic Green AB

February 14, 2013

Examiner:
Professor Gerald Q. Maguire Jr.

Supervisor:
Majid Jam, Switch Nordic Green AB

Abstract

Switch Nordic Green AB (Nordic Green Energy) is an energy company with about 40 employees. The customer service department is in-house and a lot of the work, by all departments, is done by programs running on remote servers. Today most of the network traffic is through a wired local area network, although there is a wireless guest network which is very unstable. While planning a move to a smaller office the company is planning to implement a more extensive wireless local area network.

This bachelor thesis will provide a basis for implementing the local area network and wireless local area network for the company's new office. The thesis will also establish the network platform for an eventual move of a department within the company located in Finland. This documentation will enable the company to save both time and money.

With a local area network, designed and implemented for the new office, the employees will have the best possibility to improve their work and it will also increase the efficiency of the company.

***Keywords*:** WLAN, LAN, network planning, Nordic Green Energy, VoIP, department relocation

Sammanfattning

Switch Nordic Green AB (Nordic Green Energy) är ett elbolag med cirka 40 anställda. Kundtjänsten sköts internt och mycket av arbetet, även på de andra avdelningarna, sker mot fjärrservrar. Idag ligger majoriteten av nätverkstrafiken på ett trådat lokalt nätverk, men det finns även ett trådlöst gästnätverk, som dock är väldigt instabilt. När företaget ska flytta till ett mindre kontor planerar de att implementera ett mer omfattande trådlöst nätverk.

Den här kandidatexamenauppsatsen kommer användas som grund för implementationen av både trådat och trådlöst lokalt nätverk på det nya kontoret. Uppsatsen ska upprätta en nätverksplattform som kan användas vid en eventuell framtida flytt av företagets kontor i finland. Med denna dokumentation tillgänglig kan företaget spara både tid och pengar.

Med ett lokalt nätverk som är designat och implementerat för det nya kontoret har de anställda möjlighet att förbättra sin arbetainsats och företagets effektivitet.

Acknowledgement

I would like to express my sincere gratitude to my examiner Professor Gerald Q. Maguire Jr., for all the support, feedback and encouragement.

I would also like to thank everyone at Nordic Green Energy for a great time at the office.

Contents

List of Figures

Acronyms and Abbreviations

AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISL	Cisco Inter-Switch Link
ISP	Internet Service Provider
LAN	Local Area Network
MAC address	Media Access Control address
PoE	Power over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WLC	Wireless LAN controller
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key
WPA/TKIP	Wi-Fi Protected Access/Temporal Key Integrity Protocol

1 Introduction

This chapter gives some background information about the project and then describes the goals and purpose of the thesis project. The chapter ends with a description of the structure of the thesis.

1.1 Background

Nordic Green Energy is to move into a new office. Today, almost all network traffic goes through wired local area networks (LANs). New LANs are to be set up in the new office. As part of the move the company would like to make increasing use of wireless local area networks (WLANs) in order to give their employees greater flexibility within the office. The current wireless guest network does not work as desired. For example, if too many users connect to the same access point their connections will be interrupted.

The company is using voice over IP (VoIP) software running on personal computers (PCs). As the network is currently configured, the traffic associated with VoIP calls is not prioritised over other data traffic. Having incoming calls that do not establish a session with the intended callee is not acceptable for a customer service department, hence there is a need for a better network configuration.

Since customer support has to be available every weekday the downtime of the network has to be as low as possible during the normal operating hours (09:00 to 16:00 on weekdays). For this reason, the underlying network has to operate correctly and a plan for dealing with every (expected) eventuality is necessary. This thesis project started by analysing the network and the services that are used today, determined what parts were worth keeping and what parts of the network infrastructure need to be changed, and then documented how the new office should be set up and how each of the network attached devices and the network infrastructure should be configured. When the actual move is made, the system needs to be on-line and working from the start of operations at the new site(s).

1.2 Goals

The goal of this thesis project is to design, configure, set up, and evaluate a working LAN and WLAN in the company's new office premises. The documentation of the planning, implementation, and evaluation will provide the company with information about their LAN and WLAN and facilitate the operation and continuing evolution of the company's network infrastructure.

1.3 Thesis purpose

This thesis is meant to be used as the basis for future projects of a similar nature within the company, specifically for the other sites that the company will be moving to. This also clarifies the limitations of this thesis project, as this project will focus on a single future site (for a single department).

1.4 Thesis outline

The thesis is structured into the following chapters:

Chapter 1
Introduction to the problem and its context as well as goals, purpose, and limitations.

Chapter 2
This chapter gives a brief introduction to the basic devices of a wireless and ethernet local area network, the standards used, and security protocols.

Chapter 3
The planning of a (wireless) local area network is described, along with capacity, standards, and security issues.

Chapter 4
Explains the implementation of moving the office. Preparations and tests in the current office and set-up in the new office.

Chapter 5
Conclusions of this thesis. Presents achieved goals and suggests future work that can be done.

2 WLAN and LAN

The reader of this thesis is expected to have basic knowledge of computer networking. This chapter will briefly describe the devices forming the network and connected to the network, how the connections are established, and the different security protocols that can be used to secure wireless computer networks.

2.1 Basic network topology

Figure 1 shows a simple network with clients, routers, access points, and a gateway. Each of these is further described below.

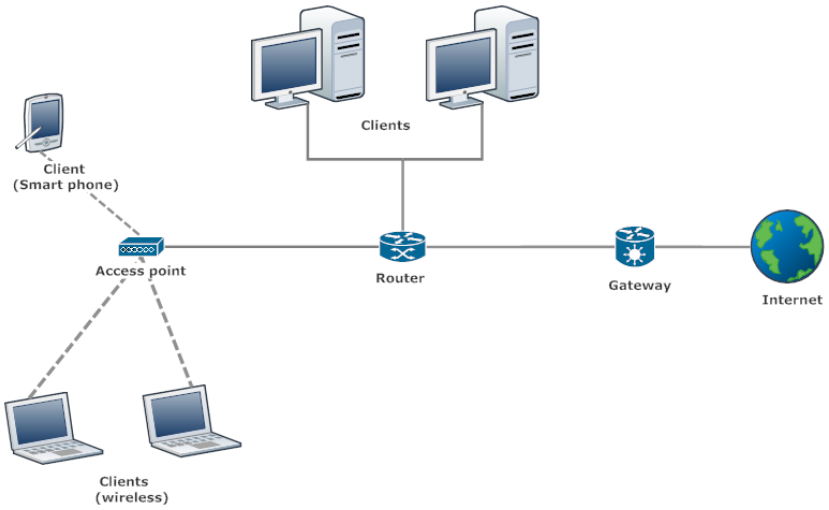

Figure 1: A simple network topology.

Client
: An end point of the network, usually a computer or a smart phone. Clients can be mobile and/or fixed computers.

Router
: The router connects different subnets and forwards information to the correct destination.

Access point
: In a wireless network clients connect to the rest of the network through an access point. The access point transmits and receives radio frames for WLAN equipped devices enabling them to communicate. The

difference between an access point and a router is that an access point only connects clients within a subnet, rather than interconnecting subnets. However, one can think of an access point as interconnecting a wireless subnet with a wired subnet.

Gateway
: The gateway is used to connect the network to another network, usually the Internet. A computer with two or more network interfaces can be used as a gateway. However, today the gateway is often implemented as a combination of a router and a firewall, with optionally many local server functions, such as acting as a DHCP server, DNS server, VPN end point, etc.

2.2 Connections

The IEEE 802.11[1] standards are widely used WLAN standards. Within the IEEE 802.11 family of standards are several different standards, the most commonly used are 802.11a, 802.11b, 802.11g, and 802.11n. The main differences are connection speed and operating frequency.

Fixed ethernet connections are generally based upon using twisted pair (TP) Cat 5 cables.[1] Cat 5 cables support bandwidth of 100 MHz which is sufficient for *Fast Ethernet* speeds (up to 100 Mbps). Optionally Cat 5e or CAT 6 cables can be used to support higher speeds. The IEEE 802 family of standards provide detailed specifications for most fixed and wireless LANs. An important standard in this regard is IEEE 802.3af Power over Ethernet (PoE) - as this standard enables the ethernet switch to deliver power to network attached devices such as IP telephones and access points. By delivering power over the network cabling there is no need to located the devices near an electrical outlet. Additionally, if there is a need for operating during a power failure the network switch and the network infrastructure might be powered by via an uninterruptable power supply so that IP telephones and other devices could continue to operate despite a power fault of the general power mains. PoE is frequently used together with light weight access points and a WLAN controller (WLC) to decrease the cost and increase the manageability of large numbers of access points. It is important to note that in a *small* configuration that it may not be worthwhile to utilize a WLC.

[1] Further details of the different categories of TP cables and the bandwidth they support can be found in e.g. [2].

2.3 Security

The most common types of security used in a WLAN are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP has been replaced by WPA since WEP was too easy to crack. The current standard is WPA2, which uses a longer key, hence it is considered to be more secure than WPA.

Both WPA and WPA2 can be used with either WPA-Personal or WPA-Enterprise. WPA-Personal is designed for small office networks and is also referred to as WPA-PSK, where PSK stands for Pre-shared key. WPA-PSK does not require an authentication server. A 256-bit key, generated from a password is used by the network devices to authenticate when they wish to use the services of the access point. WPA-Enterprise requires a more complicated setup due to its use of a RADIUS (or DIAMETER) authentication server. Extensible Authentication Protocol (EAP) is used for authentication between the supplicant (the mobile device) and the authentication server. Note that IEEE 802.1x and EAP can also be used to authenticate devices attached to the fixed LAN.

2.4 Meru Networks

Meru Networks[3] focuses on giving the customers a WLAN that is easy to manage and configure. As the amount of wireless devices in the office increases, the Meru Virtualized WLAN is easy for the internal IT managers to deploy, manage, and expand, at a low cost.

Meru Networks offers different solutions and APs to fit every customers needs.

2.5 Uno IP telephony

Uno[4] is a Swedish company that offers telephone central solutions for companies. Uno states that it should not only be easy to choose and buy your IP telephony, but also to implement and use it daily. *Uno Mjuk* is more than just a IP phone in the computer, it also gives the employees a good view of the colleagues. Details as name, title, number and email are visible. It can also easily show if they are busy with another call or in a meeting, or not in the office at all today. The solution also offers the ability to send SMS to a phone and an internal chat client.

2.6 Ringdale's FollowMe

With services like *Ringdale's FollowMe*[5], it is easy to keep track of the printing costs at the office. The service also gives the office better control over how the printers are used, where it is possible to change routines and save both money and paper.

By giving the employees separate printing quotas, the amount of unnecessary printing could be reduced.

3 Planning a network

This section will discuss some of the issues that must be considered when planning a local area network. The main focus will be on WLANs.

3.1 Capacity

Today *Nordic Green Energy* has a WLAN and wireless guest network. When many users connect to the same access point connectivity is interrupted. To avoid this problem, fixed ethernet jacks are used in all conference rooms. This leads to problems with users losing their internet session when moving their computer from their desk to a conference room. There are also frequent problems with cables that are tangled or not working. Having wireless network coverage throughout the whole office would solve these problems and would simplify life for the employees. This requires sufficient capacity for the network and careful planning and placement of access points.

Since VoIP is used it is important that the wireless connection is stable and that media packets are not dropped, delayed, or corrupted more frequently than a small fraction of the traffic (less than 5%). This would enable a user to move around in the office while in a VoIP session - without losing connectivity or termination of the session. However, unless mobile-IP is to be supported, this means that the network has to be a single subnet, since otherwise the user would move between subnet - hence her device would get a new IP address and the VoIP session would need to be modified or the session would be terminated.

Today the company has an agreement for their uplink with one ISP. However, the connection to this ISP offers some redundancy. If the fixed connection to the ISP should go down due to failure in the fixed access network, a 4G router placed in the new office can be used as backup. This means that at least the most critical work can continue.

3.2 Standards

The choice of wireless standard has to consider the desired maximum data rates and potential sources of interference. Devices that are compatible with IEEE 802.11a operate in the 5GHz band. This has the advantage in that this band is not as heavily used as the 2.4GHz band, in which IEEE 802.11b and 802.11g devices operate. The disadvantage is that 5GHz has shorter range and in some cases will not be able to penetrate walls, hence leading to a need for more access points to cover a given area. However, an advantage of IEEE 802.11a is that there is a much wider frequency band for devices

to operate in, hence multiple networks can be operating in the same area with each using a different frequency band - while there can only be at most 3 IEEE 802.11b networks operating in the same area without interfering with each other. However, a disadvantage of IEEE 802.11a is that not all WLAN devices have a IEEE 802.11a compatible network interface. Thus it is necessary to consider all of the client devices that will be used. Fortunately, many access points can operate in both bands - even doing so simultaneously. This may enable the networks to support an evolution of devices to IEEE 802.11a from the current population of IEEE 802.11b devices.

The standard commonly used for Virtual LANs (VLANs) over an Ethernet network is IEEE 802.1Q. The standard implements a system for VLAN tagging for Ethernet frames. For example, Cisco's ISL (Inter-Switch Link) encapsulates the frame and adds an supplementary header which is removed at the receiving end of the trunk line[6].

Quality of Service (QoS) especially is important for VoIP. Common problems in a network such as data loss, jitter, and latency could lead to unacceptably bad voice quality. Favouring voice data in the network, and delaying or sacrificing other data types, can improve VoIP quality.

3.3 Security

As stated in the *Considerations for Planning and Deploying a Wireless LAN*[7], WEP has many weaknesses ranging from poor security to being vulnerable to man-in-the-middle attacks. In a man-in-the-middle attack someone intercepts the data sent between two parties, thus information could be altered without anyone noticing and the contents of the communication could be accessible to others.

WPA uses longer keys derived from a user-generated passphrase, the network SSID, the length of the SSID, and a randomly chosen value[8]. This data is then hashed 4,096 times and a 256-bits long key is generated. A problem with the WPA is that it is possible to obtain the passphrase from an brute-force attack if the passphrase is shorter than 20 characters.

WPA2 eliminates the problem associated with short pass phrases and is, at the moment, considered the most secure means of protecting WLAN traffic at the link layer.

3.4 Specific requests and considerations

As part of the first planning meetings with the company, the company had some specific requests and questions:

- **As customer support is the most depending department with respect to the need for a stable network connection, an ethernet LAN will be set up for this department in the new office. The rest of the employees will be connected via a WLAN.**

  This lead to the question of whether we need to divide the departments and to have different devices utilize different access points, in order to minimize the risk of some devices reducing the throughput of a specific access point? Another question is whether the company needs to buy new access points, or can they simply upgrade?

- **Security**

  Some of the security related questions that arise are do we need to do MAC address filtering[9], does the company need to purchase a certificate, and should connecting to the network require something more than a network password. At the moment the network password is manually changed every six months.

- **Guest WLAN**

  Currently the guest network password is manually changed, once every six months. Is it possible to have a week-/day- or even one-time password? What are the advantages and disadvantages in changing passwords more frequently?

- **Test of current WLAN**

  One suggestion that came out of these initial meetings was that the company upgrade their access points, in the current office, to enable them to offer their maximum data rate. The employees could switch to using the WLAN and continue to work as usual. Manually I would monitor the network and stress test the WLAN. Some of the questions that could be addressed in this way are: Are the programs working as they should? Do the employees experience reduced throughput? Are sessions lost due to glitches in the network connectivity?

4 Implementation

The move to the new premises took place during the first weekend of December 2012, starting in late afternoon on Friday. The plan was to have the network and all services up and running by Monday morning when employees arrived for work.

The first part of this section will discuss the planning of the move and at Subsection 4.5 the actual move is discussed.

4.1 Preparing the move

A lot can be done in advance and by involving the employees, for example they can prepare their own workstations to make the relocation go as smoothly as possible. These preparations include:

- Tag computers, docking stations, and chargers with computer name. Employees will be given moving boxes to pack their workstations in. If user want a specific monitor, they should tag that monitor with their computer's name, otherwise monitors will be distributed randomly in new office.
- Everyone will have been assigned their new location in the new office before the move, this will make it easier to know where the moving boxes should be transported to.

4.2 Test in current office

The current wireless network implementation is a Meru network[3]. There are four APs, the Meru AP301, as seen in Figure 2.

Figure 2: The AP301 access point from Meru Networks[10].

The security on the WLAN is WPA/TKIP. Since the WLAN has not been used frequently by the employees, it has not been regularly updated and tested. The problems detected, such as users not being able to log in, and connections terminated was fixed by upgrading the APs to the latest software.

4.3 Schedule for the weekend of moving

Before the move, a schedule was made and shared with all the employees. It included some detailed plans for each day of the weekend.

4.3.1 Friday

- Employees will pack their workstations as described previously. Everything that is to be moved must be tagged with either an employee's name or their computer's name.
- Printers will be moved.
- The network will be taken down and the existing switches will be moved to the new office. Employees will be able to access the system via VPN, if they already have a VPN configured for their mobile computer.
- Furniture and workstations will be moved to the new office during the evening and night.

4.3.2 Saturday

- At midnight (Friday), access will be denied to the old office and granted to the new office to all employees.
- During the day, the new office will be emptied of furniture and boxes of the previous tenant.
- The new office will be set up, including workstations and furnitures.
- The WLAN will be set up in the new office, as well as a LAN for the customer service department.

4.3.3 Sunday

- Configuration of the network continues. Cables will be laid to workstations which needs greater capacity, or which depend on a stable connection, for example within the financial department.

- All employees will come to the office at some point during the day to set up their workstation and to check that everything they need works as expected.
  Checklist:
  - Their computer starts.
  - Login works correctly.
  - All resources a accessible.
  - Phone (UNO[4]) is working.

4.3.4 Monday

- Printers with *Ringdale's FollowMe print*[5] will be installed. This will make it easy to keep track of prints, by using employees access cards.
- Employee's will test printers, scanning, fax, and copying with FollowMe print.

4.4 Set-up in new office

Figure 3 shows the new office, with WLAN access points and LAN ports. This figure also shows the location of some whiteboards and where the projectors and large monitors will be placed.

During the first week cables will be laid across the floor to the workstations that needs LAN connections, the rest of the office will use the WLAN. Subsequently, these cables will then be laid in the floor and connections will be available at the LAN ports shown in Figure 3.

4.4.1 Customer support

Customer support's computers will be connect by cables to switches near their table.

4.4.2 IT room

A IT room will house two switches, as well as provide storage for computers, cables, and other IT related equipment.

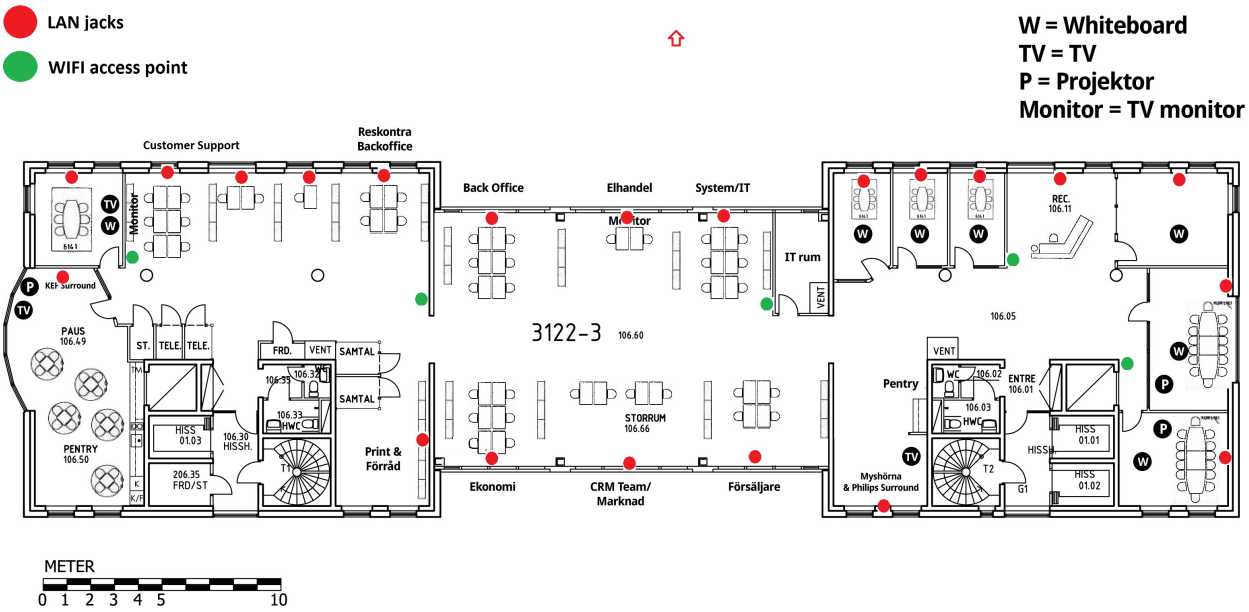

Figure 3: The new office with its APs and LAN jacks (i.e., RJ45 jacks).

4.4.3 Conference rooms

Conference rooms will initially have WLAN connectivity. After cables are laid to ports in the floor, a switch will be placed under the table in each conference room and short cables will be used from this switch to clients at the conference table.

4.5 Moving

Most of the moving went according to the plan and the schedule was followed. Since the company were changing office with another company, there were some complications with where to start and how to make the move. With only one large elevator in the old building, it could not be used by both companies at the same time.

Taking down switches and APs in the old office and putting it up in the new office was done relatively quickly. The company had help from CAG[11] with network related matters. The switches that were installed were HP ProCurve 24 ports and 48 ports[12].

Cat5 cables were laid on the floor from the IT room to the customer support. APs were placed on the ceiling, where cables were already laid out by the former tenant. After some discussion and testing, cables were laid out

to support the financial department and the system/IT department.

After a week CAG came and laid the network cables to jacks in the floor. With this done, all the workstations were able to use the LAN instead of the WLAN if the employees wish to.

The APs are operating in the 2.4GHz band using the IEEE 802.11b/g standard, as before the move. The security is also the same, using WPA/TKIP for the WLAN and the guest WLAN is open.

5 Conclusion

The initial plan to change the network of the new office to primarily WLAN was rejected due to costs. To upgrade the APs to IEEE 802.11n standard was almost as expensive as installing LAN in the new office, therefore the WLAN was kept as before. The APs were just checked to work properly and installed with the latest software to run on IEEE 802.11b/g as before and cables and jacks were installed to the LAN in the new office.

During the project, a lot of knowledge was gained about WLAN with its different standards and security issues. When planning a network it is important to pay attention to what capacity will be needed, what devices will be used in the network, and if there is a need for higher data rates and use of more recent standards.

When it comes to security, whatever the network might look like, if it is a large business or just a small home network, the best choice is WPA2 but in any case, it is always better to choose WPA over WEP.

5.1 Goals

The goals of this project were to plan and to document the move of the company to the new office. The main focus was on expanding the existing WLAN, but even though this was not implemented in the end, the material about the WLAN could be useful in the future. This report could also be used as documentation for a move of another department within the company. With a lot of the preparatory work already done, the decisions about a new network can be made a lot faster.

5.2 Future work

One thing that was not done in this project was to monitor the WLAN traffic. This should be done if the company decides to expand their WLAN. By doing so, it would be possible to see where and when the capacity is insufficient. There might be a need for more APs or to upgrade the existing APs to a later standard, such as IEEE 802.11n.

With an increasing number of mobile devices in the office, the company might want to make changes in the security of their guest WLAN. When such a WLAN is open, as it is today, it could be vulnerable to security attacks; hence this traffic might be separate from the other traffic in the office and given only a limited throughput.

5.3 Required reflections

This thesis project will give *Nordic Green Energy* a good overview of the current network implementation at the office. The documentation can be useful for the IT department when another move is to be planned.

This report will benefit *Nordic Green Energy* both in an economical aspect as well as save time in the process of planning a move or reorganizing the network implementation. The company can save money by not having to investigate the security issues of a WLAN and LAN. With a good implementation of a LAN and WLAN, the network will be able to handle the traffic in the office satisfyingly. In the customer support department, with their use of VoIP, this will lead to better quality of the calls and with that, better interaction with the customers.

Satisfied customers are very important since they will hopefully recommend the company to other customers, giving *Nordic Green Energy* more customers.

References

[1] IEEE Computer Society. LAN/MAN Standards Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, *IEEE standard for information technology telecommunications and information exchange between systems : local and metropolitan area networks–specific requirements. Part 11, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.* New York: Institute of Electrical and Electronics Engineers, 2012. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=6178209

[2] S. Karris, *Networks: Design and Management.* Orchard Publications, Jan. 2009.

[3] "Meru Networks," http://www.merunetworks.com/, [Online; accessed 21-January-2013].

[4] "UNO Telefoni," http://www.unotelefoni.se/hem/, [Online; accessed 21-January-2013].

[5] "Ringdale, FollowMe," http://www.followme.ringdale.com/, [Online; accessed 21-January-2013].

[6] Cisco, "Inter−Switch Link and IEEE 802.1Q Frame Format," Cisco, Tech. Rep., 2006, document ID: 17056.

[7] Blackberry, "Considerations for planning and deploying a wireless LAN," Blackberry, Tech. Rep., 2010.

[8] Flynn Martin, "WiFi Security Setup Guide," http://www.datapro.net/techinfo/wifi_security.html, [Online; accessed 05-October-2012].

[9] Bradley Mitchell, "Enable MAC address filtering on wireless access points and routers," http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm, [Online; accessed 18-October-2012].

[10] "AP 300 SERIES Meru Networks," http://www.merunetworks.com/collateral/data-sheets/2012-ds-wireless-lan-ap300-wireless-access-points.pdf.pdf, [Online; accessed 27-January-2013].

[11] "C.A.G Arete Datastöd," http://www.cag.se/, [Online; accessed 29-January-2013].

[12] "HP Network Switches," http://h17007.www1.hp.com/us/en/products/switches/index.aspx, [Online; accessed 29-January-2013].

TRITA-ICT-EX-2013:27

www.kth.se