Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Master's Thesis

2017

PRASHANTA PAUDEL

STUDY OF LNET USERS FOR EDUROAM BASED WI-FI IMPLEMENTATION

Examiner: Professor Jari Porras

Supervisor: PhD Ari Happonen

ABSTRACT

Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Prashanta Paudel

Study of LNET users for eduroam based Wi-Fi implementation

Master's Thesis

2017

130 pages, 81 figures, 7 tables, 6 appendixes

Examiners: Professor Jari Porras

Keywords: Wi-Fi, Wireless networking, smart services, customer centric network, WAN, Internet, developing wireless network, eduroam

The main objective of this thesis is to investigate the current service status of LNET and to find ways in which eduroam can be integrated in planned Wi-Fi implementation of LNET. Survey and interviews were carried out to determine the situation of service and expectations from the students living in LOAS apartments. Analysis of the data collected from these methods provided us with the guidelines for new service planning. Thesis also provides guidelines to find a possible design, development and implementation of wireless network without affecting the network speed and quality of services in that network. Theoretical part aims to provide enough background about the wireless networks for better understanding of thesis sections ahead. After implementing new wireless network, all LOAS students will be able to use numerous services provided by eduroam integration with ease and simplicity.

ACKNOWLEDGEMENTS

This thesis was done for the LUT School of Business and Management, Degree Program in Computer Science at Lappeenranta University of Technology.

First, I would like to thank God for keeping me motivated, protecting me and blessing me on whatever I do including this Thesis. I am very grateful for the love and support from my wife and family throughout my study in Finland. I would also like to thank Lappeenranta University of Technology for selecting me as a student in Masters of Science.

Second, I would like to appreciate the support from my supervisor Ari Happonen, for giving me opportunity to work in this thesis topic and guiding me throughout this thesis. His guidance was very important for me. I would also like to thank LOAS for giving me this opportunity to work in this thesis and providing me access to the LNET network.

Third, I would like to thank everybody who managed to take their time for participating in questionnaires and interviews that were conducted as a part of the thesis and all my friends who provide me valuable suggestions for betterment of the thesis.

Finally, I would like to thank LUT for these memorable years.

Prashanta Paudel

Lappeenranta, 10th September 2017

SYMBOLS AND ABBREVATIONS

WAN	Wide Area Network
AP	Access Point
ACL	Access control List
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
eduroam	Educational Roaming
IP	Internet Protocol
GPS	Global positioning system
IDS	Intrusion detection system
IPS	Intrusion Prevention system
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MAC	Medium Access Control
NIC	Network Interface Card
PC	Personal Computer
PCI	Peripheral Component Interconnect
RADIUS	Remote Authentication Dial in User Service
RF	Radio Frequency
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
AMPS	Advanced Mobile Phone Services
ARPA	Advanced Research Project Agency
DARPA	Defense Advanced Research Project Agency
AAA	Authenticate Authorization Accounting

LIST OF TABLES

Table 1 Various WLAN technologies Specification 26
Table 2 2.4GHz vs 5GHz 36
Table 3 Questionnaires sample 54
Table 4 Phases of project 79
Table 5 Project planning 81
Table 6 Resources required 83
Table 7 Performance test template 99

LIST OF FIGURES

Figure 1 eduroam logo 14
Figure 2 Hierarchy of RADIUS servers 15
Figure 3 eduroam authentication 16
Figure 4 Top level eduroam RADIUS servers 17
Figure 5 Hierarchy of eduroam servers 18
Figure 6 Map of eduroam connected locations in Finland (January 2017) 19
Figure 7 Customer Centricity 23
Figure 8 Wireless Networking 25
Figure 9 Classification of Wireless Networks 26
Figure 10 Ad-hoc Mode 30
Figure 11 Infrastructure Mode 30
Figure 12 Wi-Fi Certified Logo 31
Figure 13 List of SSID's 32
Figure 14 Coverage of 2.4 and 5GHz 36
Figure 15 Wi-Fi key sharing mechanism in LOAS 37
Figure 16 Using QR code for Wi-Fi 38
Figure 17 RFID 38
Figure 18 RFID inside bar-code used in tracking systems 39
Figure 19 RFID Key 39
Figure 20 How RFID works 40
Figure 21 NFC Tag 40
Figure 22 Writing into NFC tag 41
Figure 23 Reading Tag 41
Figure 24 Wi-Fi users 42
Figure 25 Ideal system 43
Figure 26 Wi-Fi prompt 43
Figure 27 Profile interface example 44
Figure 28 Device registration and update flowchart 45
Figure 29 Research process 46
Figure 30 Quantitative research process 56
Figure 31 LNET service quality 57
Figure 32 Hours per day - Study 58
Figure 33 Hours per day - Games 58
Figure 34 Hours per day - Social Network 59
Figure 35 Hours per day - Entertainment 59
Figure 36 Uses of Internet 60
Figure 37 Devices used for Internet 60
Figure 38 How do you solve your internet connection problem? 61
Figure 39 LOAS's Wi-fi or personal Wi-Fi? 61
Figure 40 Quality of Wi-Fi 62
Figure 41 Frequency and band of Wi-Fi 62
Figure 42 Wi-Fi Key 63
Figure 43 Wi-Fi Password 63
Figure 44 Where do you use Wi-Fi? 64
Figure 45 Will you replace your personal Wi-Fi? 65
Figure 46 How often do you have Wi-Fi problem? 65
Figure 47 eduroam 66
Figure 48 Is eduroam your primary connection? 66
Figure 49 Reliability of Eduroam 67
Figure 50 Have you faced any problem with eduroam? 67
Figure 51 Value Added service 68
Figure 52 LOAS Locations 74
Figure 53 Eduroam RADIUS hierarchy 75

Figure 54 Eduroam overview 76
Figure 55 Eduroam authentication process 77
Figure 56 LNET topology 80
Figure 57 LNET as SP 84
Figure 58 Connecting eduroam in Mobile 85
Figure 59 Connecting eduroam in Linux 86
Figure 60 Connecting eduroam in Windows PC 86
Figure 61 Ekahau site survey tool 89
Figure 62 LNET Wi-Fi Authentication 94
Figure 63 Testing speed in speedtest.net 97
Figure 64 Will you subscribe to Value added Service? 103
Figure 65 Will you subscribe to Smart services? 103
Figure 66 Li-Fi technology 105
Figure 67 Gender 120
Figure 68 Age group 120
Figure 69 Starting Year 122
Figure 70 Variation of application 123
Figure 71 Applications 123
Figure 72 Any other smart devices? 124
Figure 73 Smart TV 124
Figure 74 Problem with Network 125
Figure 75 Security issues 125
Figure 76 Wi-Fi password 126
Figure 77 How secure do you feel? 126
Figure 78 No of users in Wi-Fi 127
Figure 79 Have you ever had your password compromised? 127
Figure 80 Smart devices 128
Figure 81 Will you pay for new services? 128

TABLE OF CONTENTS

ABSTRACT ..... **II**

ACKNOWLEDGEMENTS ..... **III**

SYMBOLS AND ABBREVATIONS ..... **IV**

LIST OF TABLES ..... **V**

LIST OF FIGURES ..... **VI**

TABLE OF CONTENTS **8**

1 INTRODUCTION **11**

1.1 PROJECT BACKGROUND 12

1.2 THE RESEARCH PROBLEM 13

1.3 OBJECTIVES AND AIMS OF THE PROJECT 13

1.4 EDUCATIONAL ROAMING (EDUROAM) 14

1.4.1 Technology 15

1.4.2 Governance 17

1.4.3 Geographical Deployment 17

1.5 RESEARCH METHODOLOGY 19

1.6 STRUCTURE OF THE THESIS 20

2 STUDY BACKGROUND **21**

2.1 CUSTOMER CENTRICITY 22

2.2 WIRELESS NETWORKING 24

2.3 WIRELESS FIDELITY (WI-FI) 28

2.3.1 Wi-Fi Modes 29

2.3.2 Wi-Fi Alliance 31

2.3.3 Wi-Fi Service Set Identifier (SSID) 31

2.3.4 Wi-Fi Security 32

2.3.5 Wi-Fi Security Problems and Mitigations 33

2.3.6 Wi-Fi Signal Distortion 34

2.3.7 2.4GHz Vs 5GHz 35

2.3.8 Key sharing in Wi-Fi 36

2.3.9 Ideal Password sharing system 42

3 RESEARCH PROCESS 46

3.1 QUALITATIVE RESEARCH 47

3.1.1 Collecting data 47

3.1.2 Tape recording 47

3.1.3 Taking notes 48

3.1.4 Analyzing qualitative data 48

3.2 QUANTITATIVE RESEARCH 52

3.2.1 The Questionnaire 53

3.2.2 Analyzing quantitative data 55

3.3 DESCRIPTIVE ANALYSIS 57

3.4 IN DEPTH ANALYSIS 68

3.5 SUMMARY OF FINDINGS 72

4 WI-FI PROJECT 73

4.1 PROJECT DESCRIPTION 73

4.1.1 Objectives 74

4.1.2 Requirements 74

4.1.3 Coverage 74

4.1.4 Eduroam Overview 75

4.1.5 Project Infrastructures 78

4.1.6 Project planning 79

4.1.7 Resources Required 83

4.1.8 Potential Challenges 83

4.2 PROJECT IMPLEMENTATION 84

4.2.1 User Configuration 85

4.2.2 Wi-Fi Design Principles 86

4.2.3 Identity provider (IdP) 91

4.2.4 Access Point configuration 91

4.2.5 Defining the RADIUS server 92

4.2.6 Defining a wireless network 92

4.2.7 Service Provider (SP) 92

4.2.8 RADIUS Server configuration 93

4.2.9 Access Control Lists 93

4.2.10 LNET general Wi-Fi user's implementation 94

4.3 PROJECT LIMITATIONS 95

4.4 PROJECT TESTING 96
4.4.1 Speed test 97
4.4.2 Performance test.....98
4.4.3 When to test?.....100
5 CONCLUSION 101
5.1 MANAGERIAL IMPLICATIONS 102
5.2 FUTURE SERVICES.....102
5.3 FURTHER RESEARCH WORK 104
REFERENCES……..109
APPENDIX 1. SAMPLE OF INTERVIEW QUESTION
APPENDIX 2. SETTING UP FREE RADIUS ON CENTOS
APPENDIX 3. INITIAL CONFIGURATION OF AP
APPENDIX 4. LOAS BUILDINGS
APPENDIX 5. QUESTIONNAIRES DATA
APPENDIX 6. CONFIGURING MULTIPLE 802.1X AUTHENTICATION

1 INTRODUCTION

A network build in 1950's for a military project has now become one of the most important technological breakthrough human beings have ever developed. Today internet has become an integral part of everyday life for all human beings around the world regardless of profession, age, country, culture, belief or tradition. Globalization has transformed our world into a small city where people in any corner of the world can still get connected to their friends, family and office seamlessly. With the development of technology people are moving from cable connection to wireless connection. Within the last 15 years, all active land line connection has been dropped from 19.44 in 1995 to 14.34 in 2015 per 100 people. The number of people having a cellular mobile has reached from 1.58 percent in 1995 to 98.62 percent per 100 people in 2015. This shows that people are converging towards wireless connectivity throughout the world. With the increasing reach of cellular connectivity, mobile companies are providing various internet service packages for their customers.

Even though mobile companies provide various internet packages within their network it has not became as cheap as having the wireless local area network from Internet service provider (ISP) in most parts of the world. The most important use of internet is in educational sector. Nowadays, reliable and easily accessible Internet is an essential tool in aiding students in many of their educational endeavors. Distance learning and virtual classes has become a viable option for many students around the world. With that in mind most universities are already equipped with various wireless local area networking devices.

With the development of wireless technology such as 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac by Wi-Fi alliance for high speed internet connectivity it has been possible to connect considerable number of users at the same time without affecting the speed and quality of service. Nowadays, housing companies are installing Wi-Fi devices together with building infrastructures to provide it as a service to tenants. This approach is very convenient and cost effective for student's apartments as they don't have to manage routers and cables after shifting to new apartment which in turn saves time and money.

With basic internet, students today need access to university network whether they are in university or attending another university in exchange program. Trans European Research and Educational Networking Association (TERENA) developed a separate network called eduroam (Educational Roaming) for accessibility of university network and internet from another university which simplified the authentication portion of the network access.

As the expectations of students grow with growing technology they now expect to have the same network available in their student's apartments as they have in their university. First part of this thesis tries to find out the expectations of students from their network service providers and second part focuses on how to build such network and make them available to the students housing apartment.

Security in Wi-Fi network is a hot topic now as we transition from cable based network to cable less network. This transition has brought with itself the challenges to make these wireless channels as secure as possible. Several standards have already been developed to make the wireless network secure but still we hear about intrusions and hacking in wireless network every now and then.

One important security issue in wireless network is the key sharing mechanism. Even though the encryptions are developed, master key for unlocking access to the network is password which is shared via unsecured mediums. Now we have the mechanism for sharing password without speaking and writing but they are just replacement for ordinary sharing process, not the modification of how we share. The master key for unlocking access to a network in an encryption system is still text based which could be shared through an unsecured medium. In this thesis, we will look at various methods of sharing this password as well as present ideal system for sharing such passwords.

1.1 Project Background

Lappeenranta Student Housing Foundation (LOAS) is a housing company in Lappeenranta providing apartments for all the students studying in Lappeenranta University of Technology (LUT). Their apartments are specially designed for students and equipped to meet their basic day to day requirements. They have basically three types of apartment for students which are: Studio, two room and three-room apartments. Currently all the apartments have local Area Network (LAN) with internet access. LOAS's local area network is called LNET.

Maintaining a stable and reliable network in apartments with cable connections to each room has increasingly become arduous. The main problem has been the LAN ports in the apartment. Due to faulty cable connection in customers' router and various problems associated with problematic routers has always created difficulties for network administrators. This project will carry out study for planning and developing WLAN network in LOAS's apartments which will

in long term replace the problematic LAN networks at customer end as well as increase Wi-Fi accessibility that will eliminate current problems and make the network more robust. As LNET is an extensive network, we cannot replace all LAN networks at once. The full Wi-Fi coverage in apartments can be realized in several phases and when and where required as LOAS is not intending to replace working LAN just to make it wireless. This project will also study methods and procedures to replace current LAN network in LOAS apartments with WLAN network along with eduroam support.

1.2 The Research Problem

LNET as a network service provider for LOAS housing always strives to provide better service to its customers. As the use of wireless network has increased in past few years, LNET with its partner LUT tried to study the feasibility of using eduroam in LOAS apartments. This thesis is the part of that research.

The focus of this thesis work is to find the services expected by those wireless users and try to identify various behaviors related to network troubleshoot and maintenance. This will help us to include numerous services in new Wi-Fi network and finally integrate eduroam services with LNET.

The main questions to be answered are:

Main RQ: What are the expectations of LNET users from their Network service provider?

Sub-related questions are:

RQ 1: What are the attitudes and behavior of students toward their connected network?

RQ 2: How can we integrate more services in new LNET Wi-Fi network?

RQ 3: How can we improve the service quality through Wi-Fi network?

RQ 4: How to provide eduroam access to LOAS customers?

RQ 5: How can we share Wi-Fi key securely?

1.3 Objectives and Aims of the project

The main objective of the thesis is to find an answer to the main question and five sub-questions mentioned in the research problem. As wireless networking is not a new concept in today's context, this thesis will try to find the possible expansion of the services provided through Wi-Fi

networking which will be a possible add-on to the current basic internet service provided by LNET.

The questionnaires and interview selected as the quantitative approach to research will help answer the current scenario of the service and expectations from the students which in turn will help us modify our current infrastructure accordingly. Literature review at the first part of the thesis will provide industry wide practices which will guide us during the implementation phase. eduroam integration with LNET will be major feature improvement for students in LOAS apartment as they can access vast resources provided by eduroam as well as new exchange students coming from other university can authenticate themselves seamlessly without intervention from LNET administrators.

1.4 Educational Roaming (eduroam)

Eduroam as an initiative started in 2002 when TERENA's task force on mobility TFMobility started development of network based on RADIUS infrastructure with IEEEE 802.1X technology to provide roaming access across research and education institution in Europe. TERENA's Task force on mobility which is now known as GEANT Task force on Mobility and Network Middleware (TF-MNM) started an initiative to connect all Educational institution on same network in 2003. This initiative was given a name "eduroam" as short form of Educational Roaming. The technology behind eduroam is based on IEEE 802.11X standard and a hierarchy of RADIUS proxy servers. The task force created a test bed to demonstrate the feasibility of combining a RADIUS-based infrastructure with 802.1X standard technology to provide roaming network access across research and education networks. The initial test was conducted among five institutions located in the Netherlands, Finland, Portugal, Croatia and the United Kingdom. Later, other national research and education networking organizations in Europe embraced the idea and gradually started joining the infrastructure.(Marangaze 2011)

Figure 1 eduroam logo

Source: https://www.eduroam.org

From 2004, the European Union cofounded further research and development work related

to the eduroam service through the GN2 and GN3 projects. From September 2007, the European Union funded through these projects the continued operation and maintenance of the eduroam service at the European level. First non-European country to join eduroam was Australia in December 2004. Canada joined eduroam as University of British Columbia initiated the eduroam project which was continued by CANARIE as a service of Canadian Access Federation. In USA eduroam was pilot project started by National science foundation and University of Tennessee(UTK). In 2012 Anyroam LLC which was a private company from UTK announced Internet2 with eduroam as its service and administered top level servers.

1.4.1 Technology

Even though eduroam provides authentication service to large area, the basic concept on which it works is not complex. eduroam service uses IEEE 802.1X as the authentication method and a hierarchal system of RADIUS servers. The full form of RADIUS is Remote Authentication Dial in User Service which is a technology in which users authenticates via remote dialup service. This RADIUS hierarchy consists of authentication servers at the participating institutions, national RADIUS servers run by the National Roaming Operators and regional top-level RADIUS servers for individual world regions.

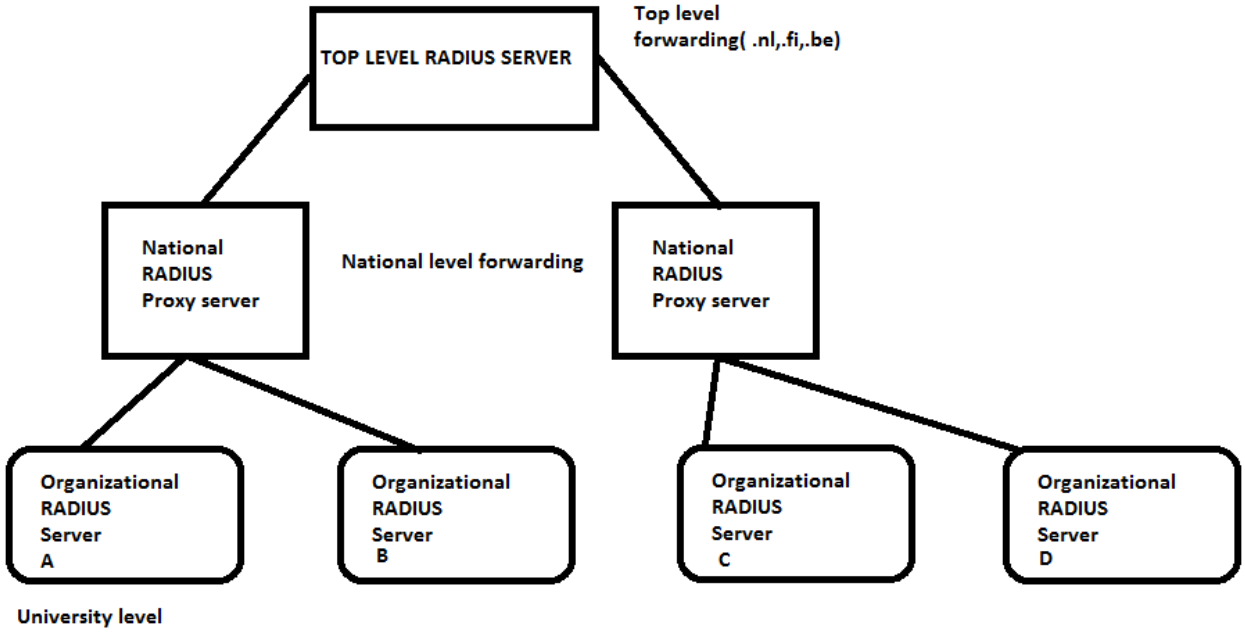

Figure 2 Hierarchy of RADIUS servers

When a user *"b"* from university *B* in country *BB* with two letter country code top level domain *bb* visits University *A* in country *AA*, *b's* mobile device presents his credentials to the RADIUS server of institution *A*. The RADIUS server located in University *A* detects that it is not responsible for the authentication of the user *b* so it forwards the authentication to top level

RADIUS server in country *AA* which in turn sends it to country *BB* and finally to University *B*. After the authentication is done in university B it forwards the result to country *AA* via the internet to University *A*. Finally, the authentication is received by user in University *A*. (scar Cnovas, HAW Hamburg, Hamburg, Germany 2007)

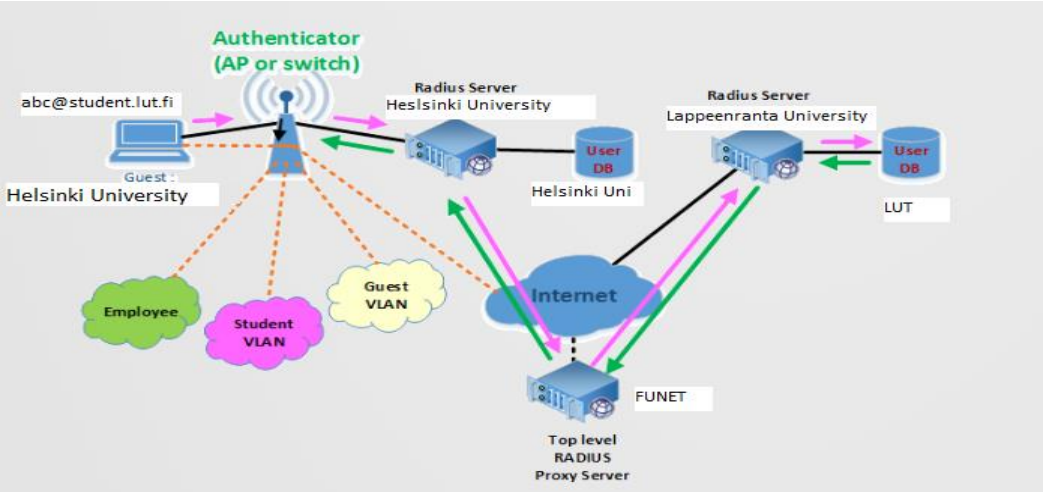

Figure 3 eduroam authentication

Since the credentials must travel outside the local network via internet it is very important to protect the information of the user. These requirements limit the type of authentication methods used for remote authentically. There are two categories of authentication methods

1. Public Key Mechanism
2. Tunneled Authentication

Most setups use a tunneled authentication method that only requires server certificates. These server certificates are used to set up a secure tunnel between the mobile device and the authentication server, through which the user credentials are securely transported.

A complication arises if the user's home institution does not use a two-letter country code top level domain as part of its realm. Instead generic top-level domain such as .edu or .org are used which later becomes reason for problems in international roaming since it is not possible to determine which national RADIUS server to forward the request. Solution to this problem is to create a routing table for this specific use.

1.4.2 Governance

The Global eduroam Governance Committee was constituted in November 2010 and currently comprises eleven senior representatives of roaming operators in Africa, Asia-Pacific, Latin America, North America and Europe. Secretariat support is provided by the GEANT Association, which finalized the summary charter for global eduroam governance after extensive consultation with eduroam leaders from these regions. TERENA has small group of people that form the governing body for global eduroam. eduroam consists of considerable number of organizations and research and education network throughout the world which follows the rules imposed on operation of eduroam. The Terms of Reference of the GeGC is also contained in this summary charter. The GeGC members are officially appointed by the GEANT Association based on nominations from their regional roaming operators or confederation.

1.4.3 Geographical Deployment

eduroam is now a worldwide network with operators located in every part of the world. It is divided into regions which are group of confederations of continent level that are again divided into group of federations in country level. In each country one institution or company operate as top-level server. All other federations in one continent are grouped under a confederation. Like federation, confederation also has one top-level server operated by an institution or company. eduroam is available in 80 countries worldwide. The map of available network is illustrated below:

Figure 4 Top level eduroam RADIUS servers

Source: https://www.eduroam.org

Eduroam is basically a Wi-Fi network. If universities want to deploy eduroam, all the infrastructural needs like access point (AP), controller, routers and switches should be installed in place beforehand by university themselves. University themselves will plan, design and deploy Wi-Fi and then connect local network to eduroam authentication. Basically, it is just different type of authentication through Wide Area Network (WAN) replacing traditional router based authentication.

Eduroam was initially started in Europe and has now expanded to extensive network covering in North America, Asia and Pacific. It is still a growing network and probably will add more services with authentication and resource access.

The Federation top-level servers take care of communication between institution's servers that belong to the same country. The confederation servers relay requests between federation's servers meaning requests between institutions from different countries. When communications between two institutions from different regions are taking place, confederations top-level servers communicate together. The view of eduroam network can be illustrated in diagram as:

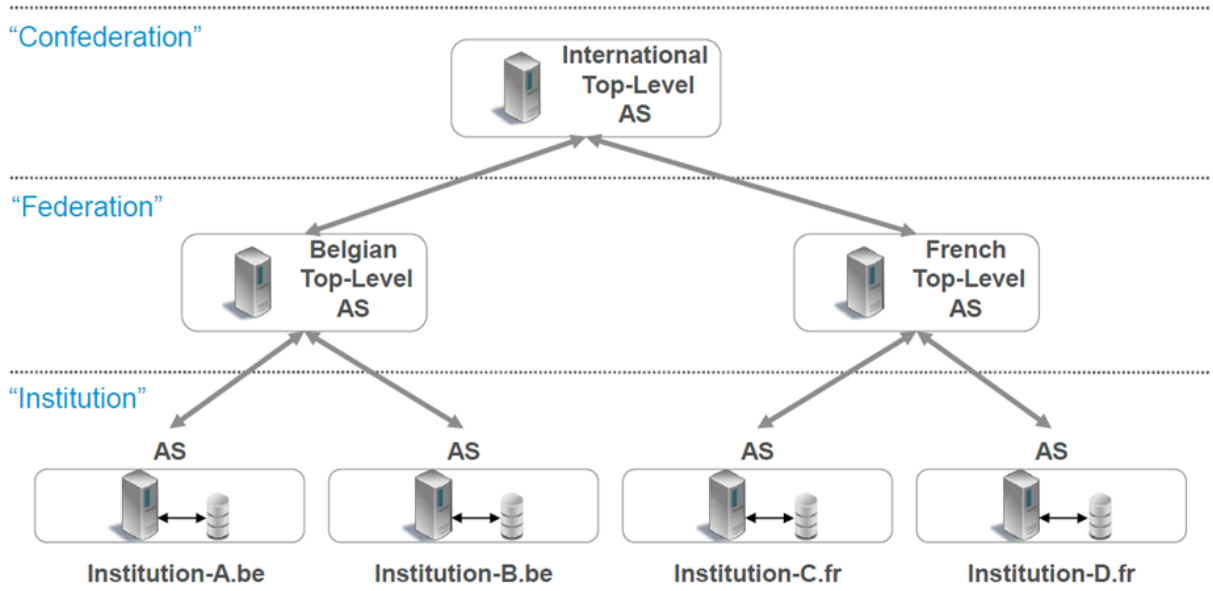

Figure 5 Hierarchy of eduroam servers

Source://www.eduroam.org

In Europe, there are 36 countries connected to eduroam network and hundreds of universities and colleges are providing roaming facility through this network. In Finland, Top-Level server is operated by CSC-IT through Finnish University Network (FUNET). FUNET connects 80

educational institutions in Finland. Lappeenranta University of Technology is a member of FUNET. eduroam network is growing in Finland too. At present 393 service locations are connected to this network.

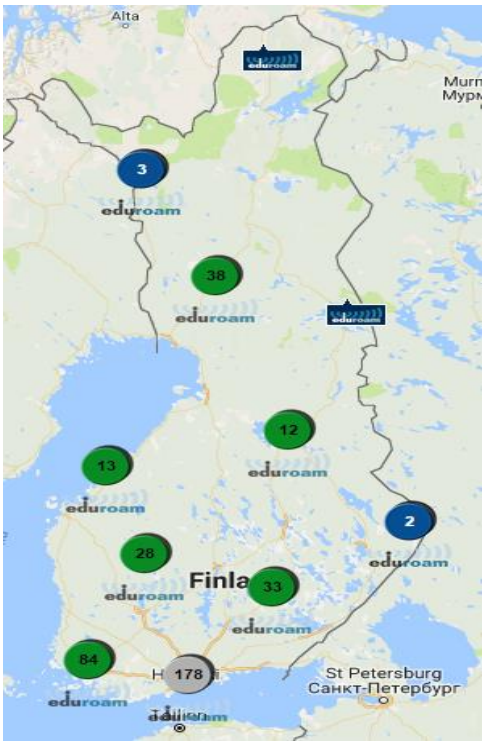

Figure 6 Map of eduroam connected locations in Finland (January 2017)

Source://www.eduroam.org

1.5 Research Methodology

To find out the expectations of the students from Lappeenranta University of Technology before going through network changes and upgrades, quantitative research method through questionnaires and interview was conducted. This research method enables us to find the actual scenario of the network usage and find out behaviors and attitudes of students toward Wi-Fi usages. We also included security and behaviors related questions to investigate current perception of Wi-Fi and expectations from service provider.

This study collected empirical data from potential future Wi-Fi users through web based survey and interview. Web based survey used in this project was carried out using survey developed from https://www.sogosurvey.com. Survey is conducted in English language as it is focused mostly on international students. Interviews are also conducted in English language and priority is given to diverse background of students.

1.6 Structure of the thesis

This thesis has both theoretical and practical parts. In theoretical part, we try to find the industry standards for planning, designing and implementing Wi-Fi network in housing apartments. This theoretical base will be used to implement Wi-Fi network in LOAS apartments with other services expected by students of LUT. To reflect these parts, thesis is divided into ten chapters.

Chapter 1 is the introduction of the project. Introduction provides overview of the topic of thesis, research problem, objectives and methods that will be followed during the thesis.

Chapter 2 is the study background of the topic which discusses the various terms and terminologies associated with the thesis. This chapter provides theoretical background of the thesis. Looking at the current context of the topic and studying various terms related to the topic will ease the planning, designing and implementation of the Wi-Fi network and will update on current progress in the industry. It deals with one of the important topic of thesis, key sharing in Wi-Fi. Here, I try to mention all available methods for key sharing and ideal solution for key sharing.

Chapter 3 is the research process which describes how we will conduct research for new services in Wi-Fi network. It will include methods in which research will be carried out. This chapter will analyze the data collected from questionnaire and interview and suggest major information out of the research. It also includes the detailed analysis of the results and summary of my findings.

Chapter 4 deals with description, planning, implementation, limitation and testing of the project. It is the core of my thesis and describes the project in detail with discussions on the entire infrastructural need for the project to successfully implement in later stages with both hardware and software requirements. I have even built a scheduled plan for implementation of the project. It also discusses the various limitations that can arise or are seen while implementing the project. This chapter discusses various test procedures available in the market to test the speed and quality of the network. New Wi-Fi network can be tested using these tools.

Finally, chapter 5 will give some solid conclusions on findings made through research and study done on various tools and technology available in the market. It will recommend some methods, tools and technology that could be used for planning, designing and developing new Wi-Fi network in LOAS apartments.

2 STUDY BACKGROUND

The term “wireless” has become a part of our everyday life as people around the world spend countless hours on their various electronic devices. With smartphone, tablets and laptops taking considerable time in day to day life of people all over the world, the term “wireless” has become part of our everyday life. In most basic form, it refers to communication without cables, but if we look at it on broad perspective it covers all communication from cellular network to local Wi-Fi. All the wireless communications travel over the air through radio magnetic waves such as radio frequencies, infrared and microwave. There is a governing body such as FCC to regulate these radio frequencies so that it doesn’t overlap and interfere with other wireless devices and services work reliably.

There are several approaches to go about building a Wi-Fi network. A single router with several connected devices is also one Wi-Fi network but building an enterprise level Wi-Fi network with robust design and reliable technology is not an easy task. This theoretical background will direct the upcoming chapters on how to build good Wi-Fi network keeping in mind all the key factors.

This literature review aims to offer readers with significant theoretical background for understanding wireless technology and basically Wi-Fi technology. During the development of networking technology from first signal transmission in ocean to internet of things (IoT) there are various achievements done for the progress of the technology. It is very important for anyone studying networking to know about these achievements before moving directly into core thesis. Here are the few important notes from that section:

a) In February 1958 Department of Defense Directive was signed which launched the Advanced Research Project Agency (ARPA) which is now known as Defense Advanced Research Project Agency (DARPA). This creation of ARPA was the most important event in the history of the internet.
b) The Stanford University Network was the developer of first LAN (local area network). It connected distant workstation via cable LAN. In 1981, NSF (national science foundation) expanded the ARPAnet to national computer science researchers when it funded the computer science Network (CSNET). Metropolitan Area Network is a large network covering larger area with several buildings and many LAN but smaller than Wide Area Network(WAN). This means that MAN could cover whole city and all the interconnected networking devices within the city. It may consist of several LAN as well

as Campus Area Networks(CAN). The diameter of MAN can be between 5 to 50 Kilometers.

c) Network topology is the physical arrangement of the network devices in the network. Network topology influences the performance of the network. It also determines the redundancy of the network and stability of the network and traffic on the network. Router and switch are both basic element of any network. Both devices have their own significance in networking. They allow us to connect to other computers and networks. The switches are generally layer 2 devices while routers are layer 3 devices but nowadays layer 3 routers are also available in market.

d) The full form of OSI is Open System Interconnection. This model defines how network devices and equipment should connect with each other independent of brand or model. All network equipment including routers, switches and bridges work in same underlying principles of OSI model.

2.1 Customer Centricity

The process of putting more focus on customers rather than on company and products is called customer centricity. Organizations that put focus on customers seem to be more successful than those only focusing on profit and products. Every customer wants good services from their service providers but those who go deep into what customers feel will do much better than just those who compare the price and make cheap products. Today every company wants to be customer centric because it is not just posture but requirement of core-business.

Customer centricity defines how the focus of the operation should be made towards customer satisfaction. Studies have shown that customer centricity is central to creating a corporate customer service culture that's devoted to the customer experience (Solomon 2014).

A customer centric behavior of organization can be instrumental in staying a step ahead of competition. It can help grow revenue, improve efficiency and increase performance. It can also lead to sustainable profitability. Some of the key factors that influence customer centricity are listed below:

1. Lead from the top with customer focused approach
2. Understand your customers
3. Design user experience
4. Empower the frontlines
5. Engage the supporting operations
6. Encourage the right behaviors
7. Use customer feedback to drive real changes to organization.

(Deloitte 2014)

Today, as customers' needs become more diverse and sophisticated, and as competition becomes fiercer on a global scale, it is important to foster strong relationships with customers and become an entity that is indispensable. (Minolta Konica 2015)

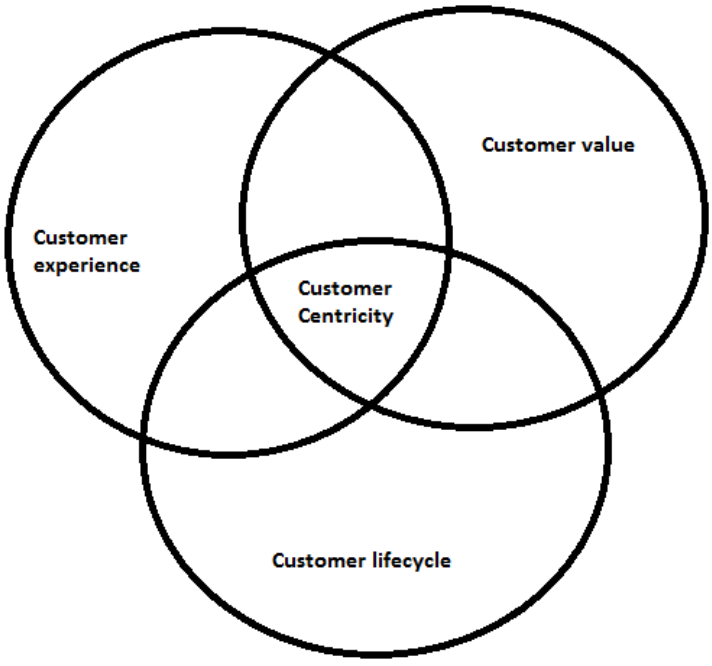

Figure 7 Customer Centricity

"Don´t wait to get a request from an internal participant in the operation. Instead, deliver your service based on customers' requirements. You have to go further out in the supply chain, realize what the customer needs, and then build your design based on that." (Rimpilainen Markku 2016)

2.2 Wireless Networking

Wireless communications and networking technologies have drastically changed the way we live. An explosion of innovation over the past two decades has resulted in wireless networking capabilities that have fundamentally changed the way we create, share, and use information. Combined with advances in computing and networking technology, the wireless internet ushered into reality the information age predicted long ago. This information era has undeniable effects on global socioeconomic and cultural conditions. These effects have had a profound impact on the operations of governments and military forces. Timely and reliable access to information is key to the success of virtually all government and military functions. Having effective communications and networking solutions is critical to mission success, and over the coming decades this requirement is expected to become even more important. Consequently, researchers at the Johns Hopkins University Applied Physics Laboratory (APL) will continue developing wireless communications and networking ideas, concepts, and solutions that are more efficient, effective, and affordable. This issue of the Johns Hopkins APL Technical Digest highlights some of the recent work by APL researchers in the areas of wireless communications and networking. Although it provides only a small sample of the wide range of work being done at APL, this issue presents articles on key topics such as leveraging commercial wireless technology in affordable military solutions, the evolution of security within the Internet community, satellite communications, high-capacity optical technologies, and network management.

Wireless Network is a communication network composed of wireless enabled network nodes that can carry data from source to destination without going through cable connection. Telecommunication networks are the biggest users of the wireless networking, as well as investors. Wireless networking has made possible to avoid costly cable installations in home and businesses and provide easy and secure network connection to users. As this provides physical connection between the nodes only physical layer of OSI model is wireless, all other layers are same and applicable for wireless networking too.

In 1901, when Guglielmo Marconi successfully transmitted radio signal across Atlantic Ocean, wireless network came into being. At that time, this test could replace telegraph and telephone communication lines with radio signal which provides a glimpse into a very exciting future. Even though radio signal was realized very early, two-way wireless communication was not commercialized for decades. The twist in the story came with the invention of transistor and development of cellular network. At bell laboratory scientist developed mobile communication

for daily use that was cheap and affordable. This development is still going on and companies around the world are developing communication sets and network from GPRS to 5G.

Wireless local area network has become the most popular tool in maintaining internet communications, especially at home, universities, hotels and workplaces. This is due to cost effectiveness, fast deployment, high data security, reliability, easy installation and maintenance as compared to wired local area network. The Wireless local area network operates in two frequency bands. The IEEE802.11 operates at 2.4GHz ISM band (Industrial, Scientific and Medical band), IEEE802.11a operates at 5GHz band where as IEEE802.11n operates in dual-band of 2.4GHz and 5GHz. Both ISMs are unlicensed bands. Basically, doubling the operations frequency would reduce the coverage distance however manufactures claim that IEEE802.11n could increase the coverage areas. According to Newton's Inverse Square Law, where the received RF signal strength is proportional to the inverse square distance from the source. This paper investigates the coverage performance between IEEE802.11b/g and IEEE802.11n. (Abdul Halim Ali, Mohd Raziff Abd Razak et al. 2015)

Examples of wireless networking are telecommunication networks, wireless local area network, wireless sensors network, satellite communication network, terrestrial microwave networks etc.

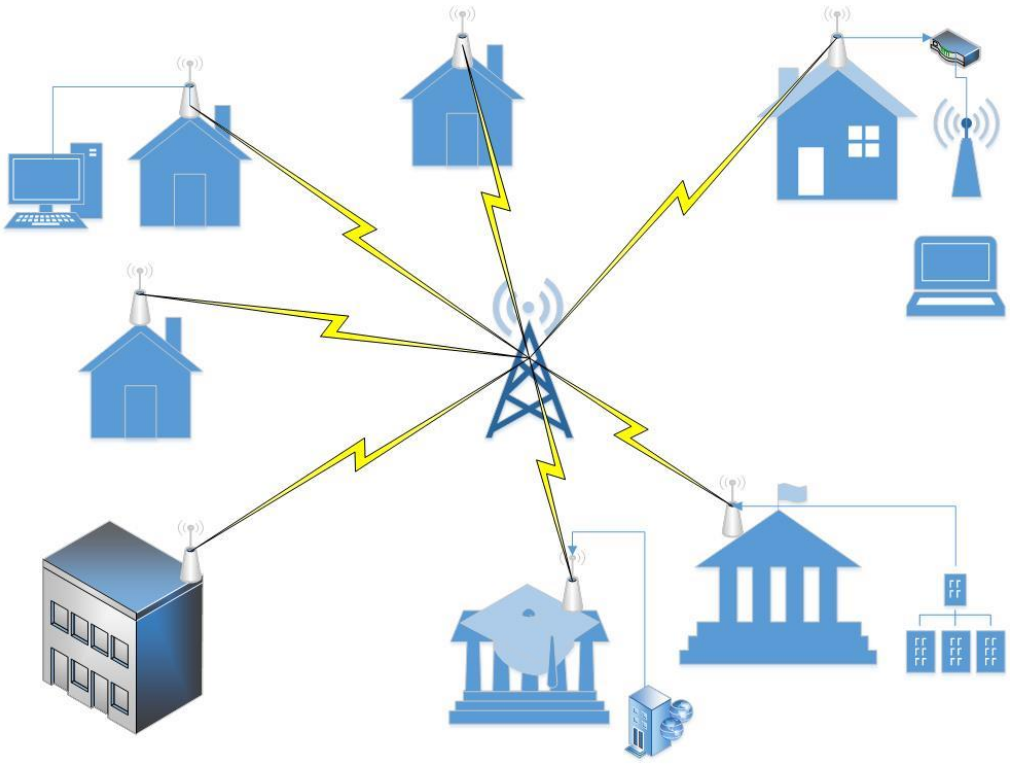

Figure 8 Wireless Networking

Wireless LANs (WLANs) bring incredible productivity and new efficiencies to organizations of all sizes. Advances in WLAN features and capabilities allow organizations to offer the benefits of wireless to their employees without sacrificing security. Properly deployed, WLANs can be as secure as wired networks. This paper discusses the five steps to creating a secure WLAN infrastructure. (Osterhage 2016)

Wireless Networks can be divided into several ways which is summarized in the diagram below.

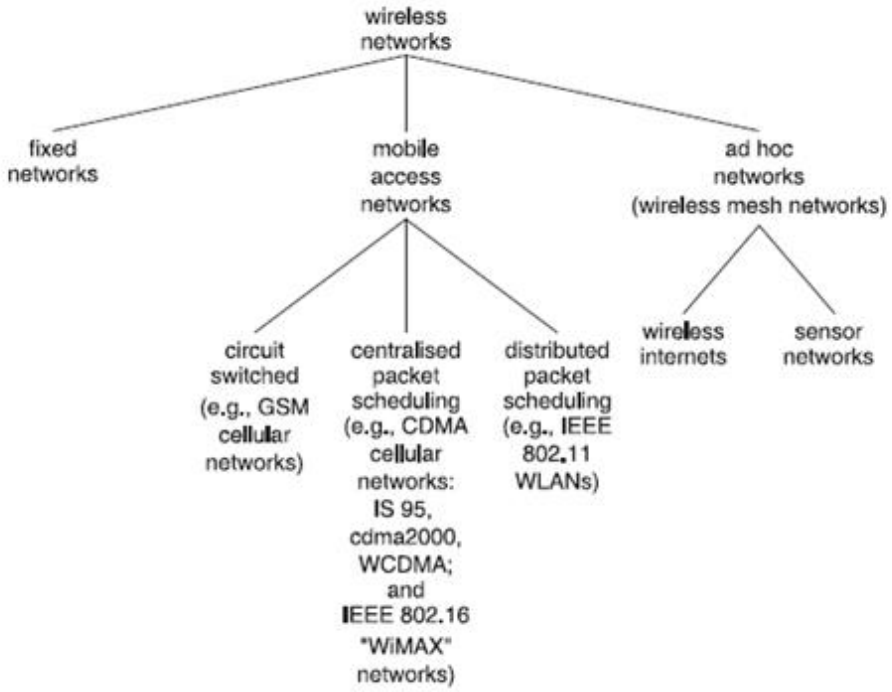

Figure 9 Classification of Wireless Networks

Table 1 Various WLAN technologies Specification

	WLAN Technologies			WPAN Technology	
Figure of Merit	802.11b	802.11a	802.11g	802.15.1 (Bluetooth)	802.15.4 (ZigBee)
Status	Widespread deployment	Mature	High growth	Mature	Mature chips
Band(1)	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Non-overlapping Channels	3	12 (8)	3	10 (2)	16+10+1
Modulation Technique	DSSS/CCK	OFDM	DSSS/CCK/OFDM (3)	FHSS (6)	DSSS
Maximum Data Rate	11 Mbps	54 Mbps (5)	54 Mbps	1 Mbps	250/40/20 kbps
Typical Coverage Range (4)	50 m	30 m (7)	40 m	10 m	70 m
Power Consumption	Medium to low	High	Medium	Low	Very Low
Complexity	Low chip count adapter	Low chip count adapter	Low chip count adapter	Single chip embedded application	Single or dual chip embedded application
Antenna	External or Embedded	External or Embedded	External or Embedded	Embedded	Embedded

The main benefit of having wireless network is freedom to connect to the network from any place within that network. Other advantages include easy installation and cost reductions. There are several benefits of having wireless network which is summarized in the points below.

1. Increased Mobility: It is by far the most important advantage of wireless network. This means that you can sit at any terminal, anywhere in the building and access the server easily which is great advantage for many business organization. For home users installing a Wireless router enables you to move anywhere within the house and still get the internet connection.
2. Enabling BYOD (Bring Your Own Device): This is the new concept developed by organizations after wireless networking became a possibility. It enables workers to bring their own laptops, tablets and smartphones to the office and do all the tasks from their own device by connecting to the corporate wireless network. This simplifies the organizations burden of managing laptops and computers for everyone. This increases the employee's productivity.
3. Hotspots: People may want internet access while in a public space far away from their home or office networks. So, hotspots provide internet access to people in a public space. We find these hotspots in coffee shops, commercial buildings, hotels, railway stations, airports, universities, hospitals etc. Almost all places where people gather or travel have some public accessible Wi-Fi. These hotspots are easily expandable for more coverage and scalability.
4. Guest Access: In cable connection, it was very difficult to add guest access to the network but wireless network makes it as simple as adding new username and password. Now every router vendors make it possible to allow guest access with all security precautions beforehand so administrator don't have to do any painstaking task to enable guest access.

There are several types of wireless network which can enable communication between two computers inside a room to computers in another continent.

Wireless communication has no physical link between source and destination. Wireless signals are spread by transmitting device in the air and if the receiving device detects the signal using appropriate frequency and antenna then they can communicate with each other. Wireless communication has no physical link between source and destination. Wireless signals are spread

by the sending device in the air and if the receiving device detects the signal using appropriate frequency and antenna then they can communicate with each other. Radio frequency is an electromagnetic wave that lies between 3KHz and 300GHz which include those frequencies used for communication and radar system. Radio frequencies are generated by antennas that propagate the waves into the air. On these frequencies, various kinds of transmission modes are used to transmit signal and data. Modes are:

1. Direct Sequence Spread Spectrum(DSSS)
2. Orthogonal Frequency Division Multiplexing(OFDM)
3. Multiple Input Multiple output(MIMO)

2.3 Wireless Fidelity (Wi-Fi)

Wi-Fi stands for Wireless Fidelity. It represents all IEEE 802.11 wireless standards. ALOHAnet developed a UHF wireless packet network to link Hawaiian Islands in 1971. ALOHAnet with ALOHA protocol were later developed to Ethernet and later IEEE 802.11 protocols. In 1985 US allowed the usage of ISM Band for unlicensed usage. These bands were used by microwave companies for their product. Later in 1991, NCR Corporation in co-operation with AT&T invented precursor to 802.11 which was used for cashier system. The first wireless product was named waveLAN which are credited for development of Wi-Fi Technology. Wi-Fi was created by the Wireless Ethernet Compatibility Alliance (WECA). When IEEE released 802.11 protocol in 1997, it had the maximum speed of 2Mbps which was later upgraded to 802.11b with 11mbps speed which was a success. In 1999, Wi-Fi Alliance was formed as a trade association to hold the trademark under which most products are sold. Devices like smart-phone, laptop, game console, digital camera, tablets, printers, security camera etc. all have Wi-Fi capabilities to connect to access point(AP). Wi-Fi compatible devices can connect to internet via WLAN and a Wireless Access Point which are typically located within 100 meters. Wi-Fi most commonly uses 2.4GHz UHF and 5GHz SHF ISM radio bands.

Even though Wi-Fi has reached unpredicted speed and capacity, users are not satisfied and progress in technology is still going on. IEEE and an industry consortium are working on even faster 802.11 versions. These radio-based technologies—IEEE 802.11ac, IEEE 802.11ad, and Wireless Gigabit (WiGig)—promise to deliver from 1 to 7 Gbps. Wi-Fi chipset vendors—such as Atheros Communications, Broadcom, and Intel—are already working with one or more of the innovative technologies. (Vaughan-Nichols 2010)

Wi-Fi reflects an impressive evolution in the use of home networking applications. Few years back having a wireless network or Wi-Fi was privilege of few people but now it has become a mainstream networking technology. Most of the smart devices that are manufactured today have the Wi-Fi interface build to connect it to the internet. (Gallo 2016)

Most of the handheld devices like smartphones, portable music players etc. are rapidly expanding and sometimes even replacing laptops as a computing and internet connecting platform of choice. A study done by EDUCAUSE in 2009 found that 51% of the undergraduate own an internet capable handheld and 12% plan to purchase one within next 12 months. A PEW study comparing 2007 and 2009 wireless internet usage found a 73% increase in rate Americans went online with their handheld. Even though the use of non-handheld is also growing, the usage of handheld is accelerating far more. By 2020, it is anticipated that there will be more than 50 billion connected devices globally, with mobile being the primary internet device for most individuals. (Gambler 2011)

2.3.1 Wi-Fi Modes

Wi-Fi modes define whether the access point can communicate directly to the devices or require intermediate access point to communicate with another device on network. 802.11 define two modes of operation for Wi-Fi access points.

2.3.1.1 Ad hoc Mode

It is based on Independent Basic Service Set (IBSS). In IBSS, client can setup connection to other clients without need of access point. This allows us to set-up peer-to-peer network connection between two clients. The main disadvantage of Ad hoc mode is that it is very difficult to secure this network since each device should be authenticated before connecting to the network.

The basic principle of Ad hoc networking is to eliminate an intermediate medium for simple peer to peer communication. These are self-organizing network that may have more than one hop. The main advantages of this network are that it doesn't require expensive devices to be installed. The complexity may arise when all the devices in ad hoc network are mobile.

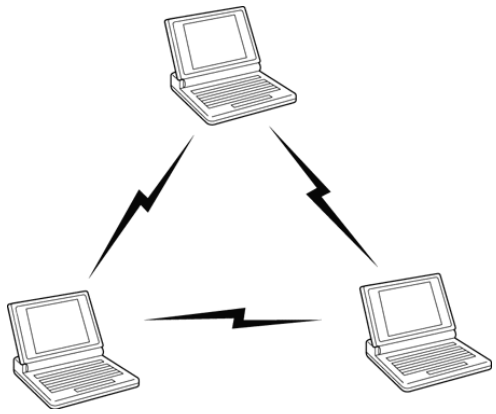

Figure 10 Ad-hoc Mode

2.3.1.2 Infrastructure Mode

Infrastructure mode represents a network mode where a dedicated device will act as an intermediate for communication between other devices in the network. It was designed to cope with the demerits of Ad hoc mode. It has capacity to deal with security and scalability issues. In this mode, each client connects to Access Point (AP) through which they can communicate with each other. There are two types in Infrastructure mode.

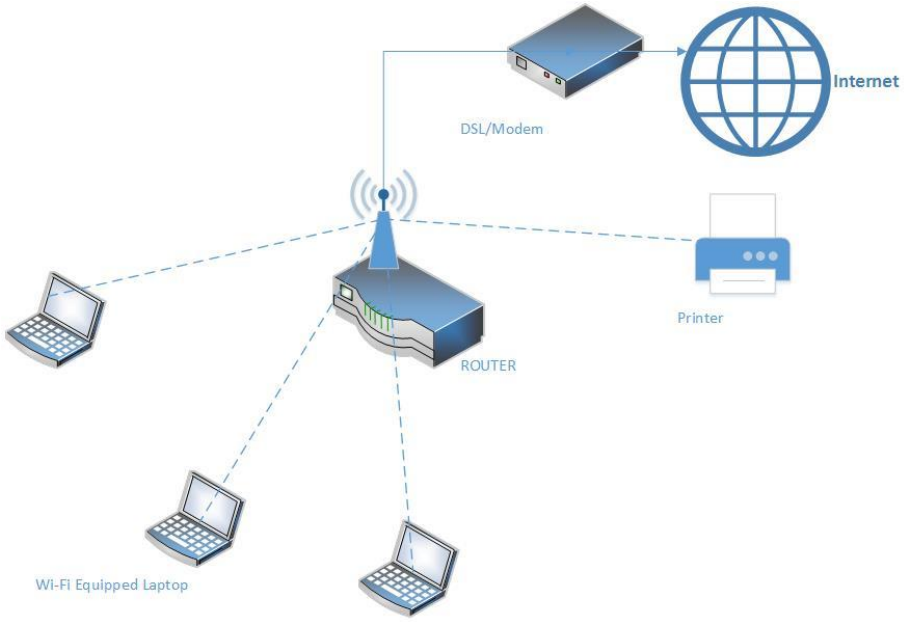

Figure 11 Infrastructure Mode

1. Basic Service Set (BSS): In this mode, all clients connect to AP, which in turn allows them to communicate with other clients or LAN based resources. The wireless network is identified by single SSID; however, each AP requires unique ID called Basic service set Identifier (BSSID), which is the MAC address of the AP's wireless card. This mode is used for wireless clients that don't roam, such as PC's.

2. Extended Service Set (ESS): In this mode, more than one BSS are connected to allow roaming distance. For convenience, same SSID is used for all the AP's so that devices like laptop, PDA and mobile see the same AP. Each AP will have unique BSSID.

2.3.2 Wi-Fi Alliance

Figure 12 Wi-Fi Certified Logo

Source: https://www.wi-fi.org/

"Wi-Fi Certified" is an internationally recognized seal of approval for products indicating that they have met the industry agreed standard for interoperability, security and range of application specific protocols. Wi-Fi certified products must undergo rigorous testing by one of the independent authorized test laboratories. When a product successfully passes the testing, the manufacturer or vendor is granted the right to use the Wi-Fi Certified logo. Certification means that a product has been tested in numerous configurations with a diverse sampling of other devices to validate interoperability with other Wi-Fi Certified equipment operating in same frequency band. Certification is available for wide range of consumer, enterprise and operator specific products including smartphones, appliances, computers and peripherals, networking infrastructure and consumer electronics. At retail, the Wi-Fi Certified logo gives consumers confidence that a product will deliver a good user experience. A company must be a member of Wi-Fi alliance to have its products tested for certification and use Wi-Fi CERTIFIED logo and associate trademarks. (Wi-Fi Alliance 2017)

2.3.3 Wi-Fi Service Set Identifier (SSID)

While configuring any access point with extended service set (ESS), each AP should be configured with same service set identifier (SSID) to support roaming function. SSID are nothing but name given to the access point. SSID is the unique name shared among all devices on the same wireless network. In public places, SSID is set on the AP and broadcasts to all the wireless devices in range. SSIDs are case sensitive text strings and have a maximum length of 32 characters. SSID is also the minimum requirement for a WLAN to operate.

Figure 13 List of SSID's

Most manufacturers of APs set some default SSID for their device which can be changed later. For security reasons, some of the AP's SSID broadcast may be blocked by Administrator but it is the requirement for any AP to broadcast SSID before any user can connect to that AP.

2.3.4 Wi-Fi Security

When new installation of Wi-Fi is done and settings are left as it is, these devices are not secured at all. We must enable Admin password for routers and encryption for Wi-Fi access points to ward off possible intrusion. If these basic features are not enabled then several problems arise from slow internet access to data loss. Low security features in routers are very severe problem that can later create big problems. So, applying all security measures available in Wi-Fi router as well as from other means is what network administrator should do. If your internet and Wi-Fi is setup by internet service provider (ISP) then they usually enable all security features but if you are responsible for all the setup then you should be very serious on this matter. Some of the security concerns that every Wi-Fi users should know are listed below.

1. Always change the default settings of the router and change Administrator password.
2. Always enable security encryption of Wi-Fi. Never let open network access to your network.
3. Always set the high security encryption in your Wi-Fi router. Encryption like WEP isn't secured, so use more secured encryption like WPA/WPA2.
4. Offer separate Wi-Fi with minimum access for guest users.
5. Physical security of the Wi-Fi devices is also important. Secure all networking devices in cabinet of lock in case of AP's.

6. Having proper door and entrance security as well as configuration authority of Wi-Fi settings is also important.
7. Use VPN for users outside physical network boundary.

2.3.5 Wi-Fi Security Problems and Mitigations

The main problem with wireless network is its simplified access. Anyone with password can access the network easily and anyone might enter network by breaking password. With ethernet one must physically be there in place to access the network but in Wi-Fi anyone within the network can access the network. The hacker who has access to the target network can perform several attacks like DNS spoofing, DDoS attack etc. Below are some of the list of problems and mitigation process:

1. Insufficient Policies

   First, every network administrator should develop a policy to use Wi-Fi network. These policies need to be circulated to the employees and they should use Wi-Fi following these policies.

2. Training

   Even though every organization has Wi-Fi nowadays, they rarely hold any training sessions for using Wi-Fi and various concerns associated with it.

3. Rough Access point

   It has been seen that even when organization provides Wi-Fi access to its employee they make their own access points that interfere with frequencies Wi-Fi is working on and creates unwanted issues. These unnecessary access points should be removed from the network.

4. Eavesdropping

   Even though unauthorized users cannot access the Wi-Fi network but they can monitor the Wi-Fi traffic and alter the data and sequence of data to gain access or to disturb the network. For this reason, elevated level of encryptions should be used.

5. Monitoring

   It is always a clever idea to monitor network for data transfer and performance on individual access point and traffic to and from internet.

6. VPN

   If you are frequent traveler and use Wi-Fi a lot, then it is important to use VPN every time you connect to public and institutional Wi-Fi.

7. Hacker Attacks

   Even with high security Wi-Fi networks are prone to attacks from hackers such as identity theft, spreading viruses, data extraction without detection etc. For this reason, implement network based intrusion detection system and network based antivirus system.

8. Geo-Fencing

   It is a process in which Wi-Fi signals are prohibited to go outside the confined space by physically obstructing the signal from travelling outside. Even though realizable it will be very costly for any organization to implement this physically. Sometimes it may not be practical to do it because Wi-Fi signal can travel from any hollow space like door and window making practically impossible to attain 100% security. (Sheth, Srinivasan Seshan et al. 2009)

These security concerns can be solved by using basic guidelines for using Wi-Fi network securely.

2.3.6 Wi-Fi Signal Distortion

There are several factors influencing the Wi-Fi signal capacity and performance. As we all know signals get attenuated as far as they reach, Wi-Fi signal cannot be exceptional in this case. The main factors influencing the Wi-Fi signal distortion are

1. Wi-Fi signal Absorption

Physical infrastructure like walls, ceilings and floors absorb RF signal waves which has direct effect on Wi-Fi signal propagation.

2. Wi-Fi Signal Reflection

Objects like glass and steel reflects RF waves that adversely affects Wi-Fi signals.

3. Scattered Objects

Objects lying scattered in the floor and in walls disperse the RF waves from its path which in-turn deteriorate Wi-Fi signal.

4. Interference

Various devices including other Wi-Fi routers working in 2.4GHz and 5GHz can produce significant frequency that will interfere with the Wi-Fi signal which will result in deteriorated performance of Wi-Fi router. Industrial equipment and microwaves also produce significant interference to Wi-Fi signals.

5. Environment

Typically, Wi-Fi routers and Antennas are expected to work in normal environment but if the Wi-Fi is setup in different or extreme environment like extreme heat or moisture then its performance will deteriorate.

(Wireless ethernet for industrial applications. 2006)

2.3.7 2.4GHz Vs 5GHz

In 1989, FCC authorized commercial use of 2.4GHz and 5GHz. After these two bands were commercialized 2.4GHz with capacity of 2Mbps was sufficient at that time. With the development of technology and performance it was upgraded to 11 and then to 54Mbps. In 1999 5GHz band was used for 802.11a and 802.11b which had the capacity of 54Mbps which was more than required at the time.

The fundamental difference between 2.4GHz and 5GHz which determines its usage as well are as follows:

1. Coverage: 2.4GHz band provides coverage at a longer range but transmits data at slower speeds. The 5GHz band provides less coverage but transmits data at faster speeds. The range is lower in 5GHz band because higher frequencies cannot penetrate solid objects, such as walls and floors, as efficiently as 2.4 GHz. However higher frequencies allow data to be transmitted faster than lower frequencies, so the 5GHz band allows to upload and download files faster.

2. Interference: Many Wi-Fi enabled technologies and other household devices use the same 2.4GHz band, including microwaves and garage door openers. The 5GHz band tends to have less overcrowding than 2.4 GHz band because fewer devices use it and because it has 23 channels for devices to use, while 2.4GHz band has only 11 channels. If the interference is more it is better to use 5HHz band.

(Moran Joseph, 2011)

Table 2 2.4GHz vs 5GHz

Standard	Spectrum	Max rate	Lay. 3 rate	Transm.
802.11	2.4 GHz	2 Mbps	1.2 Mbps	FHSS/DSSS
802.11a	5.0 GHz	54 Mbps	32 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	6-7 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	32 Mbps	OFDM

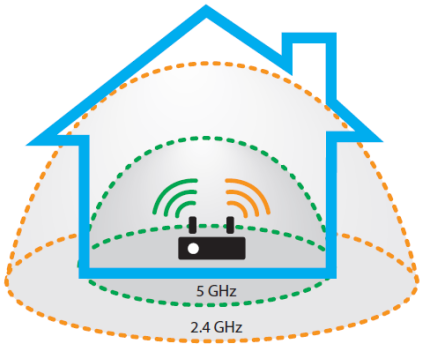

Figure 14 Coverage of 2.4 and 5GHz

2.3.8 Key sharing in Wi-Fi

About a decade ago, remembering a password was easy task as there weren't many passwords we had to remember. Now, due to advancement in information technology and authentication mechanisms it might be difficult to remember all passwords as we may need passwords for entering a door, logging into a work server, logging into a social networking site in the World Wide Web and so on. With the security threat increasing day by day, five-digit password which once was assumed secure is not allowed in many places today.

Computing power has grown by several orders of magnitude: once upon a time, eight characters were considered safe from brute force; nowadays, passwords that are truly safe from brute force and from advanced guessing attacks typically exceed the ability of ordinary users to remember. (Stajano 2011)

Wireless key is also very important security element today as placing it on wrong hand may lead to problems in your network to loss of data from your network of computers or devices. Eight years ago, until the release of 802.11n there were few wireless networks and users but now each one of us has a smartphone and everybody needs Wi-Fi for connecting to the internet. This results in security concerns for all the Wi-Fi network owners. One of the main security concerns is “How to securely relay the Wi-Fi Key to genuine users?”

Early Key sharing include telling it directly to the users via voice or by text but this technique lacks confidentiality as anyone can listen or see the password. This was still most widely used mechanism for home users which was reflected in the survey we did with LOAS’s users. The result of the survey is shown below.

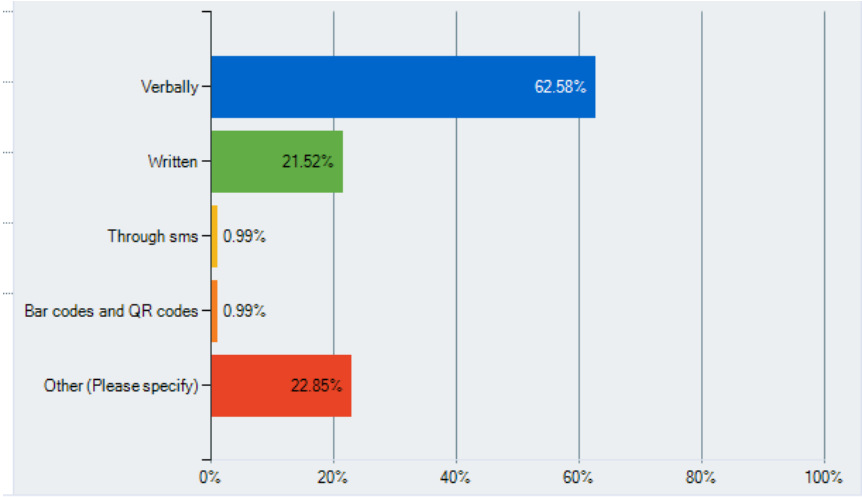

Figure 15 Wi-Fi key sharing mechanism in LOAS

Although very popular, verbal and written mechanisms are not secure mechanisms.
Some other methods of key sharing are:

2.3.8.1 Quick Response (QR) Code

Quick response (QR) codes are matrix codes like bar codes that contain certain information in the form of graphical representation. These codes are easily readable by majority of the smartphones using freely available and downloadable applications. QR codes can contain different information in the form of picture including numbers and text which make it suitable for coding Wi-Fi password. Currently QR codes are used all over the world in libraries, supermarkets to link information related to books and products. One difficulty related to using QR codes for password sharing is QR code reader application shows the passwords only but

doesn’t authenticate with the router which makes it difficult to use as full authentication system. This problem can be solved by developing application that can do this authentication.

Figure 16 Using QR code for Wi-Fi

2.3.8.2 Radio Frequency Identification (RFID)

Radio frequency identification or RFID represents a system where electromagnetic field is used to automate the identification and tracking of objects. This system consists of two parts

1. RFID tag
2. RFID reader

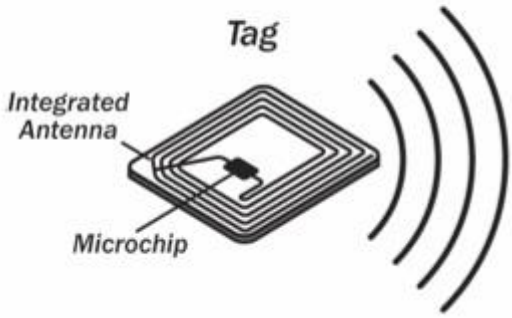

Figure 17 RFID

RFID tags contain electromagnetically stored information. RFID reader has the capacity to read the data stored in RFID tags. RFID tags can be passive or active. Passive tags don’t have their energy source so they take energy from RFID reader and can work only when they are close whereas active tags have their own power supply and can operate at hundreds of meters away from RFID reader. Unlike bar-code or QR code both devices need not be in line of sight for RFID. Passive RFID tags primarily operate at three frequency ranges:

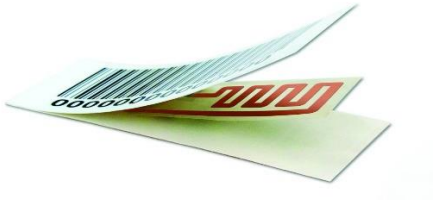

Figure 18 RFID inside bar-code used in tracking systems

Source: http://cdn.idplate.com/images/standard-RFID-tags.jpg

- Low Frequency (LF) 125 -134 kHz
- High Frequency (HF)13.56 MHz
- Ultra-High Frequency (UHF) 856 MHz to 960 MHz

Figure 19 RFID Key

Source: https://shop.cie-group.com/media/prod_images_nodel/9134174_img1.jpg

RFID are widely used in super markets since it can be attached to clothes, objects and valuable goods or even implanted for extremely valuable possessions. With the development of RFID automated shipping and automated identification has grown rapidly. RFID is expected to grow rapidly in next few years.

RFID can be used in Wi-Fi authentication in the same way as QR but we don't need to be too close or focus our camera on QR codes, after getting close enough for RFID reader to detect mobile device it will be authenticated automatically.

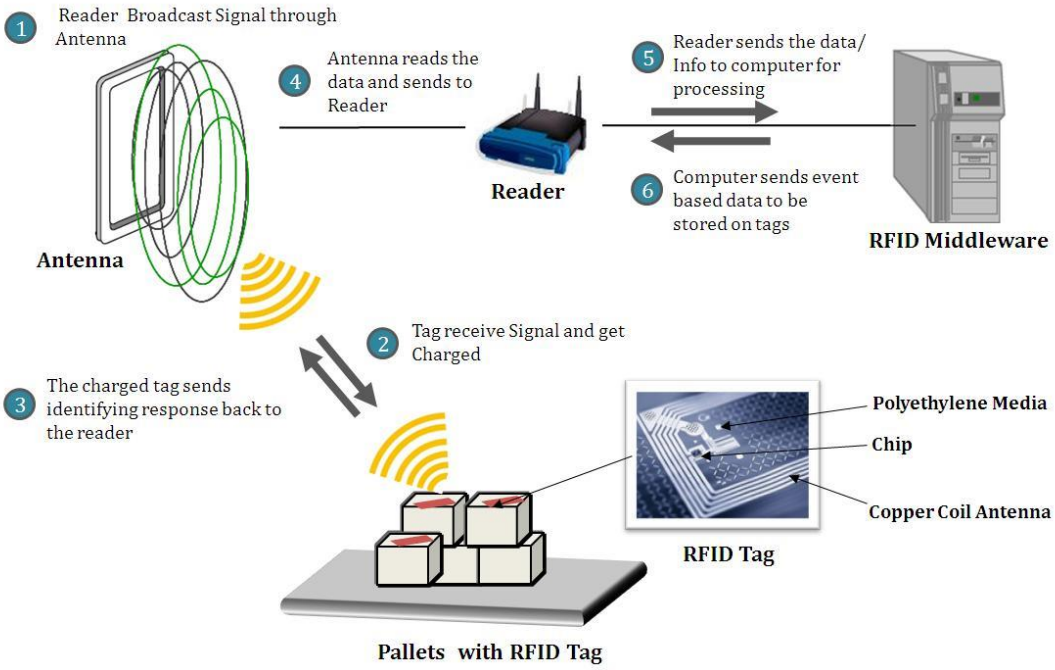

Figure 20 How RFID works

Source: http://1.bp.blogspot.com /RFID.jpg

2.3.8.3 Near field communication (NFC)

Near field communication(NFC) is a set of communication protocols used in electronics communication that enable portable device to communicate with another device by bringing them close to each other. NFC is a set of standards for smartphones and portable devices to establish radio communication with each other by bringing them near to each other. Near-field communication devices operate at the same frequency (13.56 MHz) as HF RFID readers and tags. The standards and protocols of the NFC format is based on RFID standards

Figure 21 NFC Tag

We can use this technology by allowing users to connect to the Wi-Fi by bringing their NFC enabled smartphones near the NFC tag. When tag is brought near to smartphone it will perform Wi-Fi authentication automatically so that users don't have to type any password for Wi-Fi authentication.

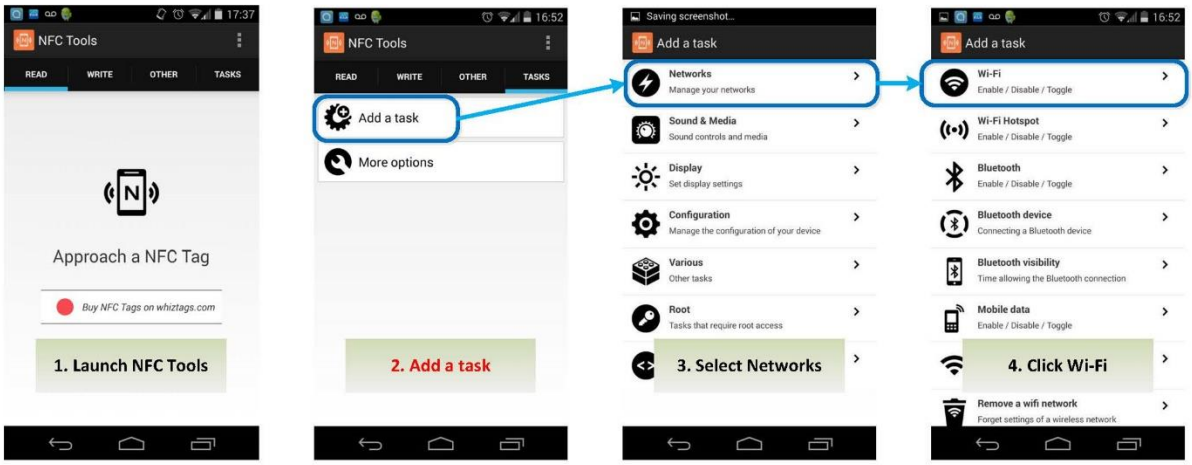

Figure 22 Writing into NFC tag

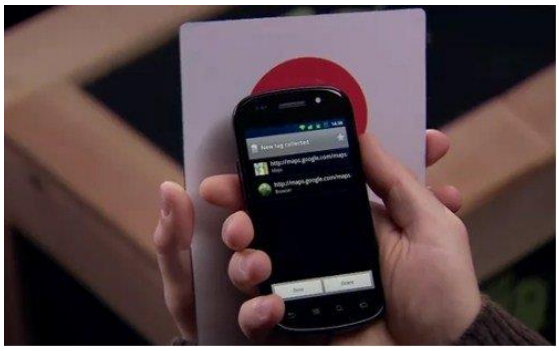

Figure 23 Reading Tag

Source: http://eezone.co.uk/wp-content/uploads/2014/09/NFC_WIFI_1.jpg

2.3.9 Ideal Password sharing system

As Wi-Fi is used in confined area and the password is used to authenticate users in that space. While these passwords are useless after leaving the area, we need to find some mechanism where user simply can connect to the network when he is within the Wi-Fi range and it is discarded once he is out from that area and will need a new one to login again. Password should be shared in a way such that:

- Eligible users easily get access without hassle
- Intruders don't pass through SSID
- Nothing can be done remotely

So, we have three scenarios:

1. User outside Wi-Fi zone: we don't have to care about these users
2. Users trying to connect/ users at Wi-Fi border: These users will try to connect
3. Users connected: we don't have to care about these as they are already connected

Users trying to connect are either new user or old users. For old users, we must have some mechanism to give new password based on some criteria and for new users we have to give them new password and verify that they are eligible to use the network. One unchangeable field for every user is their mac address. We can use this field as a method to authenticate users.

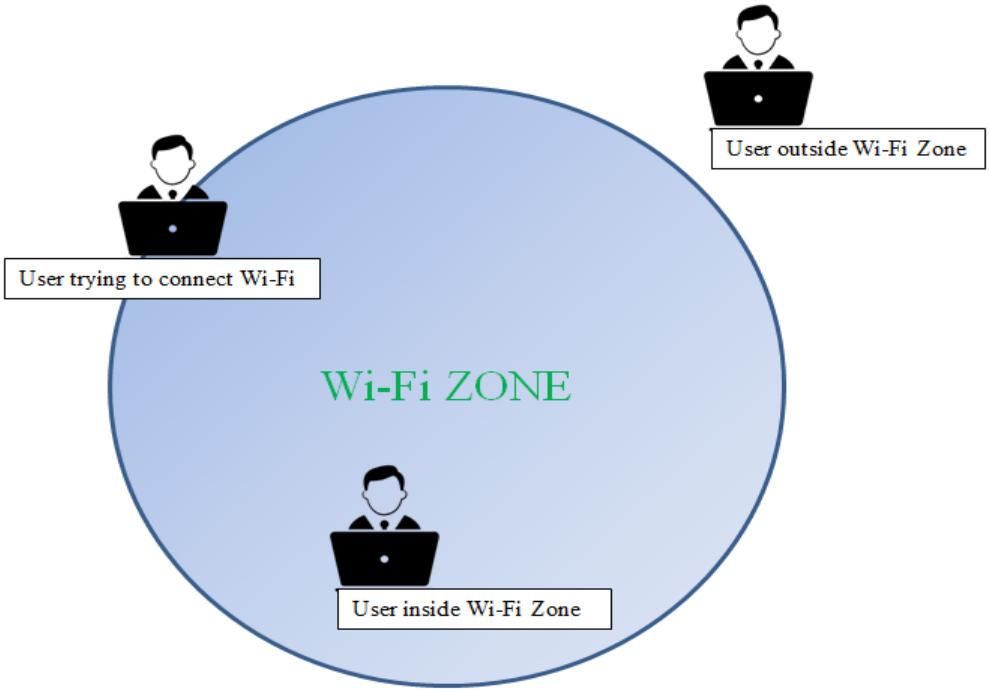

Figure 24 Wi-Fi users

Our ideal system will consist of:

- Wireless User
- Access point
- Router
- Eduroam RADIUS server
- LNET Wi-Fi authentication server

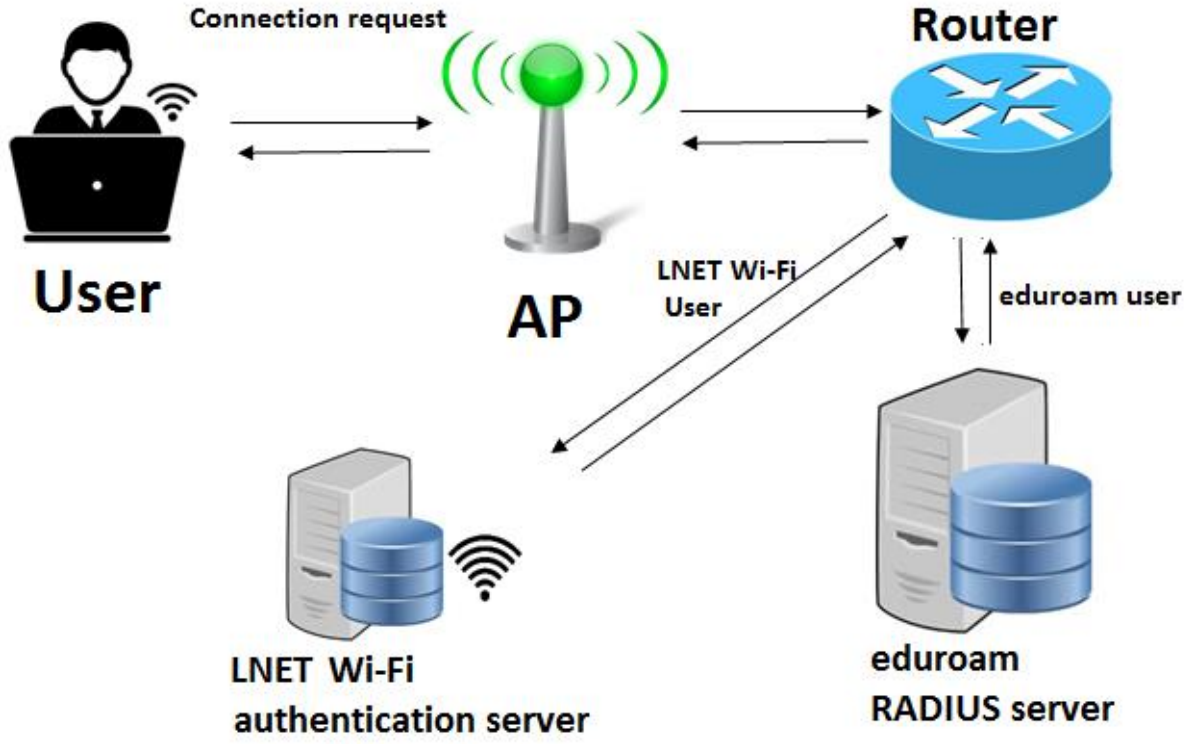

Figure 25 Ideal system

Wireless User could be any Wi-Fi capable devices that can send request for authentication. AP is the access point installed in the premises for Wi-Fi network. Routers are the network devices that route the access request to either RADIUS server for eduroam authentication or towards LNET Wi-Fi Authentication server.

When user tries to connect to Wi-Fi he will select the SSID and press connect.

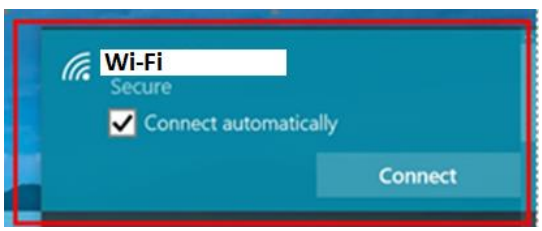

Figure 26 Wi-Fi prompt

This will initiate the authentication mechanism where the following information will be used to authenticate user:

1. Device name
2. MAC Address
3. Username
4. Password

When authenticating a user, its data will be matched against the database, which will be stored in LNET Wi-Fi user authentication server. The data in this server will be updated as new user get registered or when authenticated user registers another device in the network. For implementing this part, we can use any free or paid RADIUSserver. Some of the servers are:

1. ClearBox
2. Elektron
3. Windows Server NPS
4. Free RADIUS

After authentication, user will acquire IP address and lease time of 24 hours. At the same time, he will get an email with login details notifying him of login. After 24 hours is passed, he will need to authenticate again with same username and password. This way a profile of the user will be created in server.

If a user who has profile in server needs to provide access to another user he will simply allow other user access to the network in his profile by which he can connect without any other prompt except his username and password. Example interface is shown below.

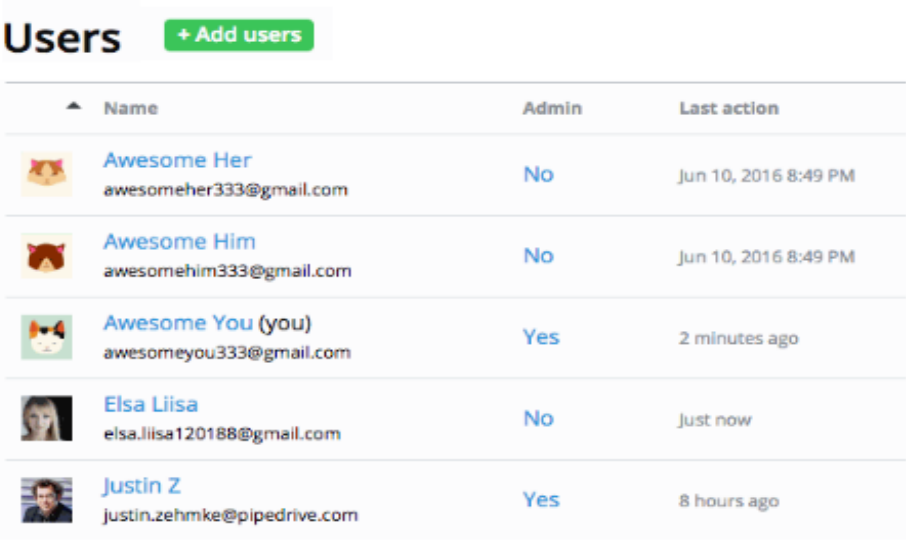

Figure 27 Profile interface example

This implementation is answer to our research question "***RQ 5: How can we share Wi-Fi key securely?".***

The flow chart for authentication process is a s follows:

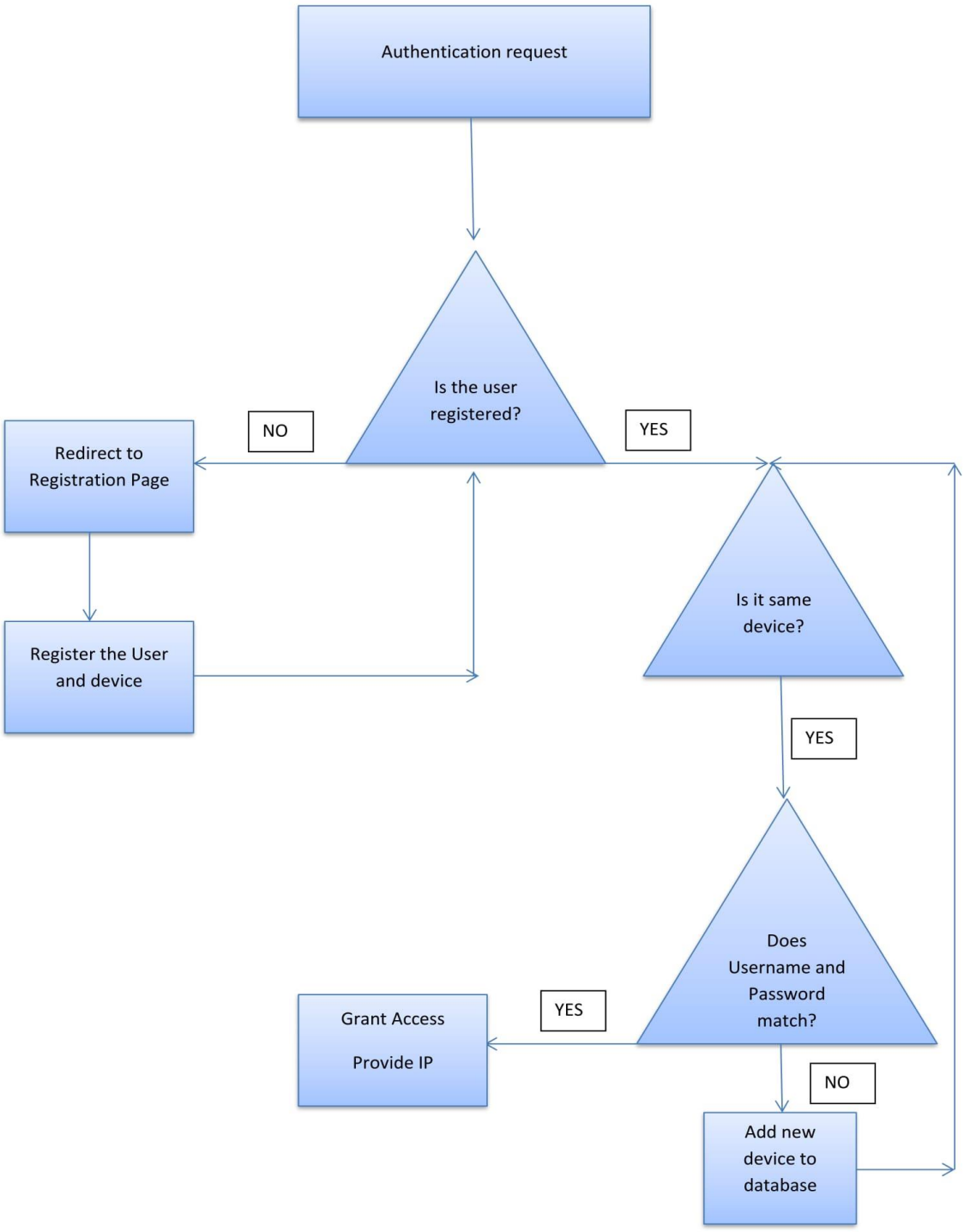

Figure 28 Device registration and update flowchart

3 RESEARCH PROCESS

As an output of the research we need to determine new smart services that can be implemented in the current network. For this purpose, we need to select proper research methodology as it is very important for investigating the research questions in hand. Proper selection of research methodology greatly improves output of the research and data representation.

In our thesis, we need to find the current trend of network usages by the students in LOAS's apartments and based on that result suggest future services for LOAS's tenants. We will use qualitative method for our research. In this chapter, we will discuss the research method, why and how we will use it for our thesis. At last we will discuss the reliability and validity of our research.

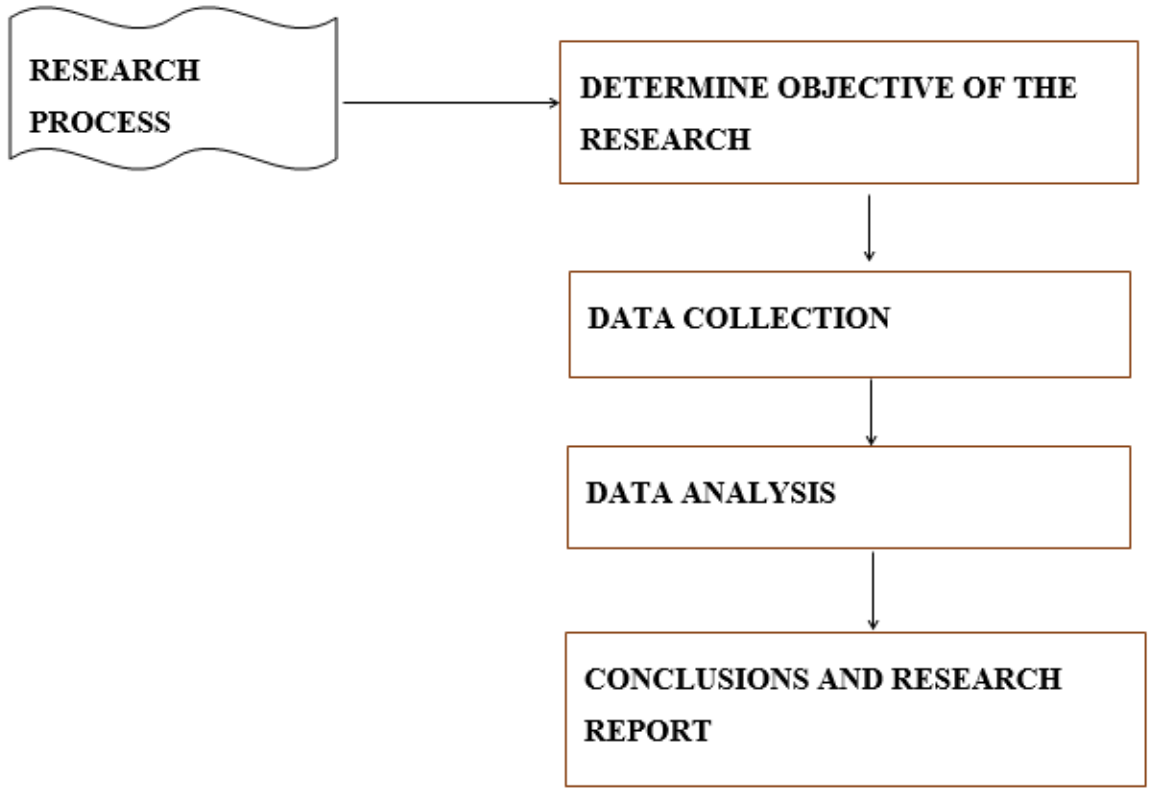

Figure 29 Research process

3.1 Qualitative research

Qualitative research is exploratory research which is primarily used to gain understanding of underlying reasons, opinions and motivations. It helps to develop ideas or hypothesis that can provide proper understanding of the problem. It can also help understand trends in data, opinions and thoughts that can help us dig deeper into the research question. Data collection method for qualitative research can vary from unstructured to semi-structured technique. Mostly used data collection method for qualitative method includes group discussions, individual interviews and participation or observations. The sample size for qualitative method is typically small. In our research, we use individual interview and note taking as qualitative method for collecting data for our research.

3.1.1 Collecting data

Collection and analysis of interview for better insight plays a vital role in the overall qualitative research. We had performed interview with related questions as in questionnaire to better understand the views of the students staying in LOAS's apartments. This gave us good chance to note actual expressions and reactions of the students which we lack in online questionnaires. Collecting data from interview was a bit challenging because we cannot note the actual expressions and reactions of the person but we took notes of the answers given by the interviewee.

3.1.2 Tape recording

The method in which interview contents are recorded plays a vital role in the data collection. Many methods are available to record the conversations with its pros and cons. Here we list some methods that are convenient and useful.

- Record the entire interview in audio and then convert it into text format. The text will be our data to be analyzed.

- Tape record the interview and take notes simultaneously. Review the tape and notes later and Tape record the interview and take notes at the same time. Later review the tape and notes as data.

- Only take notes during the interview.

For our purpose and research, we considered only taking notes as some of the interviewers didn't feel comfortable to being recorded. It turns out that interviewing with notetaking is not as easy as we thought. It becomes difficult to focus on what the person is saying if our attention is towards notetaking and we could barely note the expressions of the person if we are looking at the notes.

3.1.3 Taking notes

Taking notes is very important skills for any researcher. Taking good notes, which are clear to the reader and easily understandable is sometimes skill that comes naturally for some person but for some it is difficult to excel in. With clarity of handwriting one should also be able to write fast. Hearing the interviewee well and getting the meaning of what the person is saying is also crucial. Note taking are the basic skill on which our analysis will later depend on. For making a good note we can consider following points.

- Try to standardize what will be recorded as note.
- Divide the whole information into parts like demographic information, main data, extra information etc.
- Store the notes in standard way like filing, binding etc.

3.1.4 Analyzing qualitative data

The most critical part of the qualitative research is analysis. Analysis is done on the data collected by interview and notetaking. Daily interpretive analysis (DIA) is the process of collecting and interpreting the interview and note taken data to generate some knowledge out of it. Each day when the interview and notetaking is done for some people one of the members of research team should review all the notes and interview of that day.

In my thesis, I collected data in the form of recordings for some of the respondents and most of the respondent's interview was converted into note taking format where each respondents answer was noted in a paper. To make the note as understandable as possible later we had taken short notes and exact answer given by respondents on questions prepared for interview. This will help to construct conclusions later because exact response of the interviewee and his expressions may diminish as time passes during the research process.

Also, the method of making conclusions out of listening to recordings and looking at the notes may not be as reliable as we thought because we cannot recreate the actual knowledge that we gained while talking with the people by reading or listening to recording and notes. There is high possibility of missing a point interviewee had given during the interview. For the interview, we will analyze the data in following three steps

1. Record and Notetaking
2. Analyzing record and notetaking
3. Drawing conclusions

As many of the respondents disagreed with recording the interview, we had to process interview based on the notetaking that was done during the interview. These notes will act as raw data for the final report. The report must be clear enough that the reader can fully understand what the writer is trying to convey.

The sample of the notetaking is shown in Appendix 1.

First, the introduction part of the interview where we asked demographic information of all the respondents were filled by interviewee and then the questions related to network services from LOAS were asked one by one. We conducted the interview of 20 LOAS tenants from various apartment locations and pursuing different degrees in Lappeenranta University of Technology. We also try to include people from different countries so that we could validate the data based on variation of nationality, location and degree. Then we divided the whole interview in five sections. We will try to analyze each section separately. The five sections are

a. Services: In this section, we try to find out the experience of the LOAS's tenants during the use of LNET.
b. Wireless: This section focuses on the Wi-Fi usage of the tenants and their attitudes towards smart devices.
c. Eduroam: this section mainly asks interviewee about the knowledge of LOAS's tenants about eduroam and how their experience was till date.
d. Security: Security section deals about security of LNET. It asks tenants if they had any security issues earlier and how they act to make their network secure.

e. Value Added Services: This section is expansion of scope of our interview as we try to get any information not covered during the interview which tenants might think is important for them. We also ask for any suggestions for LOAS.

After interview is taken from all the targeted students, analysis of the finding is done. We drew these conclusions from each of the five parts of the interview as follows.

Services

1. Out of 20 respondents 18 respondents said that their internet experience from LOAS is good. So, they are happy with the internet service.
2. Almost all respondents always stay online. Either they are using or not using internet they stay online. In most of the cases the purpose is social networking and entertainment.
3. All respondents mentioned smart phone as the only smart device they possess to connect to internet. Only few respondent mention laptops as the only device he connects to internet.
4. Respondents did mention some issues with the internet connection even though they said that the service level is good. This shows that most of the respondents regarded current level of problem occurrence as occasional and expected their network to be restored in due time. Some of the problems mentioned by interviewee are
    i. Connectivity problems
    ii. Slow connection
    iii. Interruption

Most times when faced with network issues they tend to wait for some time for service to restore and then restart their router. All tenants tend to solve problem by themselves.

Wireless

1. Out of 20 respondents 19 of them have their own Wi-Fi router and one respondent have LOAS's eduroam as he is living in Lerikatu. All respondents are satisfied with Wi-Fi service from LOAS and from their own wireless router. Few of the respondents complain with coverage of their current Wi-Fi router.

2. Most of the respondents have at least 2 devices namely laptop and mobile as Wi-Fi capable devices. Some of them have tablets and e-book. None of the respondents mentioned anything specific that they wish from Wi-Fi as a service.
3. Most of the respondents are positive about the current trend of smart devices but some are skeptical about connecting all devices to internet as it may risk personal data to hackers.

Eduroam

1. Most of the students use eduroam on daily basis. Among 20 respondents only 2 of the respondents don't use eduroam at all. They use mobile data instead. Almost all students like eduroam and its features except some complain about its coverage in some underground areas and the library area.
2. Almost all students complain about coverage in building 7 and building 4. They also mentioned that connection is slow sometimes.

Security

1. Almost all respondents mentioned that they feel secured while using internet from eduroam and LNET whilst some mentioned that they feel secure in eduroam than LNET.
2. None of the students had any issue of security till now. This is the only question in which all respondents replied the same.
3. The interval of password change in eduroam is compulsory so all students change password every 90 days when they get email from university Origo office. Wi-Fi routers password change duration varied largely from few weeks to few times a year.

Value Added Services

1. On query for any other service suggestion from LNET, most of the respondent replied they are happy with current service and don't need any other service. Some of the respondents suggested of gaming server from LNET. Few students asked to focus on coverage and speed of internet.

2. Some of the suggestions for LOAS are:
    i. Make the internet connection more reliable.
    ii. Start Wi-Fi services in apartments.
    iii. Put the LAN port in suitable positions in apartment.
    iv. Make the support more prompt.
    v. Arrange for backup connection in case main link is down.
    vi. Please put router setup instruction in website
    vii. Allocate more speed for individual user.
    viii. TV channel with LNET.
    ix. Include Wi-Fi router in Rent.
    x. Expand eduroam to all apartments

3.2 Quantitative Research

The kind of research in which we can use quantify problem into numerical value so that we can represent result into some quantity is quantitative research. We generate statistics from that data which will help in drawing conclusions based on numerical values. This will help us quantify opinions, attitudes and behaviors which can be very helpful to generalize findings. Various methods can be used in quantitative research such as online survey, paper survey, experiments etc. In our research, we have used online survey as a quantitative method of research. A quantitative research method encompasses the statistical method to design and analyze the data (Williams 2007, 66).

As our research aims to find the current service status of the LNET and determine any specific problems faced by users to find out what can be done to cope with this situation and find out different solutions for tenants with several problems and demands. Quantitative research method used in this research helps to measure, quantify and find the cluster and variance which aims to help this study obtain the accurate and specific data.

3.2.1 The Questionnaire

In our research, we used online questionnaire in the form of online questionnaire to collect data from the tenants of LOAS using LNET as their network service provider. Questionnaires are particularly useful method for investigation in following ways:

1. To access the user's needs, expectations, priorities and preferences.
2. To determine the patterns, frequency, ease and success.
3. To find user's satisfaction with services.
4. To determine shifts in user attitudes and opinions.

Online questionnaire consists of mainly six parts

a. Demographic information
b. Services
c. Wireless
d. eduroam
e. Security
f. Value added services

Questionnaire used for our online survey was developed in online survey website https://www.sogosurvey.com. The survey was then sent to all tenants of LOAS studying in Lappeenranta University of Technology via email invites. All responses were collected online during 9th Feb 2017 to 19th Feb 2017. The survey was done in English language in easily understandable form. We got a sample size of 302 which was more than what we expected to achieve. The average submitting time of questionnaire was 14 minutes. Most of the questions are closed while we also gave options for respondents to suggest something if it is not covered in questionnaire.

Table 3 Questionnaires sample

Questionnaires	
Basic info	**Questions**
	Q1. First Name
	Q2. Last Name
	Q3. Email Address
	Q3. Gender
	Q4. Address
	Q5. Degree
	Q6. Country
	Q7. When did you start studying at LUT
	Q8. Age
Services	Q1. How would you rate the current internet service (LNET) from LOAS?
	Q2. How much hours per day do you stay online for the reasons mentioned below?
	Q3. In your free time, what do you use the internet mostly for? (select all that apply)
	Q4. Which of the following devices do you own that you connect to LNET?
	Q5. In LNET, which kind of application do you use most?
	Q6. How do you solve any internet connection problem that you face?
Wi-Fi	Q1. Are you using LOAS's Wi-Fi or your own wireless router?
	Q2. What is the quality of your Wi-Fi connection you are using?
	Q3. Do you check the frequency and band for your Wi-Fi access point?
	Q4. Do you own any internet enabled smart devices other than smart phone?
	Q5. Do you share your Wi-Fi key with other roommates?
	Q6. How do you share your Wi-Fi password?
	Q7. Do you own smart TV or plan to buy one in the near future?
	Q8. In LOAS Apartment where do you use your Wi-Fi connection the most?
	Q9. If LOAS provides Wi-Fi connection to all your devices will you replace your personal Wi- Fi connection?
	Q10. How often do you have a problem with Wi-Fi Connection?
Eduroam	Q1. Do you have eduroam in your Apartment?
	Q2. Do you use eduroam sometimes to access university network or is it the primary connection method?
	Q3. What do you think about its reliability?
	Q4. Have you faced any problem with eduroam?
	Q5. Will you be willing to pay if some value-added services are provided with eduroam?
Security	Q1. Have you had any security issues with LNET or eduroam?
	Q2. Have you ever been warned about internet security issues from LNET?
	Q3. How often do you change your LNET, Wi-Fi and eduroam password?
	Q4. Mention any important security concerns if you have, while connecting to any network.
	Q5. How secure do you feel when connecting to LNET or eduroam?
	Q6. Do you check how many users are connected from your Wi-Fi connection?
	Q7. Have you ever had your Wi-Fi password compromised?

Value added services	Q1. What kind of services other than basic internet connection do you wish from LOAS's LNET/eduroam?
	Q2. Have you used any of the following devices from the list ?
	Q3. Will you subscribe to services like chrome cast, security cameras, smart TV connection etc. if they are provided on same eduroam or LOAS's Wi-Fi connection?
	Q4. Please comment what you have in mind, any questions that you had that didn't come up in questionnaire or any kind of suggestions and comments are welcome.

Before finalizing the questionnaire and sending the link to students we checked and cross checked the link and questionnaire several times and corrected several error and confusions to make the survey as simple as possible. These test answers were not included in final analysis.

3.2.2 Analyzing quantitative data

Analysis of the Quantitative data is very important part of quantitative research. Here we try to quantify our findings into numbers for better understanding of the phenomenon. Quantitative data can be analyzed in numerous ways. Quantitative analysis as a method of doing analysis depends on describing and interpreting data statistically with numbers. It includes computational and statistical methods of analysis. Analysis starts with descriptive statistics analysis phase followed by more in-depth analysis.

In our thesis, we have used questionnaire as a means of quantitative analysis. We managed to collect large sample size of 302 people which will help us make our conclusions more accurate. It is very important step in quantitative research approach to analyze, interpret and present data gained from an online questionnaire.

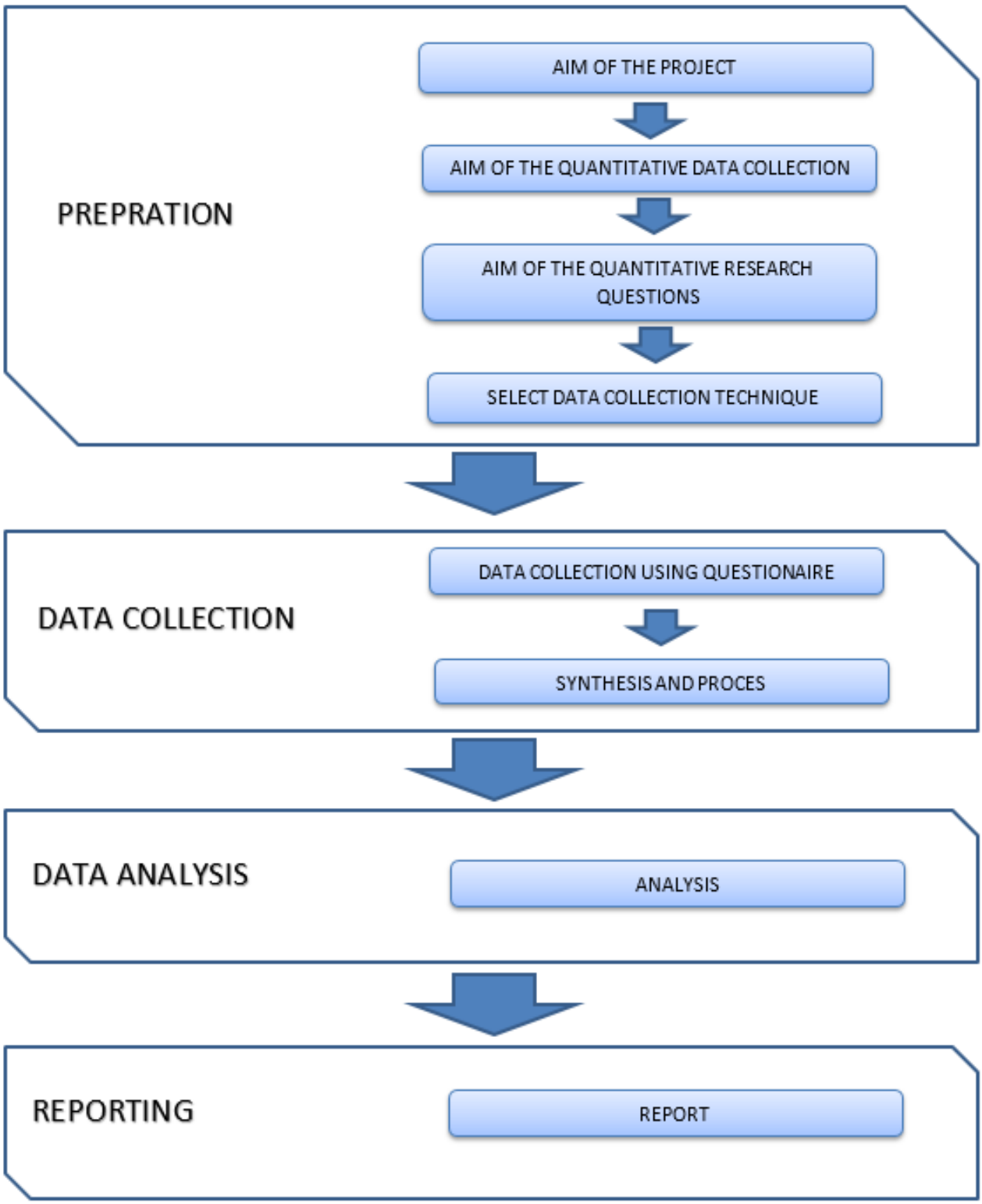

Figure 30 Quantitative research process

It is very important for any researcher to decide prior to publishing questionnaire what data types he will be using in his research. Understanding and implementing appropriate data-types determines the shape of interpretations and conclusions drawn from the analysis (Brown 2011; Denscombe 2010). Data in the questionnaire is represented by nominal, ordinal and interval data-types. In our questionnaire, we have used all the data types for different purposes.

3.3 Descriptive analysis

We used descriptive statistics for defining basic features of data collected in questionnaire. It will help us describe, show and summarize data in a meaningful way such that patterns might emerge from the data.

During data collection, many useful data were collected for analyzing users and internet usage. Many of those data are not directly related to the thesis are listed in appendix 5. So, here we have listed only those data that closely relate to our thesis.

How would you rate the current internet service from LOAS?

This shows that almost 45% of the users of LNET feel good about the quality of internet service with about 30% getting excellent service. This shows that attitudes of students toward the network service provider in general is good as per our research question "***RQ 1: What are the attitudes and behavior of students toward their connected network?".***

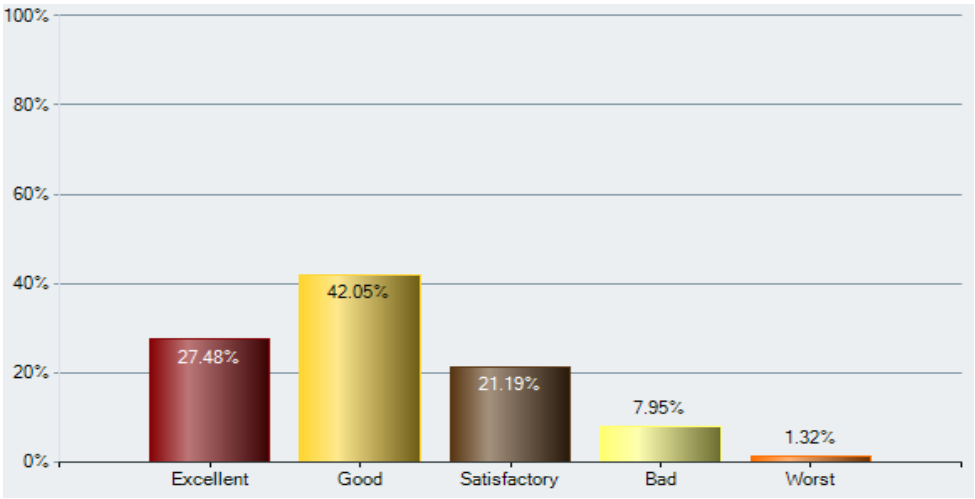

Figure 31 LNET service quality

Note: total 99.99 % is due to rounding off in software.

How much hours per day do you study online for the reasons mentioned below?

STUDY: This shows that almost 50% of the tenants spend less than 3 hours in internet for study purpose.

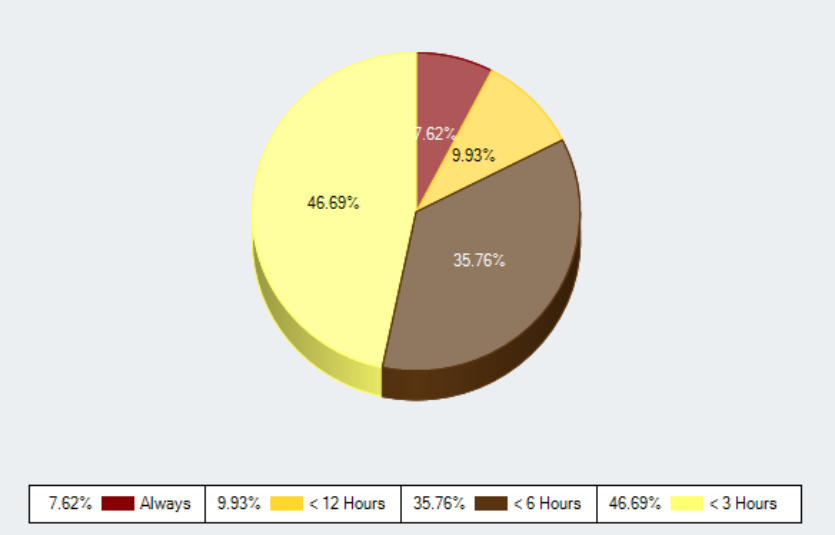

Figure 32 Hours per day - Study

GAMES: This shows that almost 80% people spend less than 3 hours in games.

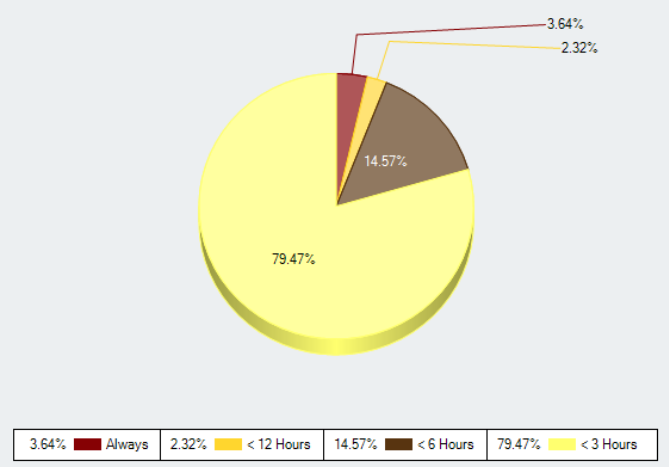

Figure 33 Hours per day - Games

SOCIAL NETWORKING: This also shows that around 65% of the people spend less than 3 hours on social networking.

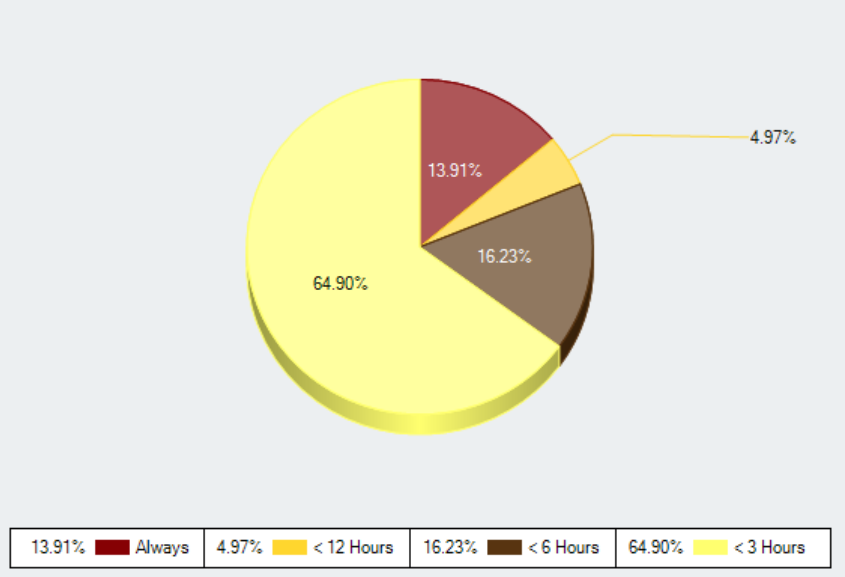

Figure 34 Hours per day - Social Network

ENTERTAINTMENT: This shows that almost 60% participants spend less than 3 hours in internet for entertainment purpose.

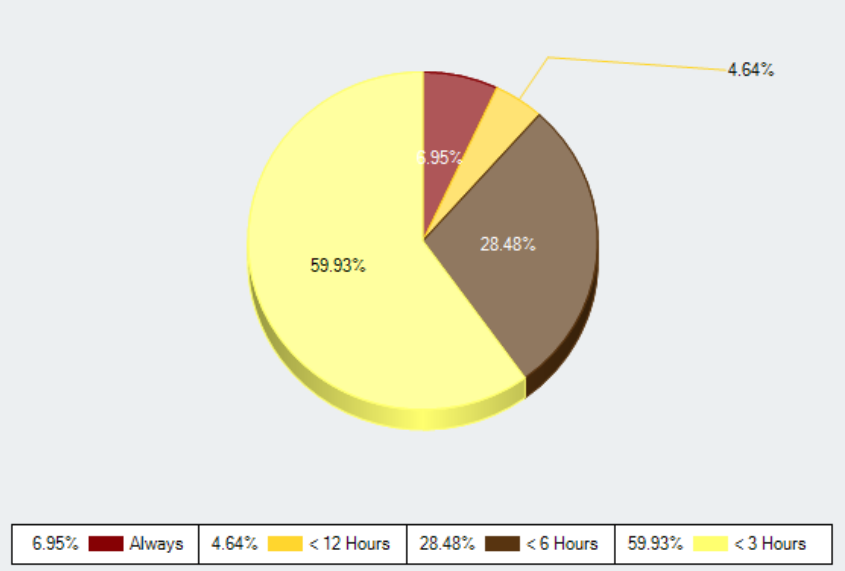

Figure 35 Hours per day - Entertainment

In your free time, what do you use the internet mostly for?

Participants use internet for various purpose during free time but as expected most of them use social networking sites and apps like Facebook, Instagram and twitter.

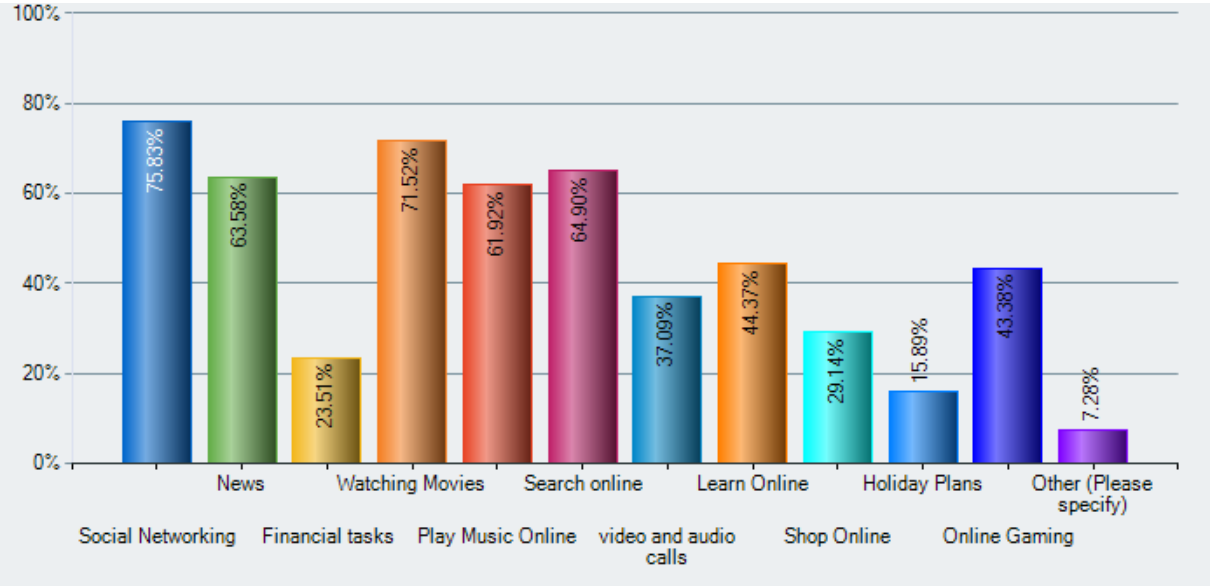

Figure 36 Uses of Internet

Which of the following devices do you own that you connect to LNET?

More than 80% of the participants use laptop as a primary device to connect the internet.

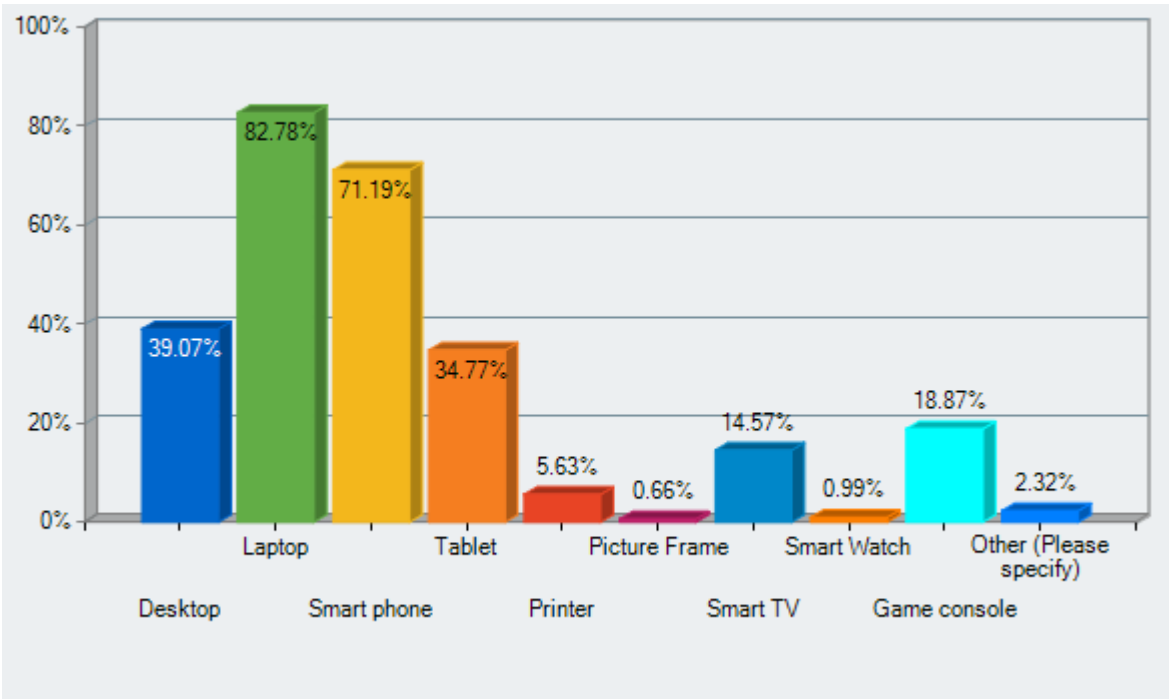

Figure 37 Devices used for Internet

How do you solve any internet connection problem that you face?

Most of the network connection problems are solved by respondent themselves.

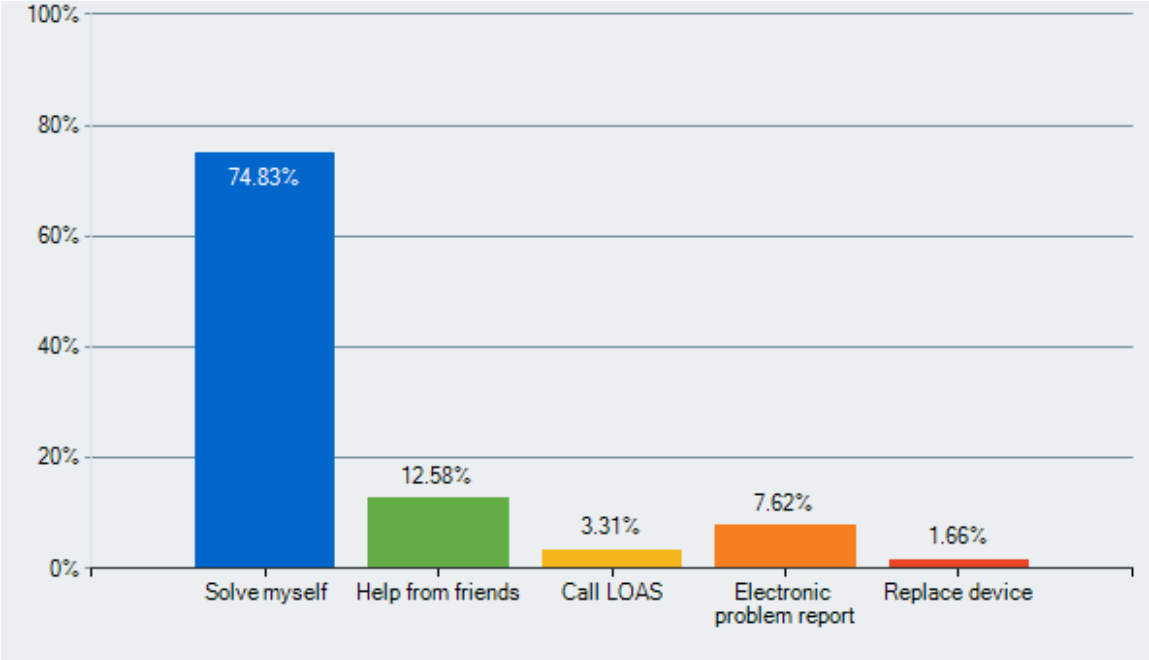

Figure 38 How do you solve your internet connection problem?

Are you using LOAS's Wi-Fi or your own wireless router?

Most of the tenants have their own wireless router.

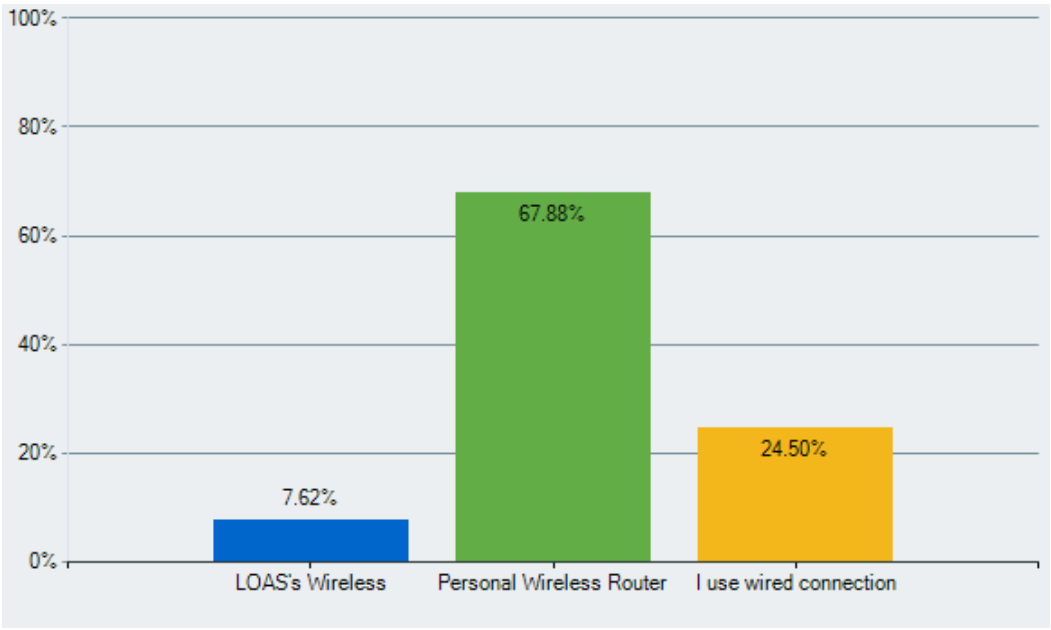

Figure 39 LOAS's Wi-fi or personal Wi-Fi?

What is the quality of your Wi-Fi connection you are using?

Around 50 % of respondents with 35 % in good and 28 % in excellent say that thay are happy with their Wi-Fi connection.

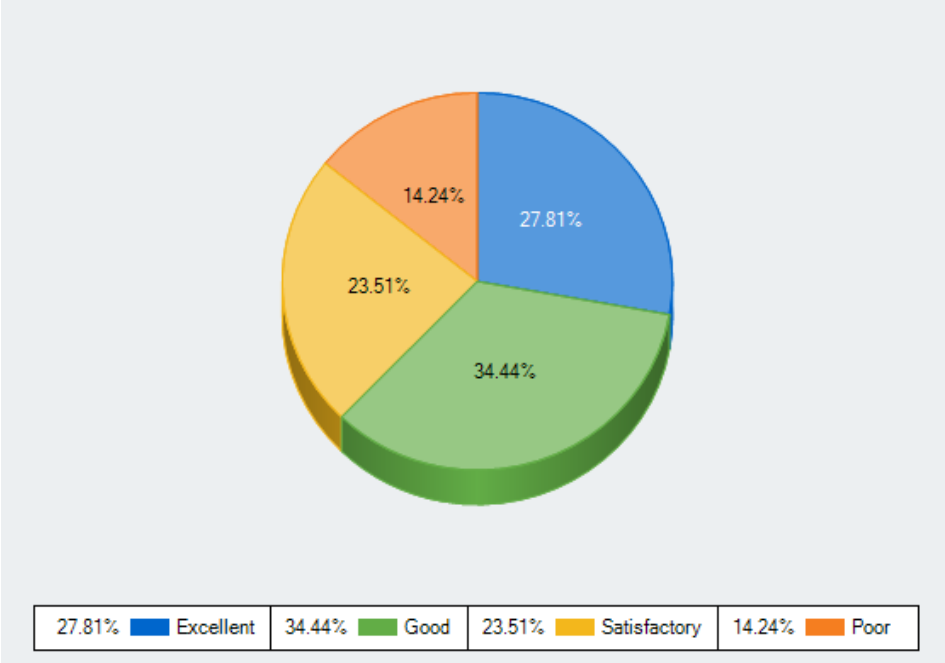

Figure 40 Quality of Wi-Fi

Do you check the frequency and band for your Wi-Fi access point?

Almost 45% of the respondents use default settings in their router.

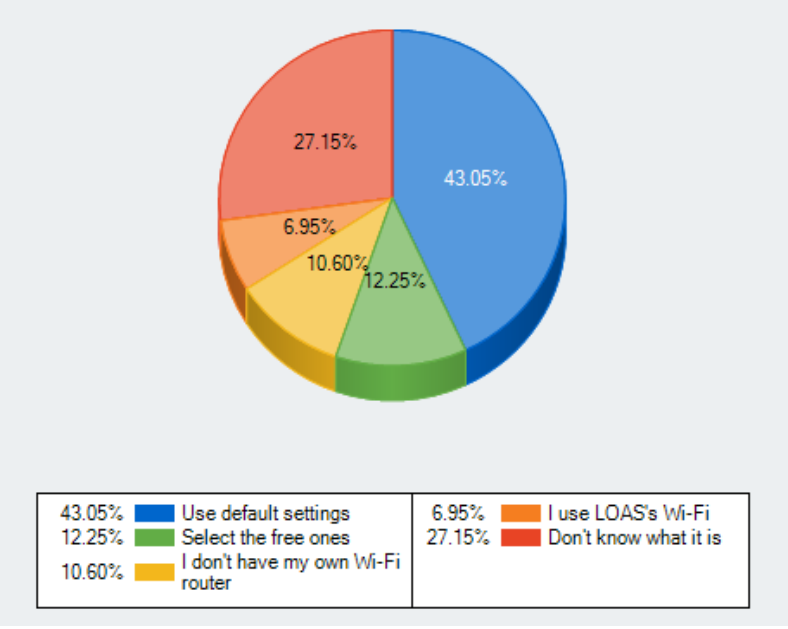

Figure 41 Frequency and band of Wi-Fi

Do you share your Wi-Fi key with other roommates?

76% of the respondent said that they share Wi-Fi connection with other roommates and friends.

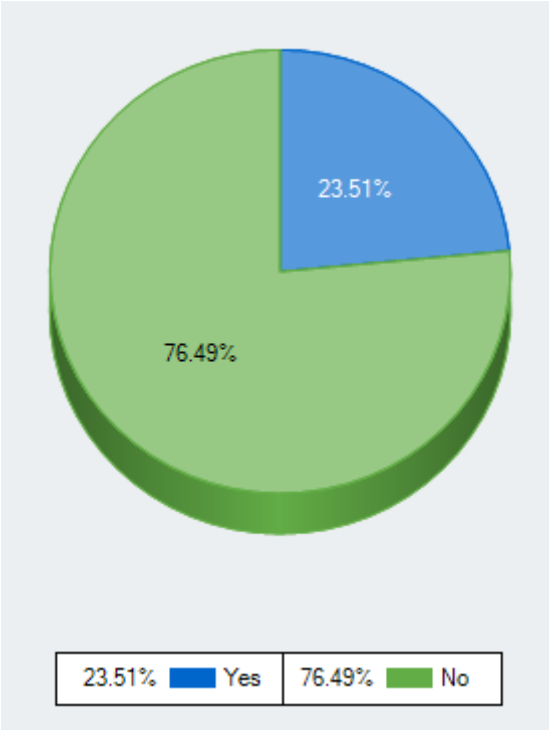

Figure 42 Wi-Fi Key

How do you share your Wi-Fi password?

Most of the users use verbal method to give Wi-Fi passwords to other friends and roommates.

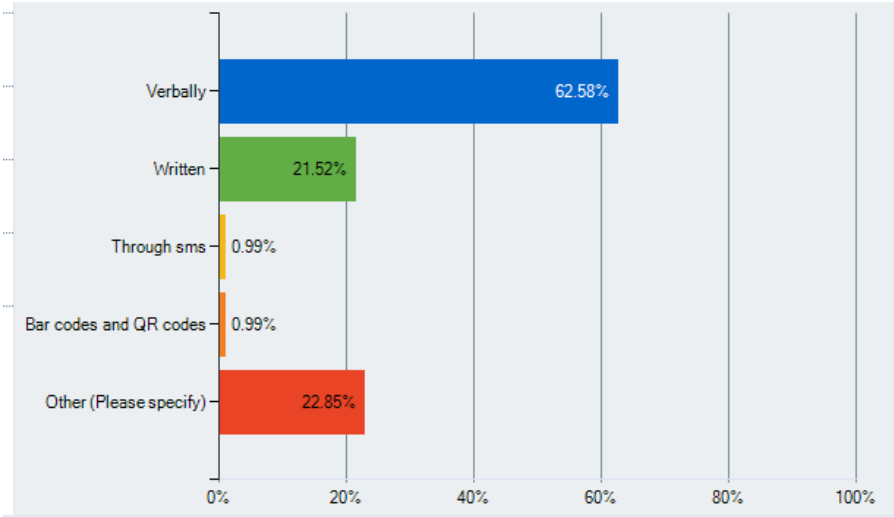

Figure 43 Wi-Fi Password

In LOAS Apartment where do you use your Wi-Fi connection the most?

Most of the tenants use internet in their room.

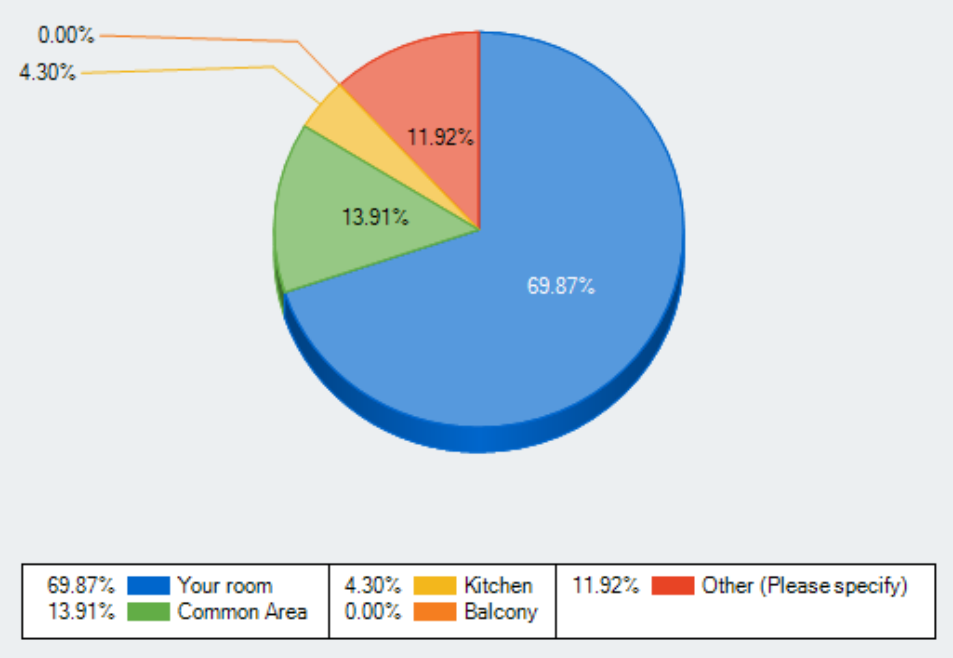

Figure 44 Where do you use Wi-Fi?

If LOAS provides Wi-Fi connection to all your devices will you replace your personal Wi-Fi connection?

More than 50% of the tenants are positive on replacing their personal Wi-Fi with LNET's Wi-Fi.

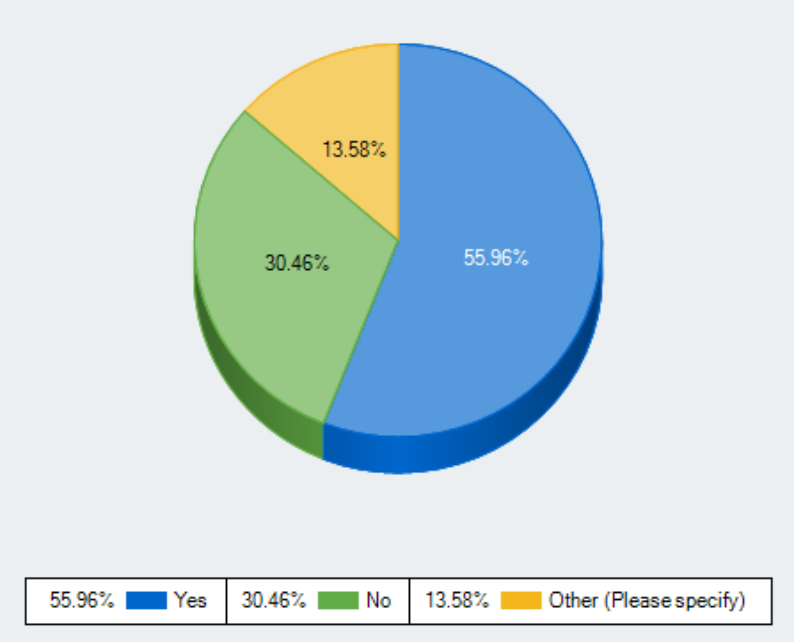

Figure 45 Will you replace your personal Wi-Fi?

How often do you have a problem with Wi-Fi Connection?

Around half of the tenants get problem sometimes with their internet connection while 34% don't have any issues at all.

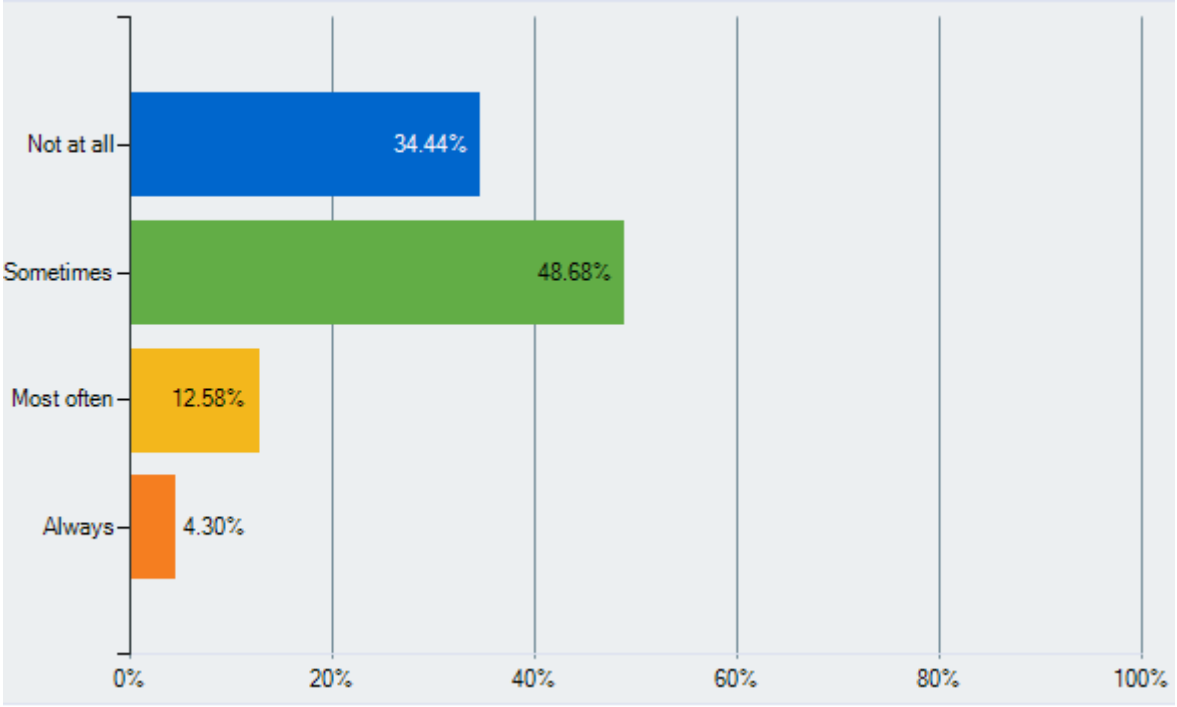

Figure 46 How often do you have Wi-Fi problem?

Do you have eduroam in your Apartment?

Very few people have eduroam access in their apartment.

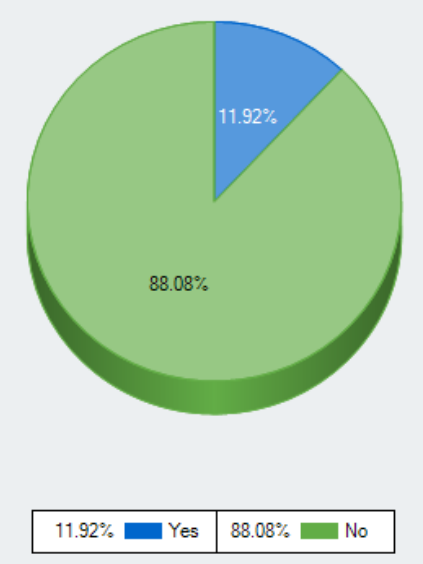

Figure 47 eduroam

Do you use eduroam sometimes to access university network or is it the primary connection method?

Most of the respondents use eduroam sometimes to access resources while one fourth of the respondents use it as primary connection method.

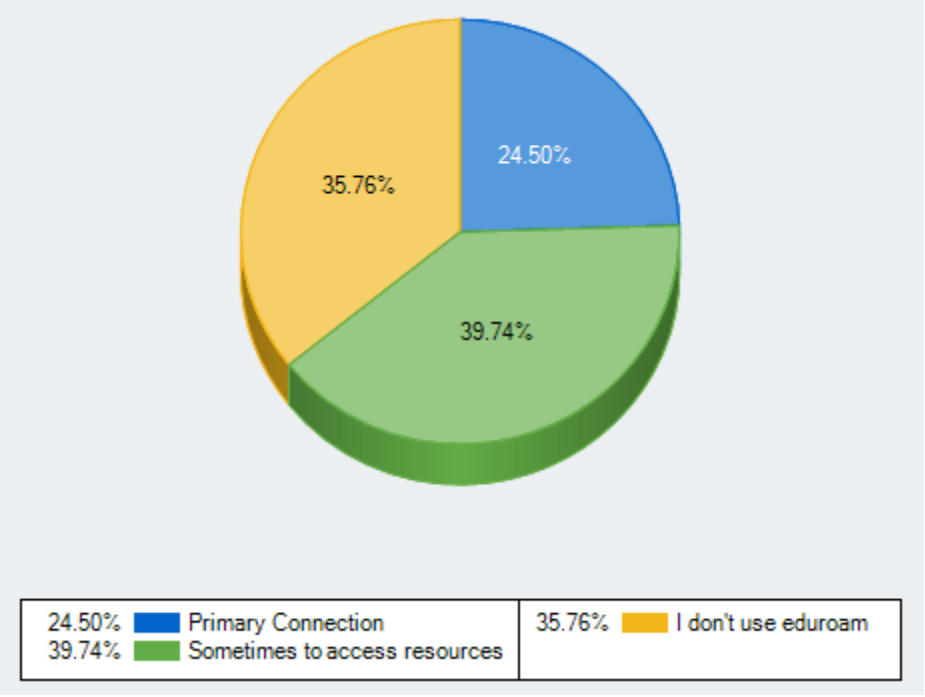

Figure 48 Is eduroam your primary connection?

What do you think about its reliability?

Very few respondents mentioned that the reliability is excellent. More than 25% don't use eduroam.

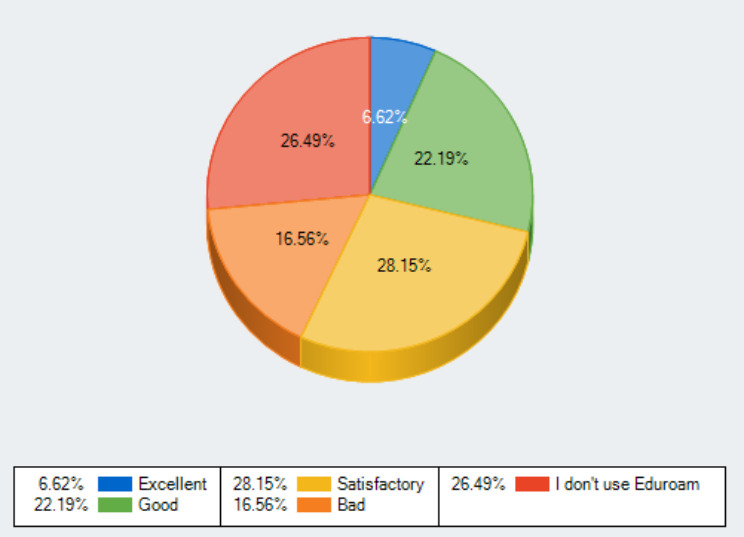

Figure 49 Reliability of eduroam

Have you faced any problem with eduroam?

Around half of the people using internet have faced problem with it sometimes using it.

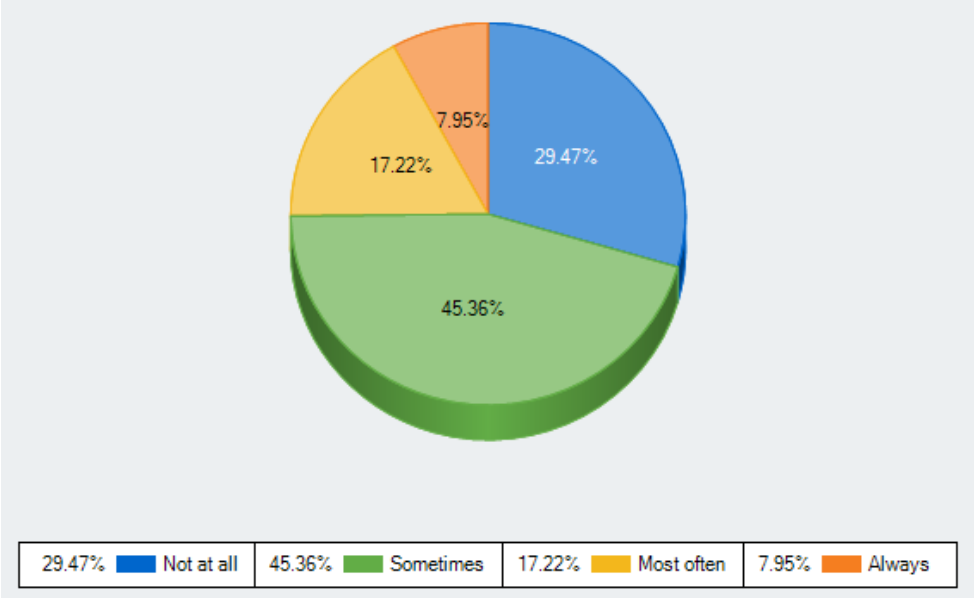

Figure 50 Have you faced any problem with eduroam?

Will you be willing to pay if some value-added services are provided with eduroam?

None of the respondents are ready to pay for any value-added service.

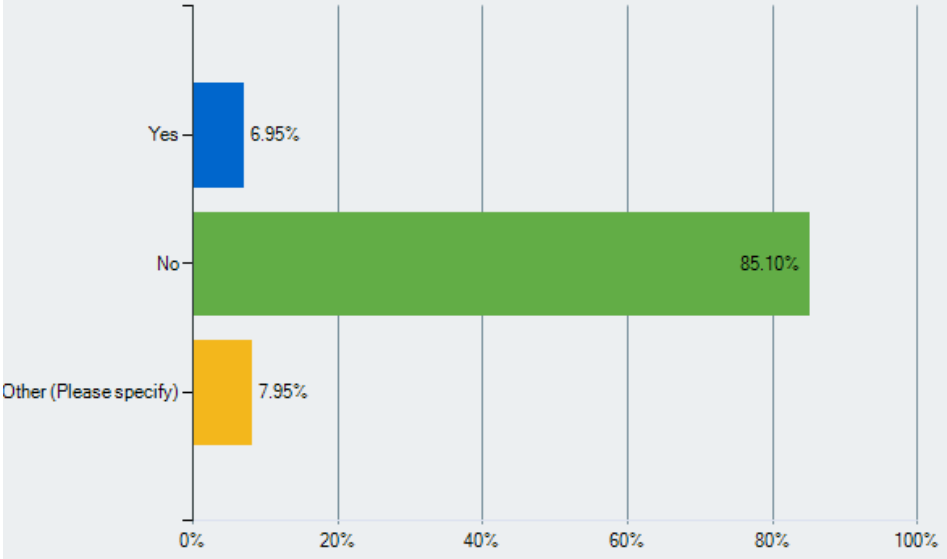

Figure 51 Value Added service

3.4 In Depth Analysis

In this section, we analyze the data collected from the questionnaire and figure out some pattern emerging from the data. Various points will be made based on the result of the questionnaires. We will also examine the data to figure out some cross relation between the data. In this section, we used descriptive analyses to obtain an overview of demographics and socio-economics information of the students staying in LOAS. In this case, our research objects were students of LUT staying in LOAS's apartments. In this research 302 responses were recorded for our sample. All the questionnaires returned were valid and without issues indicating that the questionnaire was effective.

For analysis of the texts we have used IBM's Watson text Analytics software for visualization and analysis of the data from questionnaires. Some of the conclusions made based on the data recorded from questionnaires are:

1. 72.19 % of responses are male whereas 27.81% are female. The significant difference in number may be due to actual reason that there are more male than female living in LOAS's apartment.

2. Most respondents were from Karankokatu and Ruskonlahdenkatu 13-15.
3. All respondents are either Bachelor or Master degree students.
4. Most of the respondents are from Finland and Russia. Out of 302 respondents 210 are from Finland and 27 are from Russia. Other prominent countries are Bangladesh, Nepal and India.
5. 40.07 % of the respondents started studying in 2016 and 23.18 % of the respondents started studying in 2015. So, the responses are from new students. Remaining responses are from 2008 to 2014 batch students.
6. Almost all the respondents are between the ages of 18-25.
7. Most of the users of the internet from LOAS think that the quality of internet is good followed by excellent and satisfactory. This means that internet service from LOAS has met the requirements of students but they need to improve their service quality and delivery for some uses.
8. Most of the students spend less than 3 hours per day in activities like studying, games, social networking and entertainment. These activities are not fixed in time so they may access internet for mentioned activities at any time so their experience depends on how network was performing at that moment.
9. In free time, most of the students use internet for social networking, watching movies, news, listening to music and searching online. Except watching movies all the other activities are not bandwidth consuming which guides to conclusion that we need to make the services more reliable than faster.
10. 82.78 % of the users connect laptop to the internet so we can assume laptop as primary device that connects to internet. Others include smart phone 71.19%, desktops 39.07% and Tablets 34.77%. Some of the students do have smart TV and Game consoles which we can predict will increase in future.
11. With almost 80%, Web browsing and email are the primary activities that students do in internet.
12. The study shows that almost all internet connection related problem is solved by students themselves.

13. 67.88% of the respondents say that they have their own Wi-Fi router. We can say that Wi-Fi is primary means of internet connection for vast number of LOAS's tenants. This shows that we need to develop a secure and high-performance Wi-Fi network for LOAS tenants.
14. When asked about the quality of Wi-Fi connection the answer is diverse from Excellent-27.81%, good-34.44%, satisfactory-23.51% and poor 14.24%. So, we can say that out of 302 respondents each tenant has different expectations from LOAS's internet. Only 50% of the people say that they are happy with the service.
15. Almost all the users of Wi-Fi don't change the security setting of their router. This brings us to the conclusion that security is in critical status in LNET.
16. Most of the LOAS's tenants share the security key with other tenants who could be a roommate, friend or guest in the apartment. Since they share password and don't change the key regularly it becomes security threat if it is gone to someone intending to intrude into network.
17. Most of the respondents say that they share the Wi-Fi password verbally.
18. 74.17% of the respondents say that they don't have smart TV but 16.56% have smart TV and 9.27% plan to buy so this will add load to the bandwidth requirements of the current network.
19. Most of the users are using Wi-Fi in their own room so while planning locations for LAN ports and Wi-Fi we can consider this area as main recipient area in apartment.
20. 55.56% of the tenants say that they will replace their current Wi-Fi with single Wi-Fi provided by LOAS. So, if we could provide reliable and high-speed Wi-Fi connection we could attract remaining 50%.
21. Most of the time LNET seems to be working fine in most of the area as more than 80% respondents say they don't face problem in regular basis.
22. Eduroam is implemented by LOAS in just 10% of the respondents.
23. Only 25% of the students use eduroam as primary internet connection in University and Apartment. 35% of the respondents don't use eduroam at all. 39.74% of the users use it occasionally to access resources while in university.
24. Nobody is sure and definitive about the reliability of the eduroam service because

respondents vary in their view greatly.

25. Most of the respondents have faced some kind of problem while they are using eduroam around university area.
26. Almost all respondents think they will not pay for any services added with eduroam.
27. Nearly all respondents say that they have not been through any security issues with LNET.
28. 50% of the respondents say they never change passwords generally until they receive an email from LUT to change their password which happens around every 3 months.
29. Respondents replied that they never check who is online through their Wi-Fi connection from router. Some of them don't know how to check and many don't have their own router.
30. 70% of the tenants don't have their Wi-Fi password compromised.
31. It seems very unlikely that students are going to subscribe to any excessive cost services with the internet service from LOAS. So, it will be clever to either keep the price low for new services, if that is not possible then drop the idea of implementing the services during the planning phase.

3.5 Summary of findings

Below are some important findings that directly relate to our motive of research.

1. Our primary users are young students of age between 18-25 primarily from Finland and Russia who spend most for their time studying, watching movies and social networking. They use apps and internet browsers while on the web.
2. Wi-Fi is the main gateway for around 70 % of the users while 30 % still using LAN ports for connecting their computers. LOAS should consider laptop as the basic device for its tenants. This can be related to our research question "RQ ***1: What are the attitudes and behavior of students toward their connected network?".*** Most of the students are positive towards the services provided by LNET.
3. Our findings show that the basic internet service from LOAS is good. There are still many students facing problem in regular basis who doesn't contact LOAS or go through LNET troubleshooting procedure in webpage. Almost all problems are either solved by students themselves or get solved automatically. Customer support aspect of LNET and eduroam seems unresponsive.
4. Very few of the LNET users have security problem with their connection. Few of the LNET users are sure of reliability and security status of network they are using but they believe that LNET and eduroam are secured and they have their faith in them.
5. Almost half of the LNET users are not security conscious and don't check and change passwords regularly.
6. Many students don't use eduroam at all except in some instances when they require access to library because of inconvenience. eduroam coverage has some problem in basement spaces in and around University.
7. Our data shows almost none of the LNET users interested in any paid service. It turns out that it is not profitable to integrate any paid services to Wi-Fi network which partly answers our research question "***RQ 2: How can we integrate more services in new LNET Wi-Fi network?".***

4 WI-FI PROJECT

This Wi-Fi project was the initiation of LOAS for checking the possibility of extending their Wi-Fi network in those apartments where they are having network problems and need to upgrade the network and to check the feasibility of eduroam in Old and new apartments. For starting any project, a deep study of the concepts and process involved in carrying out the project is needed. This thesis is the deep study of all the underlying concepts, process and planning that should be determined and understood properly before even starting the project. This thesis will also integrate the eduroam network in newly installed Wi-Fi network so that all LOAS tenants including eduroam and non-eduroam users could use the wireless network.

4.1 Project Description

The project consists of 35 different apartments with most of them located near University. Currently LOAS offers customers with one or combination of following connections, depending on the time phase the apartment building was built and/or renovated:

1. LAN
2. LNET Wi-Fi
3. Eduroam

These end points are connected to central switch in that apartment which are in-turn connected to router nearby. As the apartments were built in different time each apartment may have connection via cable or fiber link to next router. Our primary focus will be to study the possibility of using this infrastructure as and when possible to minimize the cost so that same network can be used for new Wi-Fi network. As LNET is a large network we cannot replace it in a brief period and requires considerations on various aspects of network like distance, speed and time required before carrying out replacement in each apartment. These tasks will take considerable time and requires good decision making before going for implementation. We should consider all the factors like distance between routers, network latency, fiber capacity etc. before finalizing any WLAN implementation. I have tried to schedule a total project for replacement in project planning section but it is just an example of how we could proceed which can be decided later at the time of project implementation.

4.1.1 Objectives

The main objective of our project is to build wireless network in LOAS. Inside these objectives, we have several other related objectives which are summarized as follow

1. To cover all area of LOAS apartments with Wi-Fi.
2. To integrate eduroam in this Wi-Fi network.
3. To use current network's resources as much as possible.
4. To integrate new services in this Wi-Fi as and when required.

4.1.2 Requirements

Most of the requirements of the project are technical. As this is highly technical work related to installation of wireless network, some of the requirements of the project are:

1. Detail of all installation and equipment's used in the current network.
2. Current map of the network including backbones and upstream.
3. Office space for daily work.
4. Adequate space in apartment for testing network.
5. Devices including router, switch and Wi-Fi antennas for testing purpose.
6. Human resources including engineers and supervisors for the task.

4.1.3 Coverage

We will cover all the apartments currently in lease from LOAS. All the buildings where we are implementing Wi-Fi are listed in appendix 4. The constituent buildings with their general features are listed from http://www.loas.fi below:

Figure 52 LOAS Locations

In these buildings, the basic design of the apartments is as follows:

1. Studios
2. Two-room apartments
3. Three-room apartments

4.1.4 Eduroam Overview

Eduroam stands for educational roaming. It offers users from participating academic institutions to access secure internet at any other participating institution. Eduroam architecture makes it possible to make the convenient user experience from eduroam. Eduroam service uses IEEE 802.1X as the authentication method and a hierarchal system of RADIUS servers. The full form of RADIUS is Remote Authentication Dial in User Service which is a technology in which users authenticates via remote dialup service. This RADIUS hierarchy consists of authentication servers at the participating institutions, national RADIUS servers run by the National Roaming Operators and regional top-level RADIUS servers for individual world regions.

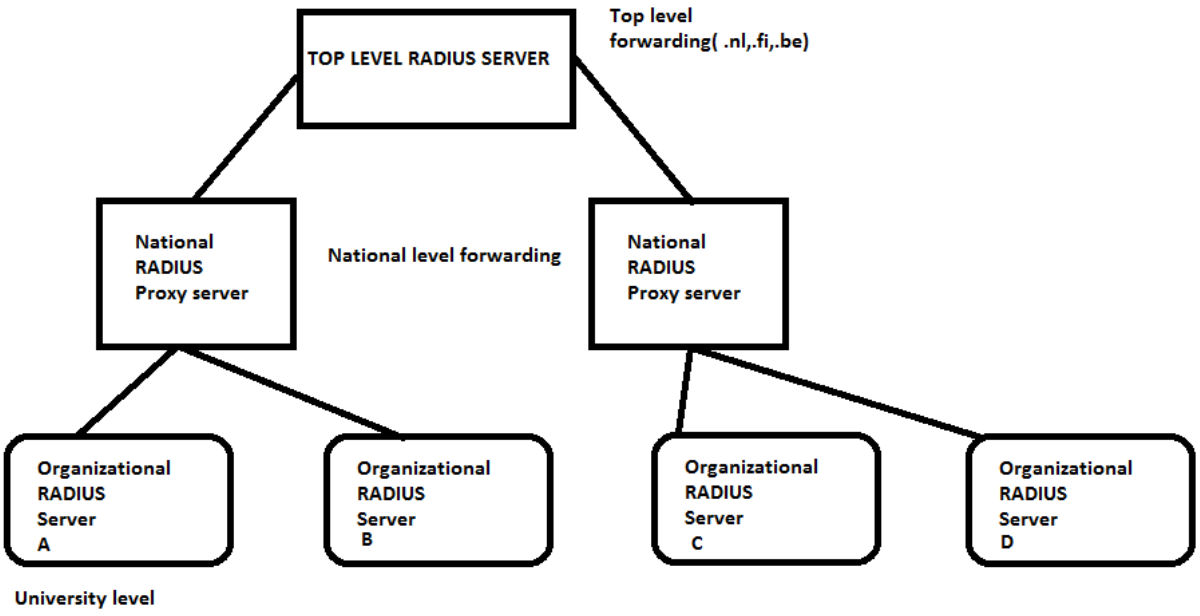

Figure 53 Eduroam RADIUS hierarchy

Eduroam provides access to the Internet via wireless LAN when a user connects and authenticates to the SSID "Eduroam"

1. Service Provider (SP) Provides Internet Access via 802.1x Wireless LAN
2. The Service Provider (SP) is responsible for transmitting user credentials through a RADIUS proxy server in hierarchical order to the RADIUS proxy server.
3. The Service Provider (SP) allows access to and use of the Internet only after approving the identity.
4. Each service provider (SP) is responsible for configuring the network, computer, or Internet network.

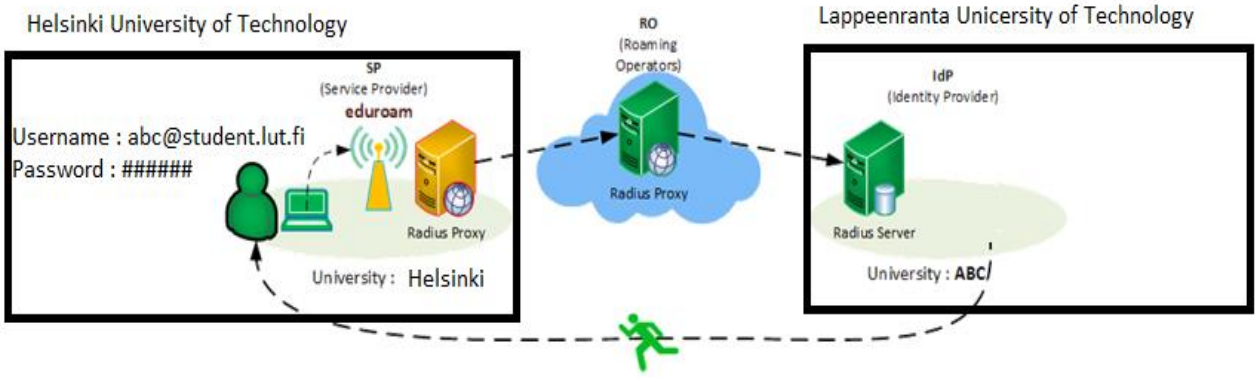

Figure 54 Eduroam overview

When a student of Lappeenranta University of technology visits Helsinki University of technology and connects to the Wi-Fi with SSID “eduroam”, first RADIUS server checks if it is user from local University. If the user is not found in the database then it checks for username for domain, in this case “.fi” and forwards it to higher level RADIUS server at FUNET which in turn forwards to users University RADIUS server and authenticates the user. After successful authentication user gets access to the internet from new location.

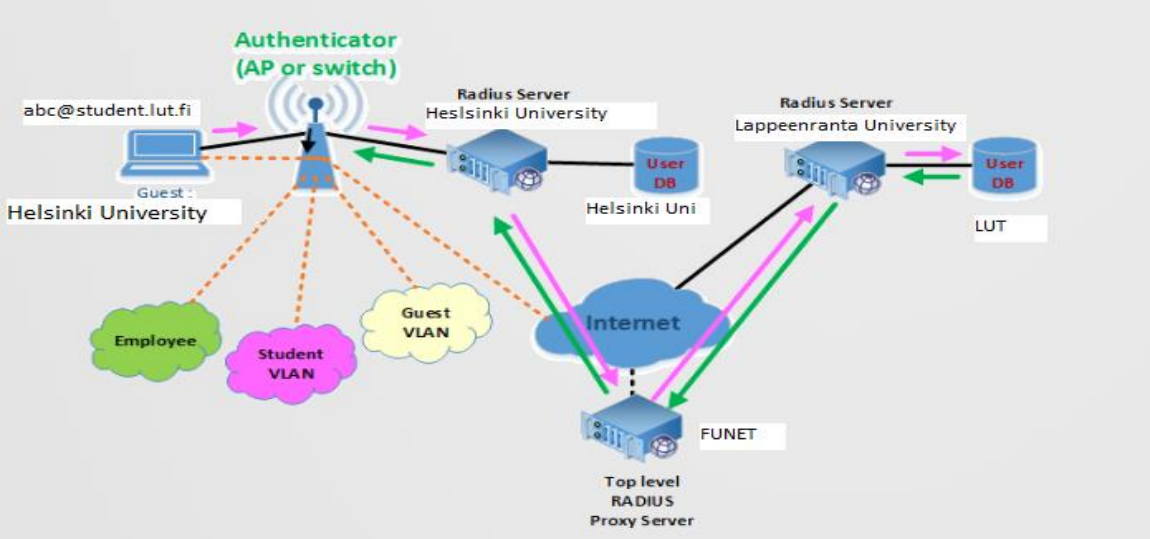

Figure 55 Eduroam authentication process

Since the credentials must travel outside the local network via internet it is very important to protect the information of the user. These requirements limit the type of authentication methods that can be used for remote authentication. There are two categories of authentication methods

1. Public Key Mechanism
2. Tunneled Authentication

Most setups use a tunneled authentication method that only requires server certificates. These server certificates are used to set up a secure tunnel between the mobile device and the authentication server, through which the user credentials are securely transported.

A complication arises if the user's home institution does not use a two-letter country code top level domain as part of its realm. Instead, a generic top-level domain such as .edu or .org are used which later becomes reason for problems in international roaming since it is not possible to determine which national RADIUS server to forward the request. Solution to this problem is to create a routing table for this specific use.

Users authentication information across the RADIUS infrastructure to their IdP is transferred using IEEE 802.1X standard that encompasses the use of Extensible Authentication Protocol(EAP). There are several EAP methods Idp can select but that must support mutual authentication.

Some of the popular EAP methods are:

1. PEAP ("Protected EAP") - a Microsoft protocol that establishes a TLS tunnel, and sends usernames and passwords in MS-CHAPv2 hashes inside.
2. TTLS ("Tunneled TLS") - an IETF protocol that establishes a TLS tunnel, and sends usernames and passwords in multiple configurable formats inside.
3. TLS ("Transport Layer Security") - an IETF protocol that authenticates users and the IdP with two X.509 certificates.
4. FAST ("Flexible Authentication via Secure Tunneling") - a Cisco protocol that establishes a TLS tunnel, and sends usernames and passwords in a custom way inside.

When the IdP server decrypts the TLS tunnel in the EAP payload, it gets the inner identity and can authenticate the user. After successful authentication by the Identity Provider and authorization by the Service Provider, this SP grants network access to the user, possibly by placing the user in a specific VLAN intended for guests.

4.1.5 Project Infrastructures

Eduroam consists of following key elements for setting up Wi-Fi network.

1. Confederation top-level RADIUS Server(TLR)
2. Federation level RADIUS servers(FLRs)
3. IdP and SP RADIUS infrastructure
4. Identity Management system
5. Supplicants
6. Switches
7. Access points

As eduroam is already implemented in Lappeenranta university of technology we only need to extend the network from LUT to LOAS's LNET and setup Wi-Fi network according to the eduroam guidelines. So, our infrastructural needs are

1. Access points
2. Switches
3. Identity Management system

4.1.6 Project planning

If you don't know where you're going, you'll end up someplace else. —Yogi Berra

This phrase simply defines how important planning is before doing anything. It can easily be said that without site surveys; it would be difficult to determine the capital investment needed to deploy the wireless network in a timely and efficient manner. (Air Magnet 2007)

Project planning is the important part of any project in which we try to streamline the project by developing schedules and charts based on which progress of the project could be reported. In every project, specific scopes of the project are defined first and then scope is divided into several tasks and divided into workgroup. The duration of task and necessary steps to complete the tasks are listed and finalized.

Various project management software is in use in recent years for easy management of time and task of the project. Some of the popular project management tools are listed below:

1. Teamwork Project
2. Work front
3. Zoho Project
4. Liquid planner

We will not go into detail for how they are used as each of them have different user interface and style for managing tasks. One of the most important part of project planning is schedule. Every project manager should make a tentative schedule ahead of starting the project which later becomes baseline time for completion of tasks in the project. I have built the tentative plan for implementing the project into three phases:

Table 4 Phases of project

First Phase	➢ Site Survey and Reporting
Second Phase	➢ Design Network
Third Phase	➢ Install Network
Fourth Phase	➢ Check and Verify Network

The network topology of LNET is shown below.

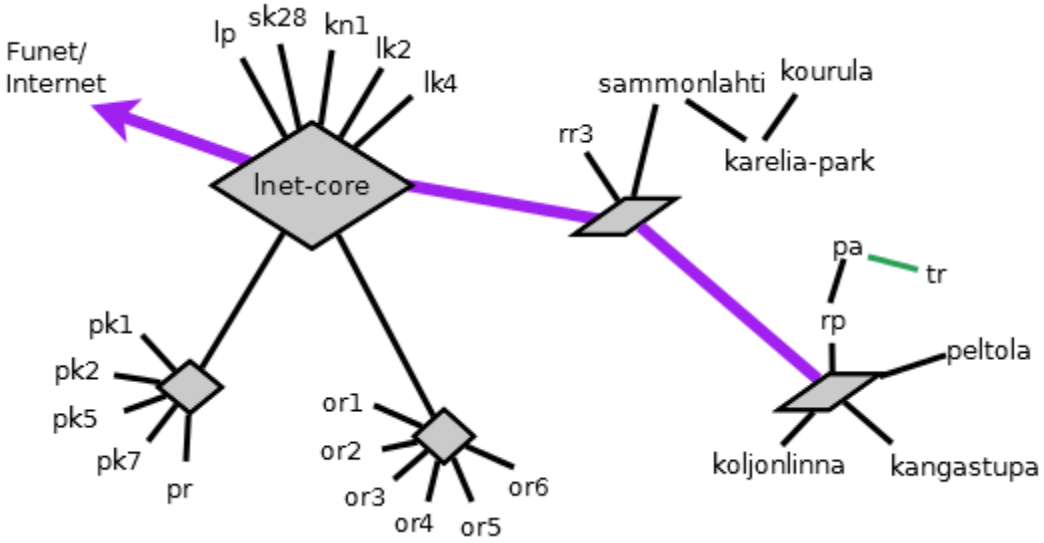

Figure 56 LNET topology

Source: http://www.lnet.fi/en/tech

There are several factors that influence whether LOAS wants to implement a new WLAN network in any apartment or not. Some of them include date of completion or renovation, problems in current network and several financial and managerial factors. Due to this reason laying out simple plan is not possible.

The best model for project implementation is to install the WLAN network first near to the core router so that we should not check any intermediate network before reaching core router but LOAS may not want to install WLAN in newly built apartment building as that may increase cost for both LOAS and tenants. The simplest way would be to look for WLAN implementation in old buildings first that are near to the core network. Unfortunately, the tentative time cannot be estimated here properly due to complexity of each network will vary upon going far from the core router.

The schedule below shows the plan for implementing the Wi-Fi project based on the thesis work.

Table 5 Project planning

PHASE	Network	Name	Detail	TASKS
FIRST	LK2 LK4	LEIRI	Completed in 1991-1992	SURVEY DESIGN INSTALL CHECK REPORT
	OR1	ORION 1	Completed in 1992	
	OR2	ORION 2	Completed in 1997	
	OR3	ORION 3	Completed in 2000	
	OR4	ORION 4	Completed in 2000	
	KARELIA PARK	PARK	Completed in 1970 Renovated in 1997	
		PALLO	Completed in 1982 Renovated in 1999	
		PUNKKERIPARI	Completed in 1977-1978 Renovated in 1997	
	PR	PUNKKERIRINNE	Completed in 1990	
		UPSEERITIE	Completed in 1999	
		SKINNARILA 3	Completed in 1998	
	SAMMONLAHTI	SAMMONLAHTI 2	Completed in 1993	
	Pk2	PUNKKERITORNI	Completed in 1981 Renovated in 1998	
	KANGASTUPA	KANGASTUPA 1	Completed in 1998	
	KARELIA PARK	KARELIA	Completed in 1971 Renovated in 1997	
		LASERPUISTO	Completed in 1992	
		KATAJAKATU	Completed in 1976 Renovated in 1996	
SECOND	OR5	ORION 5	Completed in 2003	SURVEY

				DESIGN INSTALL CHECK REPORT
	OR6	ORION 6	Completed in 2004	
	PELTOLA	PELTOLA	Completed in 1980 Renovated in 2004	
	Pk5	PUNKKERITIENOO	Completed in 1997 Renovated in 2001	
		RAKUUNAPORTTI	Completed in 2001	
		PUNKKERIRIVI	Completed in 1982-1983 Renovated in 2002-2003	
	RP	RAKUUNAPORTTI	Completed in 2001	
		KOTANIEMI	Completed in 2002	
	KANGASTUPA	KANGASTUPA 2	Completed in 2003	
		KOLJONLINNA	Completed in 2005	
		KOURULA	Completed in 1980 Renovated in 2005 and 2006	
THIRD	PELTOLA	PETOLA 2	Completed in 1983 Renovated in 2008	SURVEY DESIGN INSTALL CHECK REPORT
		SKINNARILA 1	Completed in 1985 Renovated in 2008	
	TR	TERVARANTA	Completed in 1984 Renovated in 2009	
	SAMMONLAHTI	SAMMONLAHTI 1	Completed in 1998 Renovated in 2010	
	SK28	SKINNARILA 2	Completed in 1989 Renovated in 2014	
	RR3	RUOTSALAISENRAITTI	Completed in 1975 Renovation in 1995 Renovation in 2014	
	LP	LOAS SEPPO	Completed in 2013	
	Lk1	LOAS TIMPPA	Completed in 2016	

4.1.7 Resources Required

In every project, there are so many things to be considered from infrastructure to finance for successful completion of the project in time. We have considered the following resources which can be divided into technical, administrative, human resources, financial resources.

Table 6 Resources required

TECHNICAL RESOURCES	ADMINISTRATIVE RESOURCES
Testing Lab Access points and routers Internet connection FTP Server Laptops Mobile phones Project management Software	Well-built office Network Engineers Administration staffs Financial resources

4.1.8 Potential Challenges

As this is a large-scale project where we should install wireless devices in 35 different buildings at various places, it certainly has many challenges involved. Some of the difficulties that may arise during the project can be listed below.

1. Forming a good team for the project is very important which may take time.
2. If the team doesn't communicate properly than it may result into failure or extension of time.
3. The devices we choose for our project may not be available in our region in which case, shipping will take lot of time. This will extend our project duration.
4. We currently have an assumption that we can use the current network configuration for our project but if that doesn't work out then it may take time to re-configure all the devices according to eduroam configuration.
5. Difficulties lies in carrying out setup work without disturbing the current network. So, schedule for network disturbance prior to starting project will be necessary.
6. We may face problem due to apartment designs on where to place a Wi-Fi antenna.
7. From management point of view, we may face financial issues on buying network devices and equipment as these are very costly in nature.

4.2 Project Implementation

Eduroam network is a wireless network. So, it is important to keep in mind that

- Only changing the SSID into eduroam will not make the network better. Proper management of network is preliminary requirement before shifting to eduroam
- Coverage area of eduroam should be calculated beforehand
- Allocate sufficient addresses for eduroam users

Once the institution has decided to join eduroam network, they should follow several steps for installation of network as well as perform administrative tasks for completing the setup process. Basically, eduroam has two kinds of implementation. Any organization or academic institution can join eduroam as:

1. Identity provider (IdP) or
2. Service provider (SP)
3. Both IdP and SP

As LOAS is not an academic organization, we can implement eduroam based on service provider (SP) configuration. Service provider (SP) in this context means those organization that provide eduroam connectivity services regardless of the type of organization they belong i.e. academic or non-academic. The basic implementation of SP includes:

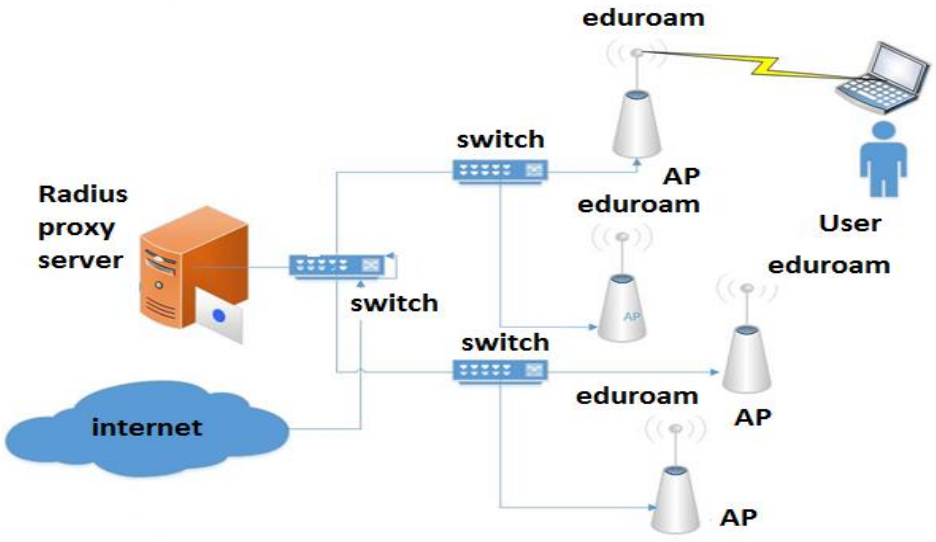

Figure 57 LNET as SP

The outer most part of the eduroam system is users. In our case, users are from

1. LUT
2. Foreign university exchange students
3. LNET users

So, we need to forward the authentication request from LUT and foreign university exchange students to their respective Identity Provider (IdP) whereas simple authentication is enough for LNET users. This implementation provides answer for our research question "***RQ 4: How to provide eduroam Access to LOAS customers?"***

4.2.1 User Configuration

Depending on the mostly used devices for Wi-Fi we will have two distinct kinds of users of eduroam:

1. Mobile users
2. Laptop users

Even though we have tablets, smart TV and other wireless capable smart devices that may request connection, the process each device must go through will be same as these two main devices. Whoever the users, they just need to find the eduroam SSID and follow the onscreen dialogues to connect to eduroam. It is possible to gain access to the internet whenever access to the eduroam is granted.

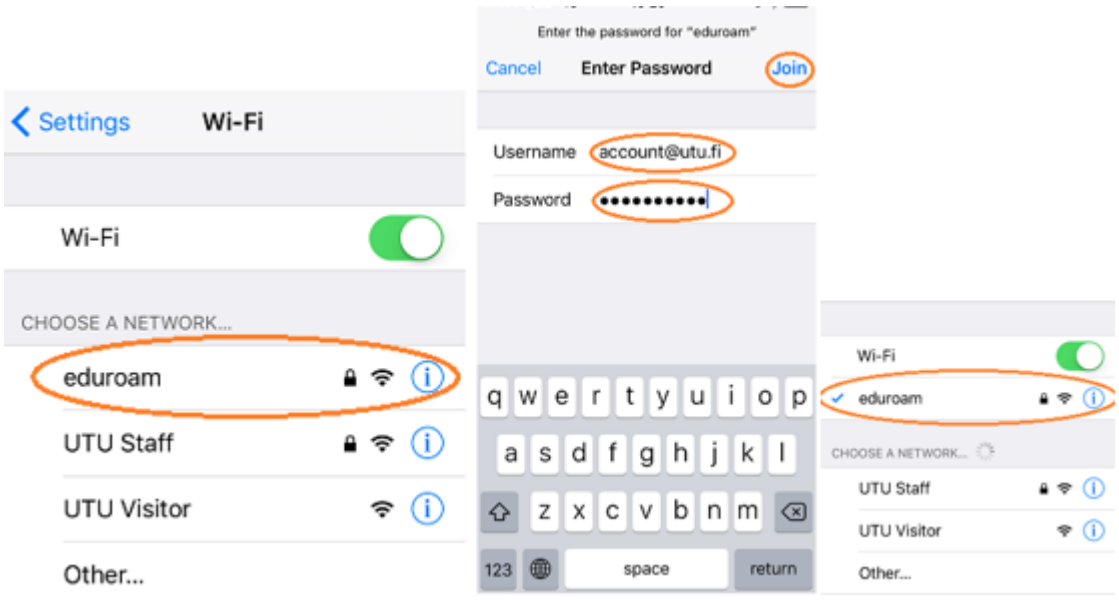

Figure 58 Connecting eduroam in Mobile

Figure 59 Connecting eduroam in Linux

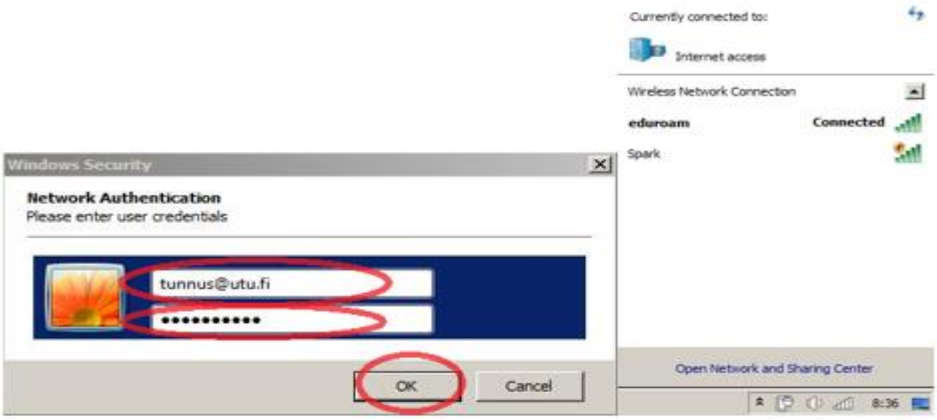

Figure 60 Connecting eduroam in Windows PC

4.2.2 Wi-Fi Design Principles

There are several principles for designing a Wi-Fi network which are rules that make up good network reception and performance. Every installation of Wi-Fi antenna should be done following these principles. Some of the principles are discussed below. The implementation principles will provide better services in Wi-Fi network which in turn answers our research question "***RQ 3: How can we improve the service quality through Wi-Fi network?".***

4.2.2.1 Wi-Fi Survey:

Wi-Fi network will give you best performance only when they are placed in correct position. Every Wi-Fi installation should start with survey. As Wi-Fi has become prominent networking technology there will be more than one Wi-Fi signal in any living space. So, survey will guide

us on which frequency should be used that will not overlap with other signals. If we neglect this point, the resulting network will be slow.

The latest technology in use today is 802.11 ac and there are so many vendors for this technology including some popular companies. In new Wi-Fi antennas, we have the option to broadcast 2.4GHz and 5GHz together so if the airspace is very much congested with 2.4GHz then using 5GHz is good option.

There are mainly three types of Wi-Fi surveys

a. Passive: passively listens to Wi-Fi traffic to detect AP, signal strength and noise levels.
b. Active: wireless adapter is associated with some access points and measures round trip time, throughput, packet loss and retransmissions.
c. Predictive: used to predict the RF environment using simulation tools.

Irrespective of wireless or wired connection, some of the basic network analyzer for checking traffic are:

1. Netstumbler
2. Wireshark

There are so many software's available in the market depending on what scale your installation will go. Some of the basic survey tools for home environment are:

1. Homedale
2. Acrylic Wi-Fi
3. AirGrab Wi-Fi Radar
4. Xirrus Wi-Fi Inspector

Some of the tools for Enterprise environment are:

1. Ekahau Wi-Fi Site Survey and Planner
2. Ekahau Heat Mapper
3. Airmagnet Survey
4. Netspot
5. HiveRadar Wireless Site Survey
6. Cisco Wireless Controller system

7. Fluke Networks InterpretAir WLAN Survey
8. Xirrus Wi-Fi designer

For our purpose, we will use Ekahau Wi-Fi Site Survey and Planner. Ekahau is a Helsinki based company and has excellent track record in wireless designing and planning tools. Some of the features of Ekahau site survey are:

1. Supports all enterprise Wi-Fi access points from all vendors for site surveys & WLAN planning
2. AP name detection. Multi-SSID detection. Multi-radio detection.
3. See Wi-Fi coverage on a map
4. Locate all access points
5. Find available networks
6. Detect security settings
7. Supports 802.11n, as well as a/b/g
8. Works on pretty much any Windows laptop
9. Full support for Wi-Fi site surveys and Wi-Fi planning: Cisco, HP - Aruba, Ruckus, Aerohive, Xirrus, Extreme, Siemens, Adtran, Avaya, D-Link, Meru / Fortinet, Juniper, Lancom, Meraki, Netgear, Samsung, Ubiquiti, Zebra, Zyxel and more
10. Over 1500 access points / antennas modelled in 3D

After deciding what software to use we also need to go through these processes in every site before beginning the survey.

1. Have a blueprint of floor plans of the area that need to be covered by Wi-Fi.

2. Determine the location of AP based on the blueprint and cablings on the building. Never place the device on places that have obstacles like walls, elevators which block signals.

3. Estimate total number of device required to cover whole area. One AP can cover 100-foot RADIUS, so use this for placing new AP's.

4. Now, use the survey tool using the same AP model in survey tool also.

5. Place the AP's at a secure place so that only authorized personnel can access it physically.

6. Relocate the AP’s depending on the result.

7. Document the findings and logs for future reference.

Figure 61 Ekahau site survey tool

Source: http://www.ekahau.com

4.2.2.2 5GHz Band

Most of the devices in use today for Wi-Fi are either using 2.4GHz band or 5GHz band.2.4GHz band are widely used so there is large possibility that it will be interfered by some signal from another router or Antenna. So, the solution to this problem is to use 5GHz only or both bands.
If the device we are using supports both band then broadcast both bands but if we have to choose between two bands we need to choose 5GHz band. (Moran Joseph, 2015)

4.2.2.3 Failover

When one of the links is down in any building then it should immediately enable another backup link so that even if main link is down the network will not be disturbed. This feature is called failover. For stable and customer-centric network we need to make failover in every building.

4.2.2.4 AP Vendor

Hardware vendor selection is very critical step in overall Wi-Fi implementation. We have diverse options for implementing Wi-Fi network in high density environment like

1. Cisco
2. Aruba
3. Rakus
4. HP
5. Motorola

As we have used cisco devices in most of our infrastructure, we will continue using cisco as network devices vendor. The specification of the device should look like

a. 802.11ac
b. 2.4GHz and 5GHz support
c. Multi-SSID support
d. Guest access
e. Centrally managed software

4.2.2.5 Signal Strength

Signal strength is very important aspect of any Wi-Fi installation. When Wi-Fi signal is placed in any object it may absorb, reflect, degrade or block signal. Some of the objects commonly interfering with the Wi-Fi signals are

1. Walls: Wi-Fi signals get reflected off polished walls and disperse in case of rough surface.
2. Ceiling: Wooden ceiling absorbs signal whereas concrete or metal reflects Wi-Fi signal.
3. People: Human body generally reflects the signal and blocks the recipient behind it.
4. Furniture: Metal furniture reflect the signal whereas wooden absorb and let signal pass.
5. Floor: Wooden floor absorbs and let the signal pass whereas concrete and metal floor reflects signal.
6. Glass: Glass passes the signal whereas coated metallic film in glass reflects Wi-Fi signal.

4.2.3 Identity provider (IdP)

When institution is connected to eduroam as an IdP then students, faculty and staff can use their personal credentials provided by institution to join eduroam anywhere in the world. The first task is to peer its RADIUS server to eduroam federation level RADIUS server. Next, their RADIUS server is connected to LDAP, AD, SQL DB and other servers required during authentication. This allows users to connect to eduroam from all over the eduroam network. eduroam Identity provider can only provide authentication service to their roaming users not to local users. This is the reason institution should also be service provider (SP) in most of the case.

4.2.4 Access Point configuration

If the access points are connected to the same subnet as the controller, they will automatically find the controller and connect to it. If this is not the case, the IP address of the controller must be found from the name server by the name CISCO-LWAPP-CONTROLLER. Once the access point has found the controller, it stores the IP of the controller, and it can connect to it from any network, if the network allowed access in the ACL (see previous section).

The next step is to define the wireless network, which must be done separately for 2.4 GHz and 5 GHz. First, choose WIRELESS and then 802.11b/g/n Network. Enabling the 802.11b standard will result in less available capacity on your network and therefore it is recommended to enable only the standards 802.11g and 802.11n. If you want to support also the 802.11-b standard, set _Mandatory_ for the lowest 802.11b-rate that you want to support (1 Mbps, 2 Mbps, 5.5 Mbps or 11 Mbps), set _Supported_ for all data rates higher than this rate and _Disabled_ for all rates lower than this rate. If 802.11b needs to be supported, it may pay off to disable the lowest rates, to avoid clients being attach to an AP far away, unwilling to roam.

Next, switch to enable the standard 802.11a for 5 GHz by selecting 802.11a/n Network. The only standard left to enable is the standard 802.11n. You can choose to enable it for either 2.4 GHz or 5 GHz. It has been suggested that 802.11n is enabled only on the 5 GHz band, to utilize the radio resources effectively. To enable 802.11n in the network select 802.11a/n High throughput (802.11n) and/or 802.11b/g/n High throughput (802.11n) and configure the settings. At this point we have enabled the radios, but not yet defined any network.

4.2.5 Defining the RADIUS server

Define the RADIUS server to be used in the eduroam network by selecting SECURITY and then AAA | RADIUS | Authentication. Define the IP address, the shared secret and the other parameters. Please note that your first server will naturally have a server index of one.

4.2.6 Defining a wireless network

Select WLANs and then WLANs | WLANs from the sidebar. Create a new network and name it. After defining the eduroam network, click on the WLAN ID number to start defining the settings for the network. Set the General settings and then click the Security tab. Next, click on the QoS tab and make sure that you have set the WMM Policy to either Required or Allowed. Otherwise, the higher transmission rates associated with the 802.11n-standard will not work. Then select the Advanced tab and adjust the settings as shown in the figure below. By choosing the parameter P2P Blocking Action to have the value Forward-Upstream, you can prevent WLAN clients to communicate directly, without involving the AP, as recommended in the Campus Best Practice document on "WLAN Information Security" Chapter 2.2 and 2.3. MFP Client Protection is known to have caused problems and can be disabled. At this stage, click Apply. In the Advanced-tab, the Client Exclusion timeout value was set to 60s. While this is a suitable value, the rules for client exclusion are a bit too strict. Hence, it pays off to adjust the rules by selecting SECURITY and then Wireless Protection Policies | Client Exclusion Policies from the sidebar and uncheck all other options except for "IP Theft or IP Reuse".

These are the basic settings for the Cisco controller.

4.2.7 Service Provider (SP)

Service provider doesn’t have the restriction to be academic institution it can be any organization providing eduroam service. So, LNET can be a service provider of eduroam.

LNET can become SP if it

1. Broadcast “eduroam” SSID on its network.
2. Has IP network configured and routed to internet for eduroam SSID with DHCP and

DNS function.

3. Has RADIUS server of its own that is configured to forward authentication requests up the eduroam chain for users that are not part of the institution.

4.2.8 RADIUS Server configuration

We can choose from various RADIUS server options such as:

1. Radiator
2. FreeRADIUS
3. Microsoft NPS
4. Juniper Steel-Belted RADIUS

We can use any of the RADIUS servers for our purpose but we will use FreeRADIUS as it is widely used in eduroam implementation. It has AAA features and is used in fortune 500 companies. It is fast, feature rich, modular and scalable. It includes RADIUS server, BSD licensed client library, a PAM library and apache module.

Steps for setting up free RADIUS server on Red Hat 6 are listed in appendix 2

Initial configuration of Cisco AP's is listed in appendix 3

4.2.9 Access Control Lists

After the initial setup, the access control (ACL) list needs to be configured, to prohibit unauthorized access to the controller. Choose SECURITY and then Access Control Lists | Access Control Lists and create an ACL by pressing New. The ACL should include at least networks from which maintenance is carried out, the address(es) of the monitoring server(s), network(s) from which the APs and the WLAN clients get their addresses, the address(es) of the RADIUS server(s).

After you have specified the ACL you need to take it into use by first selecting Access Control Lists from the side bar and by choosing your ACL and specifying the CPU ACL Mode to Wired or Both.

4.2.10 LNET general Wi-Fi user's implementation

LUT and Exchange students are the easiest group to manage for allowing Wi-Fi access. The complexity comes when we have user other than this group that only need LNET Wi-Fi. To allow access to this group, it is necessary to separate traffic between these two group in the process of authentication and divert the traffic to another authentication server. The only way to do this cost effectively is to have open source RADIUS server.

First, we can broadcast multiple SSID with name as "eduroam" and "LNET Wi-Fi". Then all non eduroam users can connect to LNET Wi-Fi and go through authentication process. This can be achieved by using proper configuration in wireless control page in most of the recent APs.

This RADIUS server will contain database of all the users who don't belong to eduroam. So, the scenario will be

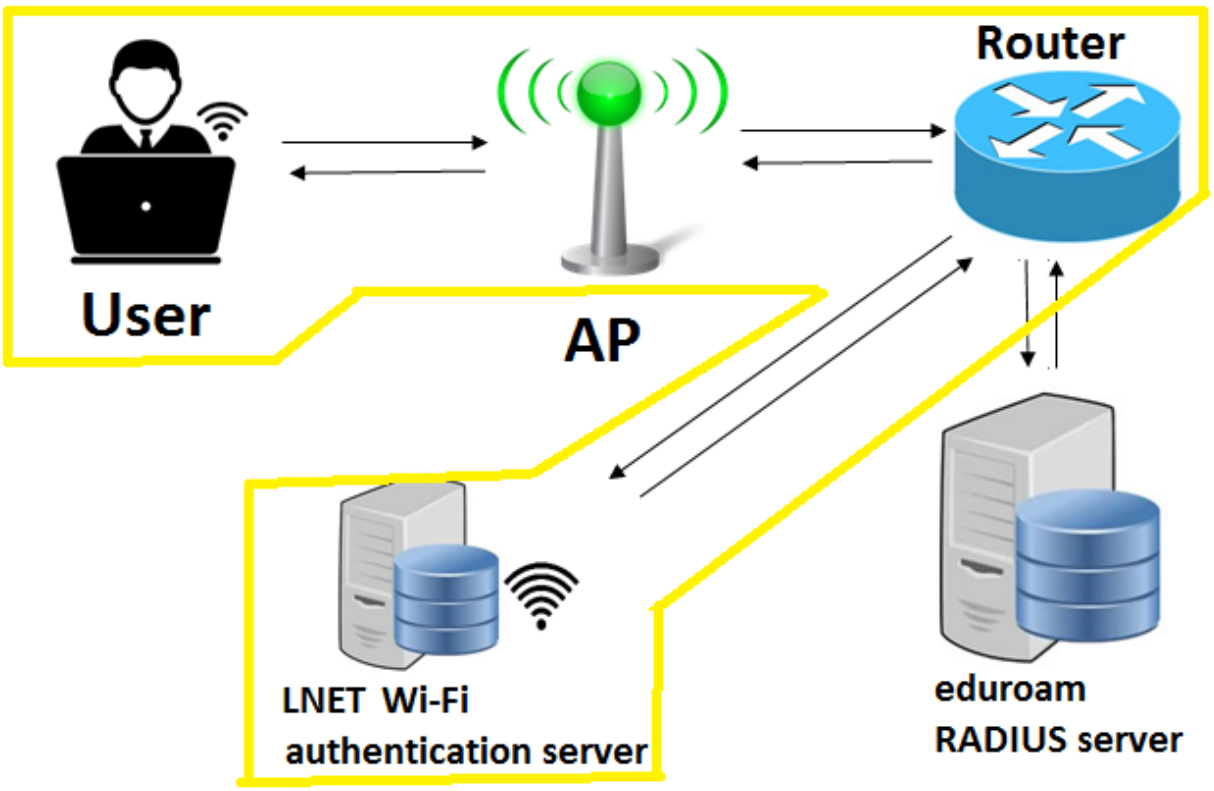

Figure 62 LNET Wi-Fi Authentication

This model is the most widely used model for Wi-Fi security in large Wi-Fi networks with substantial number of users. This process gives good control over the Wi-Fi network. RADIUS is established through Authentication, Authorization and Accounting (AAA). This can be implemented in Cisco 800, 1800, 2800, or 3800 series integrated service router.

The Multiple 802.1X configuration for Cisco router can be found on appendix 6

This will be the proper solution to authenticate “LNET Wi-Fi” users in LNET. The IP pool for these users could be separated for more simplifying the task. Hence this group of users will unable to reach eduroam, which will in-turn make network more secure.

4.3 Project limitations

Every research and study contains some limitations to the collected data due to numerous factors concerning data source or methods used for data collection, analysis or interpretation. Even though we carried out questionnaires and interview with as much precautions as possible, we cannot guarantee that the users have put their information correctly. There are always chances that respondents may fill the questionnaires in hurry or just to finish. Some of the limitations in questionnaires are:

1. Possibility of false data input by users.
2. Possibility of misinterpretation of questions in questionnaires.
3. Respondents may hurry and select answers randomly.
4. Small number of respondents may not lead us to proper conclusions but in our case, we had more than expected respondents.

Some of the limitations of interview are:

1. It is possible that interviewee misinterpret interview questions.
2. Interviewee may also feel uncomfortable speaking in front of representative of concerned company.
3. The Host of the interview may also misunderstand the point interviewee is making.
4. It is also possible that if note taking is not done in time, it is possible to forget what point was the interviewee was making after some time.

Some of the limitations of the project are:

1. All the tests are done in lab conditions.
2. Assumptions and calculations are based completely based on previous work experience.
3. Devices and equipment's interference are not taken into consideration.
4. Routers and switches capacity may differ from the manufactures specification.
5. Attenuation in signal is not taken into consideration.

4.4 Project Testing

After the installation of the Wi-Fi networks it is ideal to test the speed and performance of the network. Network testing is an important task for every network admin before allowing it for use. It not only tests for acceptance by the users but also helps to find out limits of the network so that network can be managed easily. Finding the maximum speed network support is not the only concern when it comes to testing, how much time it takes to transfer data, performance fluctuation and effect of load on networks must be some of the concern for administrators. Some studies have shown that increased bandwidth has been the most used solution for network admins. It is also important to keep in mind following things while doing testing

1. Testing network and location
2. Testing environment
3. What needs to be tested, speed, bandwidth utilization, application utilization or users.
4. History of that network
5. Normal operating condition and testing condition.

Network testing is the actual measurement and recording of a network's state of operation over a period. It involves recording the current state of network operation to serve as a basis for comparison or control. The results of the test are used to find problems and record it for second iteration of the test after the problem is solved.

4.4.1 Speed test

Speed test is carried out to determine speed of the network or speed between two nodes. There are several tools available to test the speed of the network. Most common type of speed test is test for internet speed from the host computer. This can be done in several ways.

4.4.1.1 Speed from host to internet

This is the most commonly used speed test in internet. In this test, we try to test the speed of link from host to internet.

1. Speedtest.net: This is the most widely used speed testing website in internet. In the webpage, you must select the destination server to check the speed and then start the test. After some time, results will be shown in Upload and Download. It has mobile version too.

Figure 63 Testing speed in speedtest.net

Source: https://www.speedtest.net

2. Internet speed Meter: This is also another host to internet speed tester. It can show the speed in continuous manner even when using other apps.

4.4.1.2 Speed from Host to Host

In many cases, we need to test the speed from host to another host. The host may be switch, router or another computer. These are particularly tested to confirm speed between communicating devices such as host and server and host to host.

1. LAN speed test:

   This is one of the basic testers. It has simple user interface and easy to use design.

2. NetIO: It is desktop based speed testing software for host to host speed test. It uses the netio command for testing speed in which ICMP response times are used to calculate network transfer rate.

4.4.2 Performance test

Although speed test determines bandwidth and capacity of the network, performance test is done to find more insight of the network inclusion:

1. Network utilization
2. Number of users
3. Protocols used in the operation
4. Errors encountered
5. Application Utilization

This is done by developing the testing template on which test results are done and recorded for further analysis. One example of testing template is shown below but these templates could be made according to requirement and based on what we want to focus on

Table 7 Performance test template

II. Capacity, Support, and Costs

	Time at Start-Up	6 months after startup	12 months after startup
A. Application Usage Information (To be completed by the Project Manager)			
1. Concurrent LAN users			
2. Total LAN users			
3. Concurrent WAN users			
4. Total WAN users			
5. Concurrent remote users			
6. Total remote users			
7. Total concurrent users (sum of 1,3,5)			
8. Total overall users (sum of 2,4,6)			
B. Application Resource Information (To be completed by the Project Manager)			
1. Disk storage (GB)			
2. New/upgraded desktops			
3. Peak update transactions/hour			
4. Peak inquiry transactions/hour			
5. Peak data throughput/hour			
6. Avg. data throughput/hour			
C. Technical Center Capacity Requirements (To be completed by the Manager of Systems Administration)			
1. Additional server required			
2. Type of server required			
3. Server processor upgrades			
4. Server memory upgrades			
5. Server software upgrades			
6. Disk resource upgrades			
7. Tape resource upgrades			
8. Backup media required			
9. Physical floor space			
10. Racks, cabinets, furniture			
11. Facilities (electrical, a/c, etc.)			
D. Operations Support Requirements (To be completed by the Manager of Systems Administration)			
1. FTE Computer Operator			
2. FTE Systems Administrator			
3. FTE Database Administrator			
4. FTE Network Operator			
5. FTE Call Center Analyst			

Project Manager	Date	Customer Contact	Date	Primary Operations Support	Date
Systems Administrators Manager	Date	Network Operations Manager	Date	Solution Center Manager	Date

4.4.3 When to test?

It is worthless to test a network when it is congested or having some issues. These results will not give actual results. Also, testing a network for brief period will not give you bigger picture of the test. Ideal test should last at least one week of time. The results of the week-long test then can be analyzed and more detail test can be done focusing on the result.

Network test should be carried out in regular interval of time depending on network and comprehensive record of test should be stored for future use. This information will give valuable insight of the network later while anticipating problem or load calculation.

5 CONCLUSION

This thesis was carried out in Lappeenranta University of Technology to find out current service and network status of LOAS's network and internet service called LNET. LOAS is a student housing company in Lappeenranta working closely with LUT. Literature review done at first part of the thesis will provide industry wide practices which will guide us during implementation phase. We first studied the entire industry wide standard for Wired and Wireless internet and build a solid foundation on which we develop a plan for Wi-Fi network expansion under current situation. We used questionnaire and interview as a research method to dig deep into our research questions and developed a plan to implement a new wireless network system that will enhance the service and satisfaction level of tenants living in LOAS's apartments.

We developed the plan to integrate eduroam with LNET network which is a major feature improvement for LOAS's internet service. This will ease the difficulties faced by exchange students coming from other universities. After successful implementation LUT students will get a free Wi-Fi access integrated with eduroam which will be a significant development for LOAS as well as enjoyable experience for students of LUT. This improvement will also eliminate several security issues like port problem which was primary headache in Cable based network.

The new system will cover all apartments with High speed Wi-Fi Network in both 2.4 GHz and 5GHz band which means that both new devices and old devices will get access to the network. If the Wi-Fi speed is not sufficient for any user then only LAN ports will be used to allow access to the network. Meeting every tenant's need of speed will be major challenge as Wi-Fi signals depend on how open the area is and each apartment tends to be different, which causes signal transfer to differ in each case.

5.1 Managerial Implications

Developing a big wireless network has its own management issues. If we go ahead with the project and start the projects, some of the managerial problems we could face are as follows:

1. Financial implications:

   As we are going to replace all cable networks with Wi-Fi, it will be a large financial investment for LOAS. Setting up of Project Office will accelerate the work of the project where we can conduct regular meetings and discuss issues. Huge sum of money must be invested in buying all the network elements like access points, switches, routers and fiber cables. Human resource also requires investment as we need people to build network, only buying proper devices are not enough. Other small costs may include transportation of devices and cables.
2. Technical implication:

   Getting the technical expert for these kinds of tasks is vital for project success. If the people carrying out pure technical task are unknown of the technology then it will cost lot of time and money for the project.
3. Project Schedule

   Making the project time table even before starting the actual work will significantly put the project on timeline. Team leaders and project managers should therefore meet and schedule time table for different tasks beforehand even if the work is elongated it will keep the project on track.

5.2 Future Services

In our questionnaire, we have a special section to ask tenants of LOAS if they are OK with paying for value added services with basic internet. In that question, we were surprised to find that most of the people refused to pay for any value-added service with basic internet.

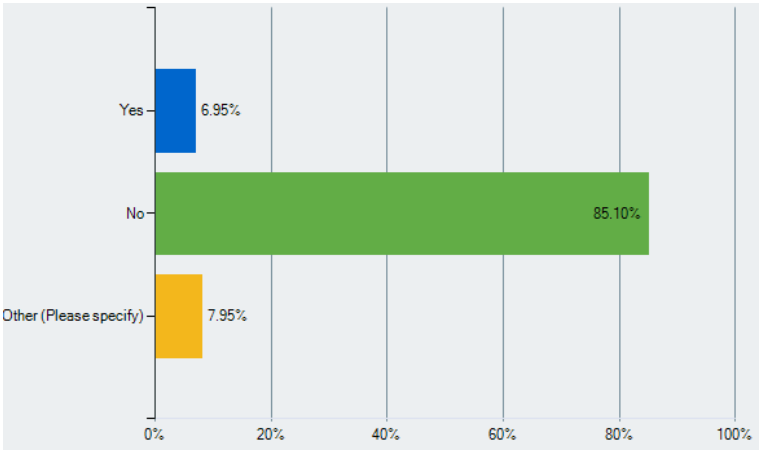

Figure 64 Will you subscribe to Value added Service?

Also on another section we had a question where we asked participants if they would subscribe to services like Chromecast, security cameras or smart TV but majority of the respondent said “NO”

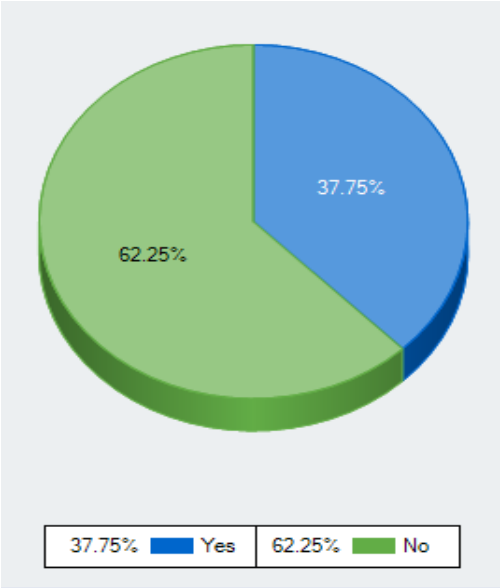

Figure 65 Will you subscribe to Smart services?

We can generalize this response in following way.

1. As most of the LOAS’s tenants as well as our respondents are students with minimum or no income of their own, introducing new services with even low price is unlikely to attract any of the LOAS tenants.
2. From our findings, we saw that large chunk of students are not using eduroam at all.

3. We can try to cover as much part of apartment and surroundings as possible so that users will not be out of Wi-Fi zone between University and Apartment.
4. Even though most of the respondents are not keen on any new services, some of the new attractive services for LOAS's tenants could be:
    1. Game server for LNET users
    2. VoIP within LNET
    3. File sharing within LNET

5.3 Further Research work

This research work mainly focuses on Wi-Fi, its planning, deployment and eduroam deployment in LNET. Despite its popularity, Wi-Fi is not a problem free technology. During our research, one interesting idea generated was mesh Wi-Fi network with several backup links and seamless roaming which was ideal for our use. Further research can be done in this kind of network. LTE is as popular networking for mobile devices as Wi-Fi but it is still not widely used because of its cost which is 10 times that of Wi-Fi. 5GHz band will be widely used in coming years and will probably replace 2.4 GHz slowly. Further study can be done on completely replacing 2.4GHz.802.11ad with 60 GHz band will be popular after few years. Much research work can still be done in using this band and its tremendous possibilities.

During our research, we also learned about Li-Fi, a mechanism to transmit signal through light. This technology is still is in primitive phase and this technology is not standardized so it seems very good and lot of research works can be done in this field.
(Sebele Brian 2016)

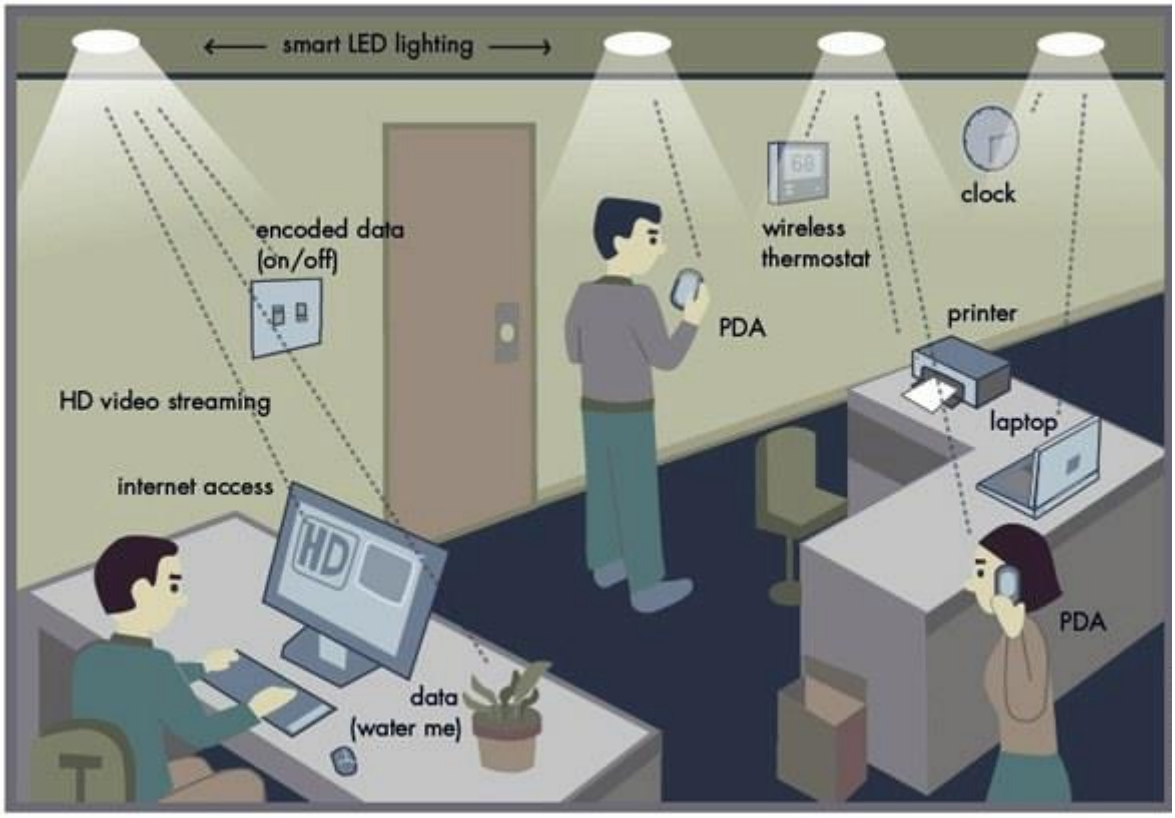

Figure 66 Li-Fi technology

Source: http://www.guidingtech.com/assets/postimages/2015/11/Lifi_environment.png

Different experiments have shown that indoor positioning system can be used with Wi-Fi since it gives high accuracy compared to other technology. This will also help to locate the position of individual inside the building and track his activity more accurately. For user inside building, it will help them navigate the area easily.

REFERENCES

1. Customers Centric Technology You Never Heard Of-08-01T09:53:38+00:00, 2016-last update. Available: https://www.tagove.com/customers-centric-technology/ [Dec 17, 2016].

2. Rules for Successful Hotel Wi-Fi - Wireless LAN Professionals --06-01T11:15:53+00:00, 2015-last update. Available: http://www.wlanpros.com/rules-successful-hotel-wi-fi-3/ [Dec 8, 2016].

3. Eduroam(R) celebrates a decade of providing secure roaming Internet access for users; Innovative service supported by GEANT and TERENA enables mobility for researchers and students across 54 countries. 2012. *M2 Press wire*

4. Wireless ethernet for industrial applications. 2006. *Assembly Automation,* 26(3).

5. 12:00PM, EDITOR POSTED 2 SEP 2015-, -09-02T12:00:22+00:00, 2015-last update, 10 steps to staying secure on public Wi-Fi. Available: http://www.welivesecurity.com/2015/09/02/10-steps-staying-secure-public-wi-fi/ [Dec 10, 2016].

6. ABDUL HALIM ALI, MOHD RAZIFF ABD RAZAK, NUR AYUNIE MOHD HAZMAN, NURFADLINA JAFAAR MOHD ZAIM MOHD JASMIN and MUZAIYANAH HIDAYAB, 2015. *The Comparison Study of RF Signal Strength between IEEE802.11b/g and IEEE802.11n.*

7. AEROHIVE NETWORKS, 2013. *Wireless LAN Best Practices for Compliant Care.*

8. AIR MAGNET, 2007. Best Practices for Wireless Site Design.

9. ALOUNEH, S., ABED, S., KHARBUTLI, M. and MOHD, B., 2014. MPLS technology in wireless networks. *Wireless Networks,* 20(5), pp. 1037-1051.

10. ANASTASI, G., 2008. 802.11 power-saving mode for mobile computing in Wi-Fi hotspots: Limitations, enhancements and open issues. *Wireless Networks.*

11. BANERJI, S. and CHOWDHURY, R.S., 2013. On IEEE 802.11: Wireless LAN Technology.

12. BHAVNEET SIDHU, HARDEEP SINGH and AMIT CHHABRA, 2007. Emerging Wireless Standards - Wi-Fi, ZigBee and WiMAX. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering,* 1(1).

13. BIJU, I., 2009. *IEEE 802.11 Wireless networks.* Saarbrucken: VDM Verl. Müller.

14. BRADLEY MITCHELL, October 16, 2016-last update, 5 GHz vs. 2.4 GHz Wi-Fi - which one is better for home networking. Available: https://www.lifewire.com/is-5-GHz-wifi-better-than-2-4-GHz-818293 [Dec 13, 2016].

15. CHARTERED INSTITUTE OF LIBRARY AND INFORMATION PROFESSIONALS (GREAT BRITAIN), 2007. Journal of information literacy.

16. COMER, D., 2009. *Computer networks and internets.* 5. ed., internet ed. edn. Upper Saddle River, NJ [u.a.]: Pearson Prentice Hall.

17. DELOITTE, 2014. Customer centricity Embedding it into your organization's DNA.

18. ENTERASYS NETWORKS, I., 2002. *802.11 Wireless Networking Guide.*

19. ERNST & YOUNG GLOBAL LIMITED, 2013. *The journey toward greater customer centricity.*

20. FUJINO NAOJI, 2015. Wireless Network Technology to support the age of lot.

21. GALLO, P., 2016. SDN@home: A method for controlling future wireless home networks. *IEEE Communications Magazine,* 54(5), pp. 123-131.

22. GAST MATTHEW, 2013. *802.11ac: A Survival Guide.*

23. GEMBER, A., 2011. A Comparative Study of Handheld and Non-Handheld Traffic in Campus Wi-Fi Networks. *Passive and Active Measurement.*

24. HALSALL, F., 2005. *Computer networking and the internet.* 5. ed. edn. Harlow [u.a.]: Addison-Wesley.

25. HUNT, C., 2002. *TCP/IP network administration.* 3rd ed. edn.

26. IEEE COMPUTER SOCIETY, 2014. 802 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. *IEEE STANDARD ASSOCIATION.*

27. JAMES F. KUROSE and KEITH W. ROSS, 2013. *Computer Networking: A Top-Down Approach: International Edition.* 6th ed., International ed. edn. GB: Pearson Education M.U.A.

28. JUNIPER NETWORKS, 2011. *Security Best Practices for the Mobile Enterprise.* Juniper Networks.

29. KAPPEL, G., 2006. *Web engineering.* Chi Chester: Wiley.

30. KHASAWNEH, M., 2014. A Survey on Wi-Fi Protocols: WPA and WPA2. *Recent Trends in Computer Networks and Distributed Systems Security.*

31. KRALICEK, E., 2016. Home Networking. *The Accidental Sysadmin Handbook.*

32. KÜHNLE, H. and DEKKERS, R., 2012. *Journal of Manufacturing Technology Management.* Emerald Group Publishing Limited.

33. LACHU ARAVAMUDHAN, STEFANO FACCIN, RISTO MONONEN, BASAVARAJ PATIL, YOUSUF SAIFULLAH, SARVESH SHARMA and SRINIVAS SREEMANTHULA, Jul 4, 2003-last update, Getting to Know Wireless Networks and Technology. Available: http://www.informit.com/articles/printerfriendly/98132.

34. LUIZ FELIPE PERRONE, YOUGU YUAN and DAVID M. NICOL, 2003. MODELING AND SIMULATION BEST PRACTICES FOR WIRELESS AD HOC NETWORKS. *Proceedings of the 2003 Winter Simulation Conference,* pp. 685-693.

35. LUK ELLIS, July 17, 2012-last update, 5 reasons why customer centricity leads to success. Available: https://www.totango.com/blog/author/ellis-luk/ [9th Jan 2017].

36. MARANGAZE, M.M., 2011. Characterizing University WLANs within Eduroam Context. *Smart Spaces and Next Generation Wired/Wireless Networking.*

37. MARECO DANNY, 5 Campus Wi-Fi Trends Every College CIO Needs to Follow. Available: http://www.securedgenetworks.com/blog/5-campus-wifi-trends-every-college-cio-needs-to-follow [Dec 12, 2016].

38. MICROSOFT INC, 2016-last update, About Wi-Fi Sense. Available: https://privacy.microsoft.com/enus/ windows10aboutwifisense [20 December 2016].

39. MIN-KYU CHOI, ROSSLIN JOHN ROBLES, CHANG-HWA HONG and TAI-HOON KIM, 2008. Wireless Network Security: Vulnerabilities, Threats and Countermeasures. *International Journal of Multimedia and Ubiquitous Engineering,* 3(3), pp. 77-86.

40. MINOLTA KONICA, 2015. Facing Customer Problems to create Satisfaction and Happiness.

41. NETGEAR, 2016. *Best Practices for High Density Wireless Network Design In Education and Small/Medium Businesses.*

42. NEWMAN, W.M. and LAMMING, M.G., 1995. *Interactive system design.* 1. print. edh. Wokingham u.a: Addison-Wesley.

43. OSTERHAGE, W., 2016. *Wireless Security.* 1 edn. Boca Raton: CRC Press.

44. RAMAN, B. and CHEBROLU, K., 2007. Experiences in using Wi-Fi for rural internet in India. *IEEE Communications Magazine,* 45(1), pp. 104-110.

45. RIMPILAINEN MARKKU, 18 April 2016-last update, 5 Ways to Become Customer Centric. Available: https://managementevents.com/news/become-customer-centric-with-design-thinking/.

46. SANDERS HELEN, 2015-last update, Are There Any Wi-Fi Health Risks? Available: https://www.healthambition.com/wifi-health-risks [13 Jan 2017].

47. SCAR CNOVAS, HAW HAMBURG, HAMBURG, GERMANY, 2007. Deploying authorization mechanisms for federated services in Eduroam (DAMe). *Internet Research,* 17(5), pp. 479.

48. SEBELE BRIAN, 2016. *Li-Fi: Lighting the Future of Wireless Networks.*

49. SEUFERT, M., BURGER, V. and HOSSFELD, T., 2013HORST - Home router sharing based on trust, 2013, pp. 402-405.

50. SHAH DARSHAN and SHAH KAVISH, 9 December 2016-last update, Basic of Wi-Fi based positioning system. Available: https://www.researchgate.net/publication/232729025 [15 January 2017].

51. SHETH, A., SRINIVASAN SESHAN and DAVID WETHERALL, 2009. Geo-fencing: Confining Wi-Fi Coverage to Physical Boundaries. *Pervasive Computing.*

55. SHI, J., GUI, L., KOUTSONIKOLAS, D., QIAO, C. and CHALLEN, G., Sep 11, 2015A Little Sharing Goes a Long Way, Sep 11, 2015, ACM, pp. 6-10.

52. SIMONITE TOM, 15 January 2015-last update, A Speedy Wireless Protocol Is Coming to Many Gadgets. Available: https://www.technologyreview.com/s/543216/a-speedy-protocol-is-coming-to-many-gadgets/ [15 January 2016].

53. SOLOMON, M., JUL 20, 2014-last update, 7 Secrets of Building a Customer-Centric Company Culture. Available: http://www.forbes.com/sites/micahsolomon/2014/07/20/customer-centric-culture/ [Dec 17, 2016].

54. STAJANO, F., 2011. Pico: No More Passwords! *Security Protocols XIX.*

55. TAHARMEKHAZNIAABDELMADJIDZIDANI, 2015. Wi-Fi Security Analysis. *Procedia Computer Science,* pp. 172-178.

56. THE ECONOMIST, 2004. A brief history of Wi-Fi. *The Economist.*

57. TORE KRISTIANSEN, JARDAR LEIRA and VIDAR FALTINSEN, 2010. *Guide to configuring Eduroam using a Cisco wireless controller Best Practice Document.* UNINETT led working group on mobility (No UFS127).

58. VAUGHAN-NICHOLS, S.J., 2010. Gigabit Wi-Fi is on Its Way. *Computer,* 43(11), pp. 11-14.

59. VICTOR, C.M.L., 2006. Advances in Wireless Personal Area Networking. *Ad-Hoc, Mobile, and Wireless Networks.*

60. WI-FI ALLIANCE, 2017-last update, Wi-Fi Certification. Available: https://www.wi-fi.org/ [15 January 2017].

61. Hing Kai Chan. 2010. Agent-Based Factory Level Wireless Local Positioning System with ZigBee Technology. *IEEE Systems Journal* 4:2, 179-185.

62. Webinar: SD-WAN and Beyond: Critical Capabilities for a Successful WAN Transformation. Date: Wednesday, Jan 25, 2017 1:00 PM - 2:00 PM EST

63. Webinar: The 11ac Wi-Fi Performance Workshop. Date: Thursday, 19th Jan 2017 11:00 – 12:00 GMT

64. Webinar: Cellular Networks – Planning and Development. Date: Date: Wednesday, 14th Dec 2016, 1:00 PM – 2:00 PM EDT

APPENDIX 1. SAMPLE OF INTERVIEW QUESTION

Open your mind. LUT.
Lappeenranta University of Technology

LOAS

Introduction

First Name: ..... Last Name: .....

Email Address: ..... Gender: Male/Female

Country: ..... Degree: .....

Starting Year:.....

Address (LOAS Apartment): .....

Age Group:

☐ < 17 ☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ >46

Interview Date : ..... Signature: .....

Services

1. Tell us about your experience on internet service from LOAS.

ANS:

2. How long do you stay online and for what purpose mostly?

ANS:

3. Have you heard about the smart devices or used any of them?

ANS:

4. Have you had any problem in LNET? How do you solve it?

ANS:

Wireless

1. What is your experience in current Wi-Fi connection? How are you connected to Wi-Fi?

ANS:

Open your mind. LUT.
Lappeenranta University of Technology

LOAS

2. What devices you own have Wi-Fi capability? Do you wish something more from Wi-Fi?

ANS:

3. What do you think of Smart devices that are trending currently in market? Do you like to own any of them?

ANS:

Eduroam

1. What do you think about Eduroam and its features?

ANS:

2. Have you faced any problem with Eduroam?

ANS:

3. What other services do you think Eduroam should provide students except basic Wi-Fi connectivity?

ANS:

Security

1. How much secure do you feel while using internet in your Apartment? (both LAN and Wi-Fi)

ANS:

2. Have you had any security issues with LNET?

ANS:

3. Do you regularly change Wi-Fi and other passwords?

ANS:

Value Added Services

1. What other services do you think will be appropriate for LNET users except basic internet connection?

ANS:

2. What could be your three suggestions for LOAS?

ANS:

APPENDIX 2. SETTING UP FREE RADIUS ON CENTOS.

FreeRADIUS is a free and open source modular, high performance free RADIUS package developed and distributed under the GNU Public License. Below is the guide to install FreeRADIUS on Red Hat 6 from

1. Install FreeRADIUS

Install MySQL-server to store free RADIUS user list. If you have not installed the MySQL in your system, then install it using the following command.

#yum install mysql-server

Once MySQL server has been installed, execute the following command to install freeradius packages.

#yum install freeradius freeradius-mysql freeradius-utils

2. Configure MySQL/RADIUS

Execute the following command to start MySQL and FreeRADIUS

#service mysqld start

#service radius start

Now login to mysql as a root user. Create a database by the name “radius” and a user by the name “usr_radius”. Grant all permissions on radius database to usr_radius.

mysql -u root -p

mysql> create database radius;

mysql> GRANT all ON radius.* TO usr_radius@localhost IDENTIFIED BY ‘somepass’;

mysql> exit;

Now import the mysql schemas from /etc/raddb/sql/mysql

mysql -u usr_radius -p radius < /etc/raddb/sql/mysql/cui.sql

mysql -u usr_radius -p radius < /etc/raddb/sql/mysql/ippool.sql

mysql -u usr_radius -p radius < /etc/raddb/sql/mysql/nas.sql

mysql -u usr_radius -p radius < /etc/raddb/sql/mysql/schema.sql

mysql -u usr_radius -p radius < /etc/raddb/sql/mysql/wimax.sql

You will be prompted to enter password for 5 times to finish the import.

3. Configure RADIUS

Edit /etc/raddb/radiusd.conf using nano

nano /etc/raddb/radiusd.conf

Search for the line $INCLUDE sql.conf and uncomment the line.

Now edit the file /etc/raddb/sql.conf and set values as such

server = “localhost”

login = “usr_radius”

password = “somepass”

……..

……

……

readclients = yes

Edit the radius default file **/etc/raddb/sites-enabled/default** and uncomment the line in Authorize section that says “sql”

Again, uncomment the line that says “sql” in **Accounting** section

4. Restart MySQL/Radius

Now restart mysqld and radiusd services to apply the configuration

service mysqld restart

service radiusd restart

5. Insert dummy entry to MySQL

To check the RADIUS server, insert a dummy entry to MySQL. Login to MySQL as radius user.

#mysql -u usr_radius -p

When prompted, type your password

Now insert a dummy entry.

Mysql> INSERT INTO radcheck (username, attribute, value) VALUES (‘testuser’, ‘Password’, ‘somepass’);

6. Test radius server

Execute the following command to check the radius server

radtest testuser somepass localhost 1812 testing123

The last line in the response should be like

rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=19, length=20

The Access-Accept word confirms that RADIUS server is up and running. Check the screen shot below.

This completes the installation of freeRADIUS

(Source: https://hostingwikipedia.com/setup-freeradius-server-centos-6/)

APPENDIX 3. INITIAL CONFIGURATION OF AP

In the first phase, the controller must be accessed through the Command Line Interface (CLI). When an IP address has been assigned to the controller, further configuration can be done using the web interface, but the CLI can be continued to be used. The example configuration shown in below was obtained from a Cisco 4400 Series Wireless LAN Controller.

Establish access to the controller by using a serial console and configure the initial settings for example as follows.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_b2:e2:83]: <your_system_name>
Enter Administrative User Name (24 characters max): <your_username>
Enter Administrative Password (24 characters max): <your_password>
Re-enter Administrative Password                 : <your_password>

Service Interface IP Address Configuration [none][DHCP]: DHCP

Enable Link Aggregation (LAG) [yes][NO]: NO

Management Interface IP Address: esim. xxx.yyy.zzz.1
Management Interface Netmask: <your_network_mask>
Management Interface Default Router: <your_router's_IP_address>
Management Interface VLAN Identifier (0 = untagged): <0 or 1>
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: esim. xxx.yyy.zzz.2

AP Transport Mode [layer2][LAYER3]: <layer2 if controller and access
points are on same subnet; layer3 if routing in between>
AP Manager Interface IP Address: esim. xxx.yyy.zzz.3

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (xxx.yyy.zzz.2):
```

Virtual Gateway IP Address: xxx.yyy.zzz.www

Mobility/RF Group Name: <choose a suitable name if you have more than one controller. Otherwise, don't care>

Enable Symmetric Mobility Tunneling [yes][NO]: NO

Network Name (SSID): <Define a test SSID at first>
Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no #Will be done later
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: <your country abbreviation>

Enable 802.11b Network [YES][no]: no
Enable 802.11a Network [YES][no]: YES
Enable Auto-RF [YES][no]: YES

Configure a NTP server now? [YES][no]: no #Will be done later
Configure the system time now? [YES][no]: no #Will be done later

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

#When the system has rebooted, familiarize yourself with the CLI by defining
(Cisco Controller) >config time ntp server 1 xyz.zyx.zzy.wyz
(Cisco Controller) >config time ntp server 2 xyz.zzz.zzy.wyz

APPENDIX 4. LOAS BUILDINGS.

CAMPUS AREA
LOAS TIMPPA
Laserkatu 1

Completed in 2016
One eight-storey apartment building with one stairwell and one five-...

VIEW LOCATION

HARAPAINEN
KANGASTUPA 1
Kangastuvankatu 4 ja 6

Completed in 1998
Two three-storey apartment buildings, each with one stairwell

VIEW LOCATION

HARAPAINEN
KANGASTUPA 2
Kangastuvankatu 2

Completed in 2003
One three-storey apartment building with one stairwel

VIEW LOCATION

KOURULA AND HUHTINIEMI
KARELIA
Korpraalinkuja 3

Completed in 1971
Renovated in 1997

VIEW LOCATION

KOURULA AND HUHTINIEMI
KATAJAKATU
Katajakatu 8

Completed in 1976, Renovated in 1996

VIEW LOCATION

CITY CENTRE
KOLJONLINNA
Snellmaninkatu 13

Completed in 2005

VIEW LOCATION

CAMPUS AREA
KOTANIEMI
Tervahaudankatu 1

Completed in 2002

VIEW LOCATION

KOURULA AND HUHTINIEMI
KOURULA
Karankokatu 4

Completed in 1980
Renovated in 2005 and 2006

VIEW LOCATION

CAMPUS AREA
LASERPUISTO
Laserkatu 3

Completed in 1992
Three three-storey gallery-access buildings

VIEW LOCATION

CITY CENTRE
LEIRI
Leirikatu 2

Completed in 1991–1992

VIEW LOCATION

CAMPUS AREA
LOAS SEPPO
Skinnarilankatu 28 G

Completed in 2013
One eight-storey apartment building with one stairwell

VIEW LOCATION

CAMPUS AREA
ORION 1
Korpimetsänkatu 5

Completed in 1992
Four four-storey apartment buildings, each with one stairwell

VIEW LOCATION

CAMPUS AREA
ORION 2
Korpimetsänkatu 10

Completed in 1997

VIEW LOCATION

CAMPUS AREA
ORION 3
Korpimetsänkatu 6-8

Completed in 2000
Three three-storey apartment buildings, each with one stairwell

VIEW LOCATION

CAMPUS AREA
ORION 4
Korpisuonkatu 14

Completed in 2000

VIEW LOCATION

CAMPUS AREA
ORION 5
Kaivosuonkatu 1

Completed in 2003
Two three-storey apartment buildings, each with two stairwells

VIEW LOCATION

CAMPUS AREA
ORION 6
Kaivosuonkatu 2

Completed in 2004
Two three-storey apartment buildings, each with two stairwells

VIEW LOCATION

PALLO AND RAKUUNAMÄKI
PALLO
Taipalsaarentie 2

Completed in 1982
Renovated in 1999

VIEW LOCATION

KOURULA AND HUHTINIEMI
PARK
Korpraalinkuja 1

Completed in 1970
Renovated in 1997

VIEW LOCATION

CITY CENTRE
PELTOLA
Savonkatu 32

Completed in 1980
Renovated in 2004

VIEW LOCATION

CITY CENTRE
PELTOLA 2
Väinölänkatu 27

Completed in 1983
Renovated in 2008

VIEW LOCATION

CAMPUS AREA
PUNKKERIPARI
Punkkerikatu 1

Completed in 1977–1978
Renovated in 1997

VIEW LOCATION

KAMPUSALUE
PUNKKERIRINNE
–

Completed in 1990

VIEW LOCATION

CAMPUS AREA
PUNKKERIRIVI
Linnunrata 10

Completed in 1982–1983
Renovated in 2002–2003

VIEW LOCATION

CAMPUS AREA
PUNKKERITIENOO
Punkkerikatu 5

Valmistumisvuosi 1979
Peruskorjattu 2001

VIEW LOCATION

CAMPUS AREA
PUNKKERITORNI
Punkkerikatu 2

Completed in 1981
Renovated in 1998

VIEW LOCATION

PALLO JA RAKUUNAMÄKI
RAKUUNAPORTTI
Väinö Valveen katu 5 ja 7

Completed in 2001

VIEW LOCATION

CAMPUS AREA
RUOTSALAISENRAITTI
Ruotsalaisenraitti 3

Completed in 1975
Renovated in 1995
Facade renovation completed in 2014

VIEW LOCATION

SAMMONLAHTI
SAMMONLAHTI 1
Ruskonlahdenkatu 13-15

Completed in 198
Renovated in 2010

VIEW LOCATION

SAMMONLAHTI
SAMMONLAHTI 2
Kalliopellonkatu 10

Completed in 1993
One three-storey apartment building with two stairwells

VIEW LOCATION

CAMPUS AREA
SKINNARILA 1
Skinnarilankatu 28

Completed in 1985
Renovated in 2008

VIEW LOCATION

CAMPUS AREA
SKINNARILA 2
Teknologiapuistonkatu 4

Completed in 1989 Renovated in 2014

VIEW LOCATION

CAMPUS AREA
SKINNARILA 3
Teknologiapuistonkatu 2

Completed in 1998

VIEW LOCATION

PALLO AND RAKUUNAMÄKI
TERVARANTA
Huopatehtaankatu 2

Completed in 1984
Renovated in 2009

VIEW LOCATION

PALLO AND RAKUUNAMÄKI
UPSEERITIE
Upseeritie 1

Completed in 1999
Renovated early 20th century barracks building

VIEW LOCATION

APPENDIX 5. QUESTIONNAIRES DATA.

Gender

According to the collected data sample most of the participants were male.

Answer	Responses	Percentage
Male	218	72.19%
Female	84	27.81%
Total Responses	302	

Figure 67 Gender

Age

This shows that most of the tenants of LOAS are between the ages of 18 to 25.

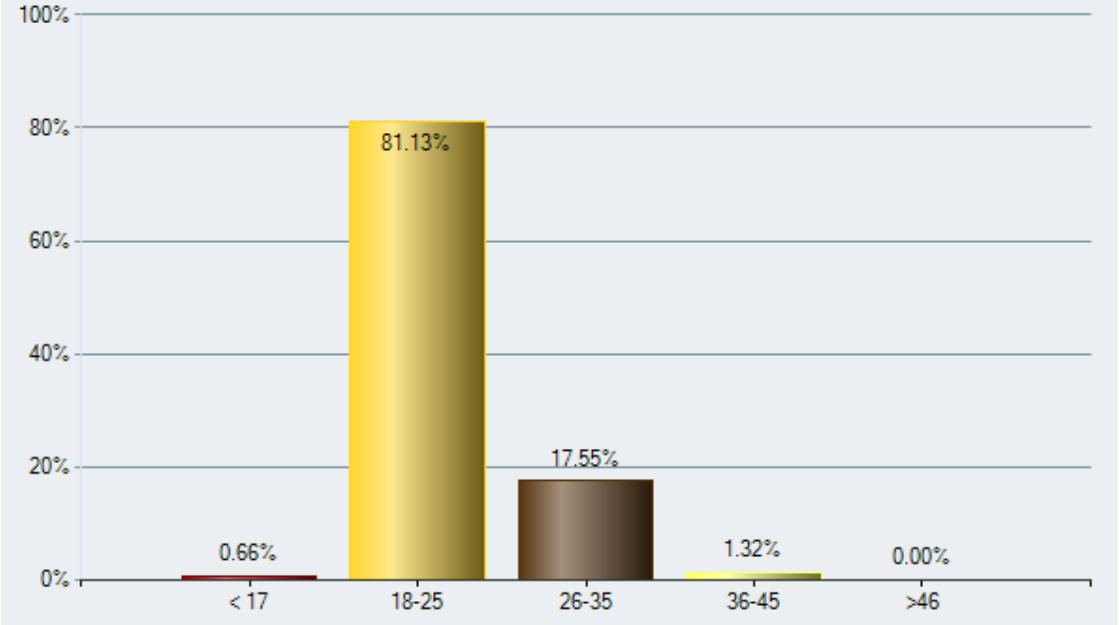

Figure 68 Age group

Country

The questionnaire was answered by enormous number of people from different background but most interesting was the variation in nationality. It turned out that the survey was answered by students from 31 nationalities which also represent the variation of students living in LOAS's apartment from different part of the world and it helps validate our finding more accurately.

Table 4 Countries

SN	Country	Number	Percent
1	Finland	210	69.54%
2	Russia	27	8.94%
3	India	7	2.32%
4	Germany	6	1.99%
5	Bangladesh	5	1.66%
6	Nepal	5	1.66%
7	France	4	1.32%
8	Italy	4	1.32%
9	Vietnam	4	1.32%
10	China	3	0.99%
11	Pakistan	3	0.99%
12	Spain	3	0.99%
13	Poland	2	0.66%
14	South Korea	2	0.66%
15	Bosnia	1	0.33%
16	Czech Republic	1	0.33%
17	Ecuador	1	0.33%
18	Ghana	1	0.33%
19	Greece	1	0.33%
20	Hungary	1	0.33%
21	Iran	1	0.33%
22	Kazakhstan	1	0.33%
23	Lithuania	1	0.33%
24	Macedonia	1	0.33%
25	Mexico	1	0.33%
26	Nigeria	1	0.33%
27	Peru	1	0.33%
28	Sri Lanka	1	0.33%
29	Taiwan	1	0.33%
30	Ukraine	1	0.33%
31	Uzbekistan	1	0.33%
	Total	302	99.97%

When did you start studying in LUT?

This question also supports our validity of findings as most of the students answering the questions are current students of LUT and living in LOAS's apartment.

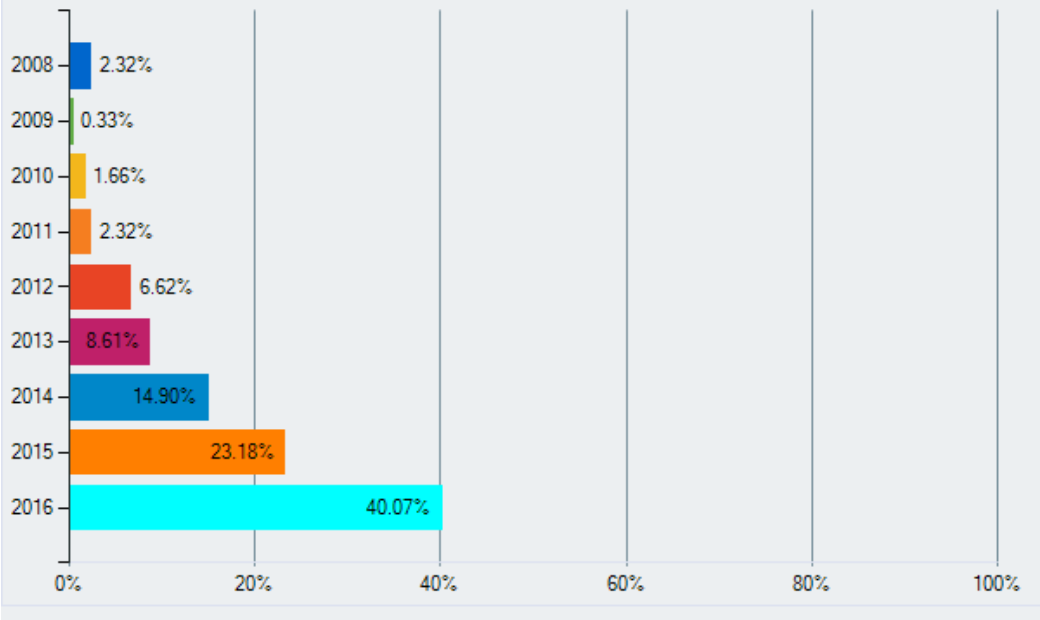

Figure 69 Starting Year

In LNET, which kind of application do you use most?

Email, web browsing and social networking are the most widely used applications by respondents.

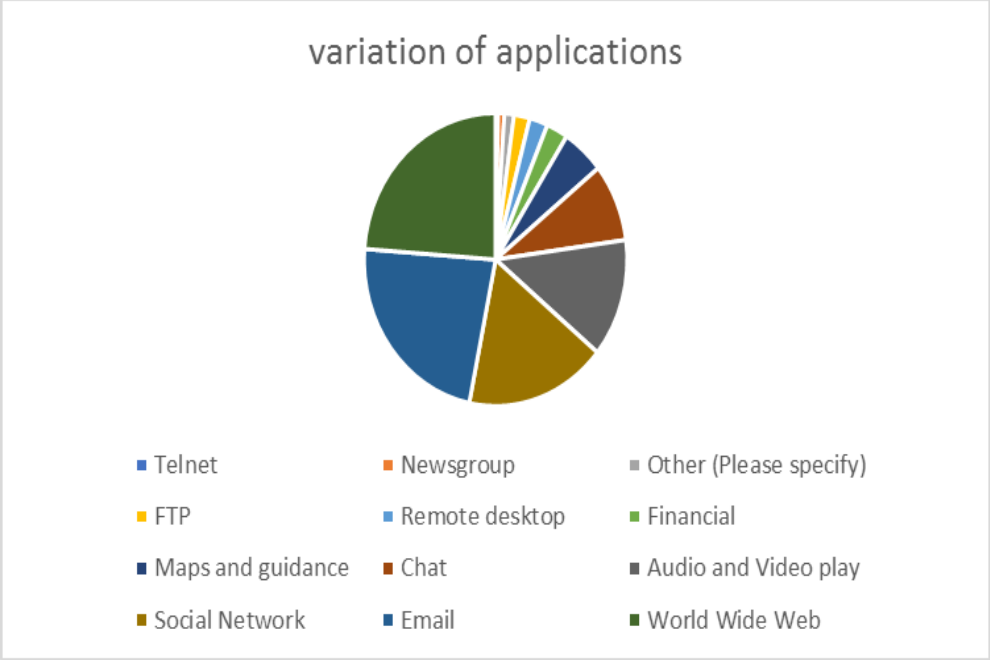

Figure 70 Variation of application

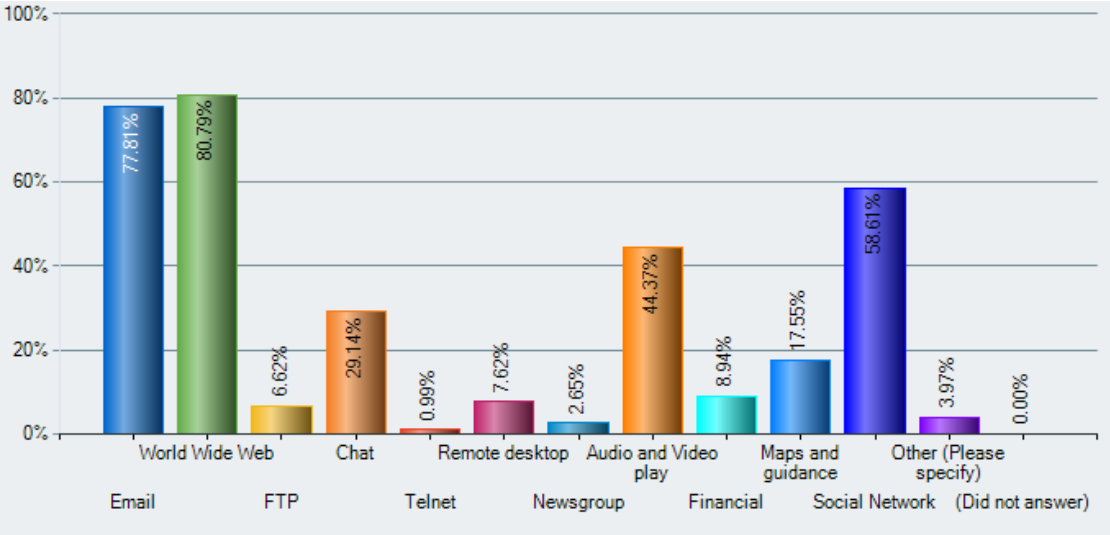

Figure 71 Applications

Do you own any internet enabled smart devices other than smart phone?

More than half of the users don't have any other smart devices except smartphone.

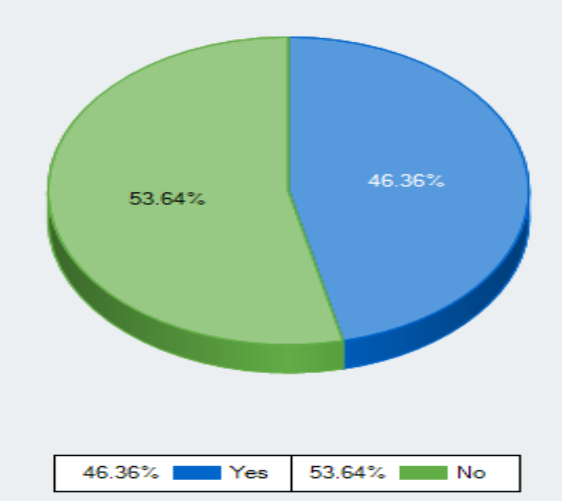

Figure 72 Any other smart devices?

Do you own smart TV or plan to buy one soon?

Very few of the tenant own smart TV.

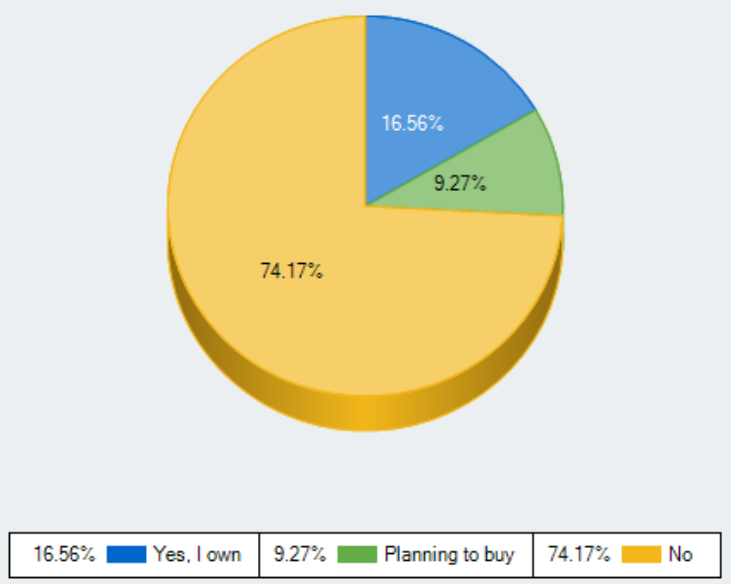

Figure 73 Smart TV

Have you had any security issues with LNET or eduroam?

Negligible respondents have security issues with eduroam.

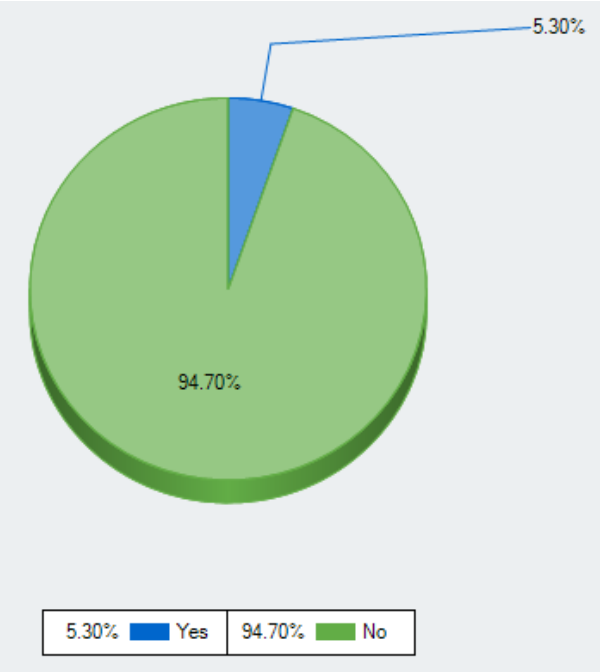

Figure 74 Problem with Network

Have you ever been warned about internet security issues from LNET?

Almost none of the people are warned of any security issues from LNET.

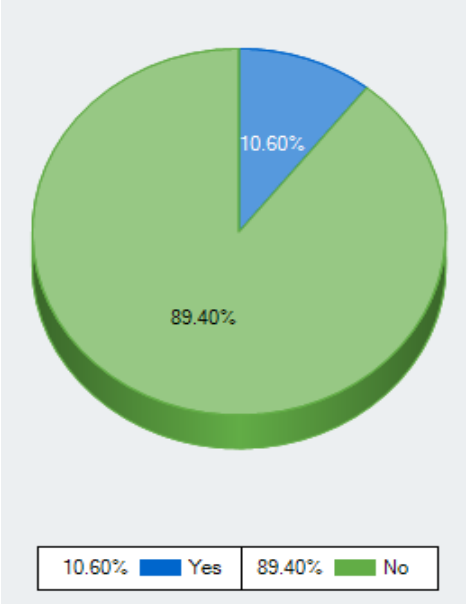

Figure 75 Security issues

How often do you change your LNET, Wi-Fi and eduroam password?

Half of the respondent never change Wi-Fi password.

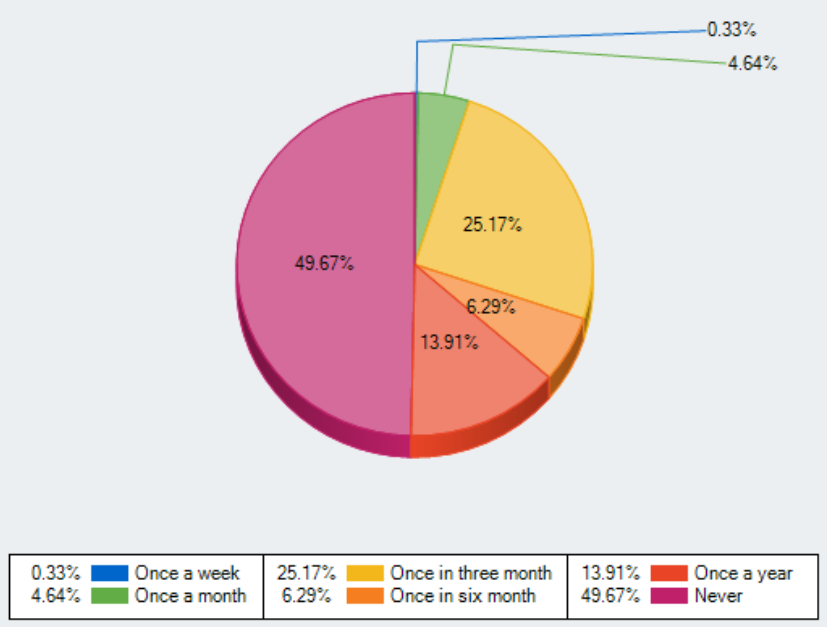

Figure 76 Wi-Fi password

How secure do you feel when connecting to LNET or eduroam?

Most of the people feel secured while connecting to eduroam.

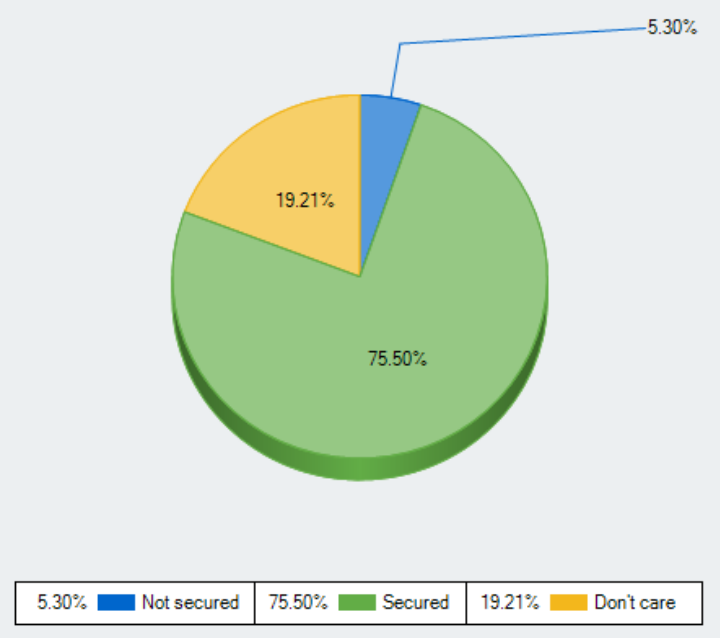

Figure 77 How secure do you feel?

Do you check how many users are connected from your Wi-Fi connection?

Only 10% of the respondent check the users of their Wi-Fi.

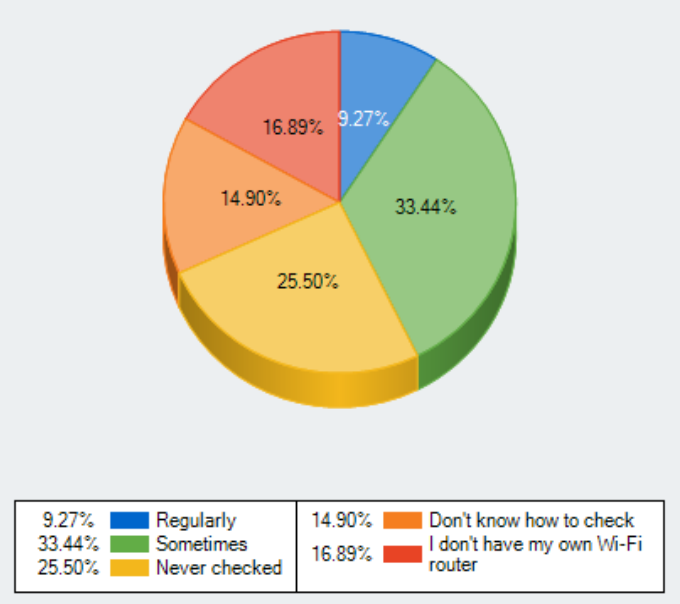

Figure 78 No of users in Wi-Fi

Have you ever had your Wi-Fi password compromised?

Around 70% of the respondents never had their Wi-Fi password stolen.

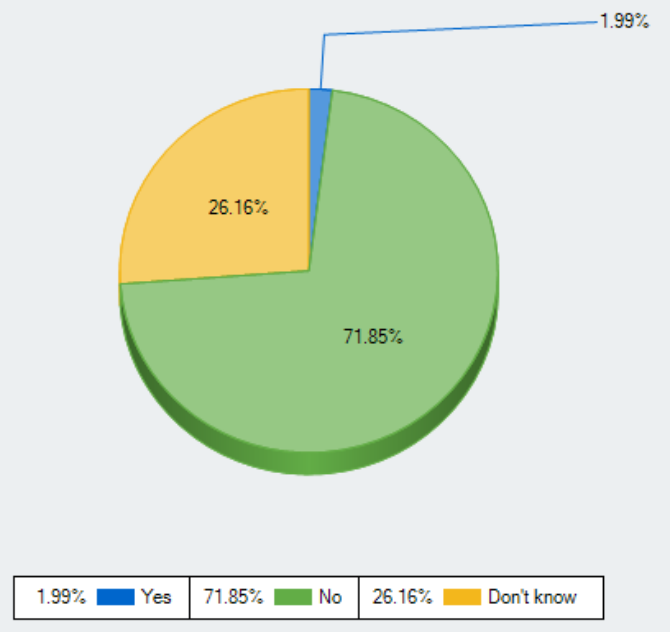

Figure 79 Have you ever had your password compromised?

Have you used any of the following devices?

Smart TV is most widely used device except smartphone.

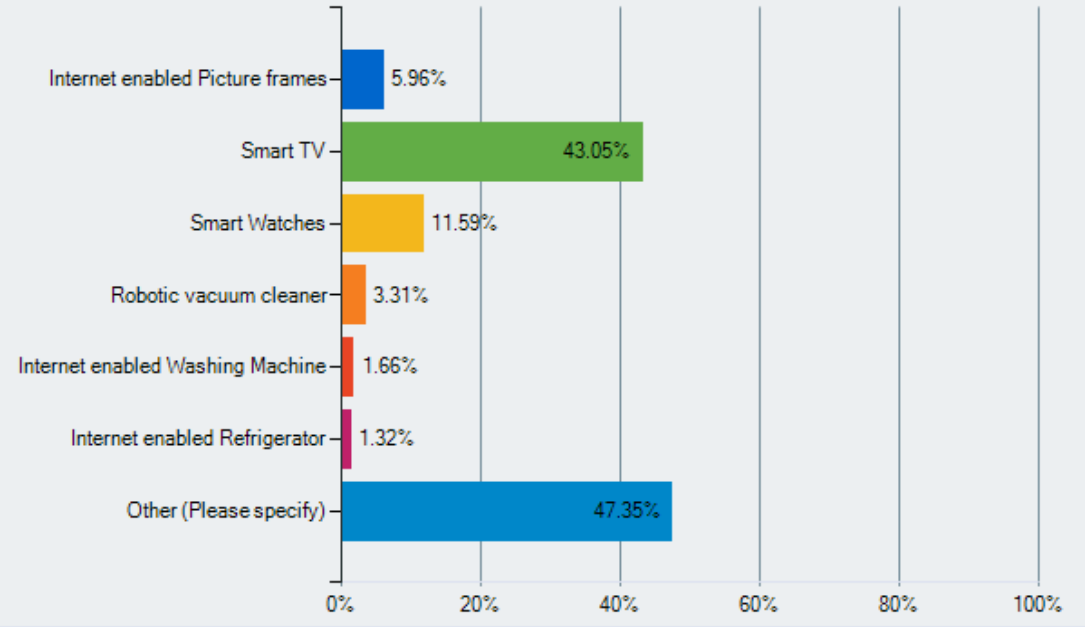

Figure 80 Smart devices

Will you subscribe to services like chrome cast, security cameras, smart TV connection etc. if they are provided on same

Very few of the respondents are ready to pay for services like Chromecast and internet TV.

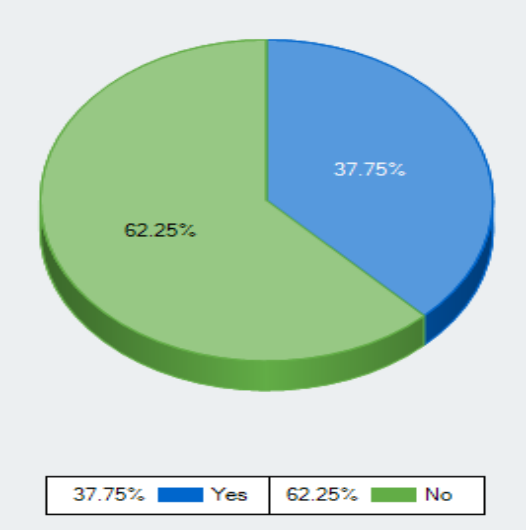

Figure 81 Will you pay for new services?

APPENDIX 6. CONFIGURING MULTIPLE 802.1X AUTHENTICATION

Command example for configuring Multiple 802.1X authentication in cisco devices.

```
aaa new-model
!
!
aaa authentication login CON local
aaa authentication login VTY local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
!
aaa session-id common
!
dot1x system-auth-control
!

interface FastEthernet1
 switchport access vlan 20
 switchport voice vlan 117
 no ip address
 authentication host-mode multi-auth
 authentication order mab
 authentication port-control auto
 mab
 dot1x pae authenticator
end
```