



Joseph Adovi M.E Aduayi-Akue

# DEPLOYMENT OF EDUROAM FEDERATED WIRELESS NETWORK

Faculty of Information Technology  
2010

VAASAN AMMATTIKORKEAKOULU  
UNIVERSITY OF APPLIED SCIENCES  
Degree Programme in Information Technology

## ABSTRACT

Author	Joseph Adovi M.E. Aduayi-Akue
Title	Deployment of Eduroam Federated Wireless Network
Year	2010
Language	English
Pages	82
Name of Supervisor	Antti Virtanen

---

The aim of this project is to deploy the federated wireless network eduroam on the campuses of Vaasa University of Applied Sciences. The project is divided into two parts: the deployment on campuses and the connection to the national network.

This thesis focuses on implementation, set up and configuration of different systems composing eduroam. The theoretical part aims to provide enough comprehensive background about the system. The network terms such as wireless network, switch, access points, server etc. are discussed. A major part of the theory is devoted to the explanation of eduroam wireless network.

During the implementation, a proxy server will be set and configured. More than 40 switches and access points will be configured. When the implementation is completed, tests will be made from VAMK campuses using local and external credentials. At the same time, VAMK credentials will be used on another eduroam-enabled campus to test the remote authentication.

After everything has been properly configured, users from VAMK can use the eduroam network from any eduroam-enabled institution in the world. Also users also from different institutions will be able to log in on VAMK campuses with their home credentials.

Moreover I will configure different client computers with different operating systems to be able to connect to eduroam. Lastly, I will write a detailed supplicant configuration that can be used by any IT unfamiliar user to get connected to the network.

---

**Keywords:** Eduroam, Wireless network, 802.1X, PEAP-MS-CHAP v2, RADIUS

## **ACKNOWLEDGEMENT**

I am grateful to Almighty God who has been with me and keeps protecting and blessing me wherever I am and in everything I do.

This thesis is dedicated to my mother Irene Mawussimé Akato who has been a key person since I decided to come to Finland and who has never forgotten me in her prayers.

I appreciate the support from my supervisor Antti Virtanen who has guided me through this thesis. His way of motivating students and giving feedback is very helpful.

My regards go to Hannu Teulahti, VAMK's Linux administrator and project manager who supported me during the implementation. Through him, my passion of using Linux operating systems has increased.

My regards also to Wenche Backman from CSC-IT (Center for Science Ltd); I appreciate the time and support she has given me during this project.

To my friends Igodo Koko, Lotchi Nyalali and MariaPia Becker I am grateful. They have always been there listening to my complaints and fears about the evolution of the project.

I would also like to thank my family, all my friends in Finland, Germany and Togo for the everlasting support during my studies.

To the staff of Vaasa University of Applied Sciences, I am deeply grateful. You helped me make my dreams true.

Vaasa, 3<sup>rd</sup> June 2010.

Joseph Adovi Aduayi-Akue

## ABBREVIATIONS

AAA	Authentication Authorisation Accounting
AES	Advanced Encryption Standard
AP	Access Point
DHCP	Dynamic Host Control Protocol
EAPOL	Extensible Authentication Protocol Over LAN
EDUROAM	Educational Roaming
ETLR	European Top-Level RADIUS server
FUNET	Finnish Universities Network
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MS-CHAP v2	Microsoft's Challenge Handshake Authentication Protocol version 2
NAS	Network Access Server
NPS	Network Policy Server
NREN	National Research and Education Network
NTLR	National Top-Level RADIUS server
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
RADIUS	Remote Authentication Dial In User Service

SP	Service provider
TERENA	Trans-European Research and Education Networking Association
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VAMK	Vaasan ammattikorkeakoulu
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

# Contents

ABSTRACT	2
ACKNOWLEDGEMENT	3
ABBREVIATIONS	4
1 INTRODUCTION	8
2 BACKGROUND AND AIMS OF THE PROJECT	9
2.1 Background Information.....	9
2.2 Educational Roaming (eduroam).....	10
2.3 Eduroam confederation.....	10
2.4 Vaasa University of Applied Sciences .....	13
2.5 Structure of the thesis .....	14
3 PROJECT DESCRIPTION	16
3.1 Eduroam concept .....	16
3.2 Network Access Server (NAS).....	18
3.2.1 Wi-Fi Protected Access (WPA).....	19
3.2.2 Wi-Fi Protected Access version 2 (WPA2).....	19
3.3 802.1X protocol.....	20
3.3.1 EAP-Tunnelled Transport Layer Security (EAP-TTLS).....	22
3.3.2 PEAP-MSCHAP.....	23
3.4 RADIUS server .....	24
3.4.1 Service Provider (SP) .....	24
3.4.2 Identity Provider (IdP).....	25
3.5 User Database .....	28
3.6 Network access .....	29
4 DESIGN AND IMPLEMENTATION	30
4.1 Project Planning.....	30
4.2 Overview of the design.....	31
4.2.1 The layer 3 switch.....	32

4.2.2	Playground policy.....	32
4.3	Implementation.....	35
4.3.1	Service provider setting up.....	35
4.3.2	Windows Network Policy Server (NPS) .....	38
4.3.3	Switches configuration .....	41
4.3.4	Access points configuration.....	44
5	TEST, RESULTS AND ANALYSYS	47
5.1	Procedure.....	47
5.2	Test of the VLAN.....	47
5.3	Test of the proxy.....	49
5.4	Test of the network by using VAMK credentials from VAMK campuses .....	50
5.5	Test from other eduroam-enabled campuses with VAMK credentials .....	53
5.6	Test with other eduroam-enabled institution's credentials on VAMK campuses ....	54
6	SUPPLICANTS CONFIGURATION	56
6.1	Definition.....	56
6.2	Certificate installation.....	57
6.3	Network card configuration.....	59
6.3.1	Configuration according to Microsoft Windows.....	59
6.3.2	Configuration based on Ubuntu.....	65
7	CONCLUSION	67
	SUMMARY	70
	REFERENCES	71
	APPENDICES	74
	Appendix 1: proxy.conf.....	74
	Appendix 2: clients.conf.....	76
	Appendix 3: freeradius -X output .....	77
	Appendix 4: Requests forwarding to VAMK NPS process output .....	79
	Appendix 5: Requests forwarding to flr.funet.fi process output .....	81

# 1 INTRODUCTION

The aim of this project is to deploy eduroam (Educational Roaming) federated wireless network. Eduroam is a wireless network connection that grants network access to visiting users. The users who are to log in into the network at the host institution use their credentials from their home institution. By implementing this system on Vaasan ammattikorkeakoulu (VAMK), students and staff members from VAMK will be able to log in into the wireless network at any eduroam-enabled institution anywhere in the world.

The eduroam network architecture is based on the 802.1X authentication method using the Authentication, Authorisation and Accounting (AAA) method of Remote Authentication Dial In User Service (RADIUS). For this project, the authentication type used is Protected Extensible Authentication Protocol Microsoft's Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAP v2).

The project will consist of setting and configuring a new proxy server running FreeRADIUS that will be forwarding RADIUS requests to either VAMK Network Policy Server (NPS) for local authentication (i.e. VAMK users) or to the next hierarchical RADIUS server for other users. It will also require configuration of all the network resources such as switches, access points and firewall.

This thesis will summarise the content of the project from the theoretical aspect to the practical one. In order to have concise description some details will be ignored.



## 2 BACKGROUND AND AIMS OF THE PROJECT

### 2.1 Background Information

With globalization, the world has become like a small village. For many reasons, people travel from city to city or from country to country. Also students and university staffs are now-a-days part of this movement of people. The first group travels for exchange studies and the second for teaching purpose, research and/or administrative reasons.

During the last decade, internet has grown a lot and has become very important in most people's lives. For business, studies, entertainment etc. internet is used almost everywhere and nearly by everybody. Internet has therefore become an important part of our lives. A natural consequence of this is that people in their mobility need internet to accomplish different matters. This fact is the same for students and staff travelling. They need to have internet access for their daily activities.

In almost all institutions, network and internet access need permissions. While visiting universities locally or abroad, students and staff want to access the network resources on their laptop. Network administrators reserve accounts for guests or visitors in order to give them access to network resources (internet). The idea and the concept are good, but not always uncomplicated. What happens for example if the visitor arrives on the weekend and is staying on the campus? Sometimes the people that want to access the network are not on a formal trip. They can be on holidays or just passing by. In this case it is not possible to apply for a guest or visitor account. These facts are some of the issues that the internet access is facing when people are roaming.

Why could not roaming people be able just to use the credentials from their universities to get internet access? It was in the process of answering this question that TERENA (Trans-European Research and Education Networking Association) came up with eduroam (**Educational Roaming**).

## **2.2 Educational Roaming (eduroam)**

The eduroam initiative started in 2003 within TERENA's Task Force on Mobility, TF-Mobility. 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 organisations in Europe embraced the idea and gradually started joining the infrastructure, which was then named eduroam. [4]

The concept of eduroam is based on wireless network. The university that wants to deploy eduroam has to add the access to the wireless infrastructure already in place. Visitors with their laptop configured will be able to get eduroam and have access to internet.

Eduroam allows users from universities connected to the network to get access to network resources in other eduroam-enabled universities by using their credentials from their home university. The basic idea is to give internet access to the users. Depending on the visited university local policy, the eduroam users may have access to some extra resources of the network e.g. printers.

Eduroam, which initially started in Europe, has nowadays become a worldwide network. Eduroam is deployed in Europe, North America, Asia and Pacific.

## **2.3 Eduroam confederation**

As stated earlier eduroam is nowadays a worldwide network. It is subdivided into regions which are groups of confederations (continent level), which themselves are groups of federations (country level).

Federations regroup all the connected institutions from one country. In each country one institution or company operates the federation top-level servers. All the federations on one

continent are regrouped under a confederation. Confederations like federations have institutions or companies that operate the confederation top-level servers.

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 communicate together. Below is a conceptual view of eduroam network:

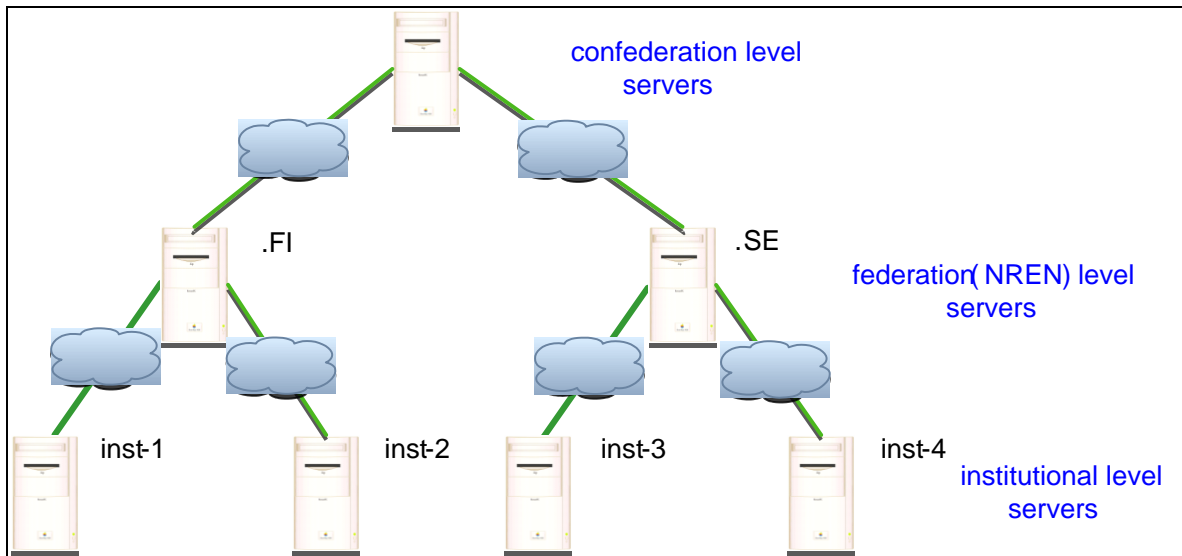


Figure 1: Servers hierarchy within the eduroam network.

In Europe, the eduroam project is driven by GÉANT2 which is co-funded by European National Research & Education Networks (NRENs) and the European Commission (EC). The Dutch NREN (SURFnet) and the Danish NREN (UNI-C) operate the top-level servers.

In Europe today, the eduroam network connects 36 countries, which means hundreds of universities providing roaming facilities. Below is the map of connected countries in Europe:



Figure 2: Map of European eduroam connected countries. [3]

In Finland CSC-IT through Finnish Universities Network (FUNET) operates the National Top-Level servers. FUNET connects about 80 institutions in Finland. Vaasa University of Applied Sciences is a member of FUNET. Since FUNET is offering the platform for eduroam, it is easy for VAMK as member to connect to it.

The eduroam network is growing in Finland. Nowadays about 15 institutions are connected to the network. The map of the connected institution is always updated to show the latest information. The map is shown in the figure below:

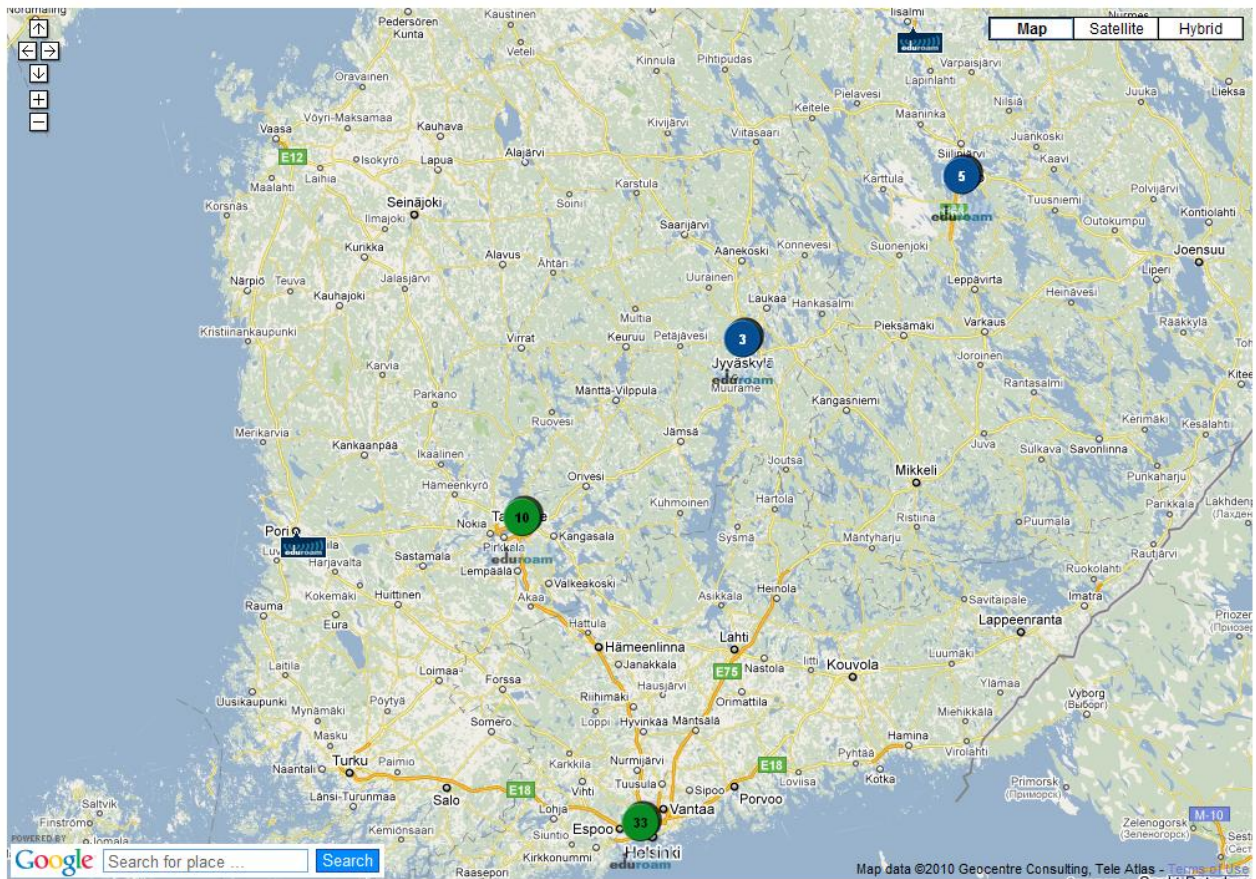


Figure 3: Map of eduroam connected institutions in Finland (April 2010). [6]

## 2.4 Vaasa University of Applied Sciences

Vaasa is a city located by the Gulf of Botnia in the western part of Finland. It was founded in 1606. Considered as the sunniest city of Finland, Vaasa has a population of about 58 900 inhabitants with more than 12 000 students making Vaasa the largest student city in Finland. With about ten institutions of higher education, Vaasa has wide range of degrees; multilingualism and internationalism are among the strengths of the polytechnics and universities in Vaasa. There are more than 30 degree programs in Finnish, Swedish, and

English, and there is a lively exchange of students and researchers with polytechnics and universities abroad. [2][15]

Vaasa University of Applied Sciences in Finnish-Vaasan Ammattikorkeakoulu (VAMK)-is one of the ten higher education institutions of Vaasa. VAMK is a multidisciplinary, multilingual and international institution providing higher education and research services within Technology and Communication, Business Economics and Tourism as well as Health Care and Social Services. VAMK has approximately 3 500 students enrolled and a staff of over 240 members. VAMK has two campuses one on Wolffintie and one on Raastuvankatu. The Wolffintie campus hosts the Information Technology department.

According to Hannu Teulahti, VAMK has currently a well-planned and secured wireless network. He states that with the current configuration, it will be difficult to hack it. With access points deployed all over the campuses, the wireless network of VAMK gives access to the standards 801.11b/g/n.

It is on this well structured computer network that I will deploy the eduroam federated wireless network. The access we will be on all the campuses and will give access for the WLAN standards b/g/n.

## **2.5 Structure of the thesis**

This thesis is divided into seven main chapters. The first chapter of the thesis is the introduction to the project. The introduction gives an overview of the topic and states the purpose of this thesis.

Chapter 2 gives an insight of the general idea of the study, which explains the project background, project aim and lastly information about the project implementation place.

Chapter 3 provides the theoretical framework of the project. The theoretical framework includes brief explanation of remote authentication, the different systems involved in remote authentication, security behind remote authentication, eduroam requirements such as authentication types and security types of access points.

Chapter 4 provides information on the design of the system and how the project was implemented. It explains the reasons behind the choices made for the design. Furthermore it shows all the components configurations files and their explanations.

Chapter 5 demonstrates all the tests made after the implementation to check the system. It shows screen shots and network packet sniffer captures. Analysis of the tests results and captures are given to explain more how the remote authentication works and the level of security.

Chapter 6 explains how to configure Microsoft Windows supplicant to be able to connect to the eduroam network. The certificate installation and wireless network card settings.

Lastly, chapter 7 gives the conclusion of the project, the limitation during implementation and an idea for further extension.

## **3 PROJECT DESCRIPTION**

### **3.1 Eduroam concept**

When a user from an eduroam-enabled institution is roaming and finds him/her (self) in an eduroam-enabled institution, he/she is able to use the facility. The user uses the credentials from him/her institution to get access to the visited institution network resources and especially internet access. The idea might at first seem unrealistic, knowing that the visiting user is not in the school database. This is possible with eduroam enabled. Based on its infrastructure, the eduroam network offers a remote authentication to the institution database of the roaming user. The concept is based on Remote Authentication Dial In Users Service (RADIUS) servers. The hierarchical architecture of RADIUS servers within eduroam network provides this facility.

The guest or visitor enters the credentials: username (in the form of username@institution.tld) and password from his/her institution to log in. The request is forwarded to the school RADIUS server which forwards the request to the National Top-Level RADIUS (NTLR) servers. If the visiting user is coming from the same country, the NTLR based on the realm in the username forwards the request to the appropriate institution RADIUS servers. The RADIUS server at the institution of the roaming user authenticates the username and the password provided in the request. If the user is found in the database, the user is authenticated and granting access. A reply is sent back to the visited institution network through a tunnel that has been created when the user was requesting authentication. The visited institution network based on the local policy gives the user access to the dedicated resources.

The process is quite similar when the visiting user is from another country (e.g. between Finland and Sweden) or from another region (e.g. between Europe and America). In the first case the visiting NTLR server will look in its known realms database. Since this one is not in the database it will forward the request to the region RADIUS servers. In Europe the region server is called Europe Top-level RADIUS (ETLR) server. When the region RADIUS server receives the request, it forwards it based on the realm and the different



NTR address in the database forwards the request to the home NTLR server which forwards it to the home institution servers.

Inst A ↔ Finland-TLR ↔ Europe-TLR ↔ Sweden-TLR ↔ Inst B

In the second case, the process is a little bit longer: the NTLR forwards the request to the region server. The region server based on the realm and the database forwards the request to the appropriate regional RADIUS server which forwards to the NTLR which at last forwards it to the home institution servers.

Inst A ↔ Finland-TLR ↔ Europe-TLR ↔ America-TLR ↔ Canada-TLR ↔ Inst B

The figure below shows how the authentication process is done.

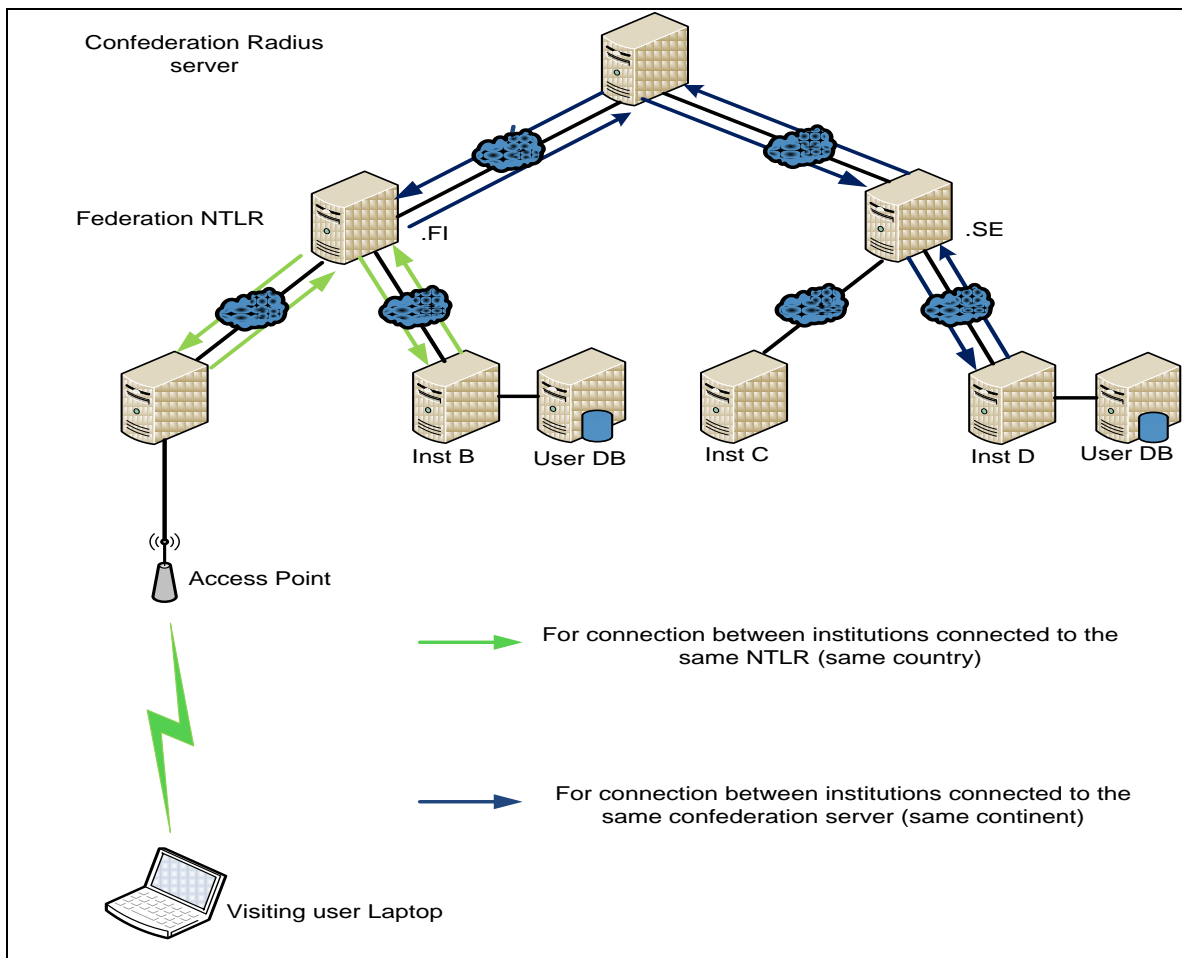


Figure 4: Authentication process within the eduroam network.

The previous line shows how the authentication is done. However, it will be clearer if we go little deeper to explain the role of every component that is used during this authentication process and the security behind this type of authentication.

The process is based on five main components:

- Network Access Server (NAS)
- 802.1X protocol
- Radius server
- User database
- Network access

### **3.2 Network Access Server (NAS)**

Network Access Server (NAS) is an access gateway that prevents users to have access to some network resources. NAS can be either a switch or an access points (AP). These devices are used in a network to control access.

When a user, also known as supplicant, connects to a NAS, the NAS connects back to a dedicated authentication server to check whether the supplied credentials by the user are corrects. Based on the reply from the server, the NAS allows or disallows the user to have access to the protected resources.

A NAS does not contain any information about the resources the user can have access to or anything to check the credentials supplied. It only forwards the credentials to the authentication server and gives access to the network.

It is obvious that the data passing through the NAS should be secured. When an access point is used as NAS, the channels must be secured. Many different types of wireless security exist. They all have their advantages and disadvantages. Since this thesis is not focusing on wireless security types, we will focus only on the frequent types of security used in eduroam:

- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access (WPA2)

### **3.2.1 Wi-Fi Protected Access (WPA)**

WPA is a security standard adopted by WiFi Alliance consortium to improve the previous standard used Wired Equivalent Privacy (WEP). WPA uses Temporal Key Integrity Protocol (TKIP) which is a security protocol used in IEEE 802.11 wireless networking standard. In TKIP, keys change dynamically to protect the communication. In WPA, the wireless device uses the pre-shared key mode to encrypt the data with either 64 hexadecimal digits or as a passphrase of 6 to 63 printable ASCII. For the user to have access to the protected network resources, he/she must enter the correct passphrase already set in the wireless device. After that all the communications between the wireless device and the user wireless enable machine will be encrypted.

WPA protocol exists in two versions: personal mode and enterprise mode. The personal mode which uses the pre-shared key has been found less secured because it can be hacked. The enterprise mode requires authentication against RADIUS by taking username and password. This second mode is the one used in eduroam since the authentication is done against RADIUS. One year after WPA was released. WiFi Alliance came up with more strong and robust protocol WPA2. [9]

### **3.2.2 Wi-Fi Protected Access version 2 (WPA2)**

WPA2 is an enhanced type of WPA. In addition to TKIP, WPA2 has much more advanced encryption method called Advanced Encryption Standard (AES). WPA2 was developed to come over the security intrusion in WPA. Theoretically WPA2 is not hackable. Like WPA, WPA2 was released in two versions: personal and enterprise. Both work as versions in WPA.

In addition to the encryption benefits, WPA2 also adds two enhancements to support fast roaming of wireless clients moving between wireless access points:

- Pairwise Master Key (PMK) caching support : allows for reconnection to access point's that the client has recently been connected to without the used to re-authenticate
- Pre-authentication support: allows a client to pre-authenticate with an access point towards which it is moving while still maintaining a connection to the access point it is moving away from. [10] [17]

Taking in consideration all the features, WPA2 is a good option for the access point's security setting in eduroam.

In eduroam, the NAS that are deployed are access points. When a user connects to the NAS, the NAS forwards the user's credentials to the RADIUS server. Depending on the reply, the user is allowed or not to have access to internet. Between the users (supplicants), the NAS (authenticator) and the authenticator server the 802.1X protocol is used to carry the credentials.

### **3.3 802.1X protocol**

The 802.1X is an Institute of Electrical and Electronics Engineers (IEEE) standard for local and metropolitan network. It is a port based network access control protocol. Initially designed for Ethernet port, it was extended to be used to wireless network. "Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of *authenticating* and *authorizing* devices attached to a LAN port that has point-to-point connection characteristics, and of *preventing access* to that port in cases which the authentication and authorization fails. A port in this context is a single point of attachment to the LAN infrastructure." 802.1X-2001 [8] [11]

802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE which is known as EAP over LAN (EAPOL). EAP is an authentication framework used in wireless network or point-to-point communication. Defined in RCF 3748, it is provided for the transport and usage of keying material and parameters generated by EAP

methods. Many different methods of EAP exist but WPA and WPA2 has adopted five types as official authentication mechanisms. [1]

The figure below shows the steps in the 802.1X authentication.

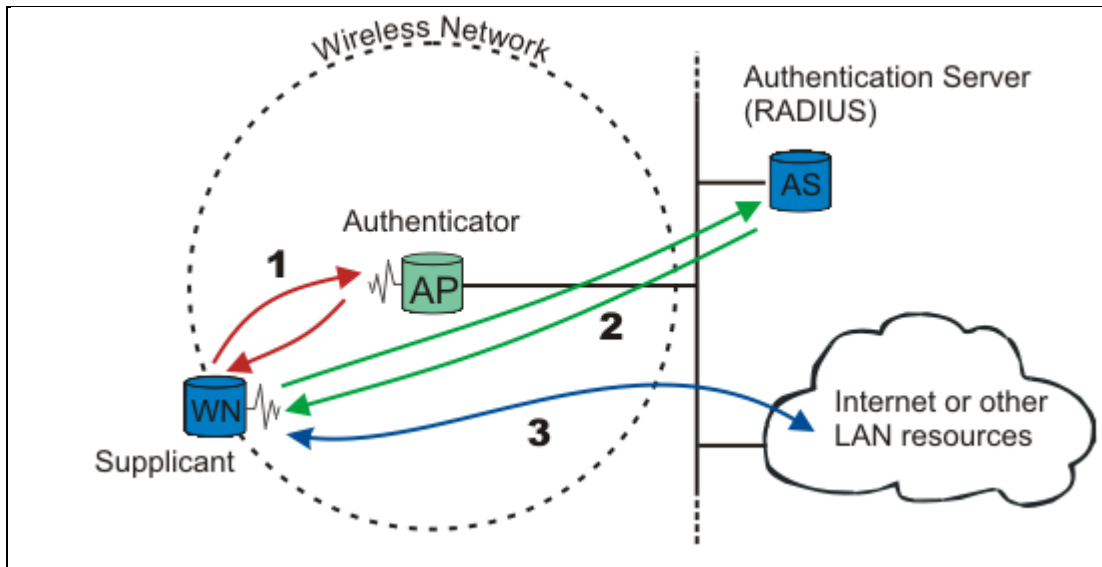


Figure 5: 802.1X authentication steps. [10]

When an authenticator detects a new supplicant, the authenticator asks for the supplicant's identity. At that point no other traffic is allowed: traffic such as DHCP or HTTP is dropped. Only 802.1X traffic is allowed. The "port" is closed. Until an encrypted Transport Layer Security (TLS) tunnel is up, the real identity of the user is not sent. Hidden identity is used. After the identity has been sent, the authentication process begins. The protocol used between the supplicant and the authenticator is EAP encapsulation over Local Area Network (EAPOL). The authenticator re-encapsulates the EAP message into radius format then forwards it to the authentication server. During the authentication process, the authenticator just relays packets between the supplicant and the authentication server. When authentication is finished, the server sends back access-success (if authentication was successful) or access-reject (when it fails) to the supplicant. If the authentication is

successful, the port is then opened. After successful authentication, the supplicant is granted access to the protected network resources. [8]

In eduroam two types of authentication method are suggested:

- EAP-Tunnelled Transport Layer Security (EAP-TTLS)
- Protected EAP Microsoft's Challenge Handshake Authentication Protocol (PEAP-MSCHAP) [3]

### 3.3.1 EAP-Tunnelled Transport Layer Security (EAP-TTLS)

EAP-TTLS is an EAP protocol which extends the EAP-Transport Layer Security (EAP-TLS) protocol. It was co-developed by Funk Software and Certicom. It is widely supported on platforms although there is no native support for this protocol in Microsoft Windows. The support on MS Windows is done through some software such as SecureW2. In EAP-TTLS, the client may or not authenticate itself. It means a client certificate is not issued during installation. Only the server authentication to the client is important. The server certificate is therefore installed on the client to be able to pass the authentication request from the server. The secure connection established by the handshake is then used by the server to authenticate the client using authentication mechanism such as EAP or others. [1]

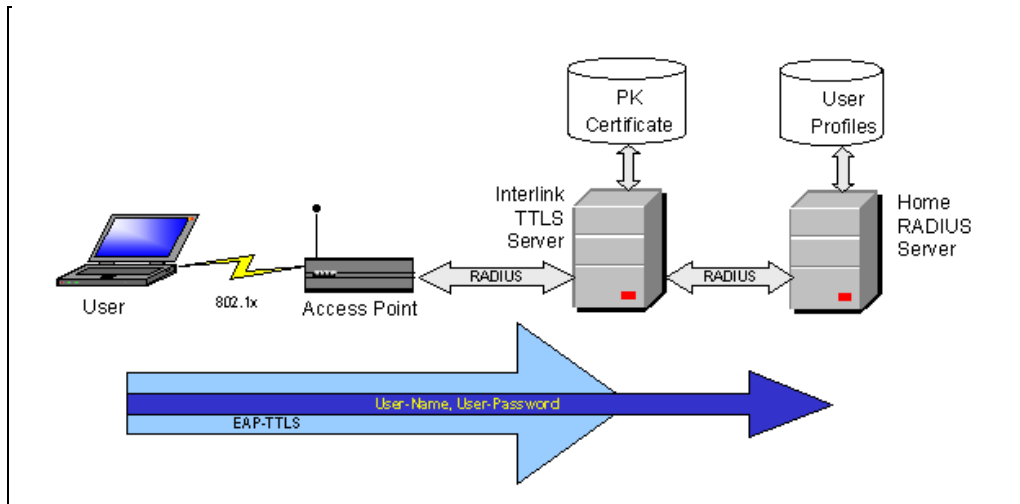


Figure 6: EAP-TTLS authentication method. [7]

One advantage of this type of authentication method is the secured tunnel established during authentication. It prevents from eavesdropping. Another advantage is even the username of the client which is also sent in encrypted form not in clear-text.

Eduroam is a remote authentication system. Having a secured authentication method is very important. EAP-TTLS is suitable for eduroam network.

### **3.3.2 PEAP-MSCHAP**

The Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates EAP communication in an encrypted TLS tunnel. Jointly developed by Cisco Systems, Microsoft and RSA Security, it was released to protect more the EAP communication.

Even though EAP is used in authentication, the entire EAP conversation can be sent as clear text (unencrypted). This situation is not secured because a malicious user can get into the transmission media and capture the EAP messages from a successful authentication for analysis.

To address this security issue, PEAP first creates a secure channel that is both encrypted and protected in terms of data integrity with Transport Layer Security (TLS). This prevents the EAP conversation packets to be hacked.

With the PEAP tunnel, different types of EAP methods are used: one of these methods is Microsoft's Challenge Handshake Authentication Protocol (MS-CHAP).

MS-CHAP is the Microsoft version of Challenge Handshake Authentication Protocol. It exists in two versions: MS-CHAPv1 defined in RCF 2433 and MS-CHAPv2 defined in RCF 2759. As a Microsoft product, it has been included in the native Operating System since Windows 2000 SP4. MS-CHAP v2 is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server

challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. [13]

MS-CHAP used alone has some security vulnerabilities. A capture of successful MS-CHAP v2 exchange by a hacker can be used to methodically guess passwords. When MS-CHAP v2 is used with PEAP, the MS-CHAP v2 exchange is protected by the strong TLS channel security. [13]

In the eduroam network, one of the important parts is authentication. The equipment that takes care of this is the Remote Authentication Dial In User Service (RADIUS) server.

### **3.4 RADIUS server**

When a visiting user logs in to eduroam, he/she sends his/her credentials in order to be authenticated. Based on the type of the RADIUS server, the data sent is either used for authentication or forwards to another RADIUS server. What types of RADIUS servers do we have in the eduroam network?

#### **3.4.1 Service Provider (SP)**

Service Provider server is a RADIUS server which does not do authentication. The server is used to proxy the RADIUS requests to the hierarchical RADIUS server in the network. This kind of server is a Proxy server. [3]

##### **3.4.1.1 Proxy server**

A RADIUS proxy server has a record of all the hierarchical RADIUS servers in the network. When a proxy server receives a RADIUS request, the server unwraps the encapsulated request. Based on the realm in the username, the proxy looks in the realms record. If the realm is known the server re-encapsulates the request and forwards it to the appropriate server. In case the realm is not then the request is forwarded to the next hierarchical RADIUS server in the network. [3]



### **3.4.1.2 Realm**

A realm in radius jargon is the domain name: for example “puv.fi” or “uwasa.fi”. In the eduroam network, username must be in the format of “username@realm”. It is not an email address: it only looks like one. The realm is very important in the eduroam network. Without it, a request cannot be forwarded to the appropriate institutional authentication Identity Provider (IdP). [3]

### **3.4.2 Identity Provider (IdP)**

The identity provider is the server that takes care of the authentication. Unlike the service provider, the identity provider terminates the radius request received by applying the radius authentication protocol. What is RADIUS? [3]

#### **3.4.2.1 RADIUS protocol**

Radius is a network protocol which provides Authentication, Authorisation and Accounting (AAA) platform to allow a client to have access to protected network resources. First developed by Livingstone Enterprises Inc. it has become later Internet Engineering task Force (IETF) standard.

RADIUS is client/server service using User Datagram Protocol (UDP) transport and running on application layer. As stated earlier it has three main functions:

- Authenticate users before granting them access to a network
- Authorise the authenticated users to have access to a particular resource
- Account for the previous services

Figure below shows the structure of a RADIUS packet:

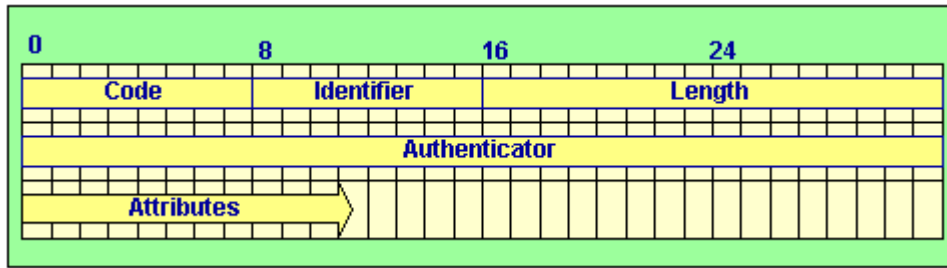


Figure 7: RADIUS packet format. [12]

*Legend:*

- *Code* - A byte containing the RADIUS command/response.
- *Identifier* - A byte used to match the command and response.
- *Length* - The length of the packet (2 bytes).
- *Authenticator* - Value used to authenticate the reply from the RADIUS server, and is used in the password hiding algorithm.
- *Attributes* - The data belonging to the command or response.

### 3.4.2.2 Authentication and Authorisation

In RADIUS conversation both authentication and authorisation happens together but one after the other.

When a client connects to a NAS, it sends its credentials to gain access to the network. The NAS then sends an access-request to the RADIUS server asking authorisation to grant access to the network. The RADIUS server checks if the supplied credentials are correct one the authentication schemes explained earlier. The RADIUS verify the received credentials with users database installed locally or remotely (on another server)

After the RADIUS server has checked the credentials it replies to the client in one of these formats:

- Access Accept : when the user is authenticated
- Access Reject : when the user could not be authenticated

- Access Challenge: when the user must supply some additional information. In the case of tunnelled authentication scheme and where the identity is hidden to the NAS, an Access challenge is sent to the user.

When an Access Accept response is sent by the RADIUS server, it includes in the message Authorisation attributes. These attributes may include for instance:

- The IP address to be assigned to the user
- VLAN parameters
- An access list ... [16]

### **3.4.2.3 Accounting**

The accounting process is an additional function that performs the RADIUS server. When authentication and authorisation is done, the user is able to get access to the network resources.

Accounting is a track of NAS resources consumption by the user. This information can be used later by the administrator to check how the network resources are used in order to plan or restructure the network. Some of the information gathered in accounting is the identity of the user, the nature of the service delivered, when the service started and ended.

When a network access is granted by the NAS, an Accounting Start (RADIUS accounting request packet) is sent by the NAS to the RADIUS server to state that the service has started. During the connection, periodically, the NAS sends an Interim Update records (RADIUS packet) to the server to update the status of the active session. Finally when the session ends, the NAS sends an Accounting Stop record (RADIUS packet) to the server. This packet provides information about the user network access. [16]

The figure below shows the flow of Authentication, Authorisation and Accounting in RADIUS:

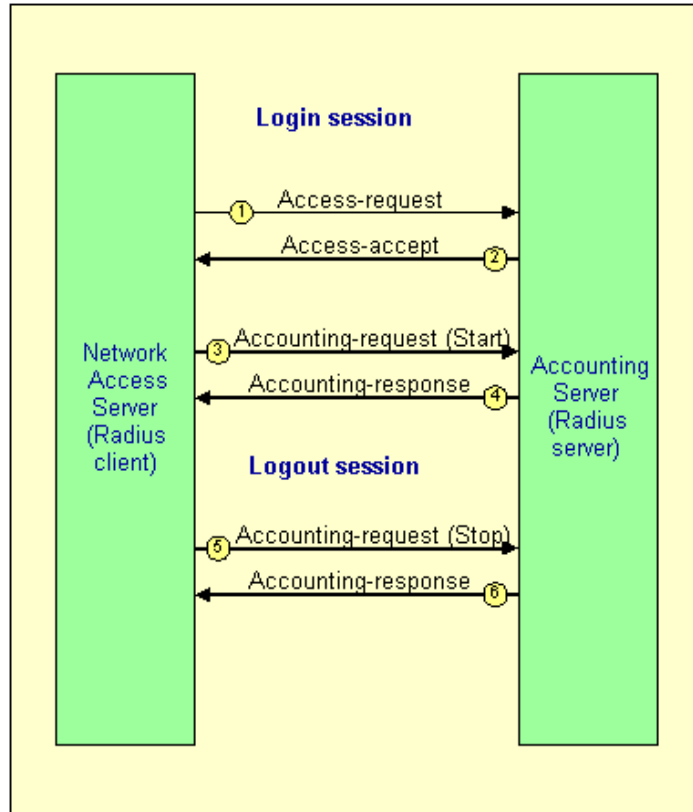


Figure 8: RADIUS message flow. [12]

### 3.5 User Database

The user who is authenticated must be first recorded somewhere. The information recorded about the user (username, password, telephone number etc.) is what is used during the authentication sequence. This information saved or recorded is what I call user database.

When the RADIUS server receives the roaming user credentials (often the username and password), it checks it against the data it has in the user database. If the user exists it checks the password. When everything is correct the server sends a reply back to notify that the user exists and the supplied password is correct.

Many user databases are today used in the authentication process. Some of them are Active directory, LDAP, SQL, Kerberos etc. These user databases can be installed locally meaning on the same server running RADIUS or remotely which means on another server.

### 3.6 Network access

The network resources that a user can have access to after having been authenticated vary. It can be only internet access or more than that, such as access to printers, Virtual Private Network (VPN) etc. Every institution defines rules or policies on the network. Usually these rules are defined in Virtual Local Area Network (VLAN).

A VLAN is logic segmentation of a Local Area Network (LAN). By segmenting a LAN, the administrator can group different people under same rules: giving them some permission or deny them some access. It is easy and simple for an administrator to design VLANs within a LAN.

In eduroam the fundamental idea is to grant internet access to the visiting user. At the same time, users who are not roaming and who belong to the host institution, have a different access to the network. It is advisable for the administrator to define a local policy bidding the rules to a particular VLAN.

Some of the rules that are defined in the VLAN are:

- The IP addresses that will be assigned to the host
- The static or dynamic route etc.

[1] [3]

Now that the eduroam concept has been clarified, let us go through the design and implementation.

## 4 DESIGN AND IMPLEMENTATION

### 4.1 Project Planning

Once the theory about the eduroam network architecture and security has been gone through, it is now important to look on the scope of how to set the system to meet the requirements as much as possible. In this stage two main issues are important to take in consideration:

- Set a system which will be scalable (i.e. a system that can be inserted easily in the existing VAMK network)
- The security level should be as high as possible since the users will be from different places and nothing about them is known by VAMK.

Having considered these factors, a design was proposed to the project manager. After discussion the following design has been agreed:

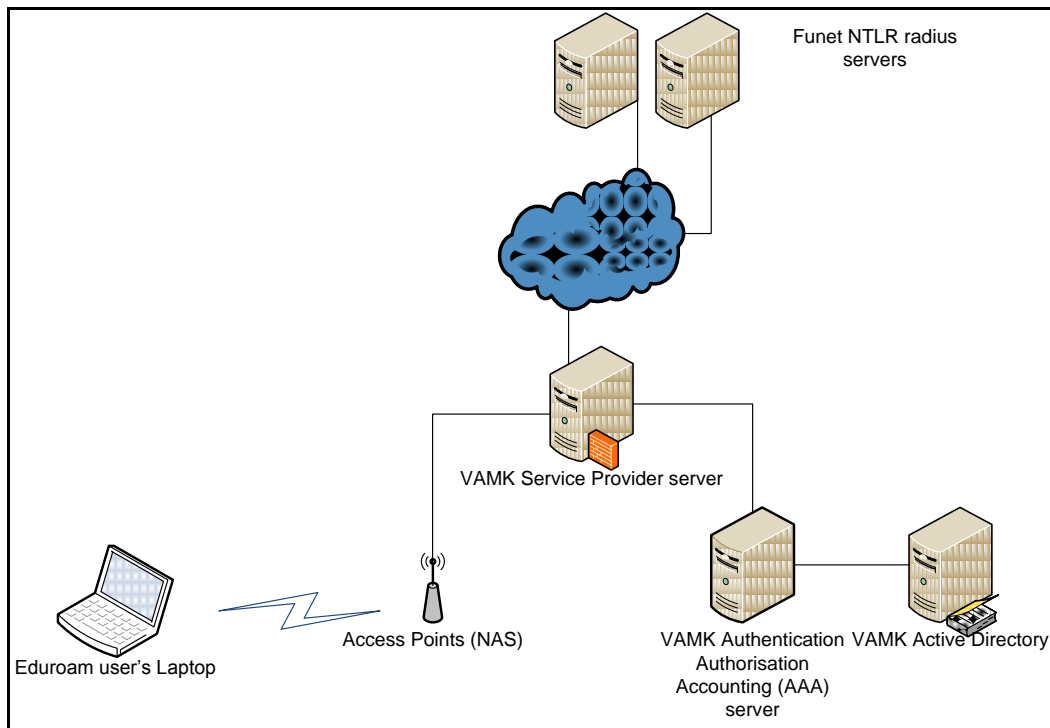


Figure 9: VAMK eduroam architecture.

## 4.2 Overview of the design

VAMK has already an authentication server set which is used to authenticate users in the wireless network. I therefore decided not to set anymore a new authentication server. The already set server will be used as identity provider (IdP). I will only set a new service provider (SP) which will acts as a proxy. This SP will then forward our guests authentication requests to Funet NTLR servers and also receives authentication requests coming through Funet NTLR servers from VAMK students and staff roaming. The SP will therefore forward the request to the IdP server in VAMK network.

According to the SP functions, it should be able to connect to VAMK's IdP and Funet's NTLR. It should have a public IP. Even though it is having a public IP, it should be behind a firewall so that the security level can still be under control. Now that the scalability requirement has been reached, the next level is the security part.

Below is the figure of what the eduroam network will look like after the guests have been authenticated:

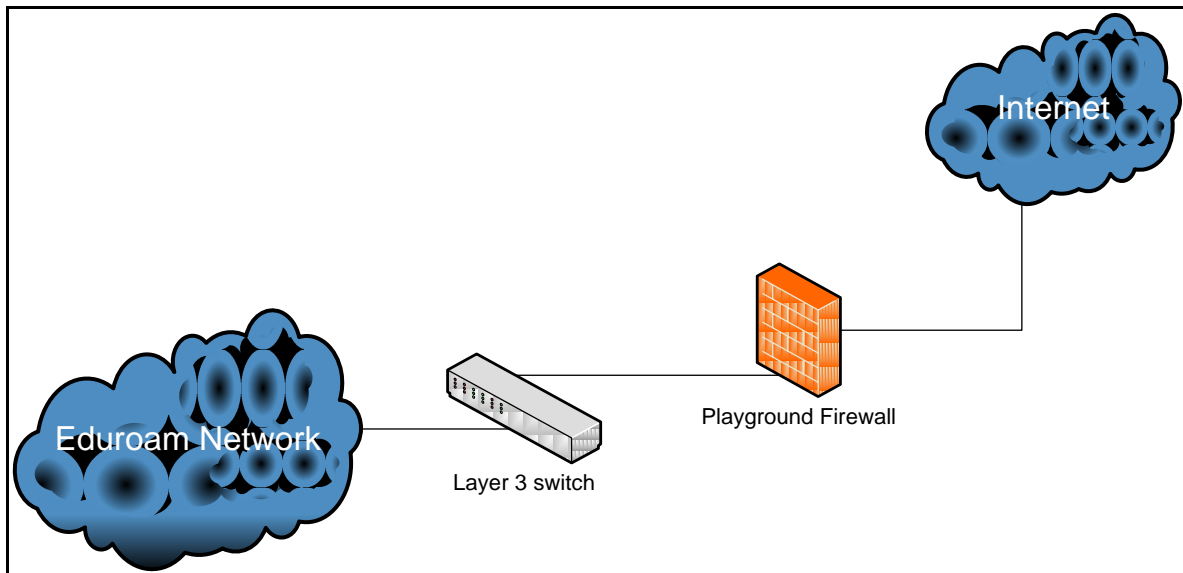


Figure 10: VAMK eduroam network.

In the figure above, two important parts have been introduced:

- The layer 3 switch
- The firewall policy named “playground”

#### **4.2.1 The layer 3 switch**

The school administrator has decided to allow only as network resources internet access. It means the guest cannot have access to VAMK resources like printers, internal servers etc.

It is then important to route all the traffic coming from the eduroam network straight to the firewall and limit every access. The best way to do this is to use a layer 3 switch and use the routing property of this one.

This is done by defining in the switch a static IP route for all the traffic of the eduroam VLAN to the firewall.

#### **4.2.2 Playground policy**

The playground policy is an existing policy. It is used for the current Palosaari Campus Wireless Network (PCWN). In this policy many rules have been defined. The rules define which resources the users can have access to and the ones they are denied access from.

Below are screen shots of the playground policy:



<input type="checkbox"/>	TCP	<a href="#">eduiXNet</a>	*	193.xxx.xxx.xxx	22 (SSH)	*		e-lomake3.puv.fi
<input type="checkbox"/>	TCP	<a href="#">eduiXNet</a>	*	193.xxx.xxx.xxx	443 (HTTPS)	*		e-lomake3.puv.fi (HTTPS)
<input type="checkbox"/>	TCP	<a href="#">mediamaisteriNet</a>	*	<a href="#">moodleHosts</a>	<a href="#">moodleHuoltoyhteysPorts</a>	*		moodle huoltoyhteys
<input type="checkbox"/>	TCP	193.xxx.xxx.xxx	*	193.xxx.xxx.xxx	143 (IMAP)	*		mail.puv.fi (moodle.tritonia.fi auth)
<input type="checkbox"/>	TCP	<a href="#">lapuaNet</a>	*	<a href="#">winTsServers</a>	3389 (MS RDP)	*		wints
<input type="checkbox"/>	UDP	<a href="#">externalRadiusServers</a>	*	<a href="#">radiusServers</a>	<a href="#">radiusPorts</a>	*		RADIUS: PCWN, eduroam
<input type="checkbox"/>	*	<a href="#">technoAdNet</a>	*	193.1		*		Luottosuhde techno.uwasa.fi -> tb.technobothnia.fi
<input type="checkbox"/>	ICMP	193.xxx.xxx.xxx	*	<a href="#">funetRouterNet</a>		*		im.funet.fi
<input type="checkbox"/>	UDP	*	*	<a href="#">Multicast</a>		*		Multicast traffic

Figure 11: WAN authorisation rules in the playground policy.

Legend:

The mouse is pointing on the screen shot to the RADIUS servers' rules. It shows that udp packets are allowed between Funet's NTLR servers and VAMK servers (ns0.puv.fi for eduroam network).

<input type="checkbox"/>	UDP	<a href="#">eduroamNetwork</a>	*	<a href="#">dhcpServers</a>	67 - 68	*	1	dhcp for eduroam
<input type="checkbox"/>	UDP	<a href="#">eduroamNetwork</a>	*	<a href="#">dhcpServers</a>	123 (NTP)	*		ntp for eduroam
<input checked="" type="checkbox"/>	*	*	*	<a href="#">vamkNetPrivate</a>		*	2	ei privateihin
<input type="checkbox"/>	*	*	*	193.xxx.xxx.xxx		*		vpn.puv.fi
<input type="checkbox"/>	UDP	*	*	<a href="#">OpenVpnServers</a>	<a href="#">OpenVpnPorts</a>	*		OpenVPN
<input type="checkbox"/>	TCP	*	*	<a href="#">shibbolethHosts</a>	443 (HTTPS)	*		idp.puv.fi
<input type="checkbox"/>	TCP	*	*	<a href="#">shibbolethHosts</a>	80 (HTTP)	*		idp.puv.fi
<input type="checkbox"/>	TCP	*	*	<a href="#">shibbolethHosts</a>	8443	*		idp.puv.fi (shibboleth)
<input type="checkbox"/>	*	*	*	<a href="#">I vamkNet</a>		*	3	kaikki auki, paitsi vamk
<input type="checkbox"/>	TCP	<a href="#">TinoWlan</a>	*	<a href="#">Bacula</a>		*		
<input type="checkbox"/>	UDP	<a href="#">TinoWlan</a>	*	<a href="#">loggers</a>		*		

Figure 12: LAN rules for playground policy.

### *Legend*

*Here are explanations for some of the rules:*

*[1]: udp packets are allowed from eduroam network to the DHCP servers; that is how the clients' computers are assigned IP*

*[2]: Nothing is allowed from this network to the VAMK private network. No network resources allowed to users to whom this policy is applied.*

*[3]: Everything is allowed but not to VAMK public network (the eduroam network is within these subnets).*

One extra setting was to assign to all eduroam network users public IP to get to internet. At first sight it looks unsecured because the users will be on the internet and will be able to do all kind of activities. There is another idea behind that: it is easy to trace someone using a public IP doing some illegal activities (since eduroam users may not be known by the school).

Also for eduroam users it is much easier to use a public IP to get Virtual Private Network (VPN) connection. They may want to connect to their own institution with VPN. Therefore the public IP is the right one to use.

In summary, the eduroam network in VAMK is built the following way:

- The Service Provider server and Identity Provider server are running one different servers.
- A layer 3 switch is used to forward all the traffic in eduroam network to the firewall
- The firewall “playground” policy is applied to the network limiting access to VAMK resources and granting access to only internet.
- The users are assigned public IP addresses in order to be able to be traced back easily.

## 4.3 Implementation

The system implementation is subdivided into four parts:

- Service Provider setting up
- Windows Network Policy Server (NPS) configuration
- Switches configuration
- Access points configuration

### 4.3.1 Service provider setting up

In the implementation it is clear that the SP server is used to only proxy requests. Besides the eduroam network is not highly used. With these facts, it is not efficient to use a new physical server to set up the SP. It will be just a waste of resources. I (in agreement with the project manager) have decided to set up a virtual server to host the SP.

#### 4.3.1.1 Choice of host server operating system

A virtual server is not costive and easy to set up. There are already many virtual servers running in the VAMK network. In this case Linux virtual server was used running Debian (lenny) 5.0.4 operating system with 2.6.31.6-t300-2626 kernel version. Debian is an open source operating system. There are already some hosts servers running Debian operating system. One was selected to create a guess virtual server.

#### 4.3.1.2 Choice of RADIUS server

Different kind of RADIUS server exists. The most used are Radiator, Windows NPS, Diameter and FreeRADIUS etc. For this project Freeradius was selected because first it is open source software, second it is simple in the configuration and finally supports all the authentication method type.

The version of FreeRADIUS was installed from Debian repository by issuing “*sudo apt-get install freeradius*” command. The 2.0.4 version was installed.

In the Freeradius configuration, five main configuration files need to be configured:

- proxy.conf
- clients.conf
- eap.conf
- radiusd.conf
- A defined virtual server configuration file

To set up a Service Provider server, the main configuration files are: proxy.conf, clients.conf and radiusd.conf

For security reasons, I would not use the real IP addresses of the servers used in the configuration files since this document is for public use. They IP addresses will be replaced by XXX.XXX.XXX.XXX

#### **4.3.1.3 Proxy.conf**

The proxy.conf configuration file is the file that contains all the information about how the Service Provider forwards the RADIUS requests. In the proxy.conf a pool of home servers are defined. The home servers are the RADIUS server used for authentication (identity provider). It also defines if the home server is handling authentication and accounting altogether or separately. The ports used in the RADIUS conversation are stated in this file. Nowadays the standard ports are 1812 for authentication and 1813 for accounting. When the home servers are more than one the proxy should define the order in which the request are been sent. The proxy also states the different known realms and where requests from those realms are forwarded to. All unknown realms requests should be forward to the next hierarchical RADIUS server. In our case it will be forwarded to Funet NTLR servers.

All these parameters are defined in the proxy.conf. The proxy.conf file used in the project is attached in Appendix 1.

#### **4.3.1.4 Clients.conf**

In clients.conf we define all the devices that are allowed to send requests to the server. These devices are servers and NAS (access points). If a request comes from a non defined client, the server drops the request.

In this project two main clients are defined in the clients.conf: the access points of VAMK and the NTLR servers from Funet since all the roaming requests from VAMK users will be coming from them. The Appendix 2 shows the content of the clients.conf.

#### **4.3.1.5 Eap.conf**

In eap.conf as the name states, the authentication method and type is defined. These variables are used when the server is used as authentication server. In the project this server is used as Service Provider. Nothing was therefore changed in this file.

#### **4.3.1.6 Radiusd.conf**

The radiusd.conf is the main server configuration file. All the functionalities are configured in that file. In our setup there is nothing to configure there. I just need to check if some options are uncommented and if some are commented. For instance make sure that the other configuration files are included in the radiusd.conf.

It is also a place where I set the format of the username and the delimiter I want to use: whether it is “@” or “%”.

By default, only error message are displayed in the log file. To easily check the number of successful authentications, I configured the radiusd.conf file to output the successful authentications into the log file.

#### **4.3.1.7 Virtual server**

Here the virtual server used is inner-tunnel. It is actually a straight forward file. There is nothing to change as in radiusd.conf.

The file defines the different steps during the authentication process.

### 4.3.2 Windows Network Policy Server (NPS)

In VAMK, the NPS server is already set and working. In the project the NPS will be used as Identity Provider. The only configuration I have to make on the NPS is to add the Service Provider set already as a RADIUS client. The proxy will be therefore able to send requests to the NPS. Beyond the client configuration, there is a network policy that must be set on the NPS. This network policy is applied to the connection during the authentication process.

Below are the screen shots of the RADIUS client network policy configuration:

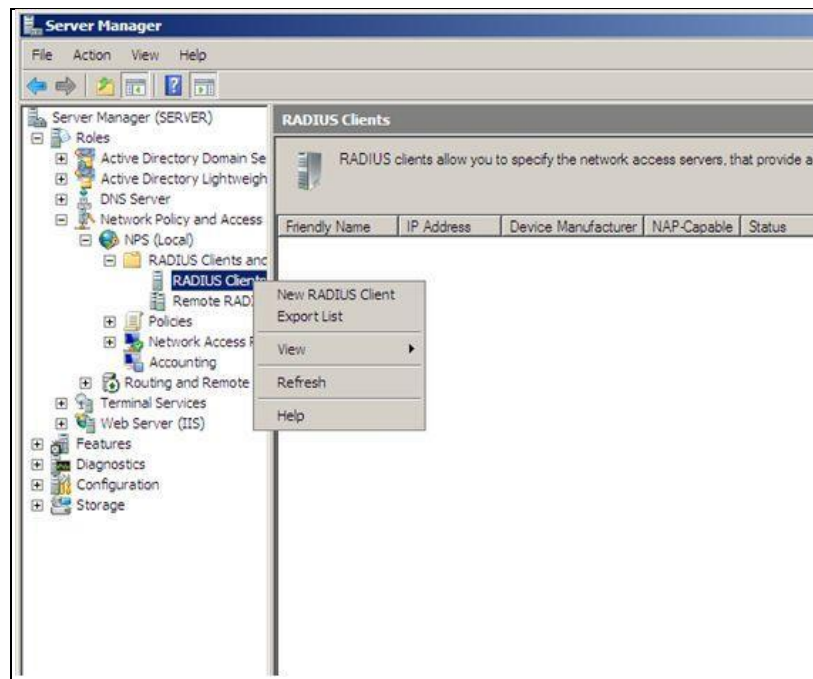


Figure 13: Adding new RADIUS client: in this case the proxy server.

**New RADIUS Client** [X]

Enable this RADIUS client

Name and Address

Friendly name:

Address (IP or DNS):

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual       Generate

Shared secret:

Confirm shared secret:

Additional Options

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

Figure 14: New RADIUS client configuration.

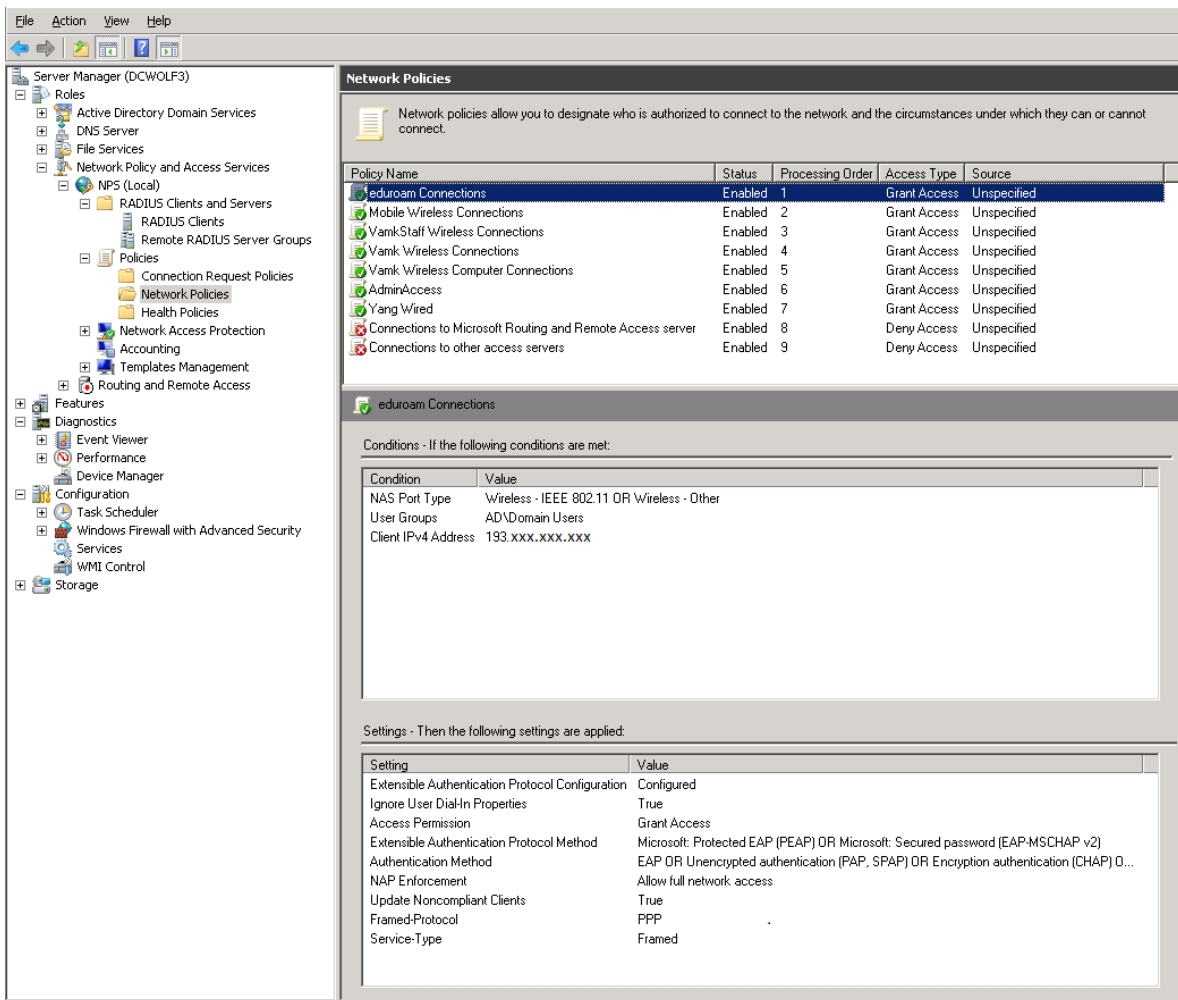


Figure 15: Eduroam network policies.

*Legend:*

*In this policy it is set that before a connection takes place:*

- *The NAS must be a Wireless-IEEE 802.11 or other Wireless*
- *The user must come from VAMK Windows domain (AD)*
- *The connection must come from the only one RADIUS client which is the proxy.*



### 4.3.2.1 Shared secret

Before there can be RADIUS conversation between two devices (NAS-to-SP or SP-to-IdP), a shared secret must be shared.

A shared secret is a common key (preferably 16 digits) used by both ends in the conversation to encrypt the packet. If there is a mistake in the secret none of the end devices can read the encryption and decode the content of the packet.

In a system the secret is used between two devices. That secret can be duplicated (used between other devices in the system) or other secrets can be used in the system.

It may look like this:



### 4.3.3 Switches configuration

In this implementation switches are used in two ways:

- The first one is the layer 3 switch routing all the traffic of eduroam network to the firewall
- The second type of switch is a layer 2 switch on which the access points are connected. Their role is to grant network access to connected users.

On the layer3 I defined static IP route for the network. The figure below shows the configuration of that static route:

```

no ip address
exit
vlan 307
  name "Eduroam"
  ip helper-address 192.168.xxx.xxx
  ip helper-address 192.168.xxx.xxx
  ip address 195.xxx.xxx.xxx 255.255.255.192
  tagged 20-24
  exit
include-credentials
password operator sha1 "446410a140d4e16355e0a38e4f924fa1a4c7790f"
password manager sha1 "446410a140d4e16355e0a38e4f924fa1a4c7790f"
timesync sntp
sntp unicast
sntp server priority 1 192.168.xxx.xxx 3
sntp server priority 2 192.168.xxx.xxx 3
ip authorized-managers 193.xxx.xxx.xxx 255.255.255.255 access manager
ip authorized-managers 193.xxx.xxx.xxx 255.255.255.255 access manager
ip ssh filetransfer
ip route 0.0.0.0 0.0.0.0 195.xxx.xxx.xxx
router rip
  no auto-summary
  exit
-- MORE --, next page: Space, next line: Enter, quit: Control-C

```

Figure 16: VLAN and static IP route definition on Layer3 switch.

The figure below shows the output of the command “show vlans 307”. This result shows that eduroam VLAN which is 307 is allowed to pass traffic by the ports 20-24 which are the trunk ports of the switch.

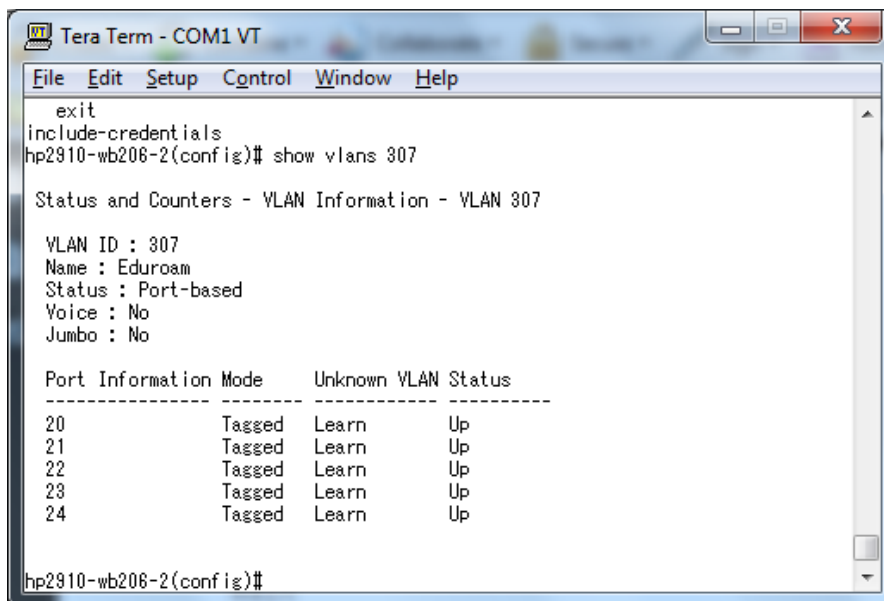


Figure 17: Eduroam VLAN status on the layer3 switch.

On the layer 2 the configuration is about the VLAN definition. The configuration requires defining the VLAN on the switch and allowing traffic through that VLAN. The figures below shows the definition of the VLAN on the switch and some devices connected through that VLAN.

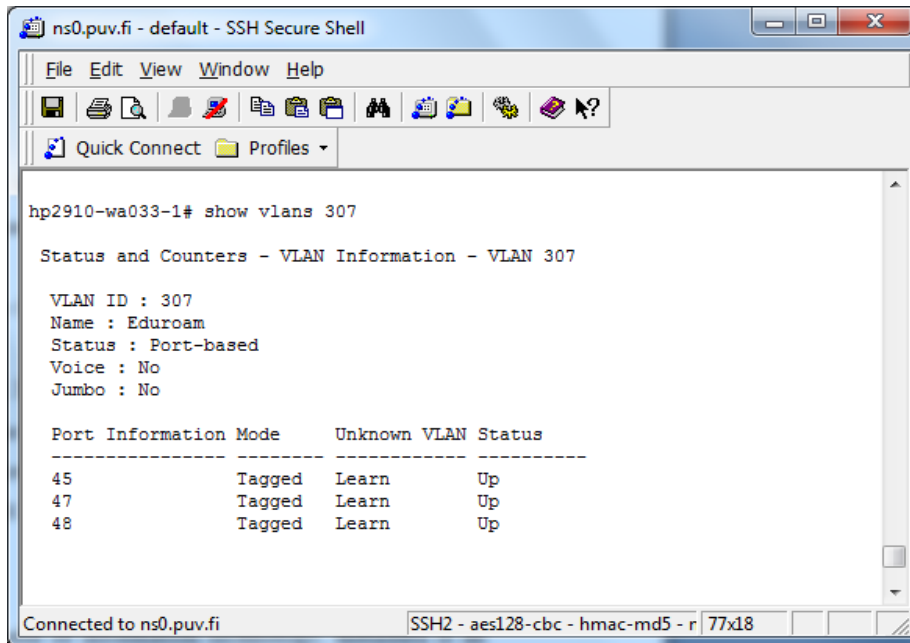


Figure 18: VLAN status on a switch.

Figure 19 below shows the outputs of two commands: “*show mac-address vlan 307*” and “*show vlans 307*”. The first one shows the MAC-ADDRESS of computers or devices connected to VLAN 307 and the port by which their traffic are going through.

The second one shows the ports on that switch which are tagged and untagged to VLAN 307. A tagged port is used by a VLANs to carry their traffic from switch to switch or router and the untagged port belongs to that VLAN.

Port 45 is the port through which the access point is connected to the switch and port 48 is the port trunk port of the switch.

```
Tera Term - COM1 VT
File Edit Setup Control Window Help
hp-1(config)# show mac-address vlan 307
Status and Counters - Address Table - VLAN 307
-----
MAC Address   Located on Port
-----
001b53-e026ac 48
001e68-aa847e 45
0024a8-c8c440 48
hp-1(config)# show vlans 307
Status and Counters - VLAN Information - VLAN 307
VLAN ID : 307
Name : eduroam
Status : Port-based
Voice : No
Jumbo : No
Port Information Mode   Unknown VLAN Status
-----
44      Untagged Learn      Down
45      Untagged Learn      Up
46      Untagged Learn      Down
47      Untagged Learn      Down
48      Tagged Learn        Up
hp-1(config)#
```

Figure 19: Screen shot showing that the VLAN is passing through the switch.

#### 4.3.4 Access points configuration

The access points in VAMK are not functioning as standalone devices. The system is centralised. This makes the access point's configuration easy. All the settings made on the control management are synchronised with the access points.

The access points are used as NAS in the implementation. It must be defined on the NAS, the server they will forward the authentication request to, the authentication type and method, the type of wireless security I want to set for the future communication between the client's computer and the access point.

It is clear that the requests from the user will be forwarded to the Service Provider set earlier. For this project the authentication method chosen is PEAP with MS-CHAP v2. It is not the easiest to set but it does have some advantages:

- This Microsoft authentication method is built inside Microsoft Windows operating system. We know that many computers are equipped with Microsoft Windows operating system. Also the other operating systems support this authentication method. It is therefore convenient to use it as authentication method.
- Since the PEAP is an inbuilt authentication method, nobody has to install any supplicant application to be able to connect to the network.

The figure below shows how the setting is done:

The first one shows how to set the profile name (eduroam), the RADIUS server profile, the ports and the authentication method.

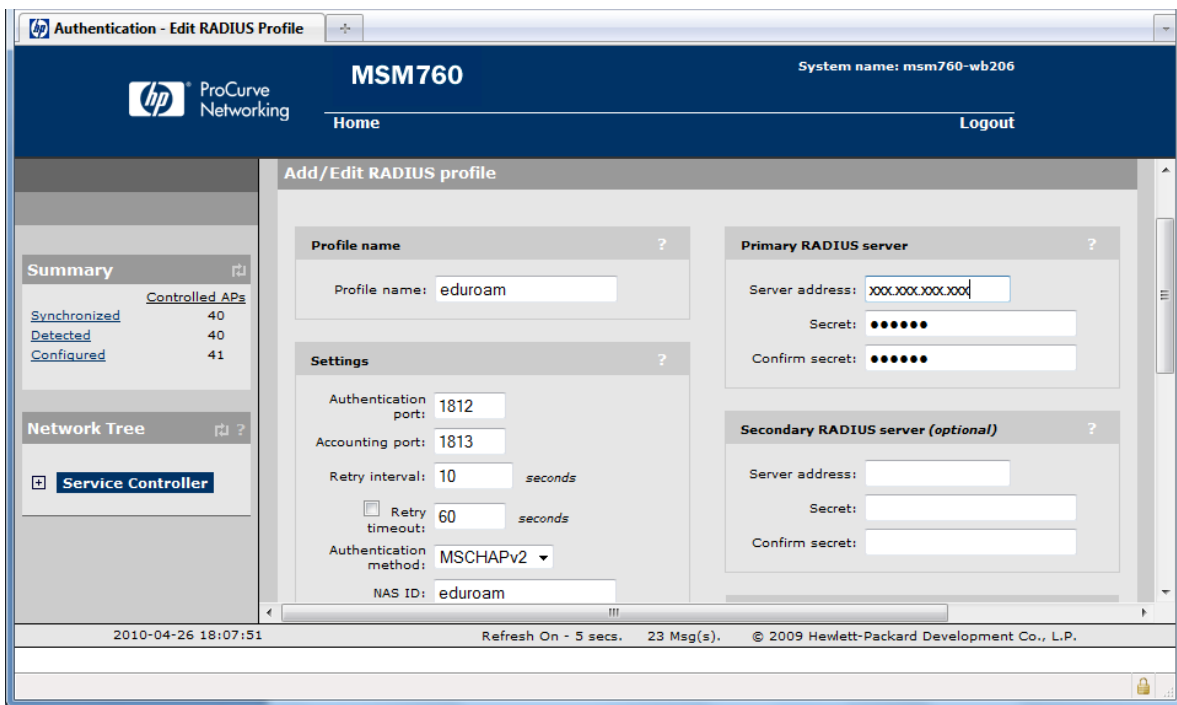


Figure 20: Radius server and authentication method configuration on access point control management

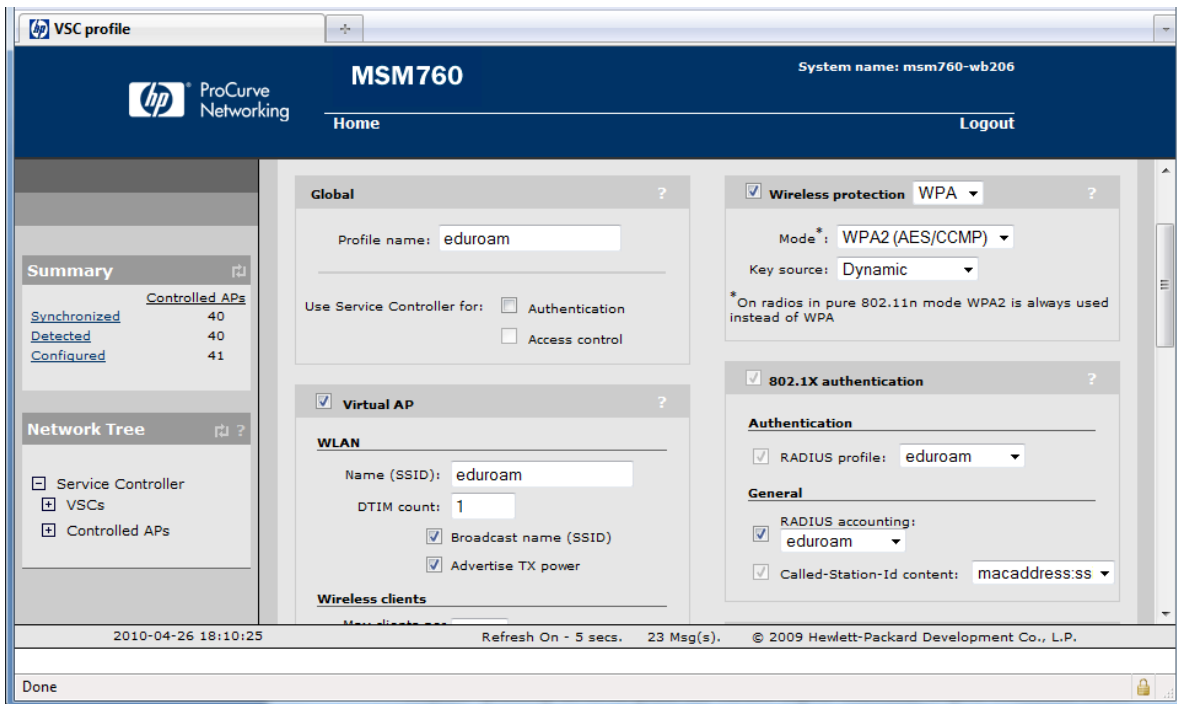


Figure 21: Wireless security settings on the access points control management.

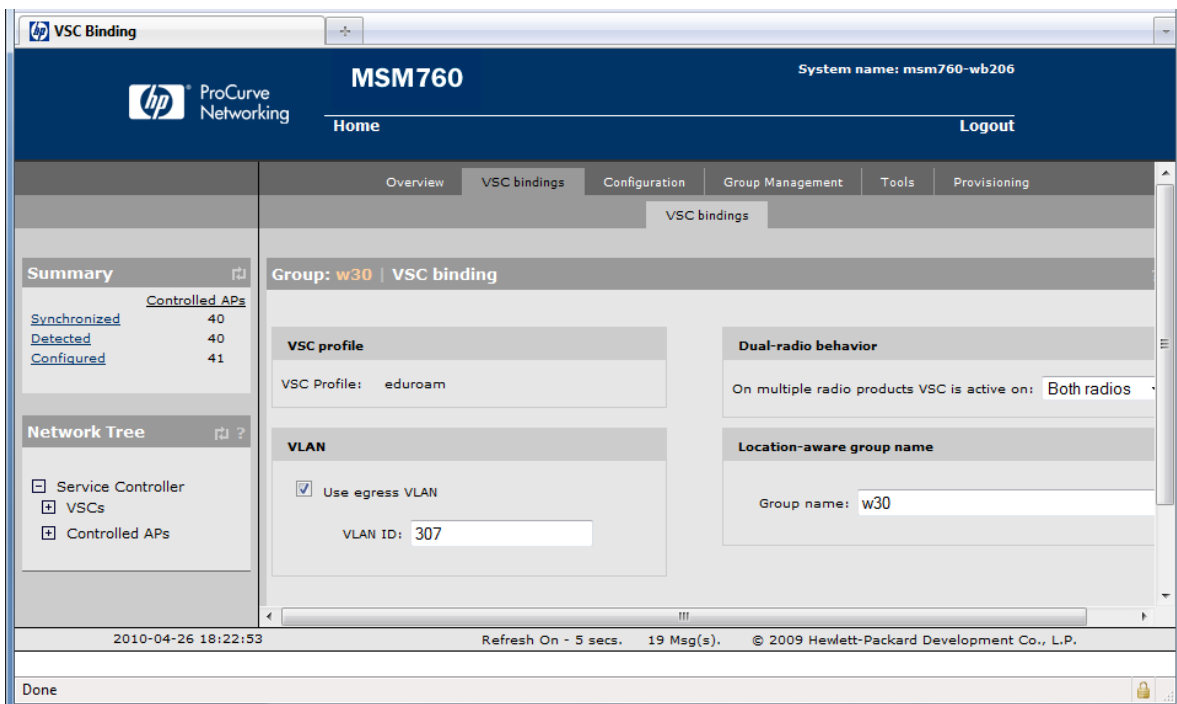


Figure 22: VLAN setting for eduroam network. (Virtual Service Controller (VCS) is the profile that is configured for every wireless connection deployed on the control manager.)

## **5 TEST, RESULTS AND ANALYSYS**

### **5.1 Procedure**

After the implementation, the next step is the test of the system. The test should be carried out methodically in order to easily detect whether there is a problem and where it may come from. The test is divided into different steps:

- Test of the VLAN
- Test of the proxy
- Test of the network with VAMK credentials
- Test of the network with other eduroam-enabled institution's credentials

### **5.2 Test of the VLAN**

The VLAN is first tested to make sure that the resources allocated or bound to it is working as it is supposed to. As said earlier a methodical test should be carried in order to easily locate problems. When the test starts from the VLAN, we make sure that they will be an IP assigned to the client laptop when the authentication is successful and the security level I set is applied to the user.

This test is done on the switch (layer 2) to which the access points are connected to. I test the connection through a wire (network cable) connected between the switch and one Personal Computer (PC). If the PC was able to get an IP, connects to the network and gets the required security access then I know that the VLAN is set and ready to work.

The figures below shows the test made on one switch:

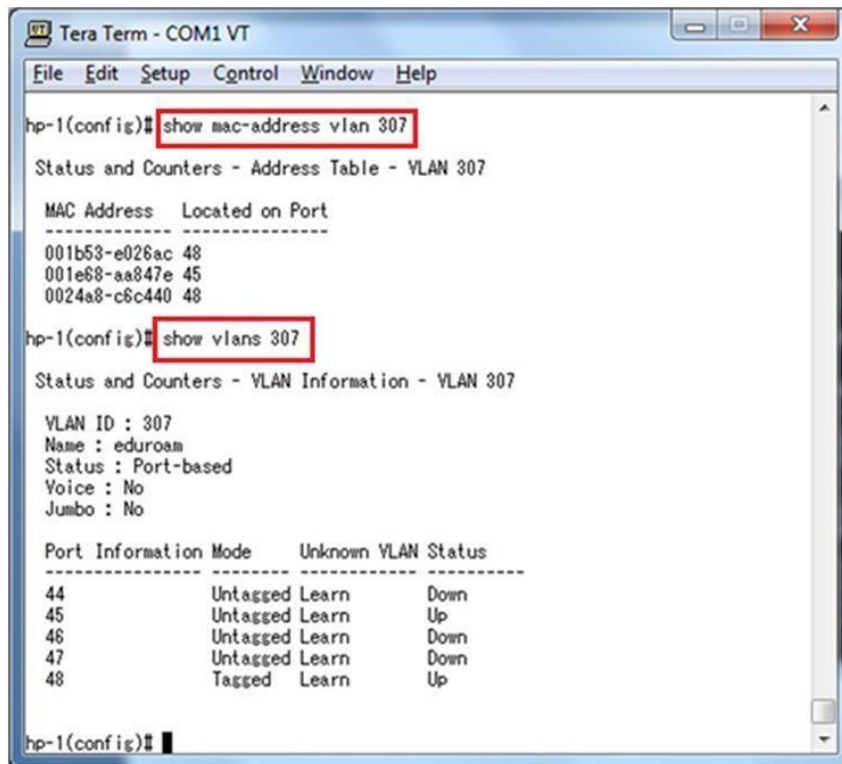


Figure 23: Screen shot of the switch showing the Mac-address and ports.

In the figure below the IP obtained by the client is a public IP.

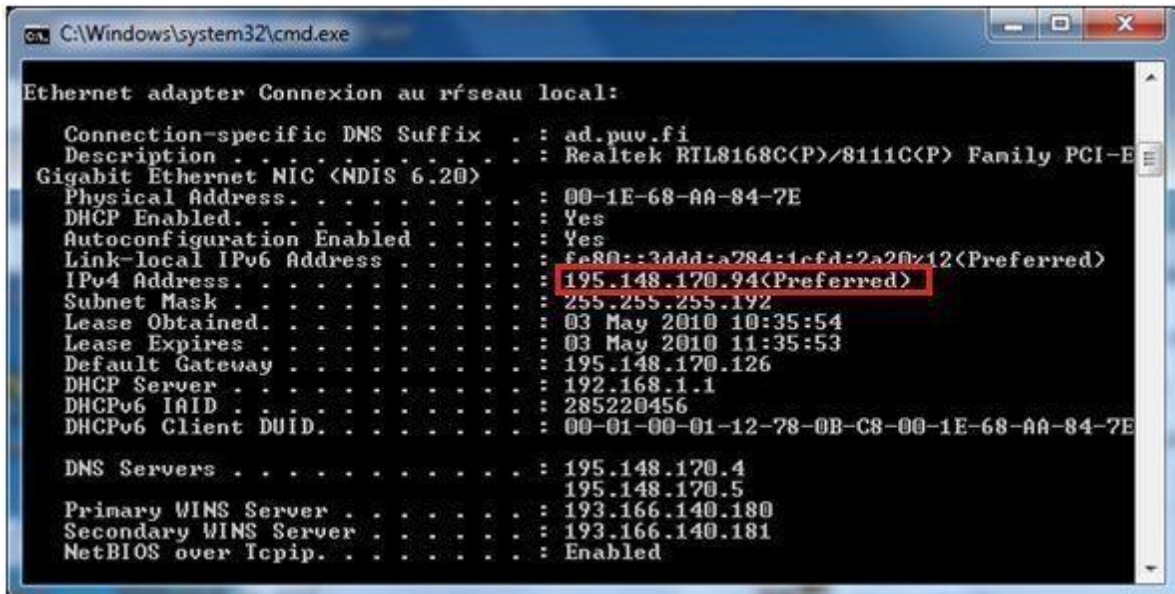


Figure 24: Screen shot of a command "ipconfig/all"



In Figure 23, the connection to the switch shows that the VLAN defined for the network is passing through. This is shown by the set of Mac-addresses that are passing through the switch and the command “*show vlans 307*” displays the ports that are connected and the ones that are up.

The Figure 24 shows the IP assigned to the host (the connected eduroam client). This is as planned a public IP. The VLAN is doing at least now some of the attributions: the IP assignment. I need to test if the network resources allocated according to the firewall are respected.

1. I tried to print a page but no printer was able to print the page.
2. I opened a browser and looked for “*www.puv.fi*” and it worked.
3. In the same browser I tried “*helpdesk.puv.fi*” and it did not work: This server is an internal server; only internal network users can access it.

After the test it was clear that the VLAN is working. The next step is to move to the proxy server.

### **5.3 Test of the proxy**

FreeRADIUS is the RADIUS server installed. The idea of this test is to make sure that the server is running and it is forwarding the requests to the appropriate server when it receives it.

The ultimate test that can be done on the RADIUS server is the “*radtest*”. The *radtest* is a test tool that sends authentication request to the server. It can be locally (using localhost) or remotely (from an added client). When the *radtest* gives an Access-accept reply then the authentication is working on the server. The format of the *radtest* command is: “*radtest {username} {password} {hostname} 10 {radius\_secret}*”.

In this project the server is not used as authentication server. Therefore the *radtest* cannot be made. The idea here will be the test of the proxy function. In that case I will run the server in a debug mode and from one computer trying to connect to eduroam network by

using credentials. The important factor here is to find out if the server is forwarding the request to the appropriate server. Not much attention is paid to a successful authentication; I just have to use a username with VAMK preconfigured realm and another username with different realm. According to the configuration, the server should forward the VAMK realm request to the home NPS server and the default realm to Funet NTLR server.

To start the server in debug mode the command “*freeradius -X*” is used. Appendix 3 shows some important parts of the output of the server in the debug mode. At this point the output of the server shows that everything is ready for the proxy function.

Then I try to connect to the network through wireless by using the credentials stated earlier. According to the settings in the *proxy.conf* file, username with realm “*ad.puv.fi*” is forwarded to VAMK NPS server and anything different is sent to Funet servers. Appendix 4 and Appendix 5 show respectively the output in the debug while using VAMK realm and other realm.

Both outputs show that the server proxies correctly the requests according to the realm. The first two steps have been successful. The network resources allocated through the VLAN and the proxy function of the server are working. The next step is to test the system by using valid VAMK credentials first from VAMK campus then from remote campus.

#### **5.4 Test of the network by using VAMK credentials from VAMK campuses**

The eduroam concept as stated earlier is for roaming purpose. It is not for any use in the home institution. In this case it does not have any meaning to test the system at the home institution. At least the test from the home institution is not that far reliable.

The idea behind the test from VAMK campuses is to test if the proxy server will be able to forward the authentication packet to VAMK NPS server and if valid credentials are provided, can we have the authentication being successful. No matter where the packet is coming from, when the proxy receives a RADIUS request containing “*ad.puv.fi*” as realm it should be forwarded to NPS server. I think that testing the network on VAMK campus is a

huge step in the testing process. If the test is successful from VAMK campuses, it should be successful from other eduroam enabled campuses. If the last case is not successful, it is easy to locate the problem and find a way to solve it. Refer to the figure(s) below:

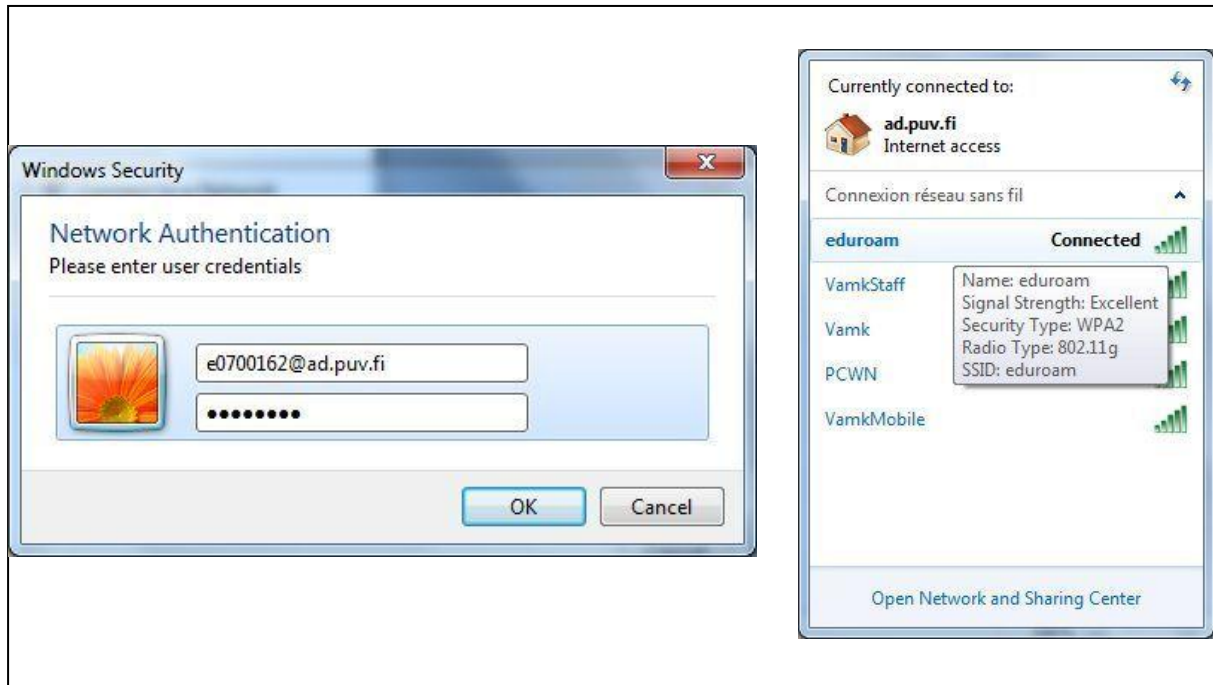


Figure 25: Eduroam login window and successful login window.

```

C:\Windows\system32\cmd.exe

Wireless LAN adapter Connexion rseau sans fil:

Connection-specific DNS Suffix . : ad.puv.fi
Description . . . . . : Atheros AR5007 802.11b/g WiFi Adapter
Physical Address. . . . . : 00-22-68-CA-2E-5C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::948h:2602:6029:dc82%11(Preferred)
IPv4 Address. . . . . : 195.148.170.117(Preferred)
Subnet Mask . . . . . : 255.255.255.192
Lease Obtained. . . . . : 05 May 2010 12:08:18
Lease Expires . . . . . : 06 May 2010 00:14:15
Default Gateway . . . . . : 195.148.170.126
DHCP Server . . . . . : 192.168.1.2
DHCPv6 IAID . . . . . : 184558184
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-78-0B-C8-00-1E-68-AA-84-7E

DNS Servers . . . . . : 195.148.170.5
                       195.148.170.4
Primary WINS Server . . . . . : 193.166.140.180
Secondary WINS Server . . . . . : 193.166.140.181
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

```

Figure 26: “ipconfig/all” command output.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	224.0.0.1	IGMP	V2 Membership Query, general
2	0.053711	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xe3e520da
3	0.107214	195.148.172.2	195.148.170.91	DHCP	DHCP ACK - Transaction ID 0xe3e520da
4	0.206016	HonHaiPr_ca:2e:5c	Broadcast	ARP	who has 195.148.170.126? Tell 195.148.170.91
5	0.270785	Procurve_c6:c4:40	HonHaiPr_ca:2e:5c	ARP	195.148.170.126 is at 00:24:a8:c6:c4:40
6	0.270840	195.148.170.91	193.166.140.180	NBNS	Multi-homed registration NB JOJO-PC<20>
7	0.286970	195.148.170.91	193.166.140.180	NBNS	Multi-homed registration NB JOJO-PC<00>
8	0.287105	195.148.170.91	193.166.140.180	NBNS	Registration NB WORKGROUP<00>
9	0.355166	HonHaiPr_ca:2e:5c	Broadcast	ARP	who has 195.148.170.126? Tell 195.148.170.91
10	0.363414	Procurve_c6:c4:40	HonHaiPr_ca:2e:5c	ARP	195.148.170.126 is at 00:24:a8:c6:c4:40
11	0.363466	195.148.170.91	195.148.170.4	DNS	Standard query A isatap.ad.puv.fi
12	0.365922	195.148.170.4	195.148.170.91	DNS	Standard query response, No such name

Figure 27: Traffic capture from the client laptop.

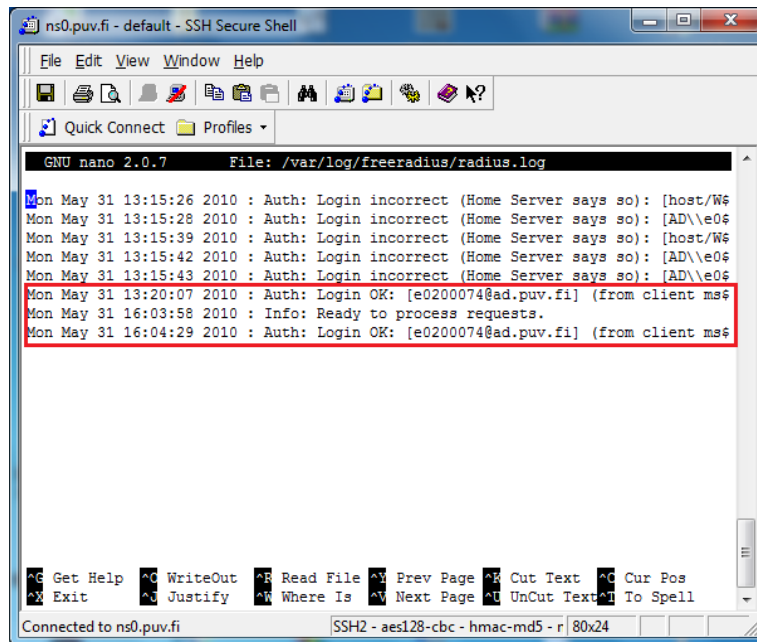
This capture shows that the conversation between the client and the system starts from the DHCP transactions. Even though there has been an authentication process it is not shown in the capture. This is explained that before the authentication is made, there is no network traffic going on the client. All the traffic starts from the DHCP transactions.

## 5.5 Test from other eduroam-enabled campuses with VAMK credentials

Obviously this part of the system testing has a big importance in the implementation. The state of the test is going to tell whether VAMK personnel can use eduroam connection while they are visiting other campuses. The test is done by using a test account from VAMK on an eduroam-enabled institution campus. The credentials are used to login in the system.

For this test, Funet premises are used. VAMK testing account was sent to a contact there to make the test. The failure or success of the test will be reported to us in VAMK. The same day that the test was carried out, I run the server in a debug mode. It was also an opportunity for me to check lively the state of the connection.

Due to the huge output that we always get from the debug mode, it will not be possible to add it as appendix to this document. I added only some key output lines to show the state of the connection. The figure below shows the remote authentication login success from the proxy logs:



```
ns0.puv.fi - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
GNU nano 2.0.7 File: /var/log/freeradius/radius.log
Mon May 31 13:15:26 2010 : Auth: Login incorrect (Home Server says so): [host/W$
Mon May 31 13:15:28 2010 : Auth: Login incorrect (Home Server says so): [AD\\e0$
Mon May 31 13:15:39 2010 : Auth: Login incorrect (Home Server says so): [host/W$
Mon May 31 13:15:42 2010 : Auth: Login incorrect (Home Server says so): [AD\\e0$
Mon May 31 13:15:43 2010 : Auth: Login incorrect (Home Server says so): [AD\\e0$
Mon May 31 13:20:07 2010 : Auth: Login OK: [e0200074@ad.puv.fi] (from client ms$
Mon May 31 16:03:58 2010 : Info: Ready to process requests.
Mon May 31 16:04:29 2010 : Auth: Login OK: [e0200074@ad.puv.fi] (from client ms$
^C Get Help ^C WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^N Next Page ^U UnCut Text ^T To Spell
Connected to ns0.puv.fi SSH2 - aes128-cbc - hmac-md5 - r 80x24
```

Figure 28: Output showing remote authentication success with VAMK credentials

## 5.6 Test with other eduroam-enabled institution's credentials on VAMK campuses

This test is as important as the previous one. The result of this test will tell if the system will play the role for which it has been implemented: let roaming students use their home credentials to have network access. In this test a username and password for remote eduroam enabled institution are used.

If the authentication succeeds, it will tell about two things:

- The proxy is forwarding the request according to the realm
- The connection from our proxy to the remote institution RADIUS server was successful.

A test account was created at Funet and sent to me. The server certificate from Funet was also downloaded. The test was done two times: without the server certificate validation and with the certificate validation. The test was done in both states to show that connection is possible with or without server certificate validation.

The login window and the successful authentication are displayed below:

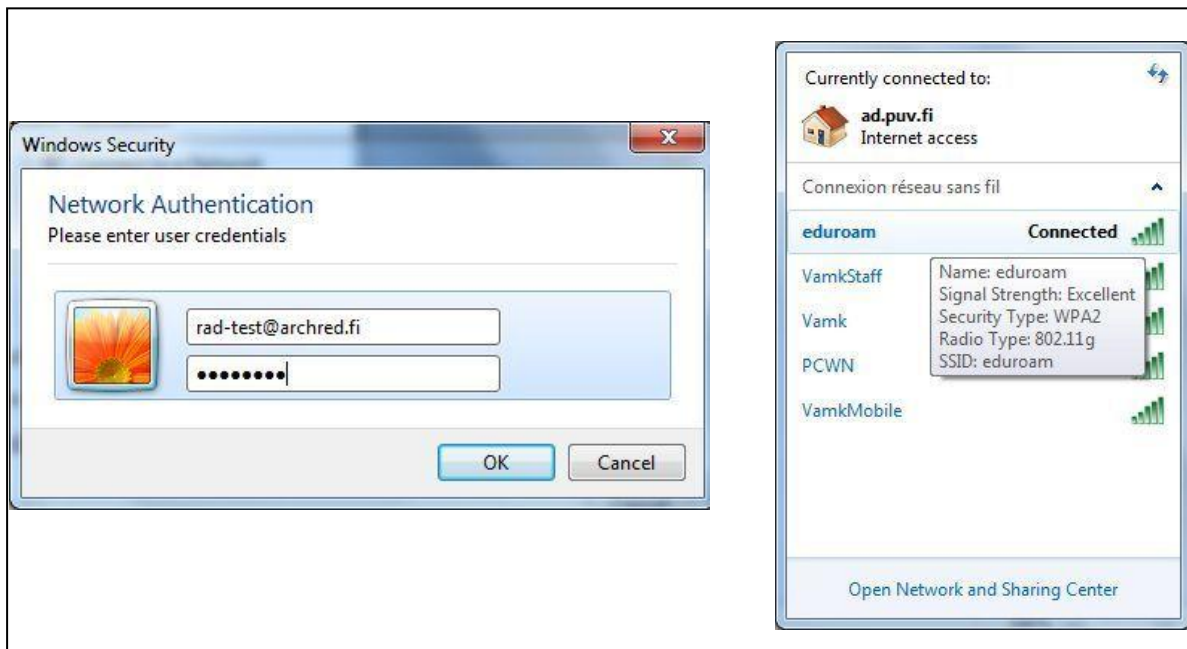


Figure 29: Eduroam login window with external credentials and successful connection.

```
C:\Windows\system32\cmd.exe

Wireless LAN adapter Connexion rfseau sans fil:

Connection-specific DNS Suffix . . . . . : ad.puv.fi
Description . . . . . : Atheros AR5007 802.11b/g WiFi Adapter
Physical Address. . . . . : 00-22-68-CA-2E-5C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::948b:2602:6029:dc82%11(Preferred)
IPv4 Address. . . . . : 195.148.170.117(Preferred)
Subnet Mask . . . . . : 255.255.255.192
Lease Obtained. . . . . : 05 May 2010 14:07:34
Lease Expires . . . . . : 06 May 2010 02:07:34
Default Gateway . . . . . : 195.148.170.126
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 184558184
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-78-0B-C8-00-1E-68-AA-84-7E

DNS Servers . . . . . : 195.148.170.4
                       : 195.148.170.5
Primary WINS Server . . . . . : 193.166.140.180
Secondary WINS Server . . . . . : 193.166.140.181
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:
```

Figure 30: “ipconfig/all” command output.

All the tests are successful. The system is ready to be used. Different computers can therefore be configured to be able to connect to it.

## 6 SUPPLICANTS CONFIGURATION

### 6.1 Definition

In an authentication process there are three components: a supplicant (client laptop), an authenticator (NAS e.g. wireless access point in our case) and the authentication server.

A supplicant by definition is a piece of software built in an end device which is used to get connection to a network through an authenticator. [3]

The supplicant sends authentication credentials to the authenticator; when the authentication is successful, the authenticator grants access to the network. Supplicant can either be an inbuilt (directly in the Operating System) or an installed application (e.g. SecureW2 or Open1X).

When it is an inbuilt application, the configuration is done on the network card. This option is good because it does not cost any extra fee. The inconvenience is the configuration that must be done by the user. In case the user does not much about some issues it may be difficult. That is why the installed application like SecureW2 can be used. This application is configured by the administrator. The user downloads it and uses it to connect to the network. The inconvenience is the cost. It is not free. The Open1X is an open source. That one can be used in replacement of SecureW2. In this work I will only show how to configure the inbuilt one.

To be able to connect to the eduroam network, someone needs only a laptop with wireless network card and valid credentials. The problems come then from different types of Operating Systems we may have on our computers and in some cases if there must be a server certificate validation during the authentication process. In that perspective I have decided to show how to configure the network card according to the Operating System which is running on our computers. This configuration will be done in two steps:

- Certificate installation
- Network card configuration.



## 6.2 Certificate installation

As stated earlier, while using PEAP-MS-CHAP v2 the client does not need a certificate. The server only authenticates itself to the client. Therefore we need to install the server certificate on the client computer. VAMK is using its own certificate authority (CA) server. The certificate generated by the CA is the one we install in the client computer.

Usually this certificate is uploaded on a web server. Users that want to get the certificate should download and install it. In VAMK the address on which the certificate can be downloaded is: [www.puv.fi/dcwolf.crt](http://www.puv.fi/dcwolf.crt).

One important thing has to be mentioned before downloading the certificate. The web browser Mozilla (Firefox) is not a good candidate since it always tries to install the certificate for its own use. However, it should be used for other purposes. Internet explorer or Google Chrome for instance should be used. It is also easier to save the certificate in a folder where it can be seen faster. I recommend for instance “Desktop” as one of the places.

The installation of the certificate is as follow:

- 1- After the file has been saved, double click on the file and it opens new window. Click on “Open” to continue
- 2- Click on “Install Certificate” and on the next window click “Next”
- 3- On the next window select the second option and click on “Browse”

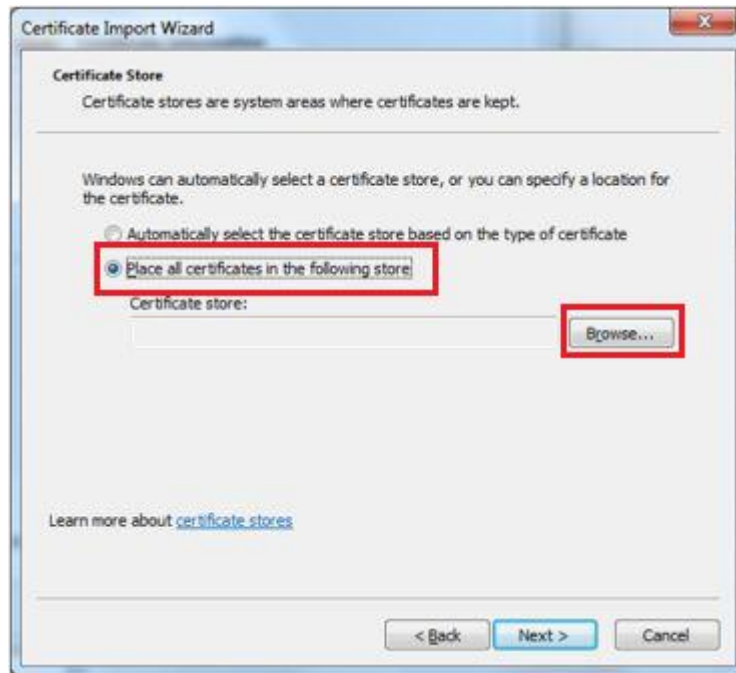


Figure 31: Certificate store selection option window.

- 4- Select on the next window the second option and click “OK”
- 5- To validate the choice click “Next” and on the next window “Finish”

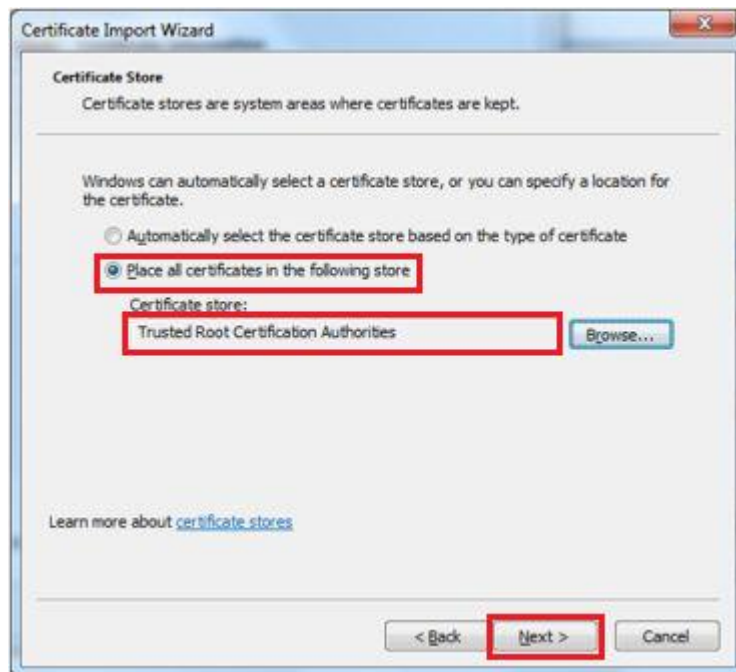


Figure 32: Confirmation window.

6- Click “Yes” on the next window

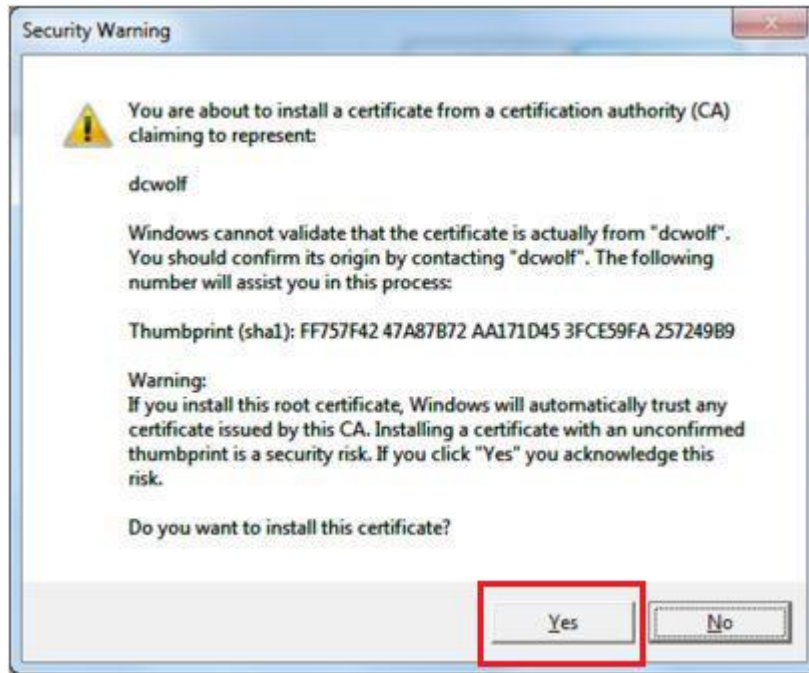


Figure 33: Thumbprint warning window.

7- New window will open and show “The import was successful”. Everything went well and the window can be closed.

### 6.3 Network card configuration

The configuration of the network card is different according to the Operating System used.

In this document I will configure based on Microsoft Windows (most used) and Ubuntu 9.10 (VAMK official Linux Operating System).

#### 6.3.1 Configuration according to Microsoft Windows

In this part the work will be divided again into two sub-parts: configuration with Windows 7, the latest version (similar configuration to Vista) and XP professional Service Pack 3 (SP3). If your system is not up to SP3, you must upgrade it to. More information is

available at: <http://support.microsoft.com/kb/322389> . The previous service pack does not support WPA2 security.

### 6.3.1.1 Windows 7

At VAMK, some laptops belong to the domain. The configuration of those computers is different from the one which does not belong to the domain.

#### Domain based computer

The configuration of the domain based computer is shown below:

- 1- New wireless connection must be added. Open “Network and Sharing Center” and click on “Manage wireless networks”

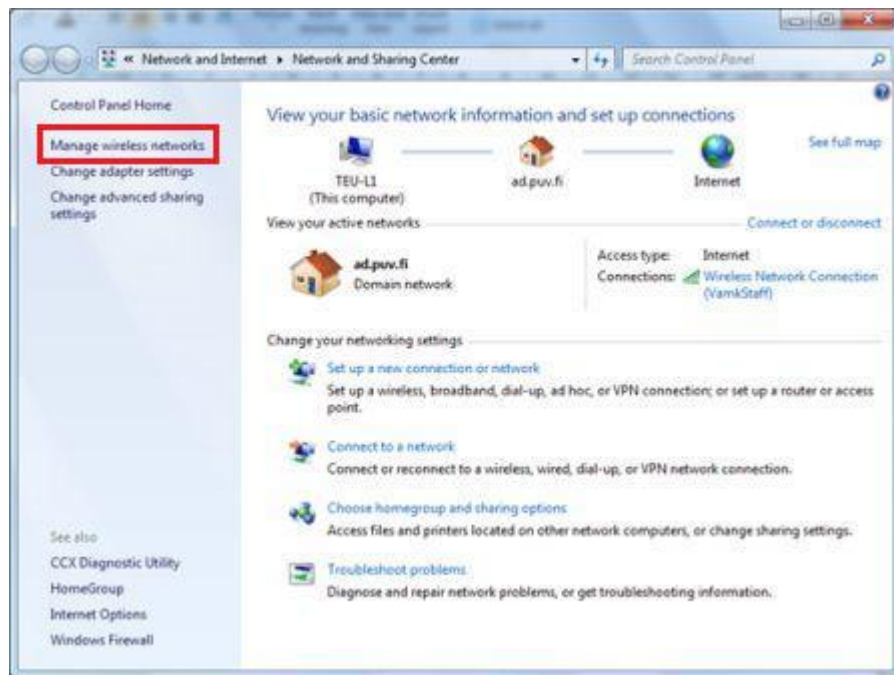


Figure 34: Network and sharing centre window.

- 2- On the next window, click on “add” and select the first option on the next window “Manually create a network profile”

- 3- On the next window use the same configuration, make sure “Connect automatically is unchecked” and click “Next”

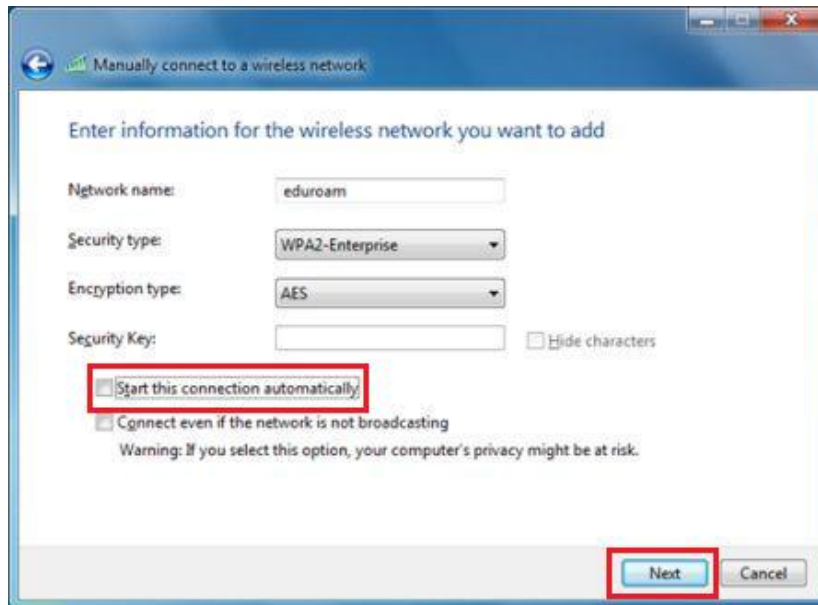


Figure 35: Eduroam wireless connection settings window 1.

- 4- To continue the settings for the new connection, click on “Change connection settings”
- 5- On the security tab make sure everything looks the same and click on “Settings”

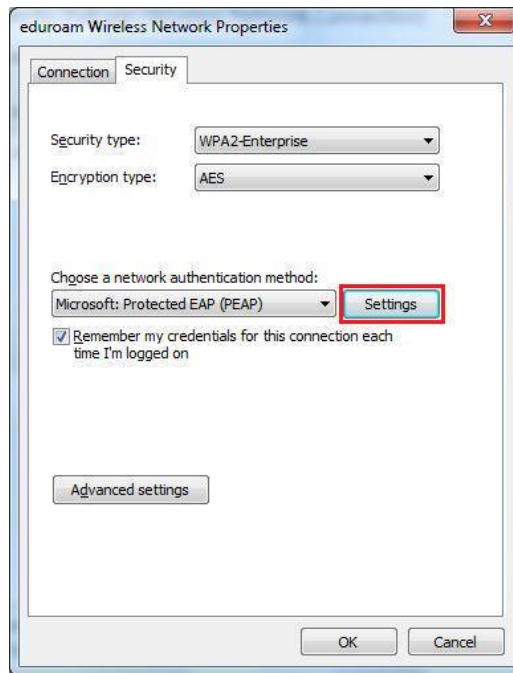


Figure 36: Eduroam wireless connection settings window 2.

6- Check the VAMK certificate, get all the settings conform and click on “Configure”

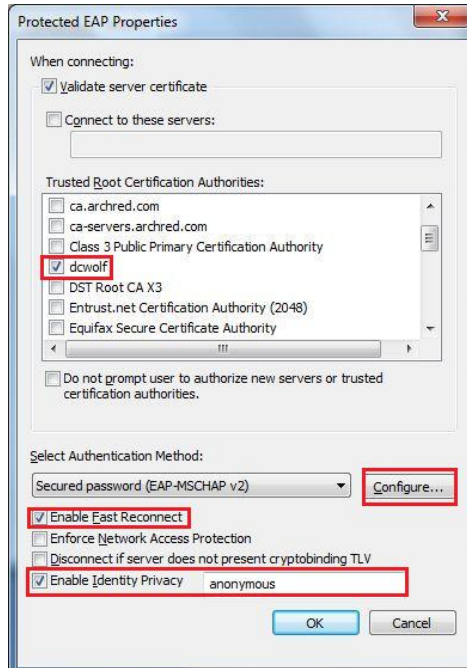


Figure 37: Eduroam wireless connection settings window 4.

*NB: The “Identity privacy” option is recommended to ensure the privacy of the implementation. When this option is enabled, the host SP server will only keep the realm of the guest not the username. The username will be replaced by “anonymous”.*

- 7- Uncheck the box and click on “OK” to return to the previous window, then “OK” again to open new window.
- 8- On the opened window click on “Advance Settings”
- 9- On the 802.1X tab, check the option “Specify authentication method” and select “user authentication”. Click “OK” to complete the setting.

The client computer is now ready to get connected to eduroam. The next figure shows the login window and the format in which the username should be written:



Figure 38: Eduroam login window.

### **Non-based domain computer**

There is no need to add a new wireless connection when the computer does not belong to the domain. After the certificate installation the connection is ready. The user just needs to

enter the credentials in the same format as we did in the domain based computer configuration.

### 6.3.1.2 Windows XP

To be able to connect to the network, we need to add manually the eduroam network to the wireless connections knowing the certificate has been already installed. The steps are the same as in Windows 7.

After the wireless connection has been configured, the connection to eduroam is possible. The login window used in XP to connect to the network is shown in the figure below. Make sure to leave the option “Logon domain” empty:



Figure 39: Eduroam login window on Windows XP.

It is recommended not to set the eduroam connection as “automatic”. Since the configuration may be different from one campus to another. When it is set as “manual”, it is then possible to modify the configuration whenever needed.



## **6.3.2 Configuration based on Ubuntu**

### **6.3.2.1 Certificate installation**

On Ubuntu the certificate is not installed like in Windows. The certificate is downloaded and saved in a folder where it should not be deleted. The downloading process is still the same as in Windows. Since Ubuntu does not contain Internet Explorer, a browser like Google Chrome should be a good candidate. It can also be obtained by using the command line. The command “*wget www.puv.fi/dcwolf.crt*” is issued in the terminal.

### **6.3.2.2 Network card configuration**

The configuration on Ubuntu looks simpler but it is different depending on the version of Ubuntu. The figure below shows how the configuration is done.

Connection name: eduroam

Connect automatically

Wireless | **Wireless Security** | IPv4 Settings | IPv6 Settings

Security: WPA & WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity: anonymous

CA certificate: dcwolf.crt

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username: username@ad.puv.fi

Password: .....

Show password

Available to all users

Cancel Apply

Figure 40: Eduroam supplicant settings on Ubuntu 9.10.

## 7 CONCLUSION

In this project I have deployed eduroam federated wireless network on the VAMK campuses. The objectives set at the beginning of the project have been met. With eduroam running, two services are offered: Staff and students from VAMK are able to use their credentials from VAMK to log in and get internet access in every eduroam-enabled institution in the world. Simultaneously, VAMK offers to visiting users the opportunity to also use their home credentials in order to have access to internet at any time.

The use of a Linux based server during this project was a good opportunity to apply once again my knowledge in that domain. Using FreeRADIUS as a proxy server on Debian server is a no cost solution. It makes it available for everybody, from students to companies.

Scalability and interoperability between open source and close source application is shown by putting FreeRADIUS and Windows 2008 NPS.

During this project, the working method was very motivating. The project manager allowed me to plan the whole project and to configure the system myself. It helped me learn a lot by reading configuration files and making the right settings.

At the end of this project, after the whole implementation, I conclude that:

- The 802.1X authentication method used secures the network by preventing the access until the authentication is successful.
- Due to remote authentication, to prevent eavesdropping, a secured data tunnel must be used to carry the credentials from the host institution to the home institution. In order to do that, PEAP-MS-CHAP v2 is used for the encrypted tunnel it uses to protect the EAP messages.
- The RADIUS servers architecture used in the eduroam network routes the authentication requests based on the realm stated in the username and keeps the privacy of the guest user by hiding it's username in the host RADIUS proxy.

- To secure the data exchange between the wireless client and the access point, the use of WPA2 is appropriate. It does not only secure the data, but smoothly offers connections and transitions between the access points.

Few days after the eduroam has been set, the server logs show that students from other enabled-eduroam universities successfully have logged in using their home credentials.

## **Limitation**

The first difficult issue in this project was the fact that I did not have an administrator privilege on the Windows NPS server. It made the work more complicated because any time there were authentication failure, I could not directly check the reason of the failure. It also limited me in exploring beyond the scope of the project in order to add more features.

The remote test of the system has been very difficult. It was not easy to get assistance from external institutions: first to test the connection with VAMK credentials and second to get a valid account from another eduroam-enabled institution. This situation delayed the completion of the project.

## **Project extension.**

For further extension of this work, it would be interesting to work on how to deny access for local users trying to get to eduroam from VAMK campuses. This would secure and keep the allocated IPs for guests only and avoid users playing around with the public IP addresses.

## **SUMMARY**

Eduroam is a wireless network which allows users to use their credentials from their home eduroam-enabled institution to log in into a host institution network in order to have access to network resources. For users this is a simple way to be connected to internet by using their laptops.

With eduroam set on a campus, two options are offered: the users of the institution itself can go to any eduroam-enabled institution and have network access; users from another eduroam-enabled institution can also use their home credentials on that campus.

During the implementation I configured the RADIUS server that is acting as Service Provider (SP), connected the proxy to the Windows server running Network Policy Service (NPS) and configured all the switches and access points.

In this project the FreeRADIUS server is used as SP server, the Windows server 2008 NPS as authentication server, the Active directory as user database, the Access points as NAS and VLAN and routing protocol configured on HP switches.

After the implementation, the tests of the system were successful from VAMK campuses and the other campuses.

The authentication process which takes place before granting network access is a good system that can be deployed in many companies or institutions to prevent unwanted connection.

## REFERENCES

[1]: Allied Telesis, 802.1X White paper [referenced 2006]. Available in www-form:

<URL: [http://www.alliedtelesis.com/media/pdf/8021x\\_wp.pdf](http://www.alliedtelesis.com/media/pdf/8021x_wp.pdf) >

[2]: City of Vaasa, geographical and social presentation of city of Vaasa; it tells about when the city was built and where it is situated. Available in www-form:

<URL: [http://www.vaasa.fi/Other\\_languages/In\\_English/First\\_page/General\\_Info](http://www.vaasa.fi/Other_languages/In_English/First_page/General_Info) >

[3]: GÉANT2, Deliverable DJ5.1.5.3: Inter-NREN Roaming Infrastructure and Service Support Cookbook – Third Edition [referenced 20.10.2008]. Available in www-form:

<URL: <http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf> >

[4]: GÉANT & TERENA, historic of eduroam about how it started and in where it was tested first. Available in www-form:

<URL: <http://www.eduroam.org/index.php?p=about> >

[5]: GÉANT & TERENA, map of eduroam coverage in Europe; it shows all the countries which are connected to the network. Available in www-form:

<URL: <http://www.eduroam.org/?p=europe> >

[6]: GOOGLE, map showing all the schools connected to eduroam network in Finland. The map shows the school's name and addresses, the SSID used, the type of wireless encryption used and the number of deployed access points. Available in www-form:

<URL: [http://monitor.eduroam.org/eduroam\\_map.php?kml=europe\\_capital](http://monitor.eduroam.org/eduroam_map.php?kml=europe_capital) >

[7]: Interlink Networks, how TTLS server interacts with the legacy RADIUS server, it shows how the TTLS tunnel is created to protect the EAP message. Available in www-form:

<URL: [http://www.interlinknetworks.com/app\\_notes/eap-peap.htm](http://www.interlinknetworks.com/app_notes/eap-peap.htm) >

[8]: JANET, IEEE 802.1X FACT SHEET [referenced 11.05.2007]. Available in www-form:

<URL: <http://www.ja.net/documents/publications/factsheets/064-ieee.802.1x.pdf> >

[9]: Joris, van Rantwijk; WPA calculation-From passphrase to hexadecimal key, [referenced 06-12-2006]. Available in www-form:

<URL: <http://www.xs4all.nl/~rjoris/wpapsk.html> >

[10]: Lars, Strand; 802.1X Port-Based Authentication HOWTO [referenced 18.08.2004].

Available in www-form:

<URL: <http://tldp.org/HOWTO/8021X-HOWTO/intro.html#p8021x> >

[11]: Lars, Strand; authentication process shown in diagram, 802.1X Port-Based authentication HOWTO [referenced 18.08.2004]. Available in www-form:

<URL: <http://tldp.org/HOWTO/8021X-HOWTO/intro.html> >

[12]: Mario, Goorden, RADIUS packet format and RADIUS message flow [referenced 10.01.2003]. Available in www-form:

<URL: <http://ing.ctit.utwente.nl/WU5/D5.1/Technology/radius/#sequencediagram> >

[13]: Microsoft, the cable guy, PEAP with MS-CHAP v2 for secured password based wireless access [referenced 06.2002]. Available in www-form:

<URL: <http://technet.microsoft.com/en-us/library/bb878077.aspx> >



[14]: Paul, Arana; Benefits and vulnerabilities of Wi-Fi Protected Access 2 (WPA2) [referenced 2006]. Available in www-form:

<URL:

[http://cs.gmu.edu/~yhwang1/INFS612/Sample\\_Projects/Fall\\_06\\_GPN\\_6\\_Final\\_Report.pdf](http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf)  
>

[15]: Student of Vaasa, educational level and ranking of Vaasa city based on study capacity [referenced 2009]. Available in www-form:

<URL: [http://www.opiskelijanvaasa.fi/In\\_English/Vaasa\\_City](http://www.opiskelijanvaasa.fi/In_English/Vaasa_City) >

[16]: TechRepublic, Solution Base: RADIUS deployment scenarios [referenced 31.08.2006]. Available in www-form:

<URL:

[http://i.techrepublic.com.com/downloads/PDF/SolutionBase\\_RADIUS\\_deployment\\_scenarios.pdf](http://i.techrepublic.com.com/downloads/PDF/SolutionBase_RADIUS_deployment_scenarios.pdf) >

[17]: Wi-Fi Alliance, Glossary of Wi-Fi Alliance website, section WPA2 [referenced 2010]

Available in www-form:

<URL: [http://www.wi-fi.org/knowledge\\_center\\_overview.php?type=3](http://www.wi-fi.org/knowledge_center_overview.php?type=3)>

## APPENDICES

### Appendix 1: proxy.conf

```
# -*- text -*-
##
## proxy.conf -- proxy radius and realm configuration directives
##
## $Id: proxy.conf,v 1.34 2008/04/18 09:29:50 aland Exp $
#####
#
# Proxy server configuration

proxy server {
    default_fallback = no /* In case one of the IdP is down, its request should not be
                           Forwarded to another one */
}

#The home servers configuration

home_server radius1 {
    ipaddr = 193.xxx.xxx.xxx /* State the IP address of the IdP */
    port = 1812 /* Specify the authentication port */
    type = "auth+acct" /* The IdP serves as authentication and accounting server */
    secret = "vamksecret" /* Common secret used by the SP and the IdP */
    response_window = 20 /* in second; time frame within the IdP must respond */
    require_message_authenticator = yes /* added to all outgoing requests */
    zombie_period = 40 /* If no response from IdP after 40s, consider it as dead */
    status_check = "status-server" /* frequently checks the dead server if it's alive */
    ping_interval = 30 /* time in between two pings */
    check_interval = 30 /* time interval in between the check packets are sent */
    num_answers_to_alive = 3 /*set IdP to be alive after 3 consecutive answers */
    num_pings_to_alive = 3 /* set IdP to be alive after 3 successful pings */
    revive-interval = 120 /* After every 120s check if server is alive again */
}
```

```

home_server radius2 {
    ipaddr = 193.xxx.xxx.xxx
    port = 1812
    type = "auth+acct"
    secret = "vamksecret"
    response_window = 20
    require_message_authenticator = yes
    zombie_period = 40
    status_check = "status-server"
    ping_interval = 30
    check_interval = 30
    num_answers_to_alive = 3
    num_pings_to_alive = 3
    status_check_timeout = 4
}

home_server_pool Eduroam { /* Defines the pool of home_servers */
    type = fail-over /* Forwards the request to next server when first failed */
    home_server = radius1
    home_server = radius2
}

# Local users authentication /* Every request with ad.puv.fi is forwarded to this pool */

realm ad.puv.fi {
    pool = Eduroam
}

# Guest users authentication /* All other realms are forwarded to funet ftlr */

realm DEFAULT {
    authhost = ftlr.funet.fi:1812
    accthost = ftlr.funet.fi:1813
    secret = funetsecret /* Common secret between this SP and funet ftlr */
    nostrip /* The username is sent together with the realm */
}

realm DEFAULT {
    authhost = ftlr2.funet.fi:1812
    accthost = ftlr2.funet.fi:1813
    secret = funetsecret
    nostrip
}

```

## Appendix 2: clients.conf

```
# -*- text -*-
##
## clients.conf -- client configuration directives
##
## $Id: clients.conf,v 1.13 2008/04/17 12:22:23 aland Exp $

# Here is the access from access points

client 192.168.29.0/24 {
    secret      = vamksecret /* Common secret between NAS and the SP */
    shortname   = msm422-AP
}

# The access from the wired network

client 192.168.4.0/24 {
    secret      = vamksecret
    shortname   = hp2910-network
}

# The access from Funet /* Remote authentication requests coming from ftlr */

client ftlr.funet.fi {
    secret      = funetsecret
    shortname   = FTLR-Eduroam
}

client ftlr2.funet.fi {
    secret      = funetsecret
    shortname   = FTLR-Eduroam
}
```

### Appendix 3: freeradius -X output

```
ns0:~# freeradius -X
```

```
FreeRADIUS Version 2.0.4, for host x86_64-pc-linux-gnu, built on Sep 7 2008 at  
17:42:33
```

```
Starting - reading configuration files ...
```

```
including configuration file /etc/freeradius/radiusd.conf
```

```
including configuration file /etc/freeradius/proxy.conf
```

```
including configuration file /etc/freeradius/clients.conf
```

```
.....  
    user = "freerad"    /* In debug mode the server is not run by root */  
    group = "freerad"  
client localhost {  
    ipaddr = 127.0.0.1  
    require_message_authenticator = no  
    secret = "testing123"  
    nastype = "other"  
}
```

```
.....  
# Loading of all the settings from proxy.conf
```

```
home_server radius1 {  
    ipaddr = 193.xxx.xxx.xxx  
    port = 1812  
    type = "auth+acct"  
    secret = "oursecret"  
}
```

```
home_server_pool Eduroam {  
    type = fail-over  
    home_server = radius1  
    home_server = radius2  
}
```

```
realm ad.puv.fi {  
    pool = Eduroam  
}
```

```
realm DEFAULT {  
    nostrip  
    authhost = ftlr.funet.fi:1812  
    accthost = ftlr.funet.fi:1813  
    secret = funetsecret  
}
```

```
# Loading of the type of suffix to be used in requests
```

Module: Instantiating suffix

```
realm suffix {  
    format = "suffix"  
    delimiter = "@"  
    ignore_default = no  
    ignore_null = no  
}
```

# Loading settings from radius.conf; especially for the port to be used

radiusd: ##### Opening IP addresses and Ports #####

```
listen {  
    type = "auth"  
    ipaddr = *  
    port = 0  
}  
listen {  
    type = "acct"  
    ipaddr = *  
    port = 0  
}  
main {  
    snmp = no  
    smux_password = ""  
    snmp_write_access = no  
}
```

Listening on authentication address \* port 1812

Listening on accounting address \* port 1813

Listening on proxy address \* port 1814

Ready to process requests. /\* The server is ready to run and proxy requests \*/

#### Appendix 4: Requests forwarding to VAMK NPS process output

```
rad_recv: Access-Request packet from host 192.168.29.253 port 32778, id=106,
length=176
  NAS-Port = 0
  NAS-Port-Type = Async
  User-Name = "e0700162@ad.puv.fi"
  MS-CHAP2-Response =
0x6a002d1cd9cef3e623ae20010031955f06760000000000000000eae1abd6cb4611ca1ecb
f2dcdaf3df851073949421c6b4
  MS-CHAP-Challenge = 0x126d320b19e0fbd0790ffb627fef6511
  NAS-Identifier = "SG9443N00P"
  Framed-MTU = 1496
  Service-Type = Administrative-User
  Message-Authenticator = 0x9c4685ee2272011904a0c511faaed256
+- entering group authorize
++[preprocess] returns ok
++[chap] returns noop
  rlm_mschap: Found MS-CHAP attributes. Setting 'Auth-Type = mschap'
++[mschap] returns ok
  rlm_realm: Looking up realm "ad.puv.fi" for User-Name = "e0700162@ad.puv.fi"
  rlm_realm: Found realm "ad.puv.fi"
  rlm_realm: Adding Stripped-User-Name = "e0700162"
  rlm_realm: Adding Realm = "ad.puv.fi"
  rlm_realm: Proxying request from user e0700162 to realm ad.puv.fi
  rlm_realm: Preparing to proxy authentication request to realm "ad.puv.fi"
++[suffix] returns updated
  rlm_eap: No EAP-Message, not doing EAP
++[eap] returns noop
++[unix] returns updated
++[files] returns noop
++[expiration] returns noop
++[logintime] returns noop
++[pap] returns noop
Sending Access-Request of id 239 to 193.166.xxx.xxx port 1812
  NAS-Port = 0
  NAS-Port-Type = Async
  User-Name = "e0700162"
  MS-CHAP2-Response =
0x6a002d1cd9cef3e623ae20010031955f06760000000000000000eae1abd6cb4611ca1ecb
f2dcdaf3df851073949421c6b4
  MS-CHAP-Challenge = 0x126d320b19e0fbd0790ffb627fef6511
  NAS-Identifier = "SG9443N00P"
  Framed-MTU = 1496
  Service-Type = Administrative-User
```

Message-Authenticator = 0x00000000000000000000000000000000

NAS-IP-Address = 192.168.29.253

Proxy-State = 0x313036

# The request is forwarded to VAMK's NPS server

Proxying request 4 to home server 193.166.xxx.xxx port 1812



## Appendix 5: Requests forwarding to ftlr.funet.fi process output

```
rad_recv: Access-Request packet from host 192.168.29.253 port 32778, id=15, length=178
  NAS-Port = 0
  NAS-Port-Type = Async
  User-Name = "student@somerealm.fi"
  MS-CHAP2-Response =
0x0f00c87049d986b943c7773272b9f6c076dd0000000000000000a238b42b1912f6187c6d8
75e2671db98d969b496c55d43ca
  MS-CHAP-Challenge = 0x5c7dbfe4b2a6dbbd84a30825321d12ea
  NAS-Identifier = "SG9443N00P"
  Framed-MTU = 1496
  Service-Type = Administrative-User
  Message-Authenticator = 0xaf736e03f4b4f7e2e6cbc5315426a579
+- entering group authorize
++[preprocess] returns ok
++[chap] returns noop
  rlm_mschap: Found MS-CHAP attributes. Setting 'Auth-Type = mschap'
++[mschap] returns ok
  rlm_realm: Looking up realm "somerealm.fi" for User-Name = "student@somerealm.fi"
  rlm_realm: Found realm "DEFAULT"
  rlm_realm: Adding Realm = "DEFAULT"
  rlm_realm: Proxying request from user student to realm DEFAULT
  rlm_realm: Preparing to proxy authentication request to realm "DEFAULT"
++[suffix] returns updated
  rlm_eap: No EAP-Message, not doing EAP
++[eap] returns noop
++[unix] returns notfound
++[files] returns noop
++[expiration] returns noop
++[logintime] returns noop
++[pap] returns noop
Sending Access-Request of id 67 to 193.166.5.150 port 1812
  NAS-Port = 0
  NAS-Port-Type = Async
  User-Name = "student@somerealm.fi"
  MS-CHAP2-Response =
0x0f00c87049d986b943c7773272b9f6c076dd0000000000000000a238b42b1912f6187c6d8
75e2671db98d969b496c55d43ca
  MS-CHAP-Challenge = 0x5c7dbfe4b2a6dbbd84a30825321d12ea
  NAS-Identifier = "SG9443N00P"
  Framed-MTU = 1496
  Service-Type = Administrative-User
  Message-Authenticator = 0x00000000000000000000000000000000
  NAS-IP-Address = 192.168.29.253
```

Proxy-State = 0x3135  
#The request is forwarded to Funet's FTLR servers  
Proxying request 5 to home server 193.166.5.150 port 1812