Bachelor's Thesis (AMK)

Logistics

Logistic Information Systems

2012

Joonas Urpi

FreeRADIUS for small and medium-sized companies

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Logistiikka | Logistiikan Tietojärjestelmät

2012 | 72 sivua

Ohjaaja Kouhia Kari

Joonas Urpi

FREERADIUS FOR SMALL AND MEDIUM-SIZED COMPANIES

Turvallisuus on yksi keskeinen alue teknistyneessä ja globalisoituvassa yritysmaailmassa. Yhä suurempi osa yritystiedoista on tietojärjestelmissä. Laitteet saatetaan varastaa tai tietoihin voidaan murtautua tietoverkon kautta mihin vuorokauden aikaan tahansa.

Yritysten tietopankkien ja -järjestelmien turvaaminen viruksilta, hakkereilta ja muilta uhilta on yhä tärkeämpää, koska lähes kaikki järjestelmät on yhdistetty tietoverkkoon.

Työssä keskitytään yhteen tietoturvallisuuden osa-alueeseen, josta käytetään lyhennettä AAA (Authentication, Authorization, Accounting). AAA tarkoittaa toisen osapuolen tunnistamista verkosta AAA-protokollalla, joka tulee sanoista autentikointi (authentication), valtuutus (authorization) ja tilastointi (accounting)

Työssä selvitetään FreeRADIUS ohjelman hyötyä AAA tietoturvallisuudessa ja sen vaikutusta pieniin ja keskikokoisiin yrityksiin. Työ rajataan FreeRADIUS:ksen toimintaan ja sen vaikutuksiin pienten ja keskikokoisten yritysten langattomaan verkkoon tietoturvallisuudessa.

Työssä käydään läpi tietoturvallisuuden perusteet ja käsitteistöä. Opinnäytteessä määritellään käsite AAA-protokolla. FreeRADIUS-ohjelmistosta kerrotaan, mikä on FreeRADIUS, miten se toimii ja, miten ohjelmisto konfiguroidaan.

ASIASANAT:

AAA, RADIUS, Wi-FI, OS, VMware

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Logistics | Logistic Information Systems

2012 | 72 page

Instructor Kouhia Kari

Joonas Urpi

FREERADIUS FOR SMALL AND MEDIUM-SIZED COMPANIES

Safety is one of the central areas in the technical and global world of business. An increasing amount of company information is currently in databases. The equipment can be stolen or information can be hacked into through the network during any time of the day.
Securing company databases and servers from the viruses, hackers and other threats is increasingly important because almost all databases are connected to the network.
This thesis focuses on one of the information security areas known as AAA (Authentication, Authorization, Accounting)
The thesis discusses the purpose of the use of FreeRADIUS in AAA information security. The work is limited to the functionality of FreeRADIUS and its effects on wireless network information security and expenses of smaller and medium-sized companies.

The operation, configuration and installation of FreeRADIUS is documented for future reference. The thesis first focuses on the question, what is information security and AAA. On the next part we discuss about FreeRADIUS. In the last part of the thesis we handle the configuration and installation of FreeRADIUS, test lab and step by step guide

KEYWORDS:

AAA, RADIUS, Wi-FI, OS, VMware

CONTENT

Abstract

Introduction

Appendix

INTRODUCTION

Today society and especially business is focused towards gathering information and having vast amounts of it in order to have an advantage over others in multiple areas. However, information can also mean something else such as the salary of the employees, names, cheques, business plans, documentations, partnerships between companies and so forth.

Crime has increased significantly in recent years, especially on data level. Information is power and it is important to protect the data of companies. Data leaks and hacking has increased dramatically in recent years and IT security has developed rapidly as a response to this. A lot of IT companies offer solutions for different security problems and providing the chance to protect the data and information of a company from outsiders.

The focus of this thesis is on the AAA: Authentication, Authorization and Accounting and its aspect FreeRADIUS. First, Information Security is discussed and after that what is User and his role on the AAA

FreeRADIUS is one solution against Internet crime and it provides an easy solution in multiple ways. A guide for FreeRADIUS and its possible effects on the company's information security does not exist. This thesis will provide you with that information

Most of the programs are expensive and mainly used by bigger companies as smaller and medium-sized companies do not have the same amount of resources. Nevertheless, this thesis might also be useful to bigger-sized enterprises.

1. WHAT IS INFORMATION SECURITY

Information Security is a definition for security in IT and provides us with an understanding of the goal. An important part of information security is also information security policy, which defines the guidelines for the administration of the information security.

1.1 Information Security

Information security stands for securing the necessary information, files, databases and services in normal and abnormal situations with legislative and other actions.

1.2 Information Security Policy

Information security policy defines the way of administration guidelines for actualizing information security and other supporting acts. It allows the administration to implement data security actions, routines and instructions. In order to establish information security policy in a company, it needs to be published and its purpose has to be emphasized for the company's operation and continuation. Without this, workers cannot be required to follow it. An important part is that the administration has to commit to the policy

2. WHAT IS SAFETY OF USING?

Safety of Using is an area within Information Security. Safety of Using defines the act of using files, databases and information safely and without danger of giving files away, recognizing the right user and securing the user acts virtually and physically.

Access rights control and different recognition and authentication processes are included in Safety of Using. The purpose is to try to achieve databases and services for efficient, meaningful and safe usage.

The user environment on virtual and physical level is kept in the working condition and out of use from unwanted people and threats. Safety of Use is also applied on the machines and equipment.

3. WHAT IS AAA?

AAA is also known as Authentication, Authorization and Accounting. This protocol is used in computer security.

3.1 Authentication

This word defines the act of recognizing the user and granting access, when registering into a network or an Internet service. Authentication can occur, for example, when logging into email. (Järvinen, P, IT-tietosanakirja, 2001, 57pg)

3.2 Authorization

This word defines the act of granting the rights to the user to use and change files as well as upload or download, write, save and erase context. The user has all the privileges (depending on the level of authorization) that allow him to use data within server or computer.

3.3 Accounting

This word defines the act of time stamping the successful or unsuccessful event of logging in and logging out. The acts completed during the time of the user will be registered and saved to log in files, so all the information will be available to be checked, if error or other malfunction occurs later.

4. WHAT IS RADIUS

RADIUS is an acronym for *Remote Authentication Dial In User Service.* This is the protocol that will provide AAA management: a way for the computers to connect and use the network services (Jaakohuhta, H 2001, IT Ensyklopedia 444pg)

RADIUS is taken in to use when a company wants to use AAA services. Local area network needs to have a RADIUS server which has switches and wireless connection base stations. RADIUS will provide centralized AAA services to users.

5. WHAT IS FREERADIUS

“FreeRADIUS was founded in June 1999 by Miquel van Smoorenburg and Alan DeKok. The first public "alpha" release of the code was in August 1999, with 0.1 being released in May 2001.”

FreeRADIUS is a security-program, which specializes in wireless networks (Wi-Fi) and remote user control AAA (Authorization, Authentication and Accounting).

The name *FreeRADIUS* refers to the *free open source RADIUS* also known as the RADIUS server. This is registered under GNU GENERAL PUBLIC LICENSE.

FreeRADIUS is based on Unix-code and it can run in multiple operating systems, although the most highly recommended are Linux ones such as Debian Red Hat, SUSE, TurboLinux, Ubuntu. Other systems are for example: AIX, Mac OSX and Solaris, although more exist. The advantage of these operating systems is their almost non-existent RAM and memory usage, and FreeRADIUS itself does not consume much space.

FreeRADIUS is campaigned as the most used RADIUS server in the world .The popularity is explained, with an easy-to-use approach, no cost required to use (downloadable from an official website), user-friendliness, quick and easy installation and comparable security to the payable servers

6. FREERADIUS ADVANTAGES AND DISADVANTAGES FOR COMPANIES

6.1 Use of FreeRADIUS

FreeRADIUS is used in a wireless-environment. This supports users to work via their own laptops or keep multiple equipments in order to get into the database and transfer files, update or change information depending on the need. This might be needed especially for employees who move a lot and hold most of their information inside their laptops.

FreeRADIUS does not require any specific interface or hardware. Users need only the user name & password (which is registered by FreeRADIUS or database), or if the company uses a certificate, this is to be given to the employee in order to have the rights to access the network and database of the company.

Updating FreeRADIUS is simple. The administrator needs to download and drive the application manually, if the update was downloaded. Updating can also be completed automatically, if the *Synoptic Automatic Loader* is used, which will download and update the current FreeRADIUS with the latest updates. However, FreeRADIUS needs to be brought down for the latest updates to start working. Administrators need to be sure that everything is correct and no important settings were changed upon updating the current version to the new one.

6.2 The costs of FreeRADIUS

Company security is an important today. Beside this costs and time are also considered, when planning out company's network and the way everything is connected together: the size, i.e. the expenses, the required hardware.

When deciding on the investment, compatibility with the existing hardware and programs should be considered as well.

FreeRADIUS offer all this, which explains its popularity. It is free software to be used with no additional cost. It is compatible with all the used protocols and able to produce its own ”security certificates”. It does not require licenses to be bought or most important of all, it does not take much time to be taken into use.

However, as a free software, it has its own traits. The more it is used, the more one has to learn and the more time it requires to study all of the functions. Based also on Unix-coding, it is not operating in the same system as Windows, which means that it has its own way of updating and changing settings. FreeRADIUS lacks GUI (General User Interface) so everything is text-based. This might prove a challenge to companies, looking for easy and no-cost solution. Simply by using SPM or manual downloading or updating is not an issue and will be easily handled. Help is also offered to new users by providing support and documents and there is FreeRADIUS Wikipedia, since no GUI exists yet to offer help with installing and basic configuring.

6.3 Maintaining FreeRADIUS

Acquiring FreeRADIUS and implementing it to the existing system does not cost anything. However depending on the company’s growth rate and the user base,

it is a good idea to consider whether new hardware is required. The question is who will perform everything and have time to maintain FreeRADIUS? In today's world of enterprise, security systems are based heavily on the Windows system.

FreeRADIUS is breaking this by giving a chance to change some of the yearly costs into nothing, by just changing the AAA security. This will take time and a designed worker is required to make the changes. The time will be used to configure settings, write up the required scripts and make a certificate as well as to transfer it to the computers in the company.

FreeRADIUS needs someone, who has the knowledge and the ability to use FreeRADIUS, configure it and maintain it. Anyone can do the basics with instructions, but to make it highly usable for the company, it is good for the administrator to have an understanding of the structure and architecture of FreeRADIUS, since there are a lot of possibilities to change and shape FreeRADIUS for the needs of the company.

Initial settings and configuration of FreeRADIUS as well as implementing it to the company topology is to give the information of needed authentication address (giving the IP address range, which is being used in the company), writing down to file ”usernames”' and ”passwords” the *user*. Changing settings for different security protocols and adding more choices and improvements to FreeRADIUS will require more learning and familiarity, since configuration becomes more complicated. It is important to remember to keep it as simple as possible when configuring the FreeRADIUS.

7. FREERADIUS

7.1 Acquiring of FreeRADIUS

FreeRADIUS, as explained earlier, requires a specific operating system in order to work. Recommended OS are Debian or Ubuntu to make installing and working in the system as easy as possible.

The first step is to download the program from the official website of FreeRADIUS. When the download is completed, the installation can begin. The program will automatically do all the default settings, which will not take a long time. To install FreeRADIUS, the Linux operating system is required. FreeRADIUS is working on a Unix -code, so Ubuntu or Debian are good choices along with others.

If Linux OS is used in the company, it will be easier to install FreeRADIUS. Nevertheless, if the company uses Windows OS, the situation can be resolved by using VMware; a virtual machine. This will operate inside another operating system: OS inside OS. VMware is free to download, so it will not require any additional costs from the company. VirtualBox is “Open Source Software under the terms of the GNU General Public License (GPL)”. We will use the term “free” or similar term later to avoid confusion.

VMware is a virtual machine which can be used to start an additional OS inside the OS. This will not take much space, RAM or power from the hosting system, but it is better to remember to include the virtual machine OS in the network plans and designing IPs, since conflicts might occur, if attention is not paid.

FreeRADIUS, upon installation, includes a server, BSD & PAM (client library) as well as an Apache Module. Other packets and modules can be added later to

FreeRADIUS by downloading them later either: 1) manually or 2) using a special ”application downloader” in Debian Operating System also known as the *synaptic automatic loader* or 3) directly using the ”source code”

The second step involves configuring and adjusting FreeRADIUS for the needs of the company: giving access and permission to the users, setting up appropriate protocol to be used (FreeRADIUS supports multiple protocols such as: CHAP, PEAP, EAP, LEAP) or creating a special certificate required to obtain access to the database.

FreeRADIUS consists of a number of necessary files, which need to be changed and configured in order to make FreeRADIUS working: eap.conf, radiusd.conf, client.conf and users. Configuration will take a while since the administrator has to pay attention to various points which will be discussed later

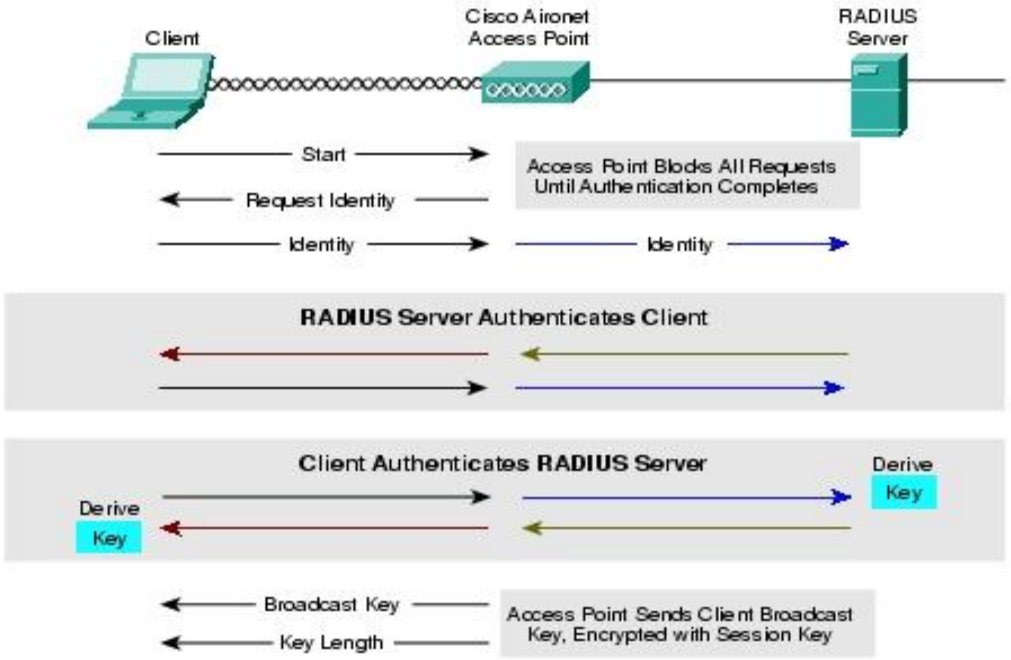
When FreeRADIUS is installed and ready, there are still files to be downloaded. Using the command “-freeradius Xx” will start FreeRADIUS in a debug mode and list all the actions taken, while starting FreeRADIUS. Problems occurring during the initial launch will be shown on the debug mode.

There is also a possibility to create a special certificate with FreeRADIUS, which is more secure. This certificate is only known by FreeRADIUS and the database offering high-level security against intruders.

However, some additional changes might have to be done before the user or administrator can have FreeRADIUS fully working. This requires additional files to be downloaded. All the files will be automatically included in the FreeRADIUS program if using the method to download files by ”application search”. This is a unique feature in Linux operating systems.

7.2 Connecting to FreeRADIUS server

7.2.1 Using FreeRADIUS or Database as an User identifier



(Picture 1. 802.1x and EAP message flow 1 [Referred 16.11.2010])

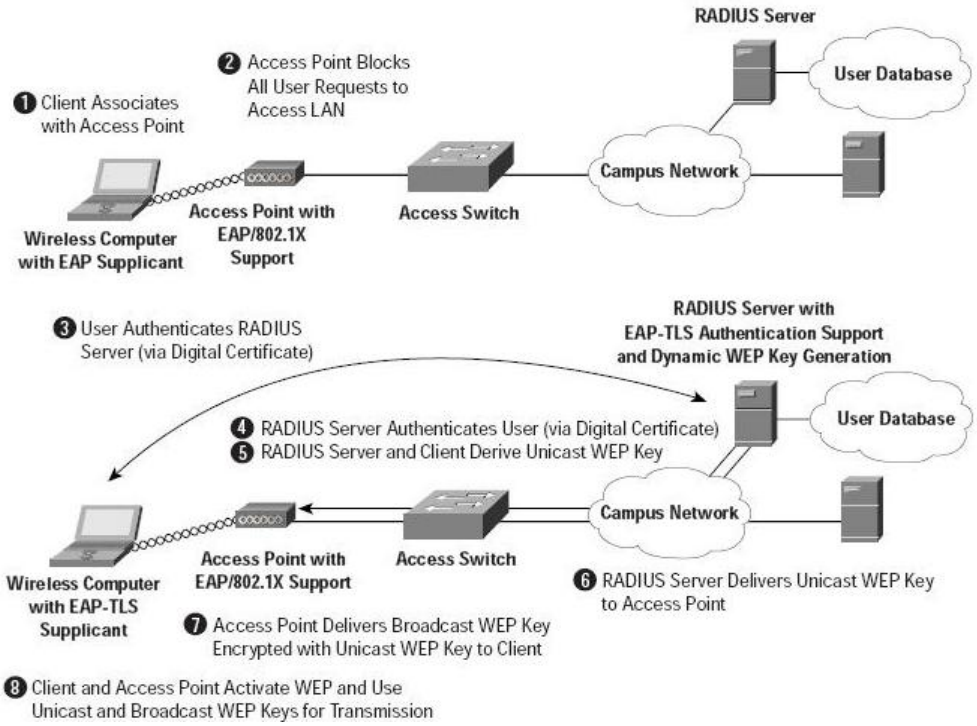
When one has installed the system and made the necessary configuration, he can try out the connectivity and FreeRADIUS can be tested. First an access point and port are set up: an access point is consigned to ask the RADIUS server to identify a client in order to enter. Then an access point is set up to ask user name and password, which an access point will direct to FreeRADIUS.

Furthermore, one can either have FreeRADIUS handle a user name and password or redirect FreeRADIUS to ask a database server for authentication. As shown in picture 1, a client will send a request to an access point. The access point sends a request for identification back to the client. The client

responds by sending the identity (user name & password) and an access point head the respond to FreeRADIUS

It is best to remember that the protocol used needs to be applied to a Laptop, Access Point and FreeRADIUS server. Connecting the laptop (using a wireless connection) to the database, one first connects through an access point. The access point sends a request to the FreeRADIUS server and the FreeRADIUS server goes through the request. Finding the appropriate user name and password (matching the given information to the access point), it will send a reply back to user through an access point ”Access – Accept”.

To put it simply, FreeRADIUS acts as a guard between the passenger and the house preventing any unwanted people coming in. The protocol will be the identity card and the information and password of the user is contained in it.



(Picture 2. 802.1x and EAP message flow 2 [Referred 16.11.2010])

7.2.3 Using Certificate as an User Identifier

During the creation and installation of the FreeRADIUS server, the administrator has the chance to create a private certificate for only the users who will be official employees of the company.

This method works in the same way as identifying the client by user name or password but using the certificate is more secure as a certificate is only known by the FreeRADIUS server. A certificate is created by FreeRADIUS and distributed only to the clients, who regularly use the wireless connection in the work place. This works like a personal identification card **(**Tarkoma, J, Tietotekniikan Sanasto, 1995, 646pg)

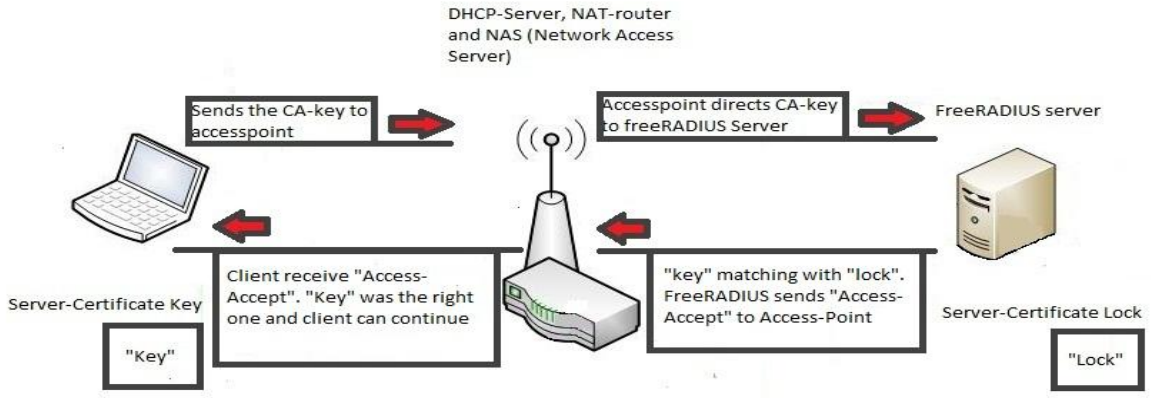


Illustration: Certificate identification

A certificate allows for a higher security on wireless-lan environment because of its public and private key infrastructure. It has its own unique key and password characterization. The only way to have a certificate is to ask the administrator to grant for you.

As in normal authentication with a user name and password, a certificate is now also required in order to connect to a network. Upon connecting, the FreeRADIUS server certificate is matched with the user certificate and the information of the user (user name and password) [Refer to creating certificate in **6.2 Configuring certificate for user and server**.] (Tarkoma, J, Tietotekniikan Sanasto, 1995, 717pg)

This method is also called PKI (Public Key Infrastructure), which creates two keys: public and private key. PKI works by controlling the keys: certificating the keys, and rendering them useless, when not needed anymore or changed (Tarkoma, J, Tietotekniikan Sanasto, 1995, 525pg)

8. COMPATIBILITY OF FREERADIUS

8.1 FreeRADIUS compatibility in general

The only requirement so far for FreeRADIUS is with the platform being used, restricted to the Linux OS System. However, when it comes up to a database, a protocol being used and environment compatibility, FreeRADIUS has a lot to offer. Protocols: WEP, WPA, WPA2, 802.1x work well. Databases from MySQL, LDAP, PostgreSQL, SQL are compatible with FreeRADIUS except SAP. SAP has its own unique password and user name system with different coding and currently, due to FreeRADIUS and SAP differences, there is no chance to use these two systems together.

8.2 FreeRADIUS and Databases

The most recommended databases to be used with FreeRADIUS are LDAP and SQL. These two installed and configured as a database can be settled to act as a “ruling” body to which FreeRADIUS sends requests of clients. It is important, as noted before, that an Access Point and a User must have the same protocol. FreeRADIUS is configured to forward this protocol (settings are configured to allow only this type) and the database (which is in use) will recognize and be able to send a reply back. A second option is to use a certificate. A certificate is a more secure option to use with the user name and password, since it rely on a trusted site.

8.3 FreeRADIUS and Virtualization

When speaking about virtualization one is referring to non-physically existing server, also known as a virtual server or machine which exists inside the actual

physical server. This allow one to create multiple amount of virtual servers using only one physical server

FreeRADIUS is able to use various of protocols: EAP, EAP-TLS, CHAP, PAP, TTLS, LEAP, PEAP: with 802.1x IEEE standards. FreeRADIUS is used to control and authenticate wireless network environment so it is compatible with all types of access points and connectivity's.

For running purposes, if companies are looking for a cost-friendly OS and acquiring Window is not a solution, the answer lies in virtualization: VMware or VirtualBox are one choice to implement in one of the computers and/or servers to run the OS system (Linux). They are fast and efficient and the usage of the hardware will not take much space.

Deciding on a virtualization of the FreeRADIUS server, the virtual and hosting machine should be bridged and virtual machines should be included in an IP-network design. Test that the virtual and the host machine are bridged together by pinging each other to secure that the connection is working between the virtual and hosting machine.

9. HOW DOES FREERADIUS WORK?

Companies have different segments divided into their own sections e.g. accounting, sales, management. Providing also access for guests to reach the Internet via their routers, a company has to protect their database. FreeRADIUS needs to be able to recognize the difference between the worker and the guest to be able to grant the correct rights.

This problem is solved by creating different “user groups” for a company. This is done with: VLAN, dot1q, 802.1x, trunking. These four methods help a company determine who gains access and how to control their wireless network security.

9.1 What is VLAN?

VLAN is a virtual local area network. This is a simple virtual version of LAN. Thanks to VLAn technology, VLAN is created with a switch to act as a broadcast domain. Normally broadcast domains are created by routers, but VLAN has changed this.

All switches have a default VLAN, which is 1. ”All ports in a single VLAN are in a single broadcasts domain: A VLAN is a broadcast domain formed by switches ”(www.petri.co.il *[Referred 17.11.2010]*) The advantage of this method is that having two switches and defining VLANs to particular ports allow only these ports to see a coming message for example; talking between Gigabit 5 on switch A and Gigabit 13 on switch B. These gigabits have been given VLAN 5 and they can talk to each other without other ports seeing “the topic”

VLAN is important for FreeRADIUS since with VLAN you can define the action and material people are able to see. Let us assume that we are assigning some VLANs for specific groups: VLAN 10 is for accounting people, VLAN 15 is for marketing people, VLAN 20 is for sales people and VLAN 30 is for guests. With VLANs an administrator is able to keep information secured from different departments as well as from unwanted people. Assigning specific VLAN for the port is called tagging. (Jaakohuhta, H 2001, IT Ensyklopedia 578pg, 579pg)

Another advantage of VLAN is the unnecessity of subnets. A creation of VLAN allows the devices and end-users to be connected to different switches and routers and be on the same subnet with each other, which eliminates the need for a location. It also allows a more secure environment for users and controlling of groups. However, all the users communicate with FreeRADIUS and there is only one server. Multiple VLANs for different departments have their own subnets, so how to have them all connect and talk with FreeRADIUS?

A solution to this problem exists with trunking. Trunking allows multiple VLANs to communicate through one link between a router and switch or two switches. This is known as a trunk port (www.petri.co.il [Referred17.11.2010]). When making trunking, standard 802.1q protocol is needed to make the trunking work. (Jaakohuhta, H 2001, IT Ensyklopedia 549pg)

9.2 What is 802.1x?

802.1x is a standard protocol designed for WLANs (wireless local area network) to enhance the security. This allows a user to be authorized by a database or other form of authenticator such as access point, but to a limited extend (this is called centralized authority). (Järvinen, P, IT-tietosanakirja, 2001, 14pg)

802.1x is uses multiple authentication protocols such as EAP, EAP-.TLS, MSCHAP, LEAP, MSCHAPv2. This is used in WLANs as in AAA it is used to exchange information between an authenticator and an authenticater. 802.1x is primarily a framework for WLANs

AAA schematic has a supplicant, authenticator and authenticater. A user (supplicant) sends a request to an access point (authenticator). The authenticator sends a message back to the user to use a required protocol (for example, EAP) and send his user name and password. The user receives a message and sends a request again with his information, encrypted in EAP to an access point. The access point now forwards the message to FreeRADIUS (authenticater). FreeRADIUS will send an answer back to the access point according to the information it has received and matching to files. The Access point forwards the answer and allows a user to advance (to the Internet / intranet) when the answer is yes. On a ”no” answer, the access is denied and the user has to try again.

802.x is an IEEE standard for local networks. Each of the different standards 802.1, 802.2, 802.10, 802.7 are meant to be used in different environments. For example, 802.2 cover the protection of Ethernet and 802.11 is for wireless network (Tarkoma, J, Tietotekniikan Sanasto, 1995, 282pg)

10. DATABASE AND FREERADIUS

FreeRADIUS is meant to control the flow of wireless local area networks. Once a user has registered, he has an access to the Internet and the information of the company and other services. However, FreeRADIUS has a capacity limit of storing user information, which is why databases are needed. A database essentially replaces FreeRADIUS as a user-information keeper and is able to store a larger amount of information.

FreeRADIUS offers compatibility with almost all the databases except for SAP. The reason is that SAP uses a unique coding and kerberos system, which cannot be connected with FreeRADIUS. LDAP and PostgreSQL are the most commonly used databases in medium-sized companies. Smaller companies do not use them or have limited use. Making the maximum use of the current software is always a top priority due to wasted resources. A current database can easily be used as a server for RADIUS to connect to ask for information.

Each new version of FreeRADIUS improves the integration and forming connection between RADIUS and a database. However, the current version (2.1.10 and also used later with the installing of FreeRADIUS) does not have any guide for installation and use to connecting FreeRADIUS and a database together. These are expected to appear soon, however.

On the appendix 1 you will find a table of the database information, which are compatible with the FreeRADIUS

11. INSTALLING FREERADIUS

11.1 FreeRADIUS HowTo

The following presents the used equipment in the test lab to make FreeRADIUS fully working. Here is the list of what equipments and commands were used during the test.

Settings	
IP Range	192.168.100.x 255.255.255.0
IP of Virtual – Debian:	192.168.100.100 255.255.255.0
IP of FreeRADIUS:	192.168.100.12 255.255.255.0
User:	Administrator
Password:	root and user = xxxx
Operating System:	Debian GNU/Linux 5.0.4 Lenny Official i386
Virtual machine:	Vmware, version 1.0.10
FreeRADIUS version	Version 2.1.10

Hardware
Cisco Switch 2950 (WS-C2950G-24-EI)
Cisco Access Point (AIR-AP1252AG-E-K9)
Fujitsu Siemens, Amilo Notebook Li 3710 (laptop)
Iphone (Apple)
Microsoft 7 and Microsoft XP
DCPH – server

Commands	
/etc/init.d/FreeRADIUS stop **or** radius stop	This will stop FreeRADIUS
FreeRADIUS -Xx **or** radius -Xx	This will start FreeRADIUS in debug mode
Mc	This will start "midnight commander“ : text editor
radtest "user“ "password“ localhost 1812 "shared secret	This is a testing command to see if FreeRADIUS is working properly. Pay attention to an output of radius
Visudo	Add new users to Debian
Control + X	Exist mc editor
Control + O	Save the changes
Control + C	Show your current position

The instructions for installing FreeRADIUS will also be included here. This will be supported by screenshots during the procedure. This is meant to help administrators who are attempting to do it for the first time, or it might even help

more experienced ones learn new ways. We will be using the Debian GNU/Linux 5.0.4 Lenny i386 operating system (fully installed). It will be built on VMware (version 1.0.10). A clear format list will be stated in a box in the end of the thematic. Debian GNU/Linux was installed to have only Standard System and Desktop Environment

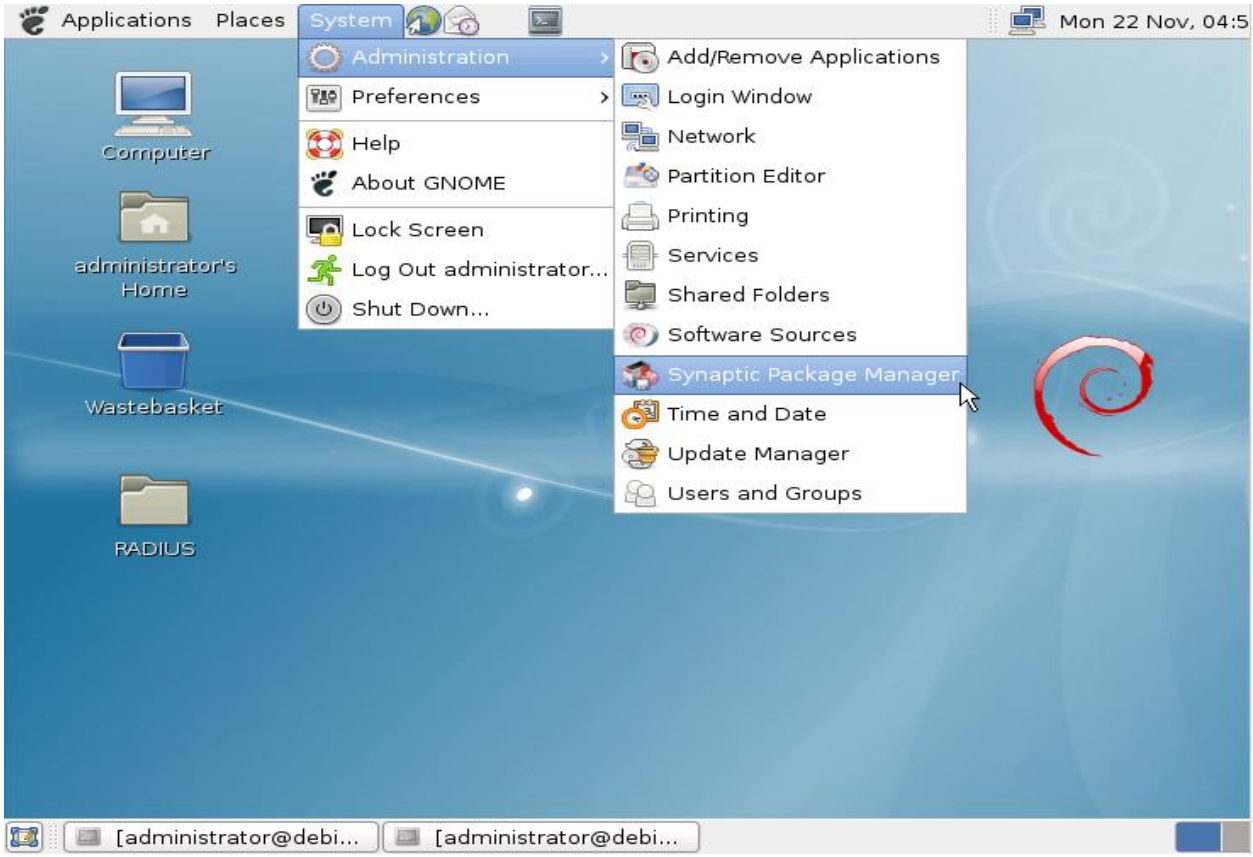
The thematic assumes that you have successfully installed and configured VMware or Virtual Box to your server or computer and it is ready to be used to install FreeRADIUS on it. This guiding thematic will consist of installing and configuring FreeRADIUS, configuring Access Point (using CLI =command line interface) and connecting successfully to FreeRADIUS

It is important to note that the administrator should not use a "sudo“ command because of a security risk. However, it is not denied, but just recommended not to use "sudo“. In this guide everything is conducted via registering as administrator "su“ and then with password "xxxx“

11.2 Initial installing and testing

The first part is to find a Synaptic Package Manager. You can get access to it via System>Administration>**Synaptic Package Manager**. Click it and type your administrative password to gain access. From this point onwards, we will call Synaptic Package Manager= **SPM**

This program allows you to organize your system; everything is called a package. This program will help you to install, upgrade and remove other programs from the operating system.



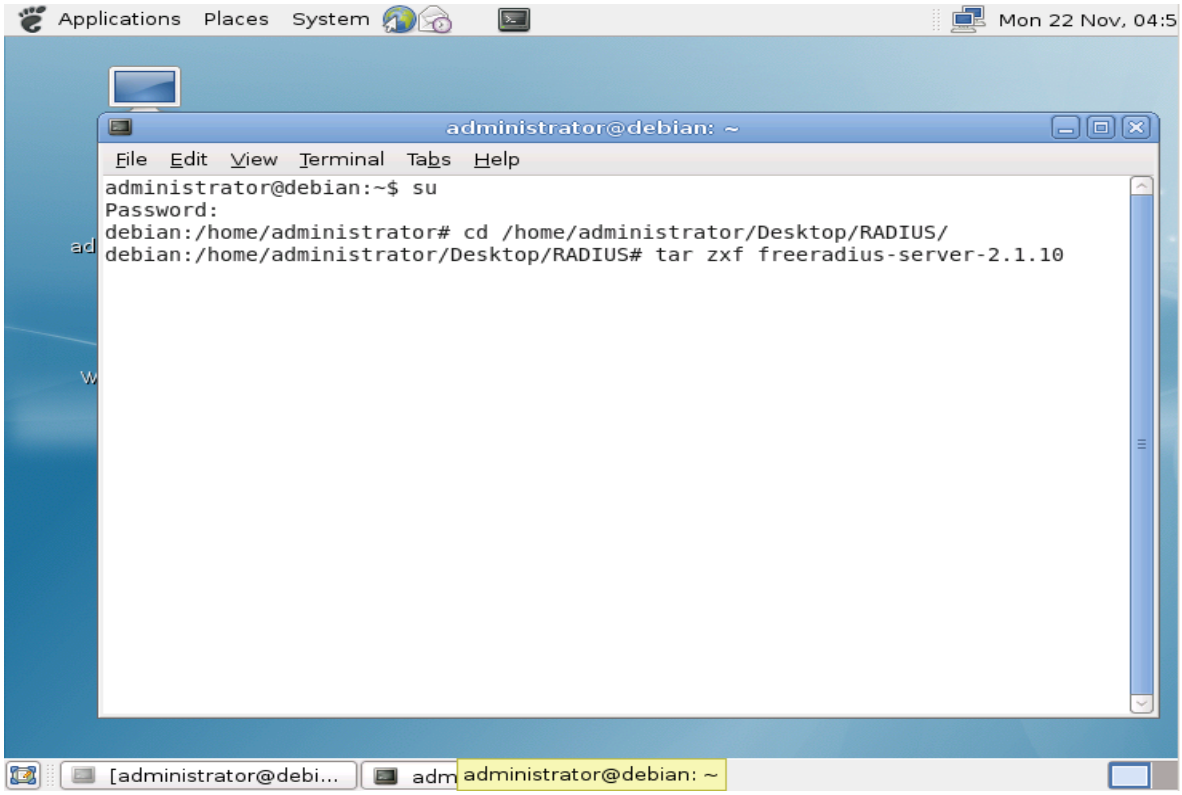
[Screenshot 1]

It is recommended to install a file manager program, which will help later in the study guide steps: one used in this guide is "Midnight Commander“. Simply search for a “Midnight Commander with file-manager program“. Search for "mc“, mark it and apply. Midnight Commander can be accessed via a terminal with a command "mc“. However, it is not necessary to install Midnight Commander since the programs can be installed manually.

The next step will be installing additional packages to FreeRADIUS to make it work and more versatile. Use "SPM“ and install the following packages:

fakeroot | dpkg-dev | libssl-dev | quilt | autotools-dev | libtool | libltdl3-dev | libpam0g-dev | libmysqlclient-dev_| libgdbm-dev | libldap2-dev | libsasl2-dev |

libiodbc2-dev | libkrb5-dev | libperl-dev | libpcap-dev | python-dev | libsnmp-dev | libpq-dev | debhelper | php5 | php5-dev



[Screenshot 2]

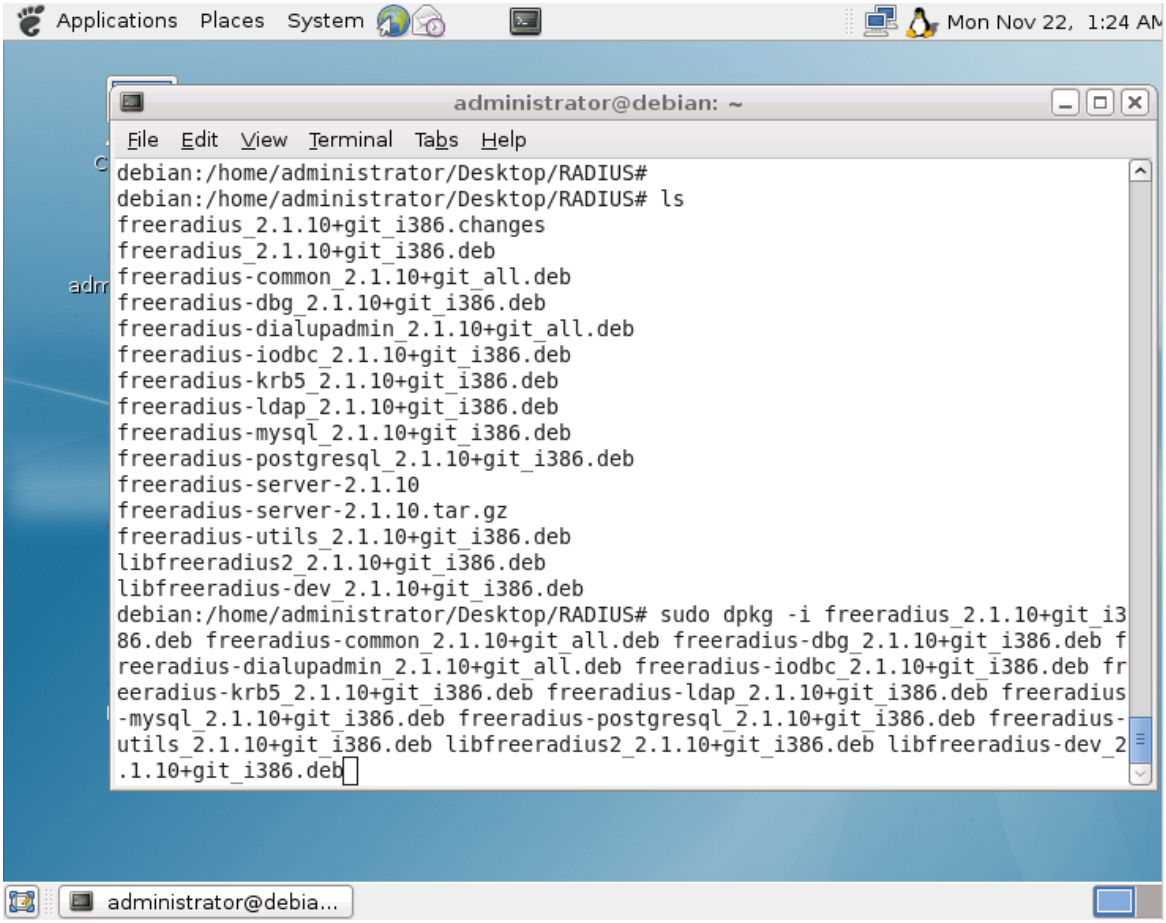
While installing required packages for FreeRADIUS, the program might ask installation of more packages. One is suggested t

It is important to have the latest release of FreeRADIUS (The one used here is 2.1.10). This can be done by using SPM or downloading it manually. In our thematic we are downloading and installing it manually. It is good to remember to mark install files to be not upgraded, when a new version should appear. The reason is that with the latest version might have compatibility problems and it should not work.

Start terminal and log in as administrator (command su; password = xxxx). Make sure you have a new folder (On this work it is called RADIUS) and the FreeRADIUS file inside it. Move to your /new folder. Extract your FreeRADIUS file (in RADIUS).

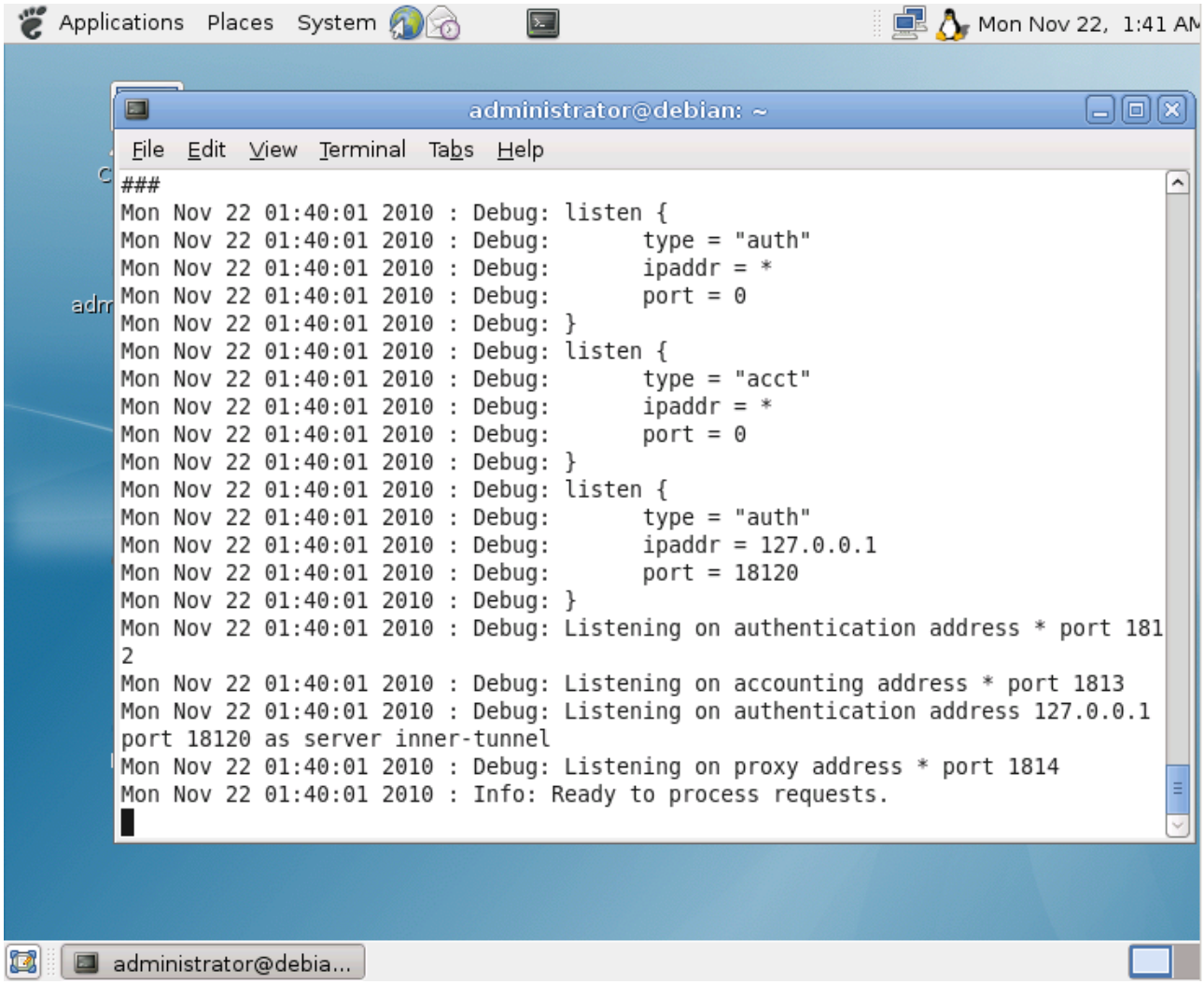
Use commands:

1) tar -**zxf** or- **xjf** FreeRADIUS-server-Z.X.Y.tar.gz [latter Z.X.Y represent version = replace them with version you are using]
2) cd FreeRADIUS-server-Z.X.Y
3) fakeroot dpkg-buildpackage -b -uc
4) sudo dpkg -i *FreeRADIUS***all the .deb files in RADIUS folder**



[Screenshot 3]

When everything is completed, issue a command: /etc/init.d/freeradius stop, to make sure that FreeRADIUS is not on. Write command – after stopping the FreeRADIUS – “freeradius –Xx”. This will start FreeRADIUS in debug mode, so all the time and errors will be taken up to terminal. You have FreeRADIUS successfully working, when you see the next message: **Info: Ready to process request**

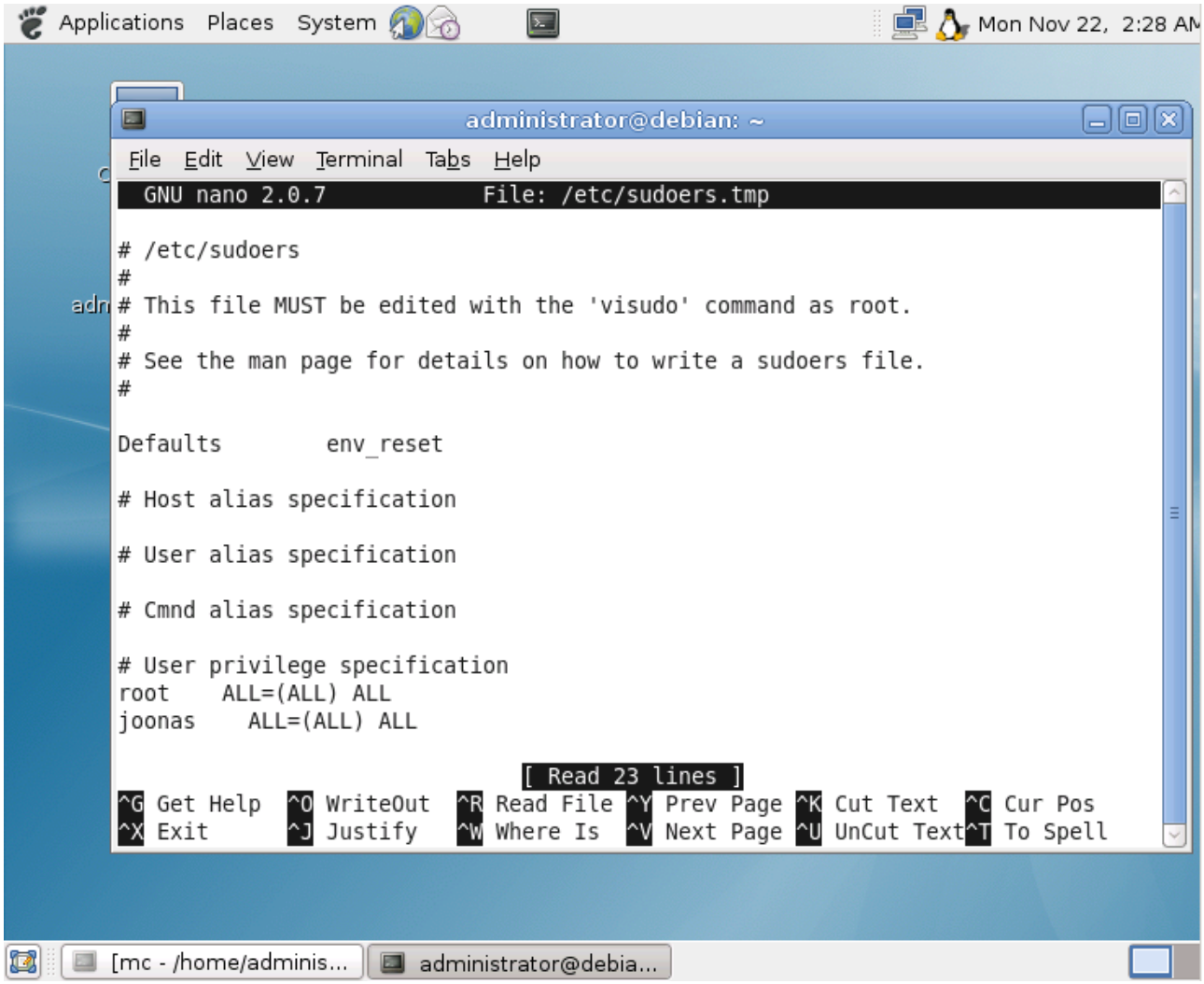


[Screenshot 4]

In the thematic, all the .deb files were unzipped. However, it is enough only to unzip 3 necessary deb files in order to make FreeRADIUS work: *FreeRADIUS-*

utils_2.1.10+git_i386.deb, FreeRADIUS-common_2.1.10+git_all.deb and *libFreeRADIUS2_2.1.10+git_i386.deb*

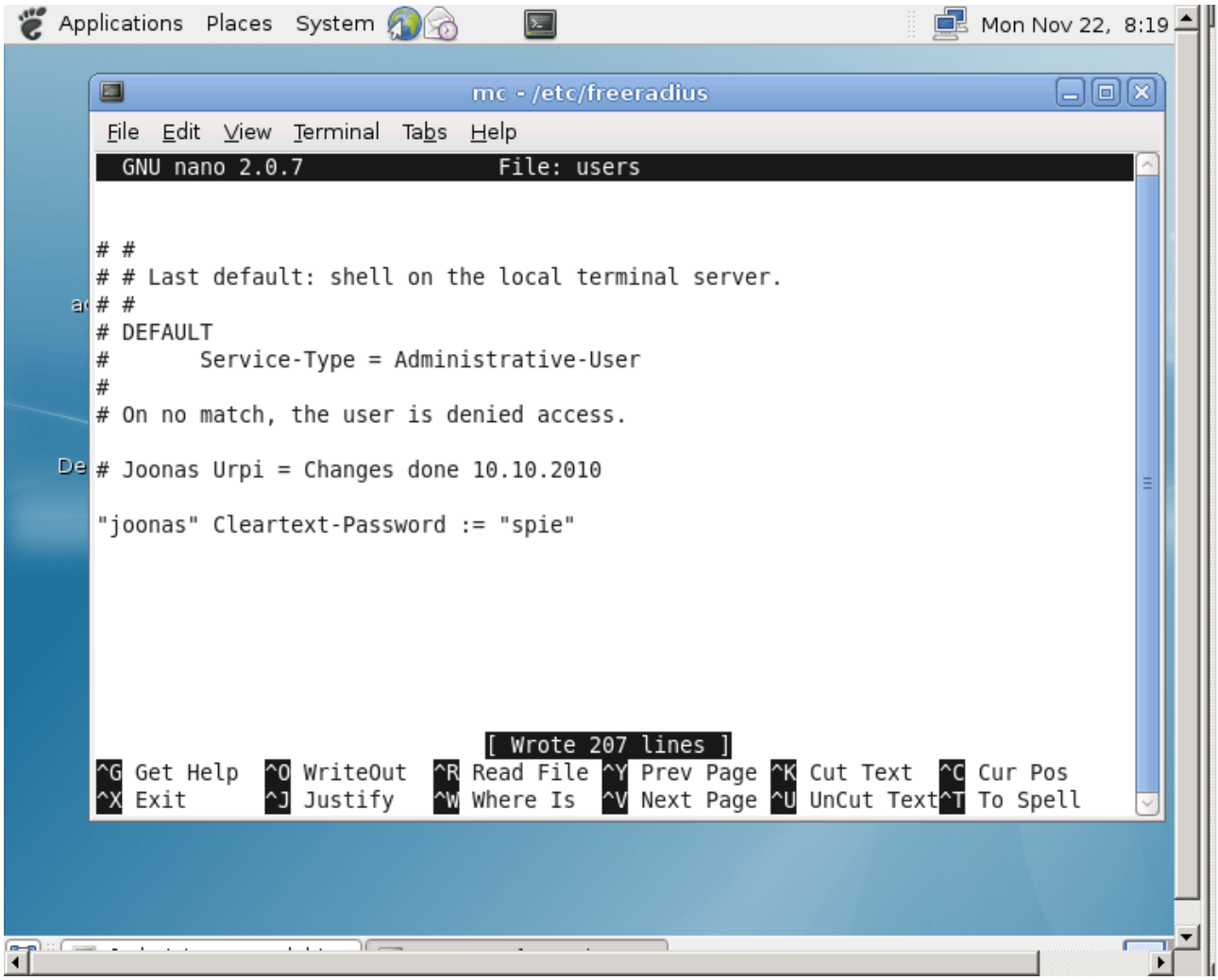
FreeRADIUS installed and working, it is time to configure it. First, start up the terminal and enter as a root, to gain privileges. Write "visudo“ and scroll down. Copy the last line and post it again under the previous one. Replace the "root“ with the wanted user name. In this work, it is "joonas“



[Screenshot 5]

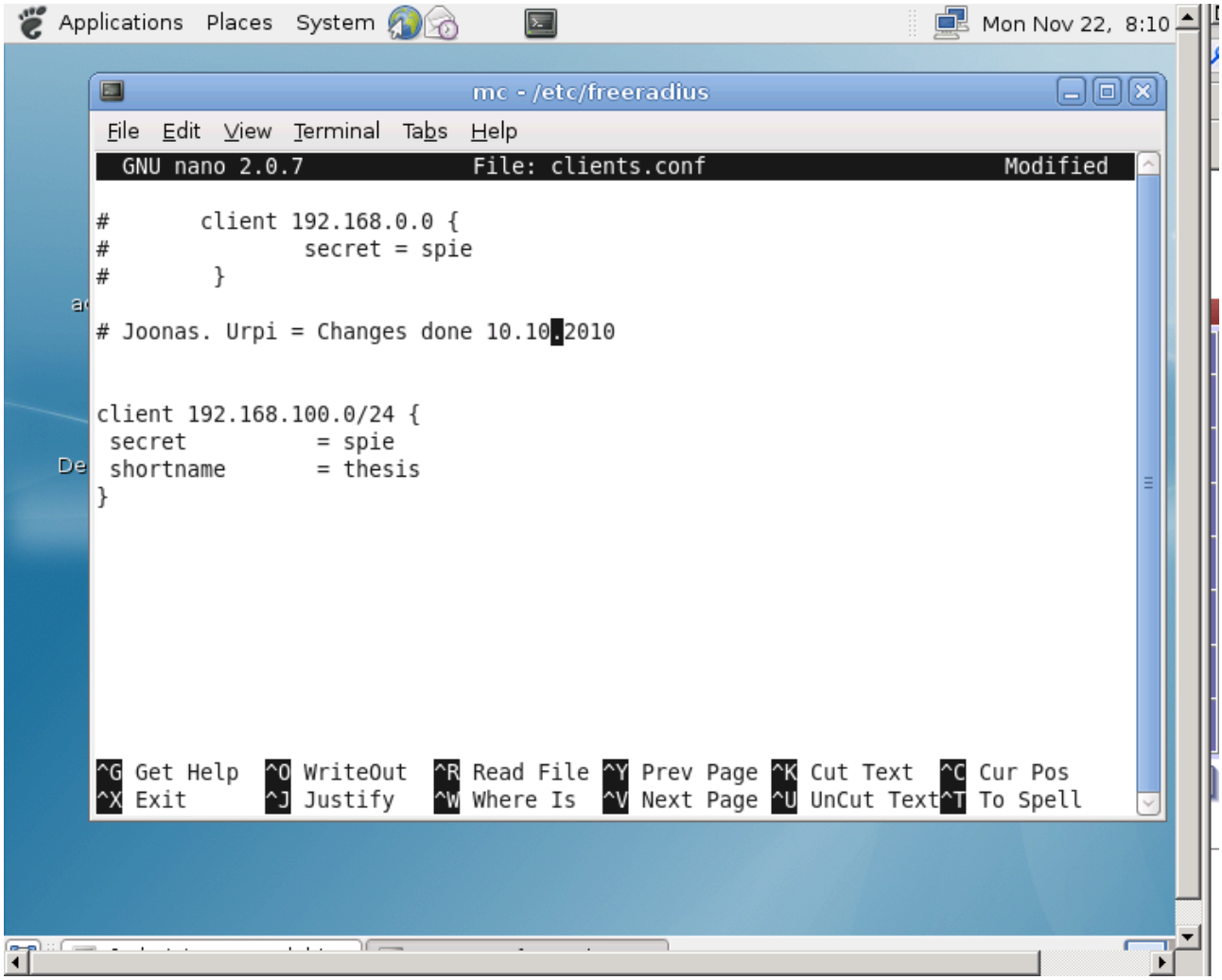
Next start up "mc“ or similar program to be able to change files. Go to /etc/FreeRADIUS: here are 4 important files, which we need to configure in order to make FreeRADIUS a fully working AAA server.

An important step is to give a user access to the Internet. Enter to /etc/FreeRADIUS/user and scroll to bottom. Enter to the end "username“ and Cleartext-Password := "password“.



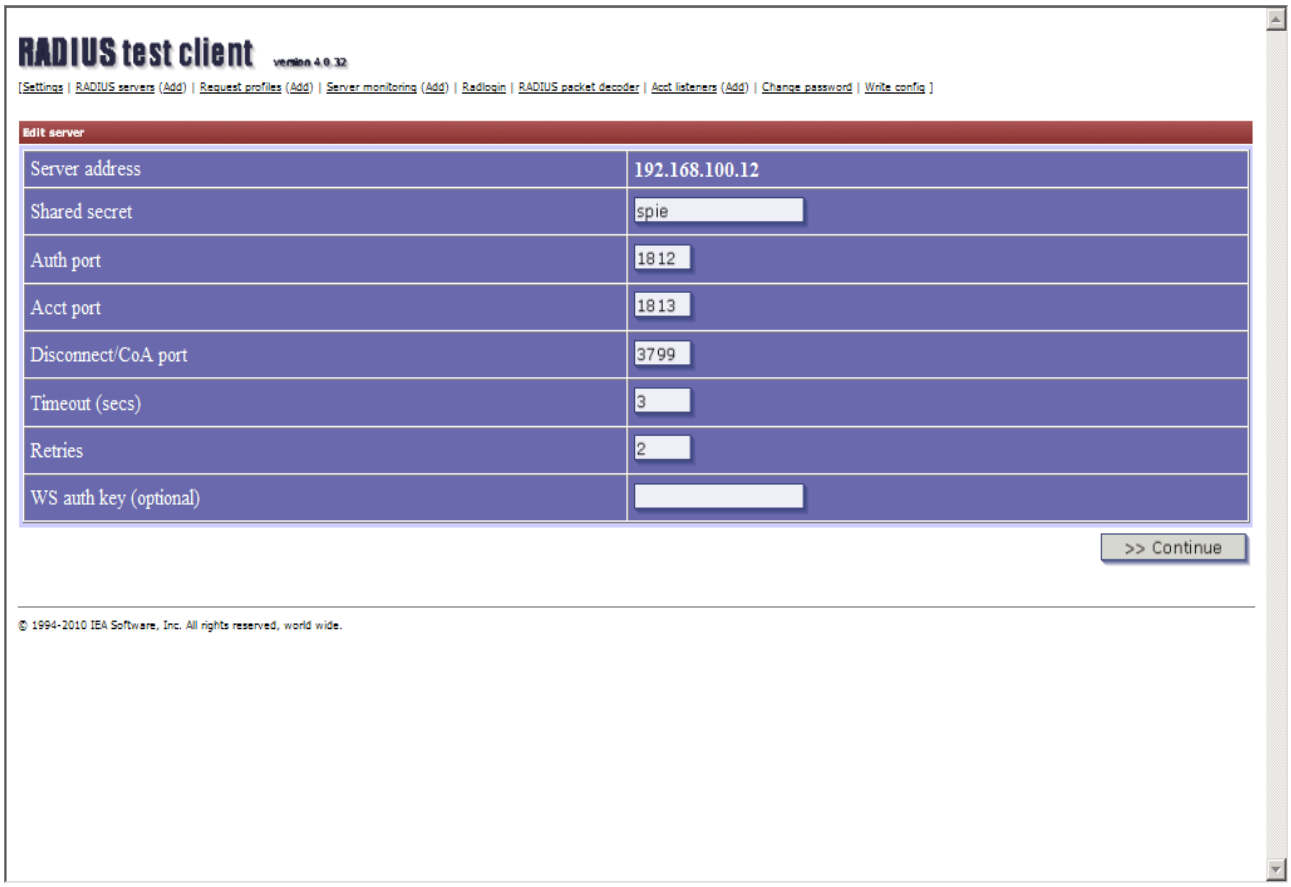
[Screenshot 6]

The next file configured is *clients.conf.* Enter to it and scroll down to last lines. Enter the required lines: network IP; secret; shortname. Here we use 192.168.100.0 "spie“ and "zzzz“ respectively



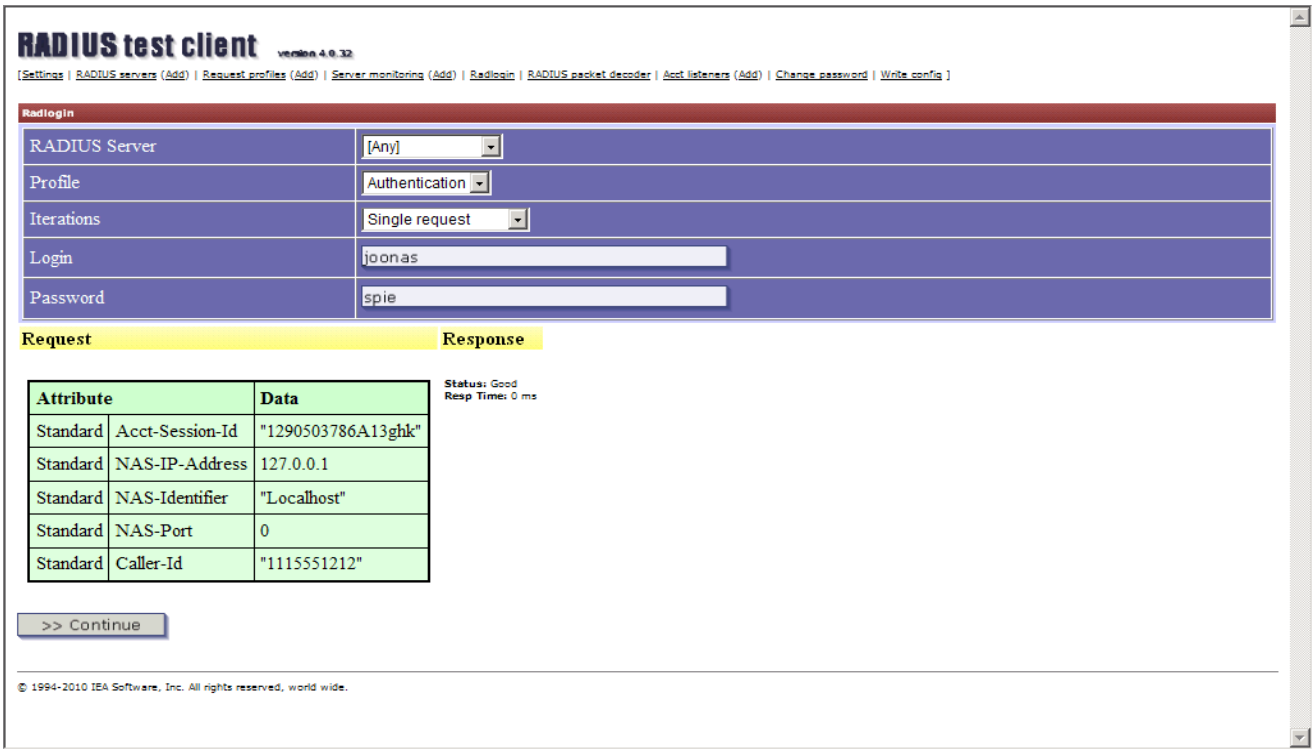
[Screenshot 7]

Now we will test with Radlogin v4 whether the simple configuration works. First, you need to configure Radlogin v4. Click (Add) button, as shown with the mouse. Then write settings down. Ports will always be 1812 & 1813 if not configured differently.

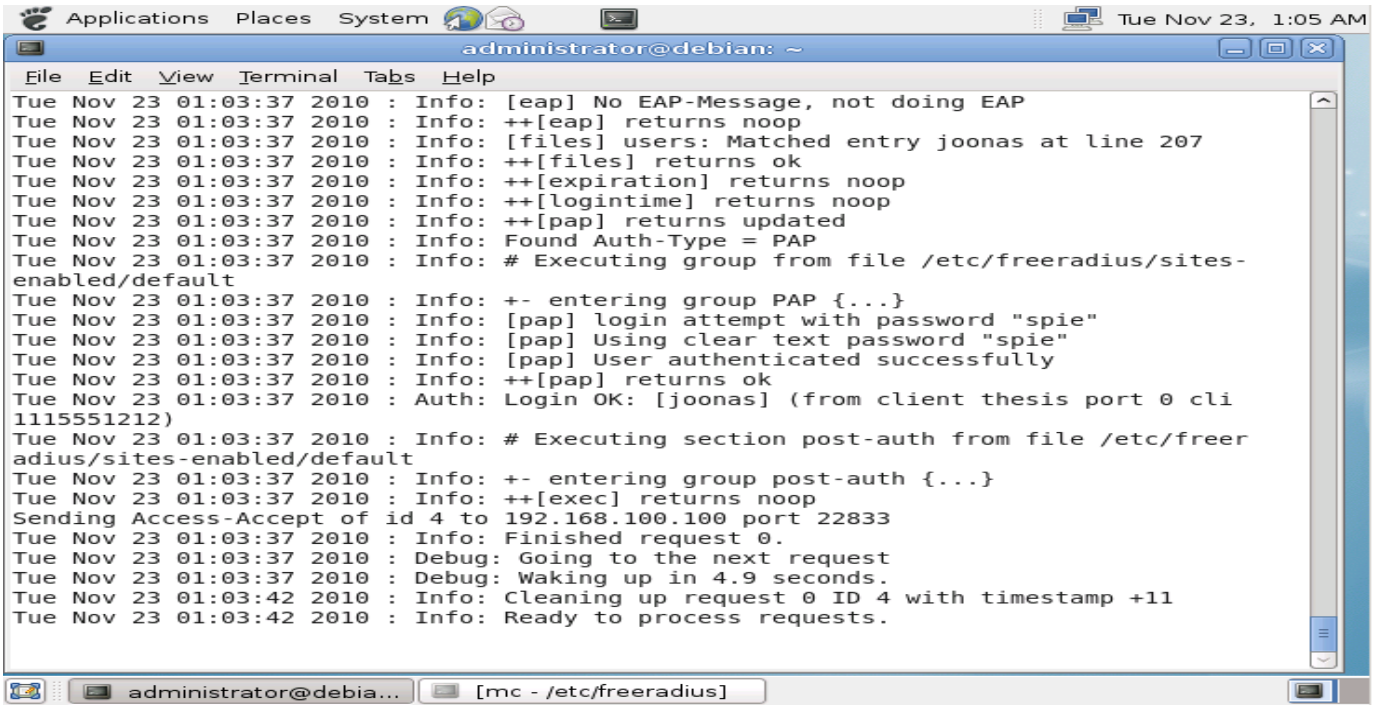


[Screenshot 8]

Move next to Radlogin and type into lines your user name and password, click continue and you should get the next message in the box and FreeRADIUS should be showing this

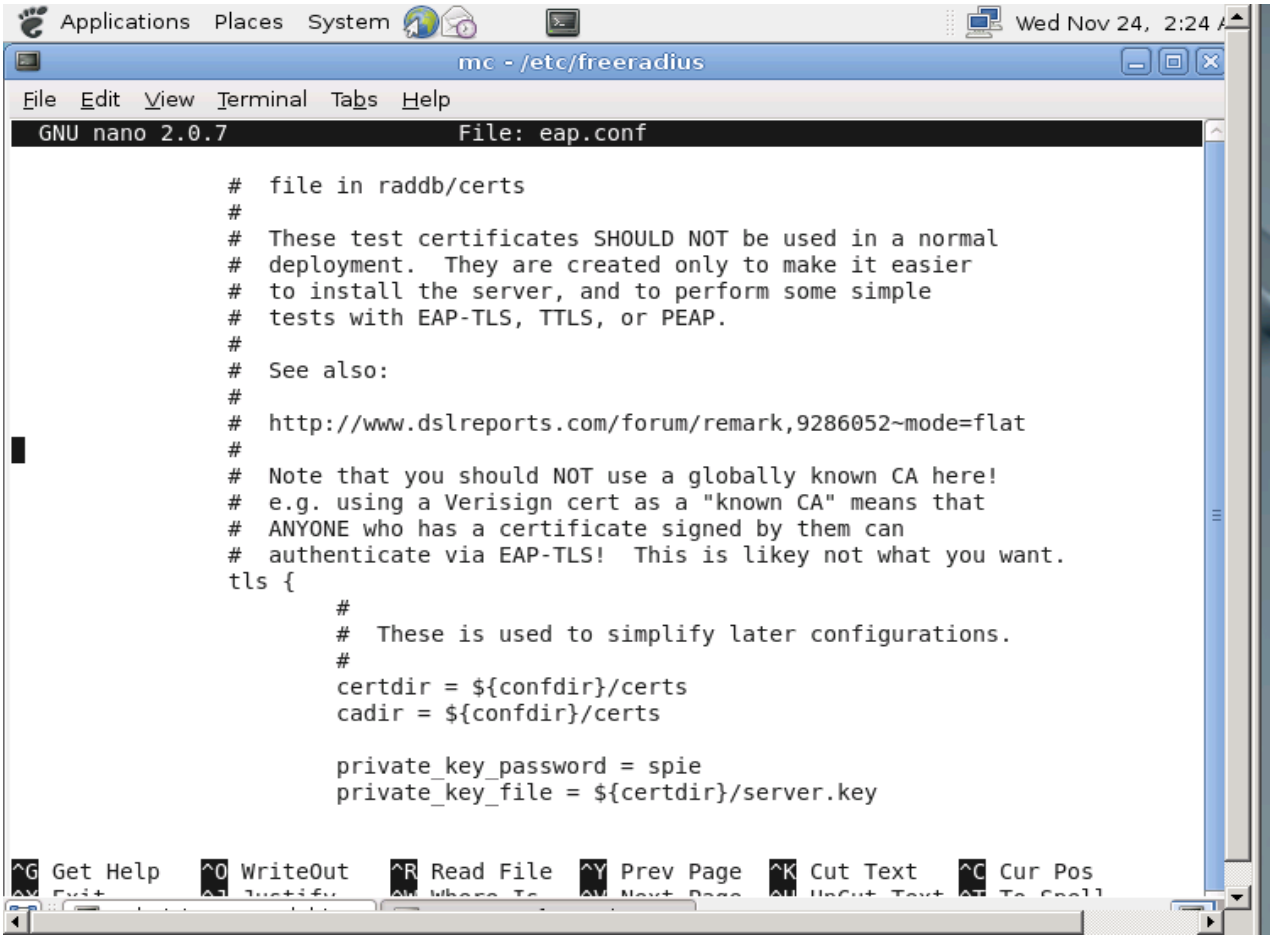


[Screenshot 9]



[Screenshot 10]

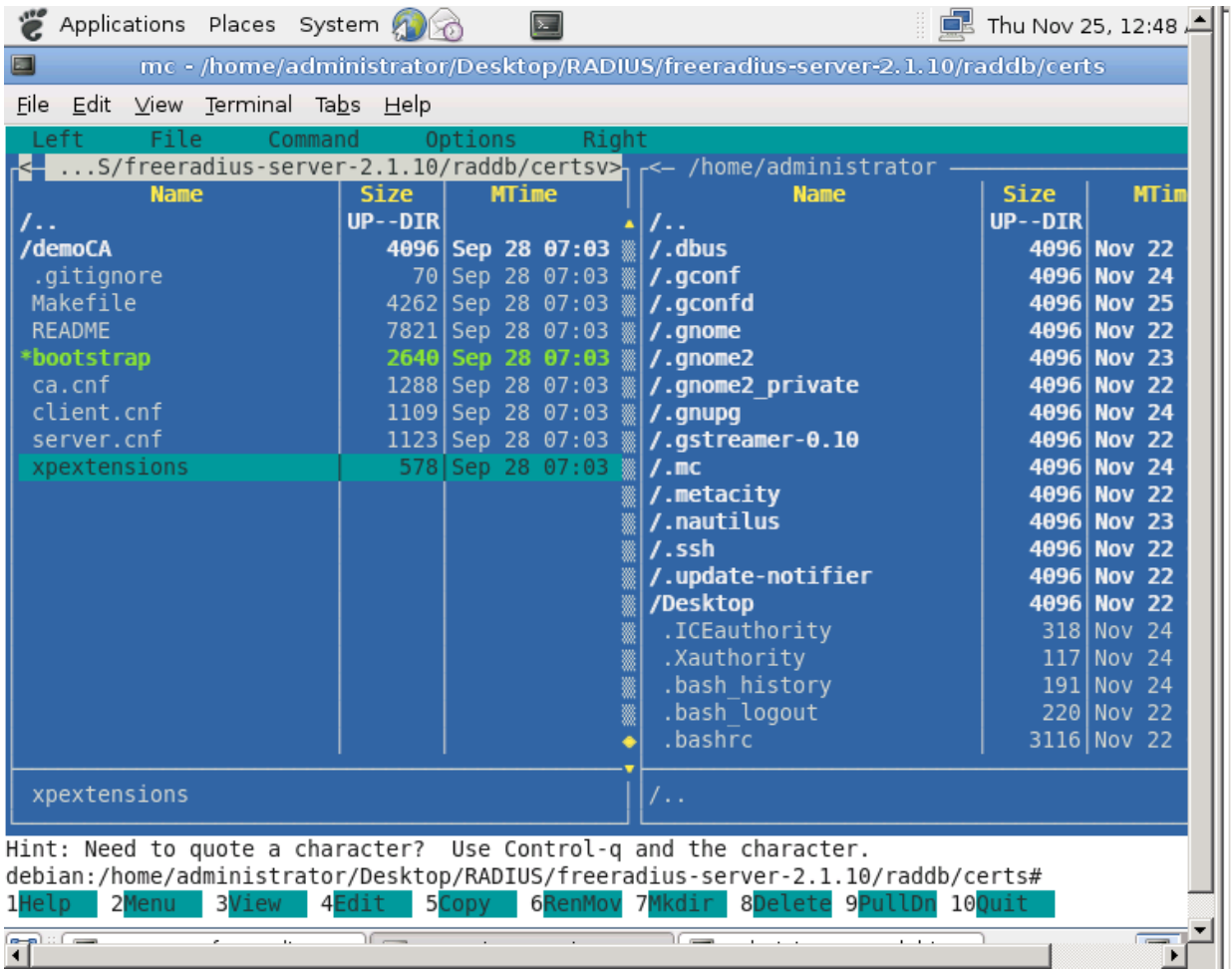
11.3 Configuring certificate for user and server



[Screenshot 11]

The test with Radlogin worked, so we are ready to continue configuration further. Open the mc text-editor again and go to /etc/freeradius/eap.conf. Scroll down to **tls** section and replace the part of "private_key_password = "xxxx". We use "spie" here. (Everything is using the same password for simplicity)

Move to Desktop and to your "RADIUS“ folder. Go to FreeRADIUS-Z.Y.X → raddb → certs. Transfer all the files you see inside .../certs (as in Screenshot 12) to /etc/FreeRADIUS/certs. After this delete **all** *.pem* .der* .csr* .crt* .key* .p12 serial* and index.tx*.*



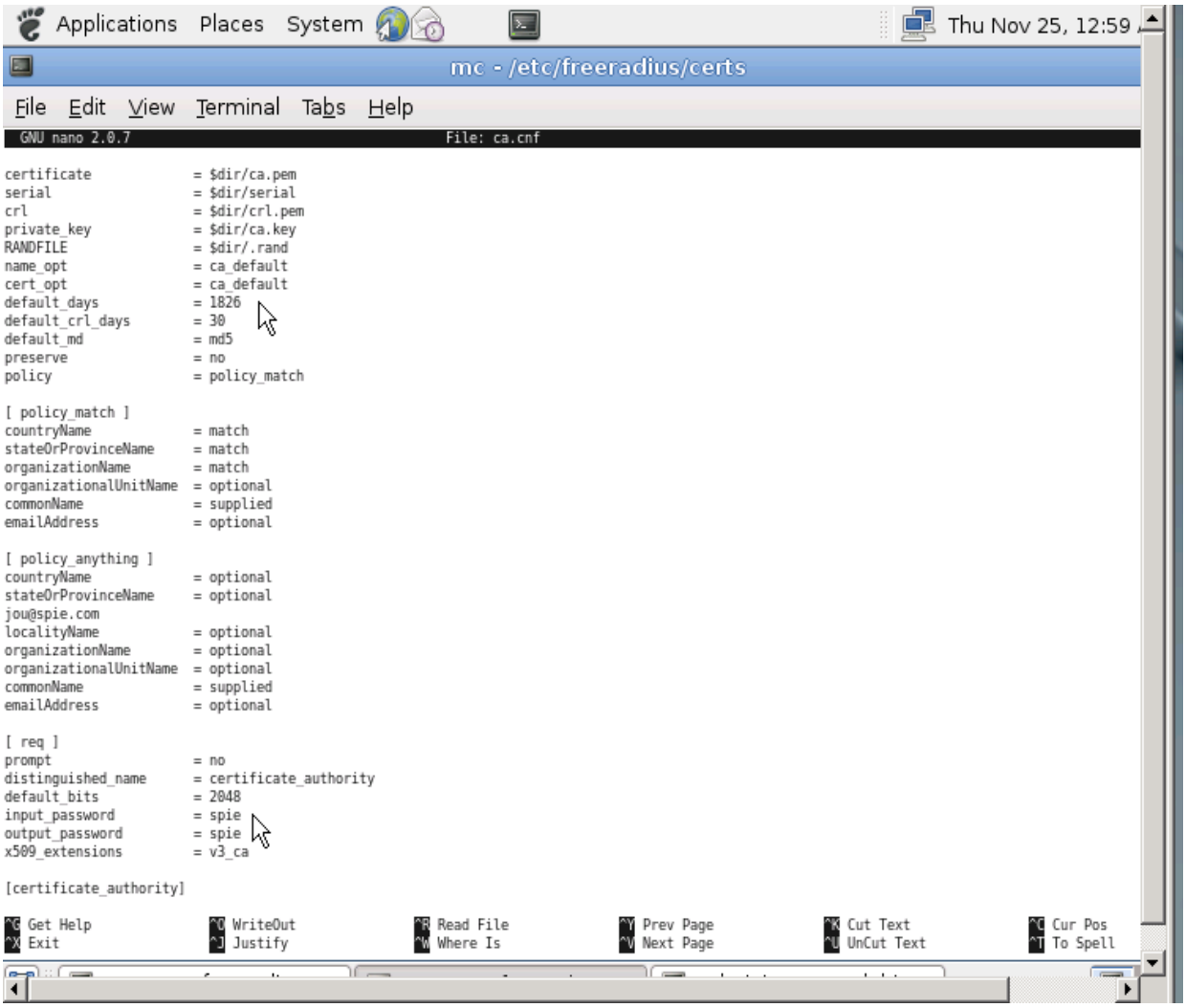
[Screenshot 12]

Finishing this, you need to configure **both** *ca.cnf & server.cnf*:

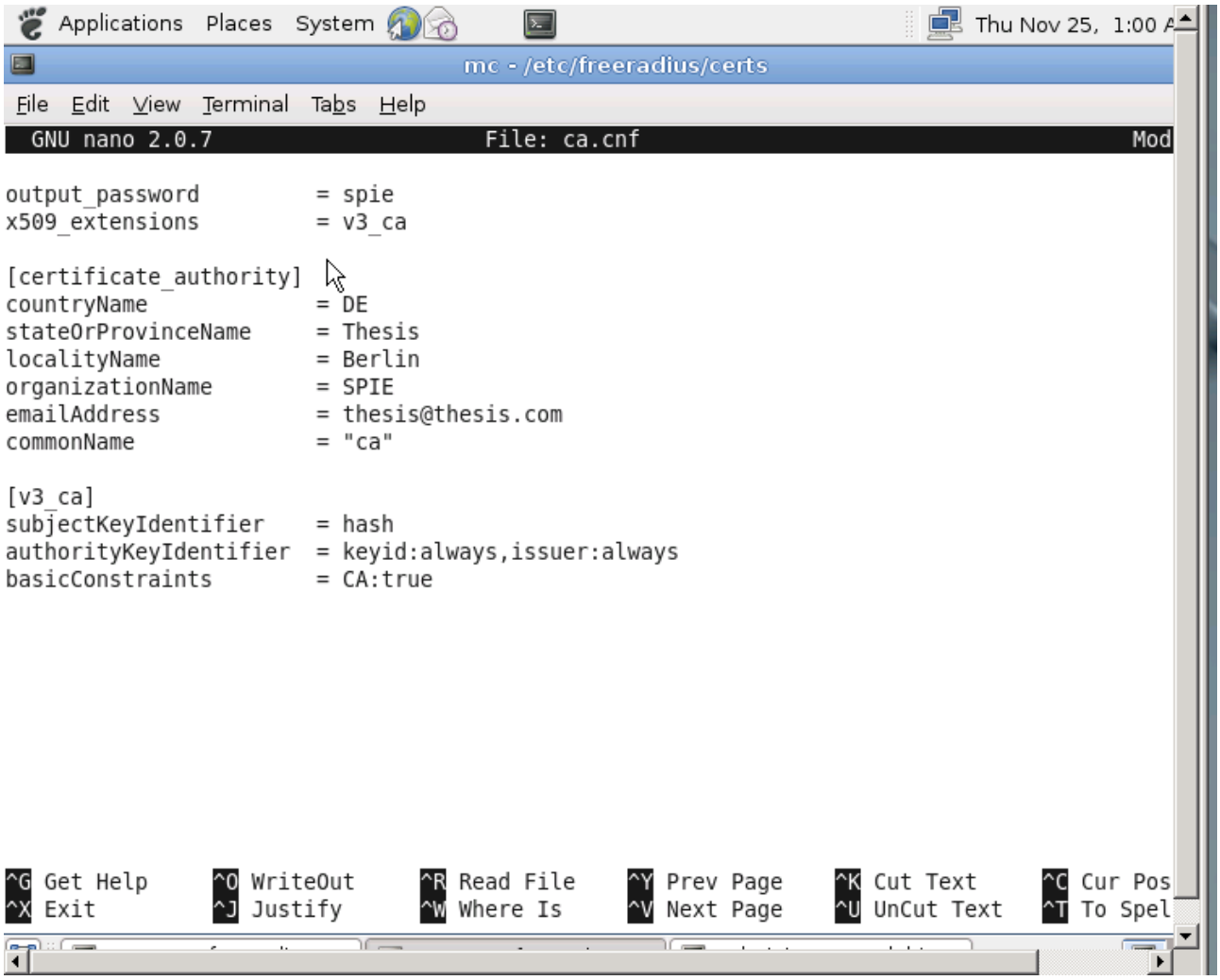
1) In CA_default → default_days : xxxx (xxxx = days. We use 1826 to represent 5 years)

2) Next is under [req] → change input_password & output_password: xxxx. Notice that these passwords must be the same! The password must also correspond to the one in *eap.conf*

3) Change everything under [certificate_authority] section



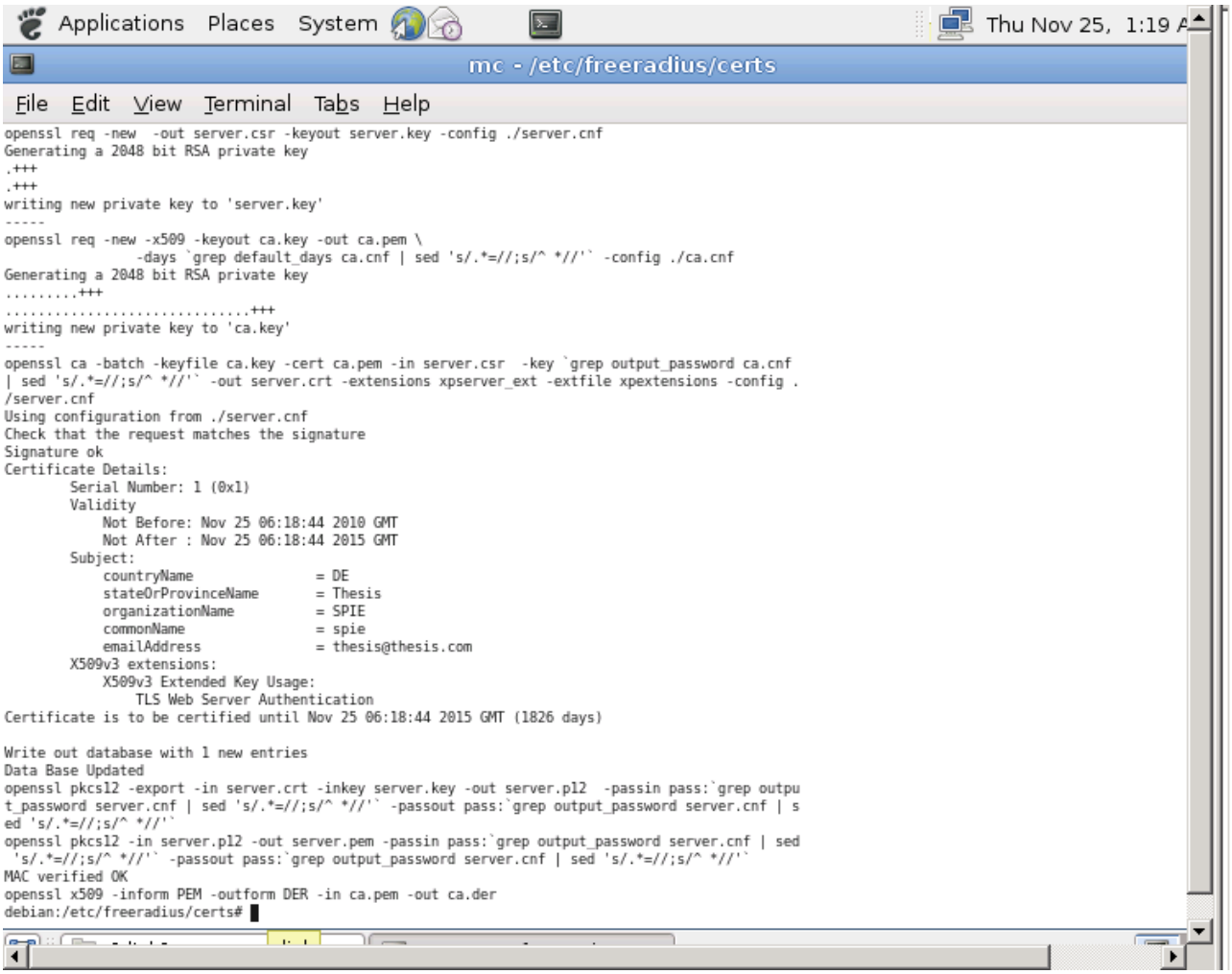
[Schreenshot 13]



[Screenshot 14]

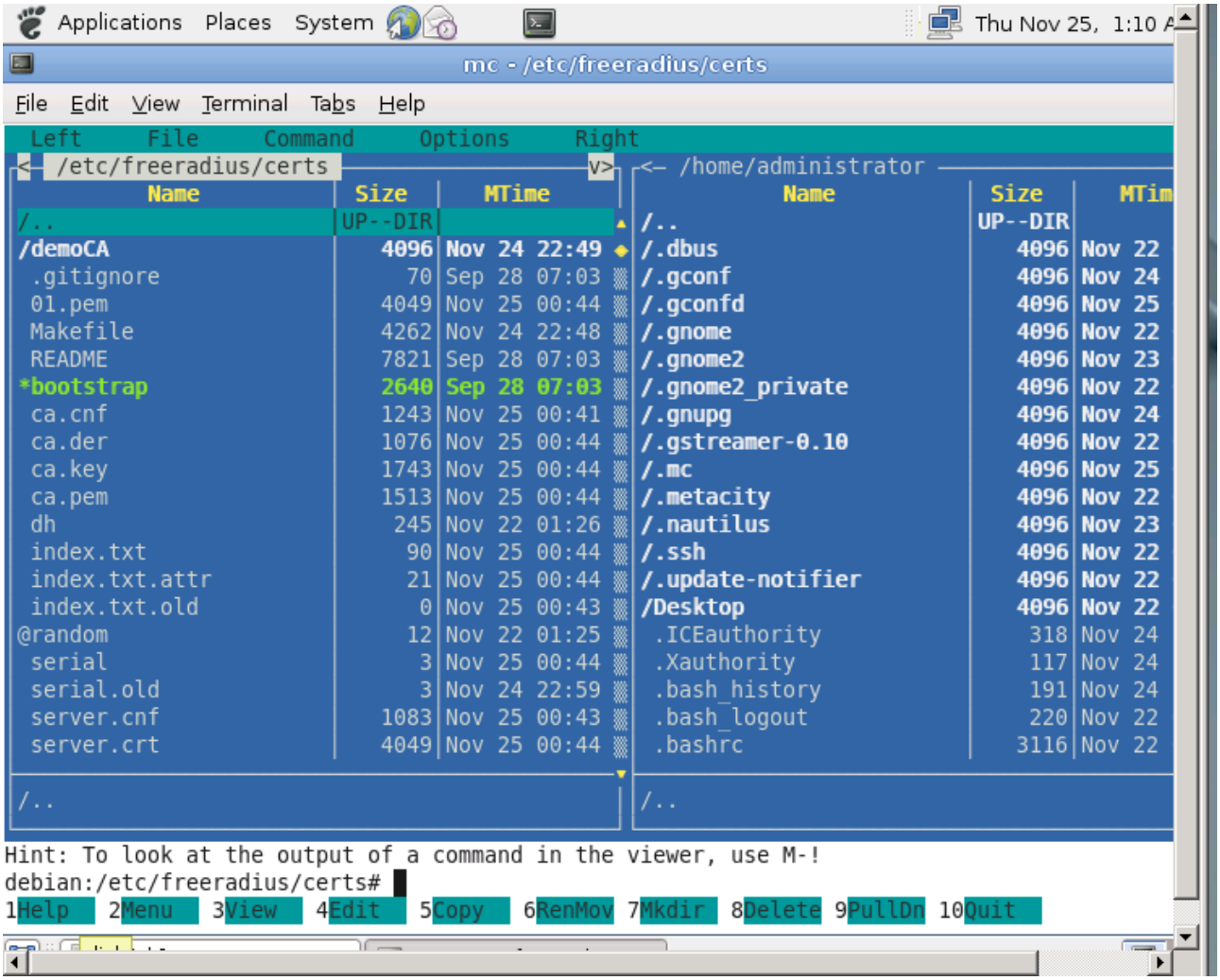
4) When finished, save the files and issue command: ***make all***

5) The certificate will be created and it is ready as shown in a Screenshot 15



[Screenshot 15]

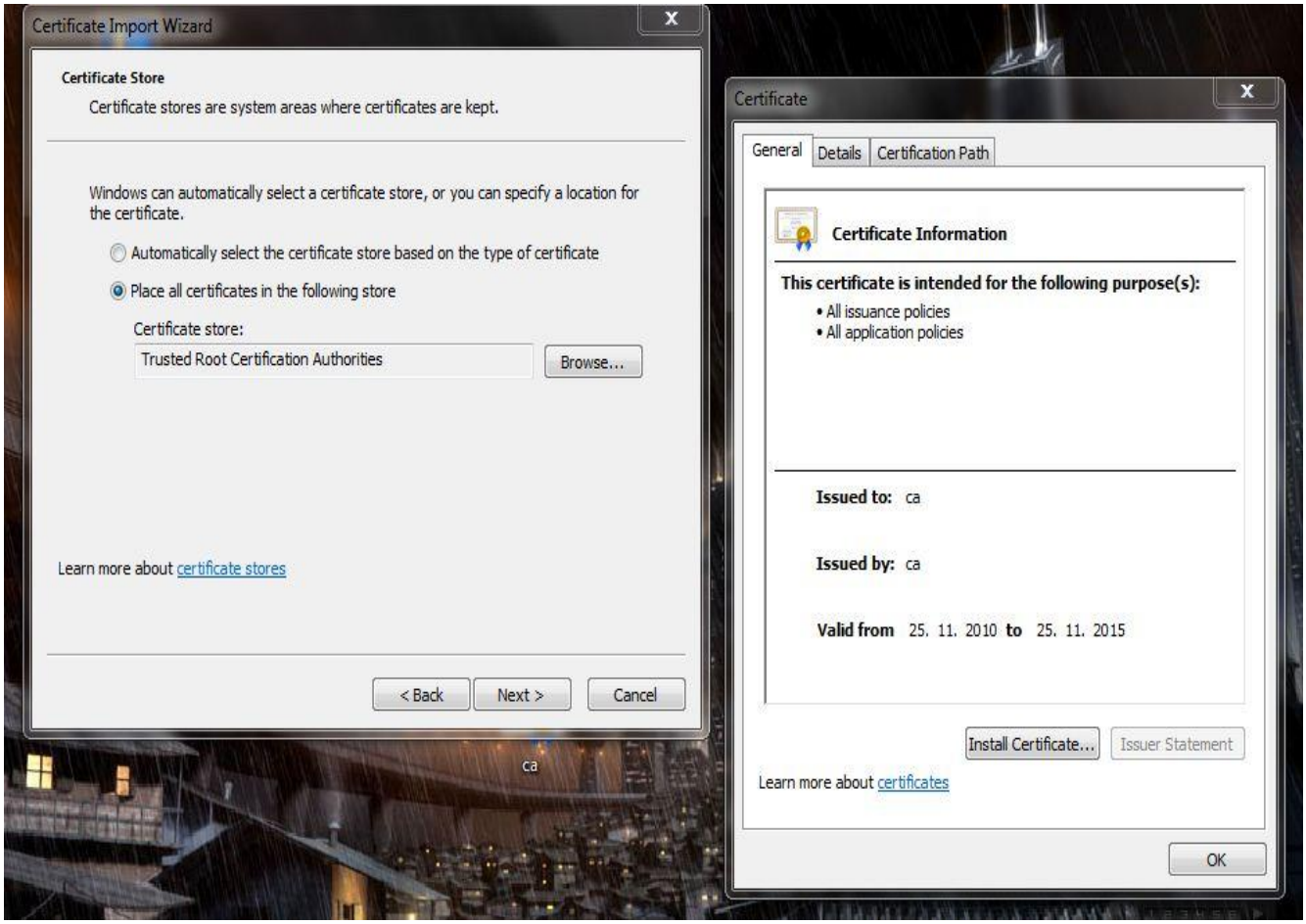
When everything is ready, your /etc/FreeRADIUS/certs file should look below in Screenshot 16.



[Screenshot 16]

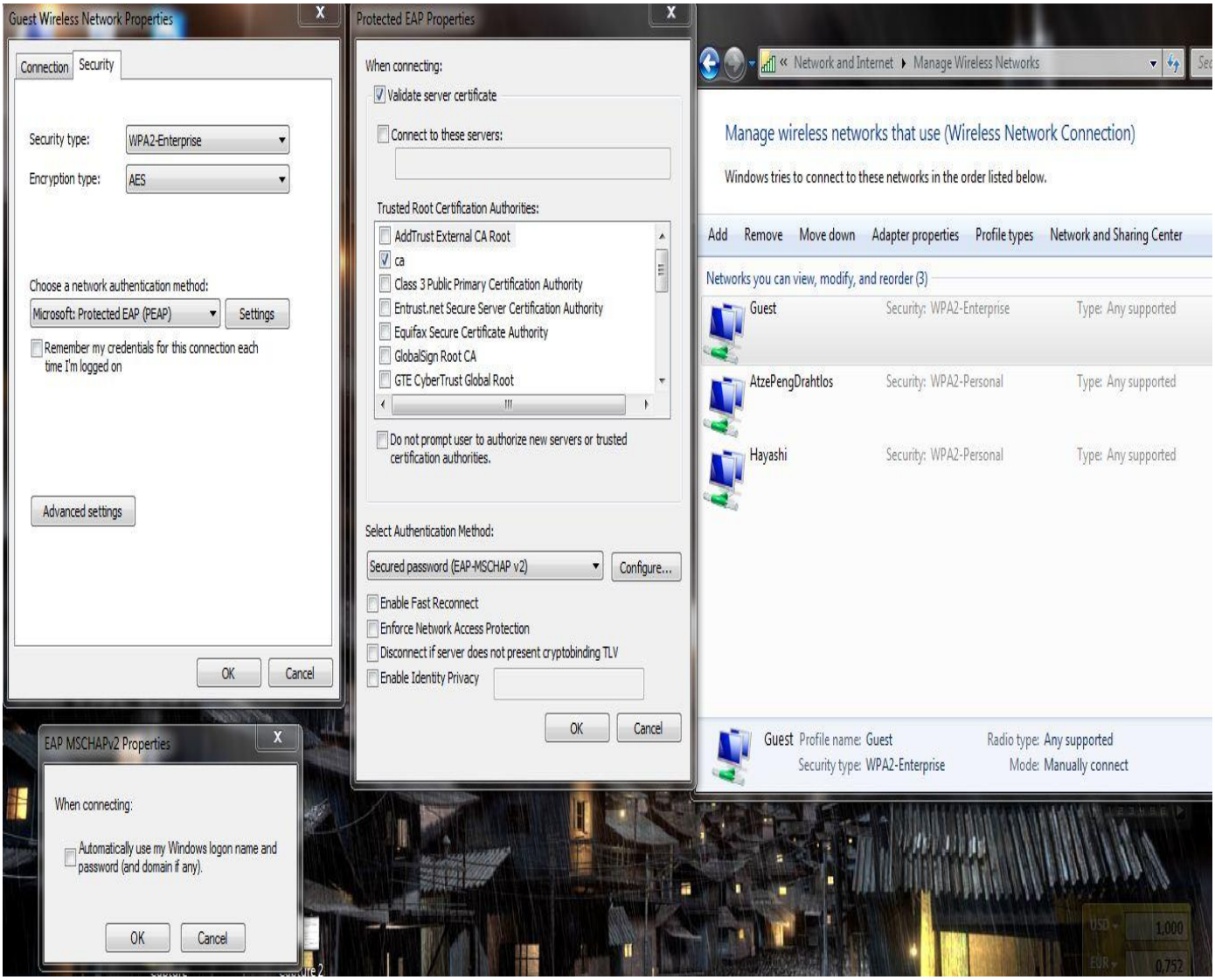
When it is ready as shown in the picture, you can copy the *ca.der* file and transfer it to your laptop. *Ca.der* is a certificate, which needs to be transferred to user laptop. In our schematic, we used USB-stick to transfer it. However, you can use server or website to distribute this or even send it via email. There are multiple ways to ensure that the employee or guest is able to receive the certificate.

In this part we use Window 7 and Window XP. Install the certificate to your "Trusted Root Certification Authorities “ files.



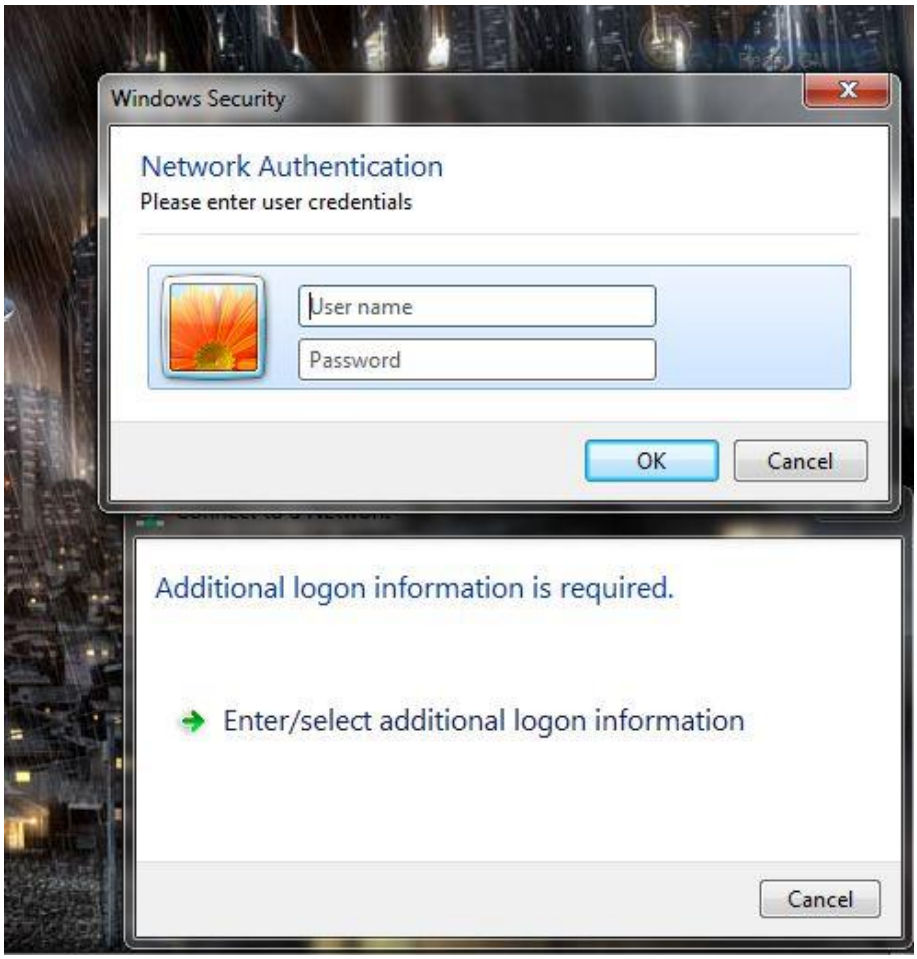
[Screenshot 17].

When you have done this then it is time to move onto wireless network settings. Go to your Network and Sharing center. There click on the bar, "manage wireless-networks“. Add network "Guest“ and configure Security Type WPA2-Enterprise and Encryption Method AES. Click settings and mark the "certificate“, which you added to your trusted certificate list. Include Authentication method Secured Password EAP-MSCHAP-v2



[Screenshot 18].

Remember also to change the user in "Advanced Settings“ *specify authentication method → user or computer authentication.* Before finishing and clicking yes, make sure you have unchecked boxes as in picture. You are ready to connect and this ”box” below should appear, when you try to connect.



[Screenshot 19]

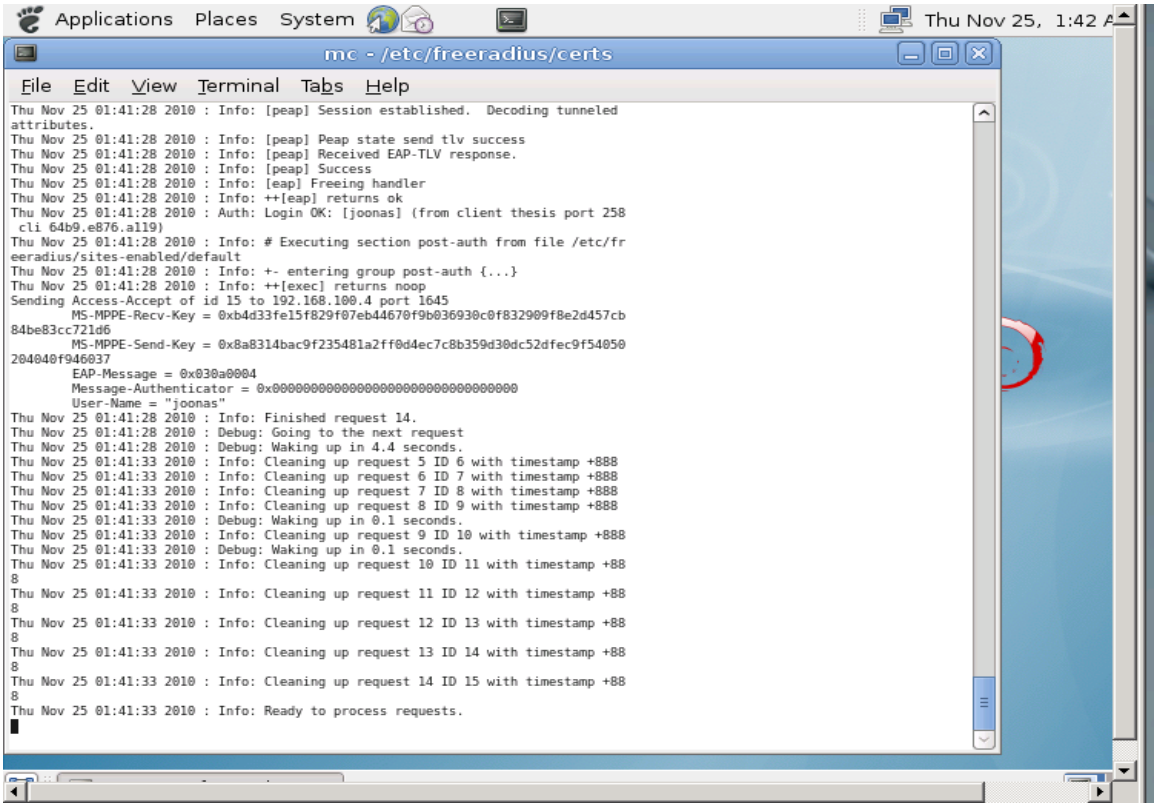
When the new network configuration and FreeRADIUS are ready, it is time to configure both Switch and Access Point. There are two options to configure them: either by CLI (command line interface) or GUI (graphical user interface). In this guide everything was done via CLI. At the end of this thesis, you will find configuration scripts for both the access point and the switch with "show version & show running-config“.

To ensure the working network do the following: ping both the access point and the switch from the FreeRADIUS server and then from the access point to the switch and vice-versa. After a successful confirmation of a working network, begin the configuration.

Fastport 0/1 is an acting gateway to FreeRADIUS server. Fastport0/2 is an acting gateway to the Internet. Fastport 0/24 is an acting gateway between the switch and the access point. The next step is to make trunking between Access point (dotradio 0 & gigabit 1) and Switch (fastethernet 0/24: vlan 100 and vlan 200). Use Chipher security AES-CCCM and make the access point ask FreeRADIUS server for information.

The script can be followed and all information can be used in it. Not everything has to be used, since the configuration includes some additional settings. It can be used and tweaked to your own purposes and settings. It is important to note that the configuration and scripts shown are usable by almost all switches and access points.

In the end, when everything has been done successfully, this will be the result.



[Screenshot 20]

12. CONCLUSION

FreeRADIUS has great potential in the market of security. It is not only because it is for its free to use but also because of the ability to perform and have low-cost maintenance. There are numbered issues with FreeRADIUS which might make some people to reject it. The code source is free, which means that anyone is able to make code for it. There is the concern whether it is balanced and broken code, and whether it can be compared to licensed products, which are guaranteed to work and maintained by the company, that sold it.

The challenging part of FreeRADIUS is its evolving structure and people maintaining and working on it every day. Broken code appears which need to be handled and there are some other malfunctions as well. The compatibility with a wide range of components and programs are is the advantage of FreeRADIUS although the administrator has to be skilled to make them function together.

My own personal experience while working on the FreeRADIUS has been blissful. I learned a lot new things such as programming, Linux structure and how does the security and protocols work as well how to apply them. The learning process was long and hard since it was completely out of my field as well new for me. In the end it was rewarding to know that I had learned something new.

In the end, FreeRADIUS has great potential for all companies because it is a free software providing AAA comparable to licensed and payable RADIUS servers. It is upgraded and maintained in daily basis and it meets the needs of any company and can be changed. It has low requirements for the hardware and suitability for long-term use.

SOURCES

Literature sources

Jaakohuhta, H, IT Ensyklopedia, 1. painos, 2001, Edita Oyj, Helsinki

Tarkoma, J, Tietotekniikan Sanasto, 4. painos, 1995, Juva

Järvinen, P, IT-tietosanakirja, 2001, Tummavuoren Kirjapaino Oy, Jyväskylä

Lehmonen, H, insinöörityö 802.1x-autentikoinnin käyttöönotto toimistoverkossa, 2007, Helsinki

Gast, M, 802.11 Wireless Networks: The Definitive Guide, 2002, O'Reilly Media,

Santuka, V, Banga, P, Carroll, B.J AAA Identity Management Security, 2010, Cisco Press

Internet source

http://FreeRADIUS.org/

http://www.cisco.com/

http://www.vmware.com/

https://learningnetwork.cisco.com/servlet/JiveServlet/download/53910-8800/Explanation%20and%20recommendations%20for%20EAP%20Implementations.doc

http://www.smallbusinesscomputing.com/testdrive/article.php/3819231/What-is-Virtualization-and-Why-Should-You-Care.htm

http://www.virtualbox.org/

http://www.cs.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.htm#WhatVLAN

http://www.petri.co.il/csc_setup_a_vlan_on_a_cisco_switch.htm

http://www.articsoft.com/public_key_infrastructure.htm

http://www.gnu.org/licenses/gpl.html

http://www.ietf.org/rfc/rfc2904

http://tools.ietf.org/html/rfc2865

http://net21.ucdavis.edu/newvlan.htm

http://tools.ietf.org/wg/aaa/

http://howfunky.net/temp/cz/AAA.pdf

http://www.commandprompt.com/ppbook/

http://docs.oracle.com/cd/B10500_01/appdev.920/a96624/toc.htm

http://www.oracle.com/technetwork/indexes/documentation/index.html#previous

http://www.postgresql.org

http://www.tech-faq.com/understanding-certificate-authorities.html

Picture:

Picture 1:
https://learningnetwork.cisco.com/servlet/JiveServlet/download/53910-8800/Explanation%20and%20recommendations%20for%20EAP%20Implementations.doc

Picture 2:
https://learningnetwork.cisco.com/servlet/JiveServlet/download/53910-8800/Explanation%20and%20recommendations%20for%20EAP%20Implementations.doc

APPENDIX

Database Information

Database	Company	Info	Usage
SQL	Oracle Corporation	Written in C++ and C. Does not have a GUI tools: choice to download MySQL Workbench. MySQL supports multiple amounts of platforms	Relational Database Management System (RDBMS)
Oracle	Oracle Corporation	Data is stored in the tablespace form and data files are in the physical form (two type of storing)	Object-Relational Database Management System (ORDBMS)
LDAP	Originally created by Tim Howes, Steve Kille and Wengyik Yeong	Gives an access over Internet Protocol to maintain and access distributed directory information (An application protocol)	The Lightweight Directory Access Protocol (**LDAP)**
PostgreSQL	Consist of various contributors on Internet	All major operating systems are supported. ACID compliant. Large binary object storages are supported.	Open source Object-Relational Database System (ORDBMS)

Configuration

Switch – configuration

show version

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2010 by cisco Systems, Inc.

Compiled Tue 26-Oct-10 10:35 by nburra

Image text-base: 0x80010000, data-base: 0x80680000

ROM: Bootstrap program is C2950 boot loader

Switch uptime is 26 minutes

System returned to ROM by power-on

System image file is "flash:/c2950-i6k2l2q4-mz.121-22.EA14.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

cisco WS-C2950G-24-EI (RC32300) processor (revision E0) with 19911K bytes of memory.

Processor board ID FOC0645X1WK

Last reset from system-reset

Running Enhanced Image

24 FastEthernet/IEEE 802.3 interface(s)

2 Gigabit Ethernet/IEEE 802.3 interface(s)e

32K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address: 00:0B:5F:50:C4:00

Motherboard assembly number: 73-7280-05

Power supply part number: 34-0965-01

Motherboard serial number: FOC06440ZNZ

Power supply serial number: PHI06380ASW

Model revision number: E0

Motherboard revision number: A0

Model number: WS-C2950G-24-EI

System serial number: FOC0645X1WK

Configuration register is 0xF

```
Switch#
Switch#
Switch#show running conf     -config
Building configuration...

Current configuration : 1523 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
```

```
!
interface FastEthernet0/1
 switchport access vlan 100
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 200
 spanning-tree portfast
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
```

```
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport access vlan 100
 spanning-tree portfast
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport access vlan 200
 spanning-tree portfast
```

```
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan100
 ip address 192.168.100.11 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

Switch#

Access Point – configuration

show version

Cisco IOS Software, C1250 Software (C1250-K9W7-M), Version 12.4(21a)JY, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2010 by Cisco Systems, Inc.

Compiled Wed 28-Apr-10 10:44 by prod_rel_team

ROM: Bootstrap program is C1250 boot loader

BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc2)

ap uptime is 26 minutes

System returned to ROM by power-on

System image file is "flash:/c1250-k9w7-mx.124-21a.JY/c1250-k9w7-mx.124-21a.JY"

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

cisco AIR-AP1252AG-E-K9 (PowerPC 8349) processor (revision A0) with 49142K/16384K bytes of memory.
Processor board ID FCZ1229P0G9
PowerPC 8349 CPU at 533Mhz, revision number 0x0031
Last reset from power-on
1 Gigabit Ethernet interface
2 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:22:90:0B:9C:0C
Part Number : 73-10425-05
PCA Assembly Number : 800-27630-05
PCA Revision Number : A0
PCB Serial Number : FOC12283AJ7
Top Assembly Part Number : 800-29531-02
Top Assembly Serial Number : FCZ1229P0G9
Top Revision Number : A0

Product/Model Number : AIR-AP1252AG-E-K9

Configuration register is 0xF

ap#

ap#

ap#

ap#show running-config

Building configuration...

Current configuration : 6116 bytes

!

version 12.4

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname ap

!

enable secret 5 1n6XF$0TcFMyKCqgyHYruyFSspB1

!

aaa new-model

!

!

aaa group server radius rad_eap

server 192.168.100.12 auth-port 1812 acct-port 1813

```
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap2
 server 192.168.100.12 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac1
!
aaa group server radius rad_mac2
!
aaa group server radius rad_eap4
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods2 group rad_eap2
aaa authentication login mac_methods1 group rad_mac1
aaa authentication login mac_methods2 group rad_mac2
```

```
aaa authentication login eap_methods4 group rad_eap4
aaa authentication dot1x default group rad_eap
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
no ip domain lookup
!
!
dot11 syslog
!
dot11 ssid Employe
   vlan 100
   authentication open eap eap_methods
!
dot11 ssid Guest
   vlan 200
   authentication open eap eap_methods2
   authentication network-eap eap_methods2
   authentication key-management wpa version 2
   guest-mode
!
dot11 ssid Phone
   vlan 10
   authentication open
!
```

```
dot11 ssid boss
   vlan 1
   authentication open eap eap_methods4
   authentication network-eap eap_methods4
!
power inline negotiation prestandard source
!
!
username Cisco password 7 106D000A0618
username 001644ef03ad password 0 001644ef03ad
username 001644ef03ad autocommand exit
username 001de08ce96d password 0 001de08ce96d
username 001de08ce96d autocommand exit
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 200 mode ciphers aes-ccm
 !
 ssid Employe
 !
 ssid Guest
```

```
 !
 ssid Phone
 !
 ssid boss
 !
 antenna gain 0
 channel 2462
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 no cdp enable
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
interface Dot11Radio0.10
 encapsulation dot1Q 10
 no ip route-cache
 no cdp enable
 bridge-group 10
 bridge-group 10 subscriber-loop-control
 bridge-group 10 block-unknown-source
```

```
 no bridge-group 10 source-learning
 no bridge-group 10 unicast-flooding
 bridge-group 10 spanning-disabled
!
interface Dot11Radio0.100
 encapsulation dot1Q 100
 no ip route-cache
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.200
 encapsulation dot1Q 200
 no ip route-cache
 bridge-group 200
 bridge-group 200 subscriber-loop-control
 bridge-group 200 block-unknown-source
 no bridge-group 200 source-learning
 no bridge-group 200 unicast-flooding
 bridge-group 200 spanning-disabled
!
interface Dot11Radio1
 no ip address
```

```
 no ip route-cache
 shutdown
 !
 encryption vlan 200 mode ciphers aes-ccm
 !
 ssid Employe
 !
 ssid Guest
 !
 ssid Phone
 !
 ssid boss
 !
 antenna gain 0
 no dfs band block
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 no cdp enable
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
```

```
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.10
 encapsulation dot1Q 10
 no ip route-cache
 no cdp enable
 bridge-group 10
 bridge-group 10 subscriber-loop-control
 bridge-group 10 block-unknown-source
 no bridge-group 10 source-learning
 no bridge-group 10 unicast-flooding
 bridge-group 10 spanning-disabled
!
interface Dot11Radio1.100
 encapsulation dot1Q 100
 no ip route-cache
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.200
 encapsulation dot1Q 200
 no ip route-cache
```

```
 bridge-group 200
 bridge-group 200 subscriber-loop-control
 bridge-group 200 block-unknown-source
 no bridge-group 200 source-learning
 no bridge-group 200 unicast-flooding
 bridge-group 200 spanning-disabled
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10
 no ip route-cache
 bridge-group 10
 no bridge-group 10 source-learning
 bridge-group 10 spanning-disabled
!
```

```
interface GigabitEthernet0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.200
 encapsulation dot1Q 200
 no ip route-cache
 bridge-group 200
 no bridge-group 200 source-learning
 bridge-group 200 spanning-disabled
!
interface BVI1
 ip address 192.168.100.4 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
radius-server local
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.100.12 auth-port 1812 acct-port 1813 key spie
radius-server timeout 30
```

```
radius-server key avvid4amec
radius-server vsa send accounting
bridge 1 route ip
!
!
!
line con 0
 logging synchronous
line vty 0 4
 password 7 094F471A1A0A
 logging synchronous
line vty 5 15
 password 7 094F471A1A0A
 logging synchronous
!
end

ap#
```