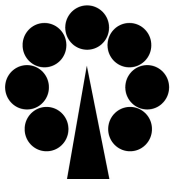


Satakunnan ammattikorkeakoulu

Mikko Kerstinen

Langattomanverkon käyttäjätunnistuksen toteutus freeradiuksen ja ldap-hakemiston avulla.

Tietotekniikan koulutusohjelma

Ohjelmistotekniikan suuntautumisvaihtoehto

2009

Langattomanverkon käyttäjätunnistuksen toteutus freeradiuksen ja ldap-hakemiston avulla.

Kerstinen, Mikko
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
lokakuu 2009
valvoja, DI Niemi, Juha
ohjaaja, Petri Asikainen.
Sivumäärä:48

Asiasanat: FreeRADIUS, Novell, eDirectory, SLES, Autentikointi, VMware

---

Tämän opinnäytetyön aiheena oli Langattoman käyttäjän autentikointi. Projekti toteutus tapahtui virtuaalisesti. Työkaluina toimivat SLES 10, FreeRADIUS, eDirectory, LDAP ja fyysisenä asemana D-Link WLAN.

FreeRADIUS on avoimen lähdekoodin periaatteella, kehitettävä RADIUS-palvelin. RADIUS on palvelin/asiakaspohjainen tunnistamiseen, pääsynvalvontaan, asetustietojen välittämiseen ja käyttötilastointiin kehitetty tilaton yhteyskäytäntö. RADIUS:ta käytetään usein suljetuissa verkoissa joihin verkon ulkopuolisten käyttäjien on mahdollista liittyä liityntäpisteiden eli NAS:ien välityksellä. NAS voi olla esimerkiksi WLAN tukiasema kuten tässä projektissa. WLAN mahdollistaa esimerkiksi 300m alueen josta päästään käsiksi sisäiseen verkkoon. Esimerkiksi koulu ja sen asuntola. Serverin alustana käytämme SuSe Linux Enterprise Server-järjestelmää, koska asetukset halutaan tehtävän Linux-järjestelmään.
Käytettävä hakemistopalvelu eDirectory on oppilaitosten suosiossa koska siihen päästään hyvin käsiksi monella protokollalla. Käytämme projektissa LDAPa koska sen pääasiallinen käyttötarkoitus on käyttäjäntunnistus.

Wireless user authentication using FreeRADIUS and LDAP

Kerstinen, Mikko
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information technology
October 2009
Niemi, Juha
Number of pages:48

Key Words: FreeRADIUS, Novell, eDirectory, SLES, autentication, VMware

---

The subject of this thesis was the authentication of wireless users. The project was executed in a virtual environment. The tools used were SLES 10, FreeRADIUS, eDirectory and WLAN as a physical site.
FreeRADIUS is a RADIUS server to be developed based on an open source code.
RADIUS is a server/client based authentication, access control, configuration transmit and user logging stateless protocal. RADIUS is used in closed networks which outside users are able to join by using connection stations , e.g NAS connection. NAS can be e.g. a WLAN-station as it was in this project. WLAN makes it possible to connect to intranet from a distance of over 300 meters, e.g. between a school and a dormitory. The project was built on Suse Linux Enterprise Server-system as the configurations will be done on Linux.
The used eDirectory is commonly used in schools because it provides good connection with different protocols. In this project LDAP-protocol was used as the main purpose of use was user authentication.

SISÄLLYS

1 JOHDANTO

Langattoman verkon käyttäjän tunnistus palvelu. Alustana toimii SUSE Linux Enterprise Server 10. FreeRADIUS on avoimen lähdekoodin periaatteella kehitettävä RADIUS-palvelin. Käyttäjien hallinta Novell Edirectory järjestelmällä. LDAP (Lightweight Directory Access Protocol) -hakemisto on tiedon lukua, etsimistä ja selailua varten optimoitu tietokanta.

Työllä pyritään parantamaan tietoliikenne toimintaa oppilaitoksessa ja sen asuntoloissa. Ja tulevaisuudessa pyritään laajentamaan oppilaille suunnattuja palveluita ja parantamaan tiettyihin palvelimiin pääsyä.

2 NOVELL EDIRECTORY

Novell eDirectory (entinen Novell Directory Service NDS) on x.500 nojaava palvelinriippumaton hakemisto joka julkaistii 1993 Novell,Inc toimesta. Tarkoitus oli päästä käsiksi moniin servereihin ja tietokoneisiin annetusta verkosta. eDirectory on monipuolinen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon palveluista. eDirectory hakemistopalvelu mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa selkeän tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. eDirectory ei ole rajattu Windows-käyttöjärjestelmään, kuten siitä löyhästi mallia ottanut Microsoft Active Directory, joka ei oikeastaan ole aito hakemistopalvelu, vaan uudempien Windows-palvelinkäyttöjärjestelmien ominaisuus.

eDirectory on tuttu ainakin 1990-luvun palvelinkäyttöjärjestelmistä, ensimmäisistä IT-infran hallintajärjestelmistä, erilaisista kirjautumisjärjestelmistä ja käyttäjänhallintapalveluista.

Nykyään eDirectorylle on saatavana täysi spektri palveluita sekä hallintavälineitä sekä Windows- että Linux ympäristön hallintaan ja kirjautumisten suojaamiseen sekä automatisointiin.

Se on laajasti käytössä mm. oppilaitoksissa, kovempaa tietoturvaa vaativassa julkishallinnossa ja yrityksissä. Siihen pääsee käsiksi LDAP, DSML, SOAP, ODBC, JDBC, JNDI and ADSI ja se tarjoaa yli biljoona objektia. eDirectoryn arvo tulee vielä nousemaan Linuxin nousun myötä ja nyt, kun sisäisten palveluiden hakemiston rooli on muuttumassa ja esimerkiksi pitää avata sitäkin sisäverkosta ulos.[25][20][15][12]

2.1 SUSE Linux Enterprise Server 10

SUSE Linux Enterprise Server (SLES) on Novell-yhtiön käyttöjärjestelmä.Joka on tarkoitettu kaupalliselle markkinoille. Palvelin puolen käyttöliittymäksi mut sen voi myös asentaa työpöydäksi. Uudet versiot julkaistaa 24kk-36kk sykleissä, kun taas päivitys versiot 9-12kk välein. SUSE Linux Enterprise tuotteisiin kuuluu SUSE Linux Enterprise Server joka on paljon tehokkaampi kuin openSUSE tuote perheen tuotteet.

SLES 9 versio julkaistiin Elokuussa 2004 ja päivitys Joulukuussa 2007. Se tukee kaikkien suurien yhtiöiden kuten IBM, HP, Sun Microsystems, Dell, SGI and Fujitsu Siemens tietokoneita.

SLES 10 versio julkaistiin Kesäkuussa 2006 se jakaa saman lähdekoodi pohjan kuin SUSE Linux Enterprise Desktop 10.

Suuri muutos tapahtui kun käyttäjät itse saattoivat osallistua tulevien versioiden testaukseen ja avustaa kehitystyössä. Aiemmin kaikki kehitystyö ja testaus oli suoritettu sisäisesti SUSE:n toimesta ja versio 10.0 oli ensimmäinen, joka päästettiin julkiseen beta-testaukseen. Osana muutosta myös pääsy YaST Online Update -päivityspalvelimille tuli vapaasti kaikkien käyttäjien saataville.

SUSE Linux Enterprise Server 11 on suunniteltu julkaistavaksi 2009 vuoden ensimmäisellä neljänneksellä.[23][27]

2.2 VMware Worksation

VMware Worksation on VMware Inc. yrityksen virtualisointiohjelmisto. EMC Corporationin omistuksessa toimiva VMware Inc. muut tuotteen ovat VMware Player VMware Server, VMware ESX Server.

Ohjelmisto luo ja ajaa yhdellä fyysisellä koneella yhtä tai useampaa virtuaalikonetta joihin voidaan asentaa eri käyttöliittymiä kuten Windows,Linux tai BSD. Kuitenkin vain yksi per virtuaalikone.

Muut VMwaren työkalut helpottavat tällaisten virtuaalikoneiden keskitettyä hallintaa ja päivitystä.VMware Workstation tarjoaa virtuaalisen työympäristön tietokoneen omaa prosessoria ja muistia käyttäen. Viruaalinen työympäristö antaa mahdollisuuden tutkailla haluttuja laitteita, työkaluja tai vastaavia oheislaitteita jotka testauksen yhteydessä voivat jumittaa tai jopa vahingoittaa fyysisen koneen ohjelmistoa tai ylikuormittaa sen omia komponentteja. Palvelimien ja päätteiden siirto yhden fyysisen tietokoneen alaisuudessa toimiviksi virtuaalikoneiksi helpottaa niiden hallintaa, lisää joustavuutta ja ennen kaikkea vähentää lattiapinta-alan tarvetta toimistossa.

VMwaren asennus on yksinkertaisesti toteutettu molemmille Windows ja Linux käyttyliittymä tyypeille. Ohjelmisto pyrkii pitämään asennuksen itsellään mahdollisimman laajana jotta sen hallinnoiti olisi helpompaa. Linux:n ja Windows:n asennukset ovat erilaiset johtuen Linux:in muutamasta komponentista sekä muuttujista jotka puuttuvat Windows ympäristöstä. Joudut vastailemaan muutamiin kysymyksiin asennuksen aikana, kysymykset liittyvät käytettäviin ympäristöihin ja niiden tyyppeihin.

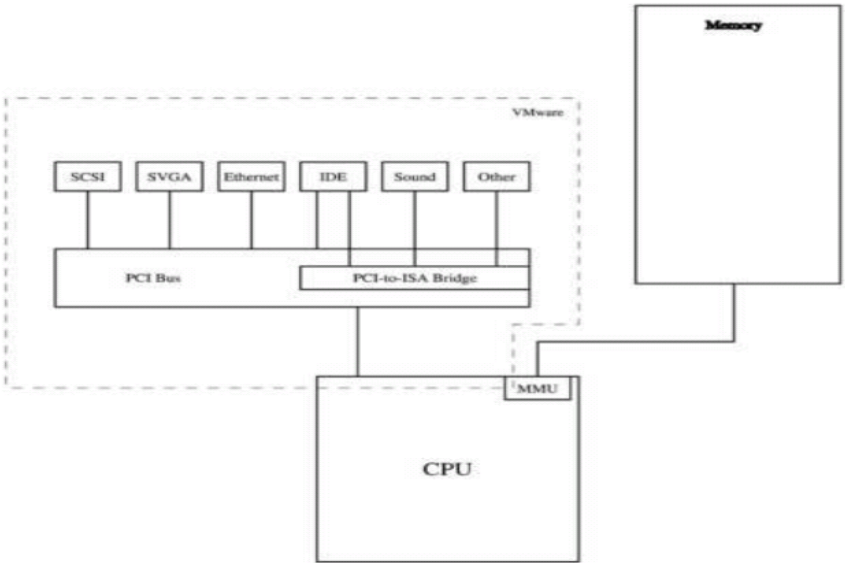
2.2.1 Virtuaalikoneen komponentit

Tietokoneella on kolme oleellista komponenttia: prosessori, muisti ja I/0-laitteet. CPU eli central processing unit. Tämä toimii koneen “sydämmenä”. Se ei vain aja mutta myös ohjaa liittymää. Koska ajon aikana prosessori ei pysty suorittamaan samaan tahtiin kuin haluttuja ajoja, tulee olla koneella ulkoinen muisti eli random-access memory (RAM). Muisti on liitetty lähes suoraan kiinni prosessoriin, koska RAM on hyvin tärkeä CPU:lle Näiden kahden välillä on memory management unit (MMU) joka paloittelee RAM:in pieniin paloihin nimeltä pages eli sivut.MMU:lla on kartta jokaiseen sivun muistiin nimeltä the page table jota vastaa oikea muistipaikka. Muisti jota käyttäjä käyttää ohjelmissaan on nimeltään virtuaalimuisti. Eli kun CPU esittely kysyy tiettyä osoitetta muistista, MMU ohjaa uudelleen läpi sivu-kartan suoraan fyysiseen muistiin.

Ei ole järkevää vaivata prosessoria yhdistämällä laitteita suoraan siihen. Koska ennen kuin tuleva tieto on oikeassa järjestyksessä ja luettavassa muodossa että prosessori ymmärtäisi sitä on kulunut mahdottomasti aikaa työn suorittamiseen. Täten prosessorilla on ”apuna” yhteinen väylä eli common bus joka yhdistää laitteet prosessoriin. Liittimissä voi olla lisä-ohjaajia ja käyttöliittymiä laitteen ja väylän välissä. VMware:ssa on kaksi virtuaaliväylää. Kuten yleisimmissä moderneissa tietokoneissa PCI ja PCI-to-ISA bridge. ISA on vanha standardi IBM ajoilta.
Vaikka ISA on ala-arvoinen ja hidas, sen yhteensopivuus on pitänyt sen hengissä. Vaikka jotkin laitteet käyttävät kuten serial-port:it ISA-käyttöliittymää, useimmat kehittäjät yrittävät välttää käyttöä sen rajoitteiden takia.
Pahimmat lienevät interrupts ja I/O-portti. Laite lähettää keskeytyksen(interrupt) väylän yli prosessorille ja kertoo olevansa valmis lähettämään dataa tai keskustelemaan haluttua toimintaa. Prosessori tunnistaa sen, lopettaa toimintansa ja työstää keskeytyksen. ISA numeroi keskeytyksen keskeytys pyyntön eli interrupt request (IRQ) tason.
Valitettavasti IRQ-numeroita ei ole montaa joten jos kaksi laitetta jakaa saman numeron tulee ristiriitainen tulos. Samantyyppinen ongelma laitteeille jotka käyttävät I/0-portteja keskustellakseen väylän kanssa. PCI:ssä ei ole näitä virheitä koska PCI

laitteilla on enemmän tietoa joten ne pystyvät jopa jakamaan saman IRQ-numeron. Sekä piiri järjestää automaattisesti koneen käynnistyessä.

Kartta VMware Workstation koneesta.



2.2.2 Virtuaalikoneen laitteet

Äänikortti

Äänikortista on monia variaatioita mutta VMware Workstation käyttää Creative Technology SoundBlaster 16 card, at the factory settings: IRQ 5, I/O ports 0x220 to 0x22f, DMA channel 1 (16-bit DMA channel: 5). Koska nämä asetukset ovat monilla ajureilla vapaana.

BIOS

Kaikilla tietokoneilla on BIOS eli basic input/output system. Se on pieni osa firmwarea(rom-muistissa olevat ohjelmat) joka sijaitsee emolevyllä. BIOS tietää kuinka keskustella laitteille hyvin pienellä kapasiitilla.BIOS esittää muistin ja oheistietoa tietokoneestasi kun käynnistät koneen.BIOS:in on pakko säilyttää parametrejä ettei käyttäjän tarvitsisi laittaa niitä joka käynnistys kerralla. BIOS säilöö tiedot nonvolatile memory, tai NVRAM. Se säilöö tiedot vaikka flash-muisti ja patteri-toiminen muisti häviäisi.

IDE levyt ja CD-ROM ajurit

Yleisin levy tietokoneilla on Integrated Device Electronics eli IDE levy. Tavallisessa levyssä oli levyn controller jossain päin emolevyä. Nämä controllerit hoitivat kanavia levyn ja minkä tahansa levyn välillä. Tämä tekniikka kuitenkin lisäsi huomattavasti koneen hintaa. SCSI-I tai II controllerit esimerkiksi voivat hoitaa seitsemää levyä tai laitetta samaan aikaan. Kuitenkin koneissa on yleensä kiinni vain yksi tai kaksi kovalevyä kiinni ja toiset käyttävät Industry-Standard Architecture eli ISA-korttia. Koneiden suunnittelijat päättelivät pystyvänsä alentamaan kustannuksia käyttämällä tätä ominaisuutta. He päätyivät IDE-levyyn jossa controllerit ovat integroituja levyyn itseensä.
IDE levystä tuli nopeasti yleisin levy ja hinta putosi. IDE ei kuitenkaan tukenut CD_ROM ajureita, joten insinöörit kehittivät ATAPI eli AT Attached Packet Interface joka yhdisti CD_ROM:in ja kasetit IDE-liittimellä.Kuten tietokoneen emolevyllä, VMware Workstation:ssa on kaksi IDE-controlleria, ensisijainen ja toissijainen liitin. Virtuaali asemat ovat Intel 82371AB PIIX4 piiri. IRQ ja portit:

Interface	IRQ	I/O Ports
Primary	14	0x01f0 to 0x01f7, 0x03f6
Secondary	15	0x0170 to 0x0177, 0x0376

Kuten IDE liittimessä kukin porteista tukee kahta laitetta (*master* ja *slave* laitteet).
VMware:ssa levyt ovat rajalliset, CD-ROM/DVD-ROM, CD-R, ja CD-RW ajureita voidaan konfiguroida muutamilla tavoilla. Levyt ovat image muodossa. Virtuaali asema näin luulee että asemassa pyörii oikea levy vaikka virtuaalikone pyörittää vain data koneella.

SCSI levyt

VMware Workstation:ssa on virtuaalinen SCSI kovalevy. Sitä isännöivä controlleri on PCI-based BusLogic BT-958 Ultra Wide SCSI adapteri. Voit konfiguroida seitsemää levyä tai CD-ROM:ia VMware:n controllerilla. Koska virtuaalinen SCSI controlleri on PCI laite, systeemi hakee automaattisesti ja konfiguroi IRQ-numerot ja I/O-portit kun käynnistetään.

Disketti

Ehkä kaikista laitteista alkukantaisin tuki VMware:ssa on levyke asema.
Like the actual floppy disks themselves, the hardware specification hasn't changed in years.
Vaikka nykyään levykkeet ovat melkein kuolleet sukupuuttoon, on tuki Vmware:ssa toivottua. Voit käyttää sitä virtuaalisesti lukemaan tiettyjä tiedostoja vaikka et käyttäisikään oikeaa levykettä. Levyke käyttää IRQ 6 ja I/O porttia 0x3f0 to 0x3f5 ja 0x3f7.

Ethernet Interfaces

A *network interface card* (NIC) on adapteri joka pysäyttää verkkosignaalit, suodattaa ne ja lähettää ne CPU:lle prosessoitavaksi. Ethernet on yleisin tyyppi lähiverkoista. Halpa hinta on ajanut monet valmistajat sisällyttämään laitteisiinsa Ethernet liittimen. VMware:n virtualinen Ethernet sovitin on AMD PCnet II joka pohjautuu AMD 79C970A piiriin.
Voit lisätä kolme sovitinta virtuaali koneeseen ja konfiguroida kolmella tavalla:
host-only network ,*bridged networking* sekä .*NAT networking.*

Verkko tuki on yksi VMware:n vahvuuksia. Verkko ei ainoastaan anna jakaa tiedostoja vaan verkko tarjoaa SSH tunneloinnista etäohjattaviin tulostin servereihin.

Serial Portit

VMware Workstation:illa on neljä serial porttia:
DOS Name Linux Name IRQ I/O Ports
COM1: /dev/ttyS0 4 0x3f8 to 0x3ff
COM2: /dev/ttyS1 3 0x2f8 to 0x2ff
COM3: /dev/ttyS2 4 0x3e8 to 0x3ef
COM4: /dev/ttyS3 3 0x2e8 to 0x2ef
VMwaressa voit yhdistää laitteen seriali porttiin ja ohjata ulostulon tiedostoon isäntä systeemissä.

Parallel Portit

Toisin kuin serial portti, joka lähettää tietoa yksi bitti kerrallaa laitteelle, parallel portit lähettävät kahdeksan bitti kerralla.
VMware Workstation tukee kahta Tietokoneen parallel porttia.
DOS Name Linux Name IRQ I/O Ports
LPT1: /dev/lp0, /dev/parport0 7 0x3bc to 0x3be
LPT2: /dev/lp1, /dev/parport1 5 0x378 to 0x37f

USB Interface

VMware Workstation tukee USB (universal serial bus). USB liitäntä on nimeltään hot-pluggable, joka tarkoittaa että lisälaitteen voi kytkeä ja poistaa tietokonetta sammuttamatta. Liitäntä on tarkoitettu laitteille kuten näppäimistöt,hiiret, tulostimet, scannerit. USB-laitteelle voidaan antaa virta suoraan väylän kautta mikä antaa laitteille edun yli kuormittamatta virtalähdettä liikaa. Liitäntä siirtää dataa kuten seriali portti, mutta tukee monta laitetta kuten SCSI.

Graphics

VMware:ssa on oma näytönohjain adapteri mutta asentamalla VMware Tools paketin saat näytönohjaimeen saman määrän värejä kuin isäntä koneessakin on.
Toinen parannus joka tulee VMware Tools:in mukana on full-screen mode eli kokonäyttö toiminto, joka sivuuttaa kokonaan VMware ikkunan ja antaa kokonäytön käytettäväksi. On helppo vaihtaa edes takaisin eriympäristöihin.

Mouse

Hiiri on IRQ 12 paikassa ja jakaa I/O portin näppäimistön(0x060 to 0x06f) kanssa.[24]

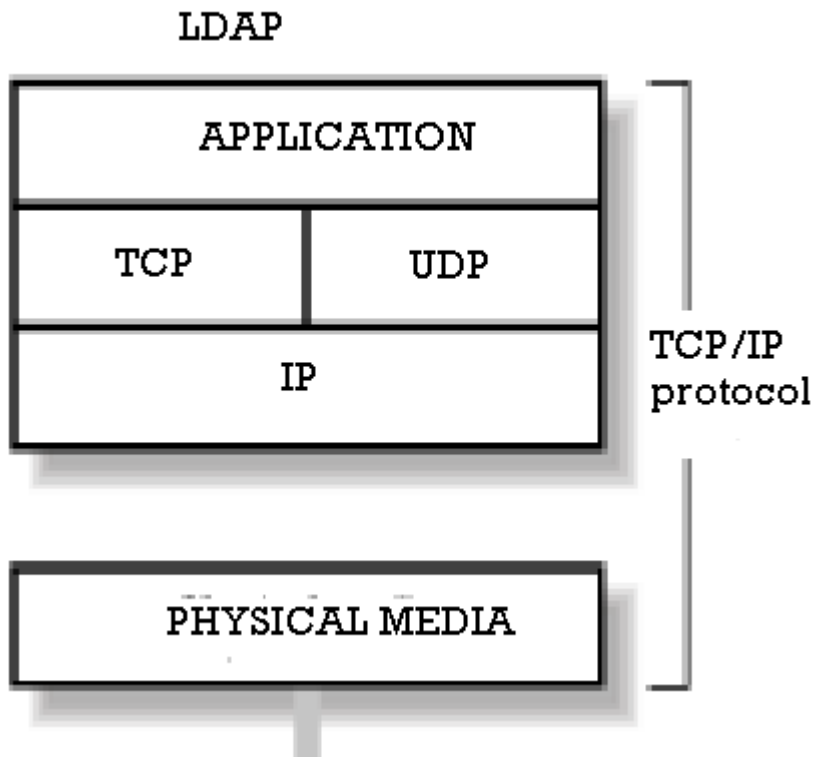
3 LDAP—A DIRECTORY SERVICE

Lightweight Directory Access Protocol on hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla. LDAP syntyi yksinkertaistettuna vaihtoehtona täydelliselle ja monimutkaisemmalle X.500-hakemistopalvelulle. LDAP seuraa X.500-mallia, jossa hakemiston tiedot on järjestetty hakemistopuuhun avain-arvopareina. Se käyttää DNS-nimiä hierarkian nimeämisessä.

Alkuperäinen versio LDAPista kehitettiin Michiganin
yliopistossa 1993, mutta nykyään sen kehityksestä vastaa IETF eli International Engineering Task Force.

LDAP käyttää TCP/IP-verkkopalveluna TCP-protokollaa ja porttia 389 tai SSL-tunnelointia käytettäessä porttia 636. Verkkoprotokolla on määritelty ASN.1:n (Abstract syntax notation one) pohjalta ja se käyttää BER-binäärikoodausta (Basic encodingrules).LDAP-URLkäyttäämuotoa
"ldap[s]://host:port/DN?attributes?scope?filter?extensions".

Kuva 3.1 LDAP TCP/IP:n päällä



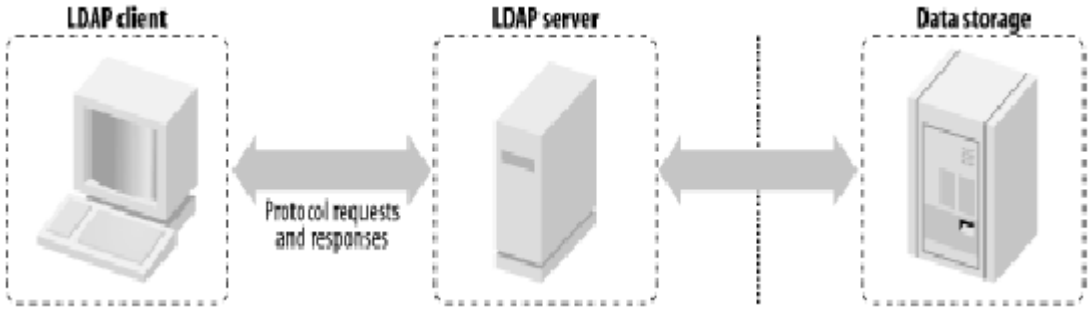
LDAP:in käyttötarkoitus on pääasiassa käyttäjäntunnistus. Käyttäjän tunnistuksessa LDAP-palvelin palauttaa oliko annettu käyttäjätunnus ja salasana oikein.
Sitä tukevat useimmat UNIX-järjestelmät ja Microsoftin Active Directory käyttää LDAPia pohjanaan Kerberoksen ohella. Myös useat muut tuotteet käyttävät LDAP:ia, mm. Apache Directory Server ja Oracle Internet Directory. LDAP soveltuu myös käyttöoikeuden tarkistamiseen.Käyttöoikeuden tarkistuksessa LDAP-palvelin palauttaa onko käyttäjällä oikeus kysyttyyn resurssiin. LDAP-palvelin voi sisältää myös muuta tietoa kuin käyttäjän tunnuksen ja salasanan. Suodattimen avulla voidaan käyttää lisätietoja tunnistamiseen.

LDAP koostuu kolmesta osasta, jotka ovat tietomuoto, protokolla ja API eli ohjelmointirajapintaTietomuoto määrittelee, kuinka hakemistotieto tallennetaan ja haetaan. Tietomuotoon suunniteltu olevan sekä monialustainen sekä monikulttuurinenkin. Se on suunniteltu siten, että sillä on käytössään globaali nimimäärittely, josta käytetään termiä nimiavaruus. Tieto tallennetaan LDAP-palvelimelle sekä hierarkisessa että suhteellisessa muodossa. Hierarkisuudella

tarkoitetaan sitä, että tallennettavat tietueet, juuritietuetta lukuunottamatta, sijoittuvat puurakenteessa toisen tietueen alapuolelle. Suhteellisuus ilmenee puolestaan siinä, että tietueita voidaan ryhmitellä yhteen.

Ylintä tasoa LDAP-hierarkian puurakenteessa kutsutaan toimialueeksi (engl. domain). Toimialueita voi olla useampia riippuen toteutuksesta. Puun oksat muodostuvat organisaatiollisista yksiköistä. Yleensä ne ovat organisaation osastoja, mutta ne voivat olla mitä tahansa alajaotteluja kyseiselle organisaatiolle. Tietomuodon määrittelyn mukaan niin sanottuja lehtiä ovat ne tietueet, jotka eivät ole toimialueita, eikä organisaatiollisia yksikköjä.
Hakemistoissa ei yleensä ole relaatiotietokantojen tapaisia monimutkaisia transaktio-ominaisuuksia, vaan pääpaino on mahdollisimman nopeassa tiedon haussa. Hakemiston päivitykset tapahtuvat yleensä keskitetysti, kun taas hakuja voi tapahtua useilta eri käyttäjiltä. Arkimaailman hakemistoja ovat esimerkiksi erilaiset puhelinluettelot.

Kuva 3.2 Riippuvuus suhdanteet



LDAP-protokolla on noussut suureen suosioon. Markkinoilla on runsaasti sekä kaupallisia että ilmaisia LDAP-palvelintoteutuksia. LDAP-asiakasohjelmistojen luominen onnistuu myös eri ympäristöissä, useilla ohjelmointikielillä.[16][17][18][12][15]

4 FREERADIUS

FreeRADIUS on avoimen lähdekoodin periaatteella, GPL-lisenssin alla, kehitettävä RADIUS-palvelin. FreeRADIUS sai alkunsa elokuussa 1999 haarautumalla Cistronista omaksi projektikseen. FreeRADIUS on vielä hyvin yhteensopiva Cistron ja jopa Livingston RADIUSohjelmiston kanssa. Ohjelmisto helposti laajennettavissa ja kaikki AAA-spesifiset toiminteet ovat omissa moduuleissaan.

Selkeä rajapinta palvelimen ytimen ja moduulien välillä tekee omien moduulien kirjoittamisesta suhteellisen helppoa.

Dokumentaatiossa on tyypillisen avoimen lähdekoodin projektin tyyliin toivomisen varaa.Monen FreeRADIUS-palvelimen moduulin tärkein dokumentaatio onkin vain konfiguraatiotiedostojen kommenteissa.

Osa Livingstonin RADIUS-palvelimen dokumentaatiosta soveltuu myös FreeRADIUS-ohjelmiston perustoiminteiden dokumentaatioksi.

Serveristä tuli nopeasti suosittu. Siihen on vuosien varrella laajennettu erilaisia tietokantoja kuten LDAP ja SQL. EAP tuki laajennettiin 2001 vuonna, sekä PEAP ja EAP-TLS tuet vuonna 2003.

PPP Extensible Authentication Protocol (EAP) on PPP:n autentikointimallin päivitys, joka mahdollistaa useiden uusien autentikointimetodien käytön. EAP-TLS on TLS-pohjainen varmenne/sirukorttitunnistus. Versiossa 2.0.0 julkaistiin vuoden 2008 alkupuolella ja siihe on lisätty monia EAP tukia kuten EAP-FAST ja EAP-TNC. Siihen oli myös lisätty virtuaalisia moninaisuuksi,Ipv6, VMPS sekä uusi toimintaperiaate joka helpottaa monimutkaisia konfigurointeja.

Nykypäivänä serveri tukee jo tavallisimpiä autentikointi protokollia ja tietokantoja.[1][3][21][26]

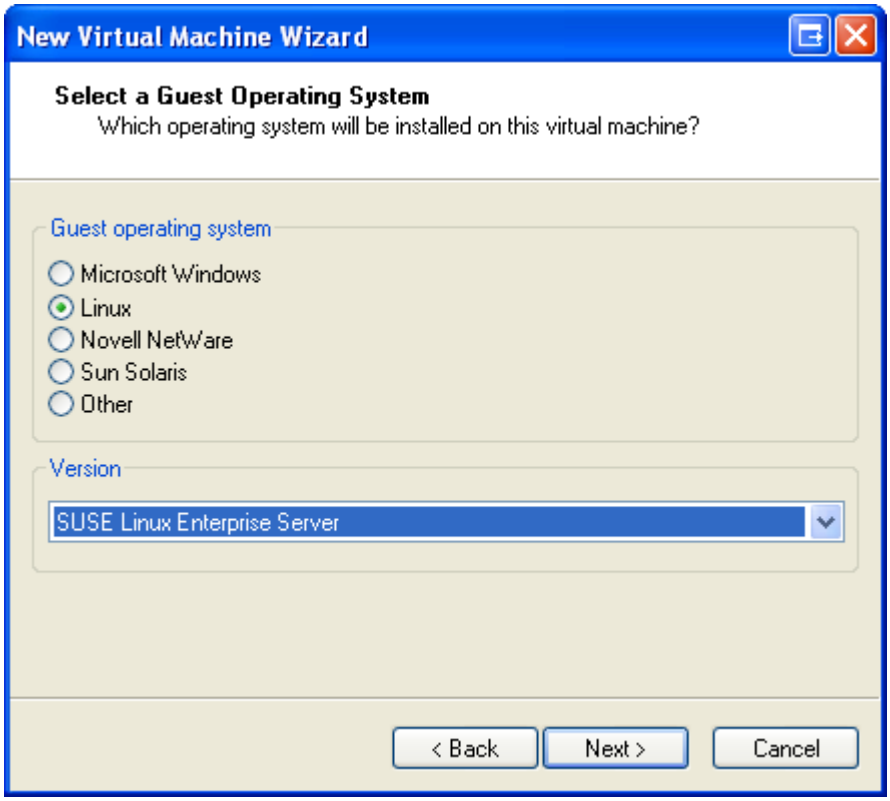
4.1 WPA eli Wi-Fi Protected Access

WPA on välivaiheen tietoturvatekniikka. Sitä käytetään langattoman käyttäjän pääsyn kontrolloinnissa langattomaan verkkoon. WPA:ta voidaan käyttää pre-shared

key salausta eli reititin ja asiakas tietävät molemmat salaisen avaimen tai autentikointi tapahtuu RADIUS-serverillä. [4]

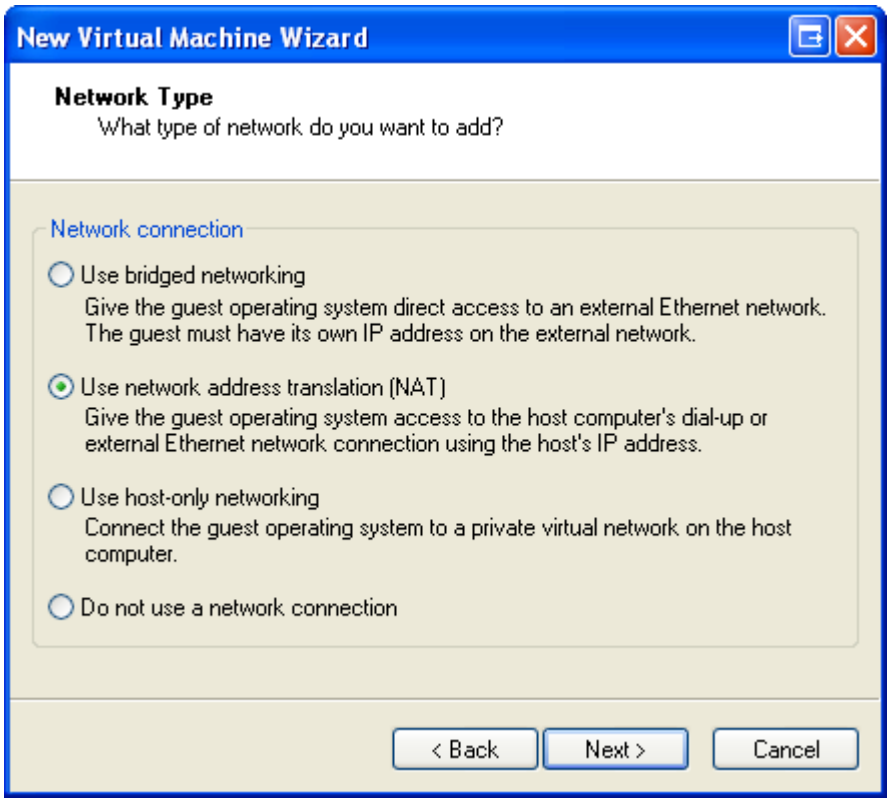
5 VMWARE WORKSTATION

Kuva 5.1 Järjestelmät

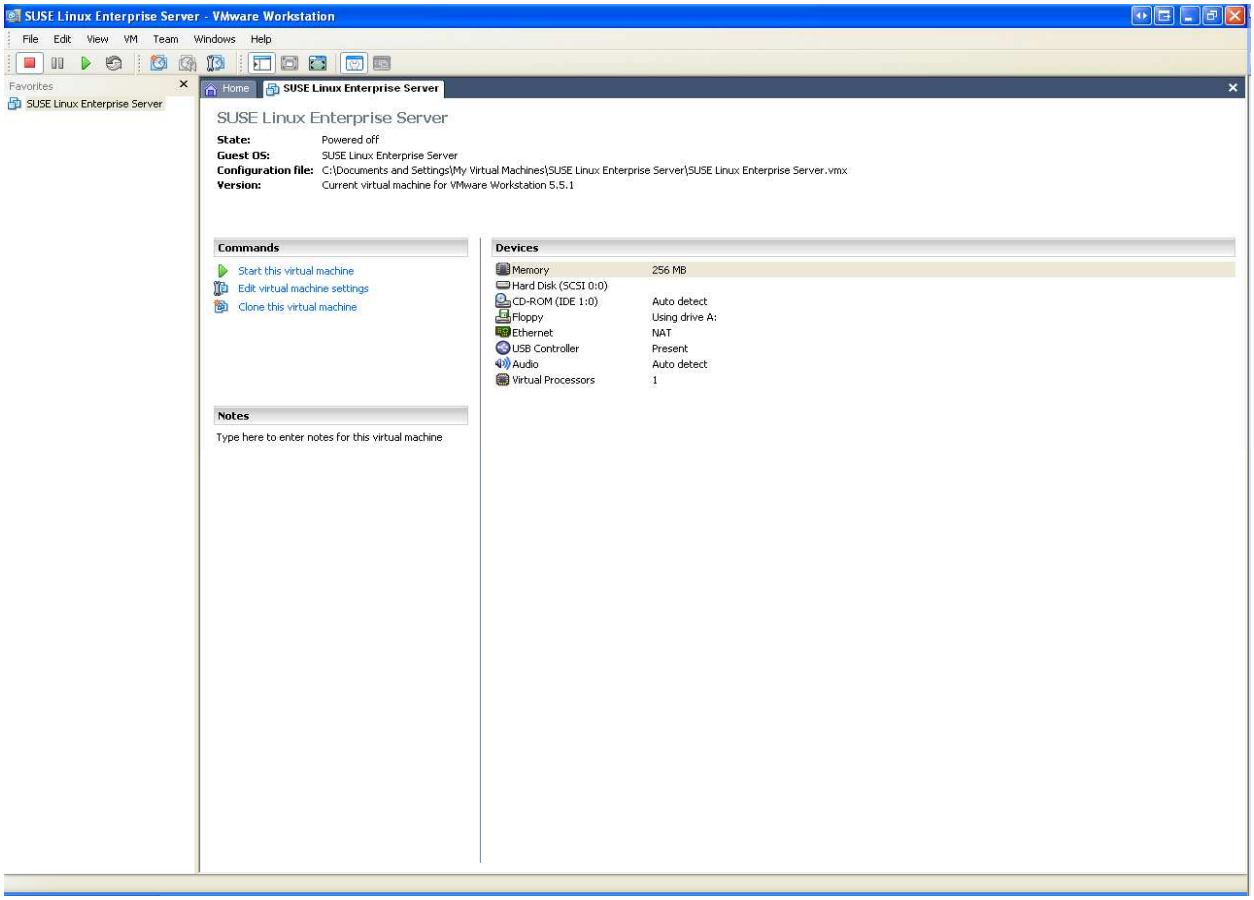


Kuten edellä olevasta kuvasta voidaan havaita että virtuaali koneen eri järjestelmiä on lukuisia. Käytämme SLES 10 järjestelmää joten valitsemme Linux -> SUSE Linux Enterprise Server.

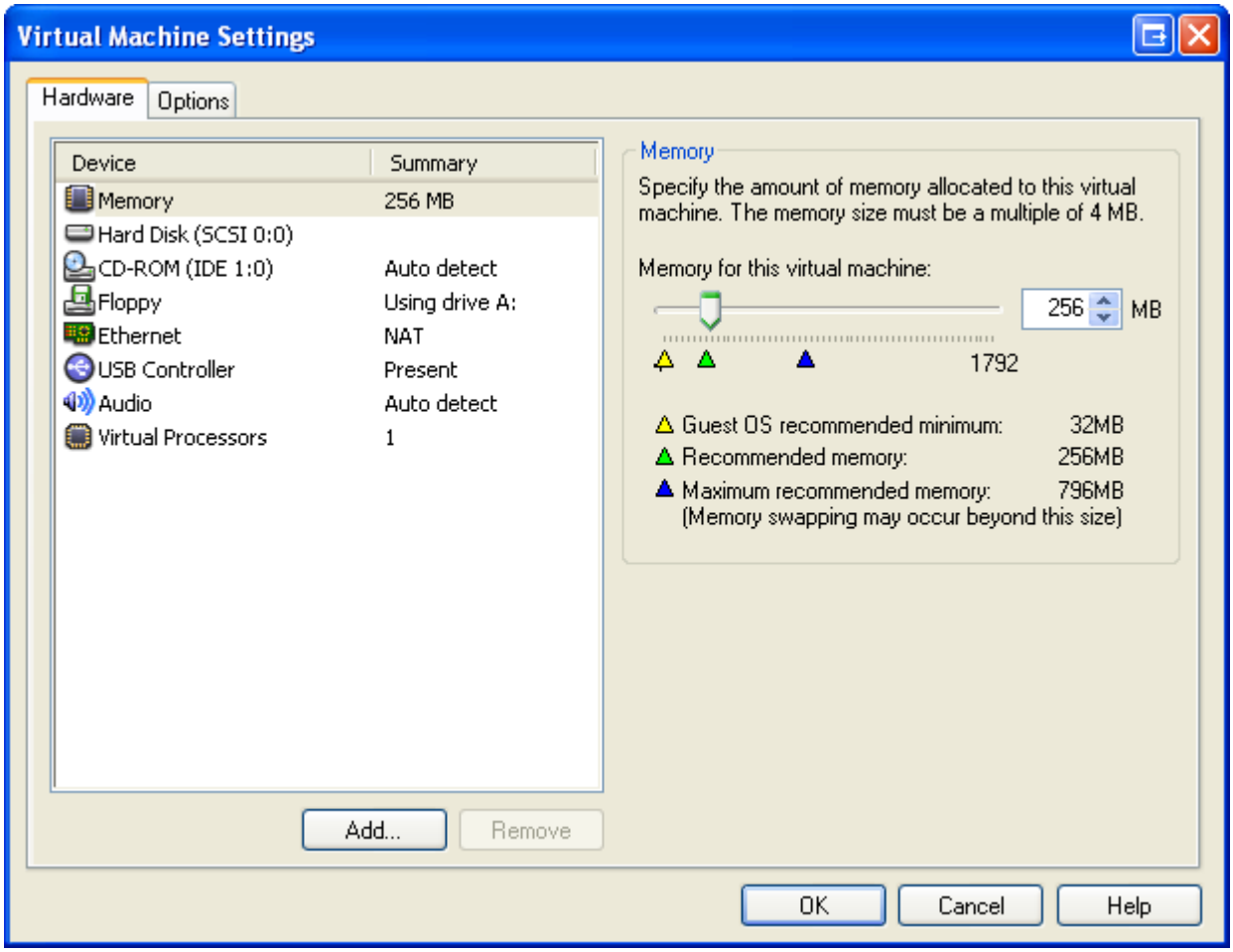
Kuva 5.2 Verkko tyyppi.



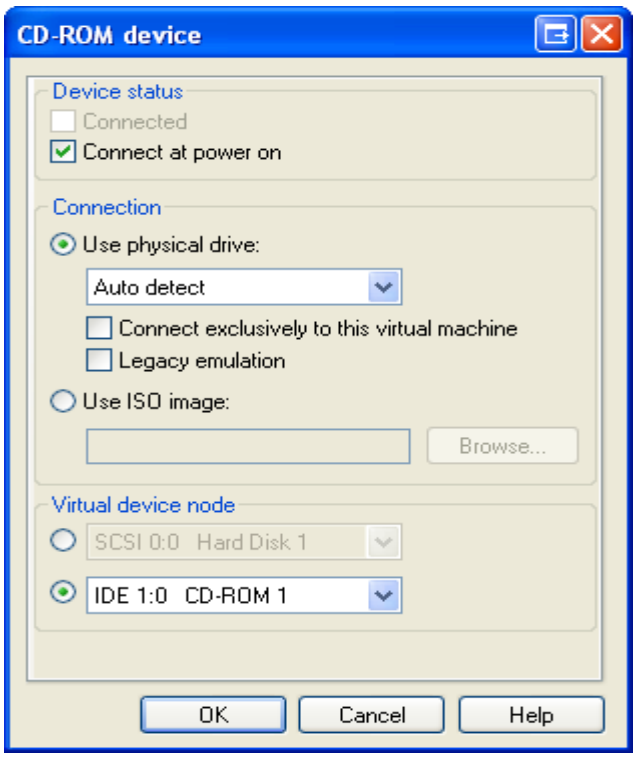
5.3 Luodun koneen sisältö



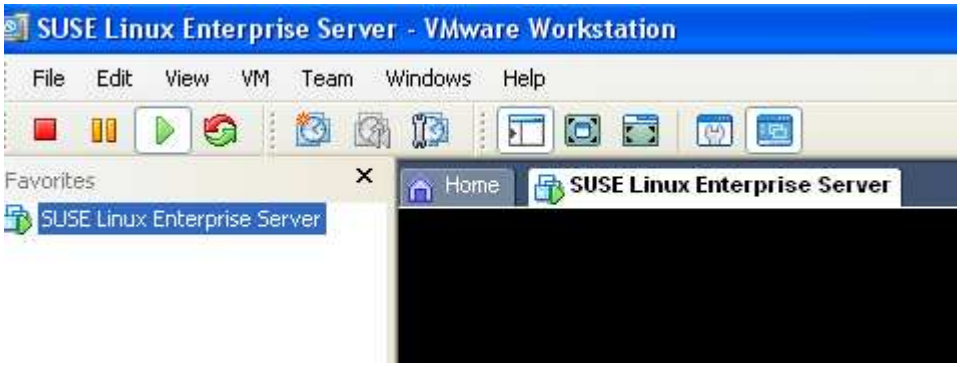
Kuva 5.4 Virtal Machine asetukset.



5.5 CD-ROM asetuksista

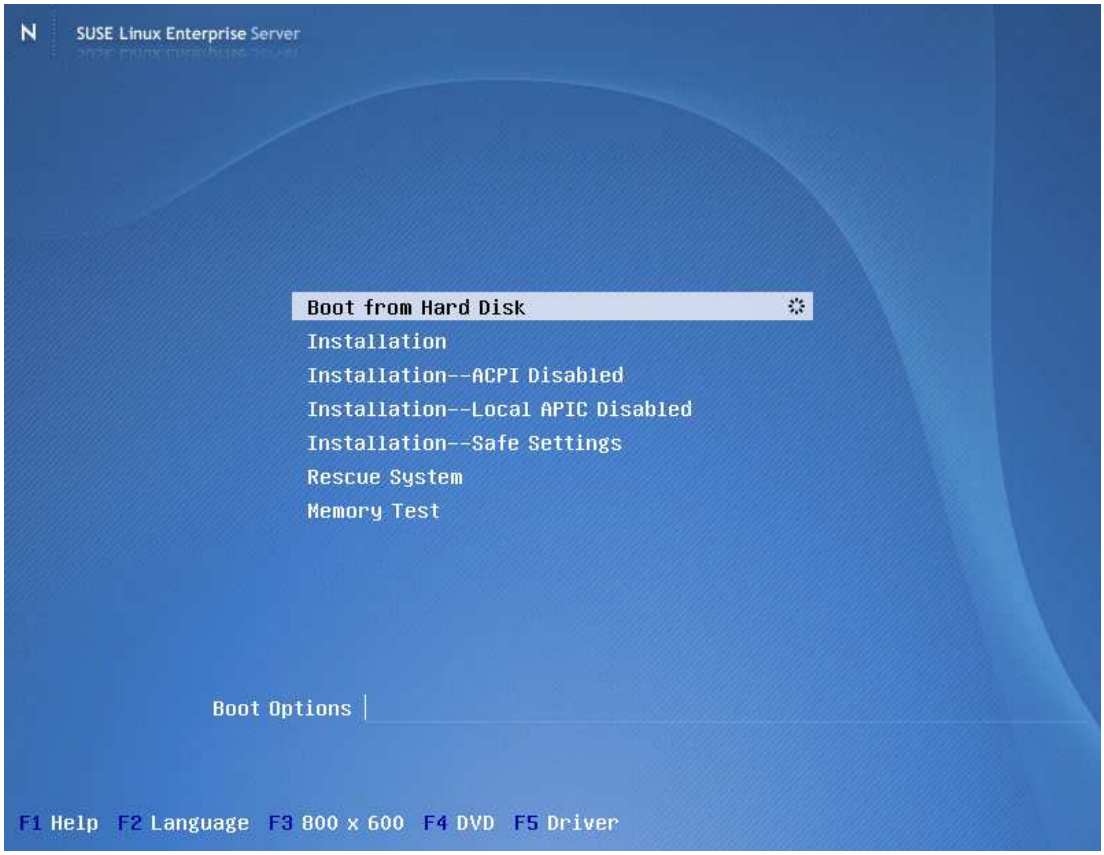


Kuva 5.6 käynnistys PLAY-nappulasta



5.1 SUSE Linux Enterprise Server 10

Kuva 5.1



Boot from Hard Disk. Boottaus kovalevyltä

Installation. Aloittaa normaalin asennus prosessin

Installation - ACPI Disabled. Aloittaa asennuksen ACPI (Advanced Configuration and Power Interface) poissa päältä. Jos normaali asennus epäonnistuu, voi syynä olla ettei kone tue ACPI:tä. Joten voit tällä asennus muodolla asentaa sen ilman ACPI:tä

Installation - Local APIC Disabled. Käynnistää asennuksen käyttäen APIC (Advanced Programmable Interrupt Controller) poissa päältä.

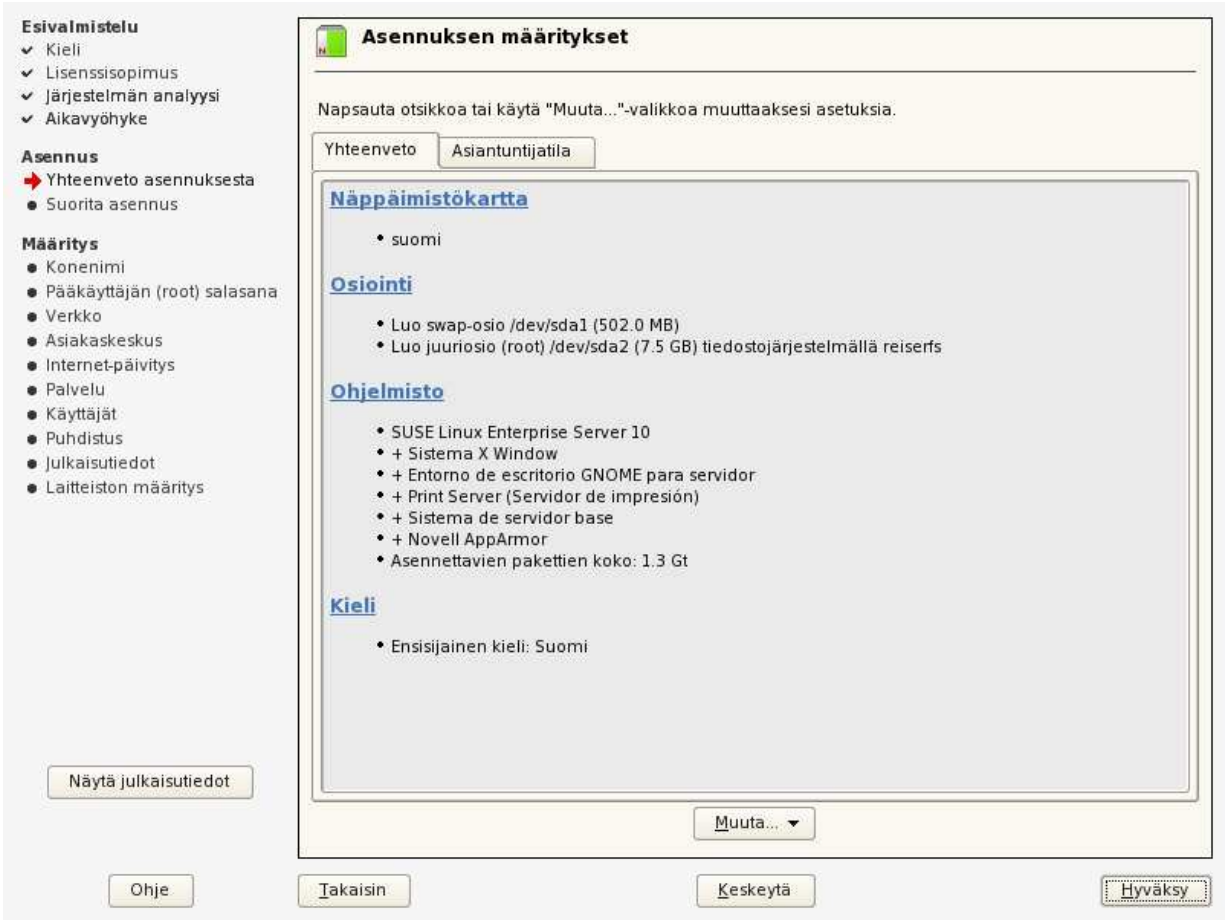
Installation - Safe Settings. Aloittaa asennuksen käyttäen DMA (Direct Memory Access) Käytä tätä vaihtoehtoa jos tavallinen asennus epäonnistuu.
Rescue System. Aloittaa SLES 10 järjestelmän elvytyksen. Jos et voi uudelleen käynnistää Linux:ia voit käyttää käynnistykseen DVD:tä. Tämä käynnistää minimoidun Linux järjestelmän ilman mitää lisä asetuksia jotta pääset käsiksi järjestelmään ja korjaamaan sitä.

Memory Test. Aloittaa muistin testaus ohjelman, joka testaa RAM käyttäen toistuvia luku ja kirjoitus syklejä. Ja näin luoden loputtoman kierron. Näin havaitaan jos muisti on rappeutunut.

Yhteen veto SLES:n asennuksesta

1. Valitse kieli
2. Valitse asennus tyyppi
3. Mahdollisuus vaihtaa asennus valintoja
4. Esitys kovalevyn osituksesta
5. Mahdollisuus vaihtaa vääriä valintoja
6. Asennus käynnistyy

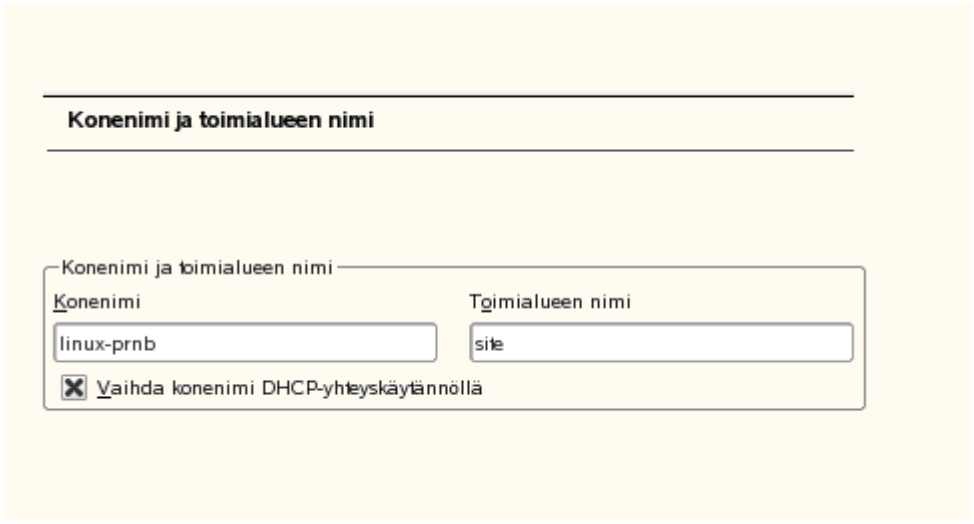
Kuva 5.2 yhteenveto asennuksen määrityksistä.



Yhteen veto SLES:n asetuksista

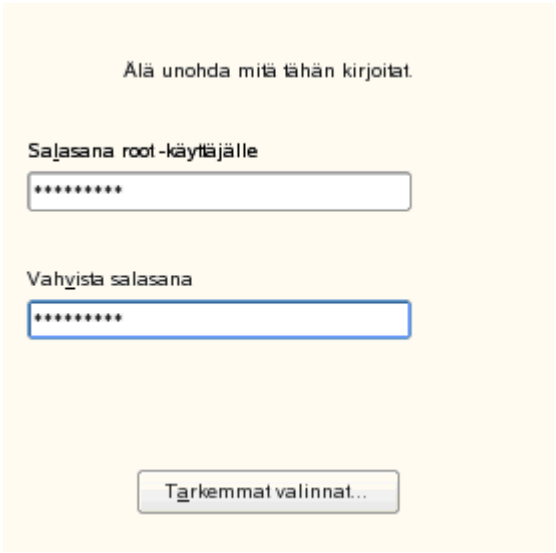
1. Asennetaan koneelle nimi,toimialue
2. Root-käyttäjän salasana
3. Verkko asetukset
4. Verkko palveluiden asetukset
5. Käyttäjä tilit
6. Kovalevyn asetukset
7. Viimeistellää asennus

Kuva 5.3 Nimitys



Koneelle annetaan nimi jolla se voidaan tunnistaa esim.verkossa.
Root-käyttäjän salasanalla päästää konfiguroimaan verkkoa sekä hallinnoimaan konetta.

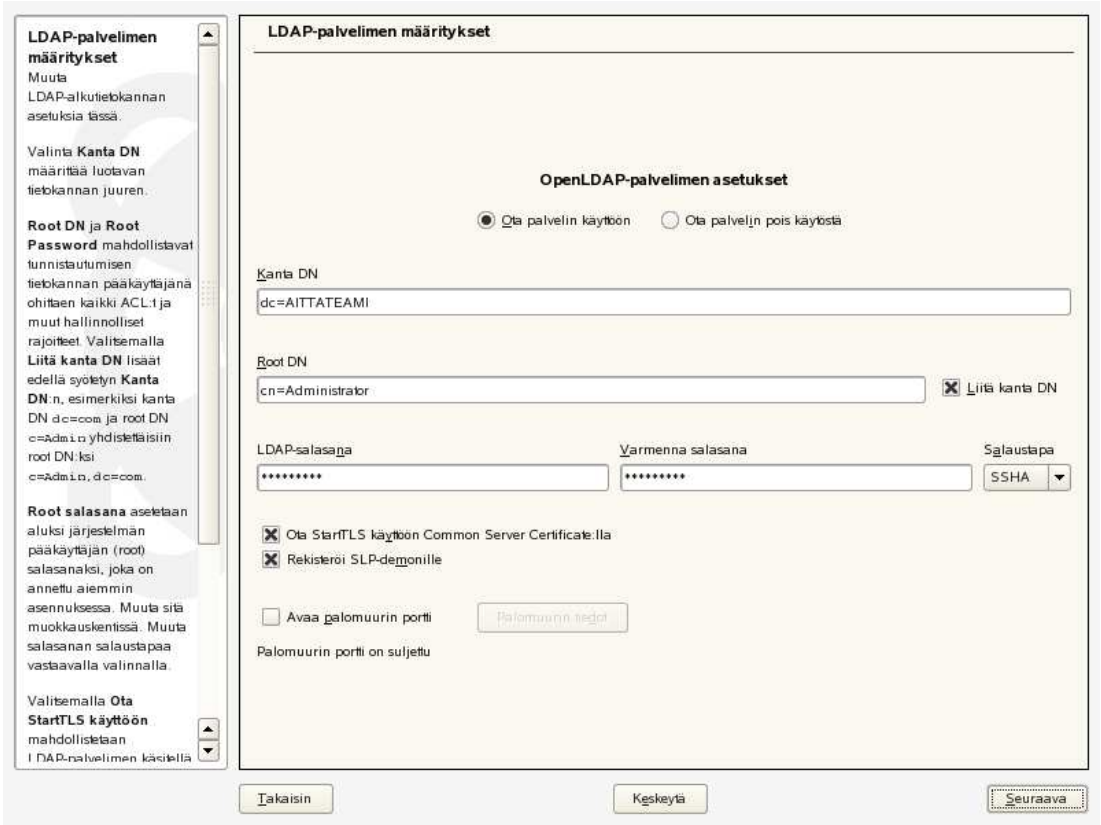
Kuva 5.4 Pääkäyttäjän salasana



Verkko määrityksessä asennetaan NetworkManager, ja testataan toimiiko yhteys.

Kuva 5.5 Testaus

Kuva 5.6 OpenLDAPpalvelin



Kanta DN. LDAP-puun DN-juuret.

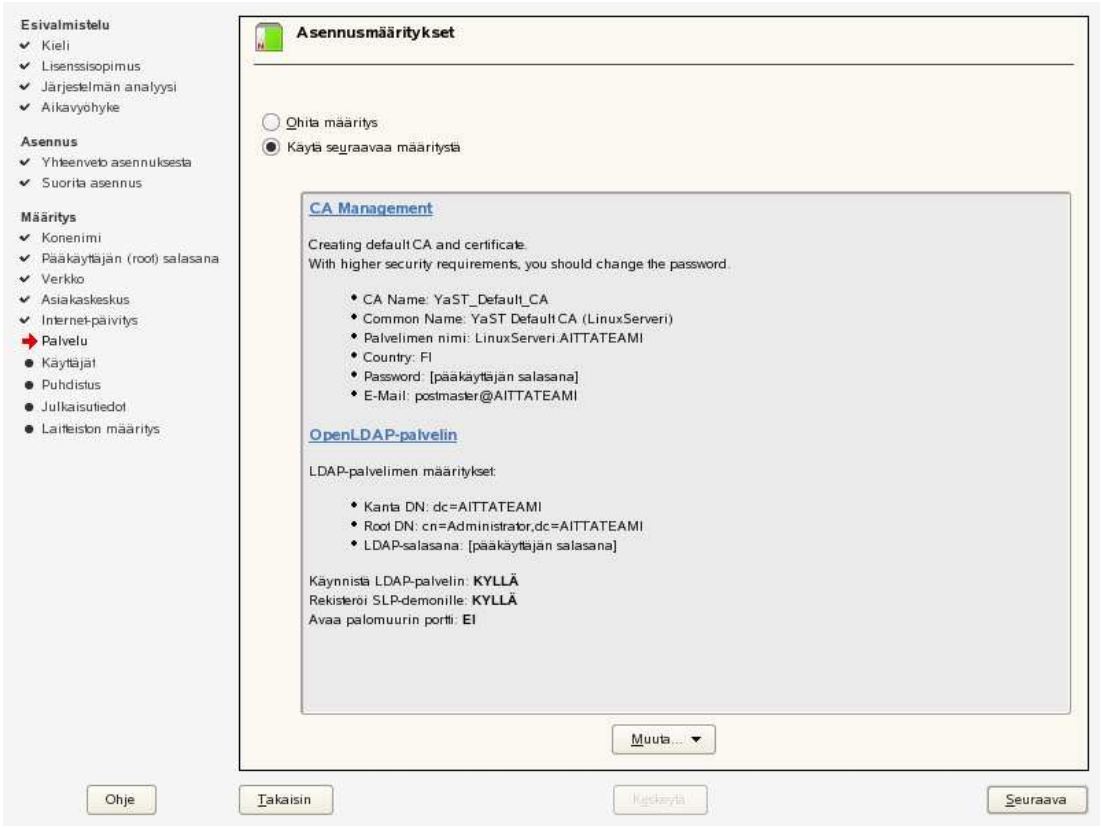
Kanta DN liittää sisääntuloon Root DN automaattisesti.

Root DN. Pääkäyttäjän DN.

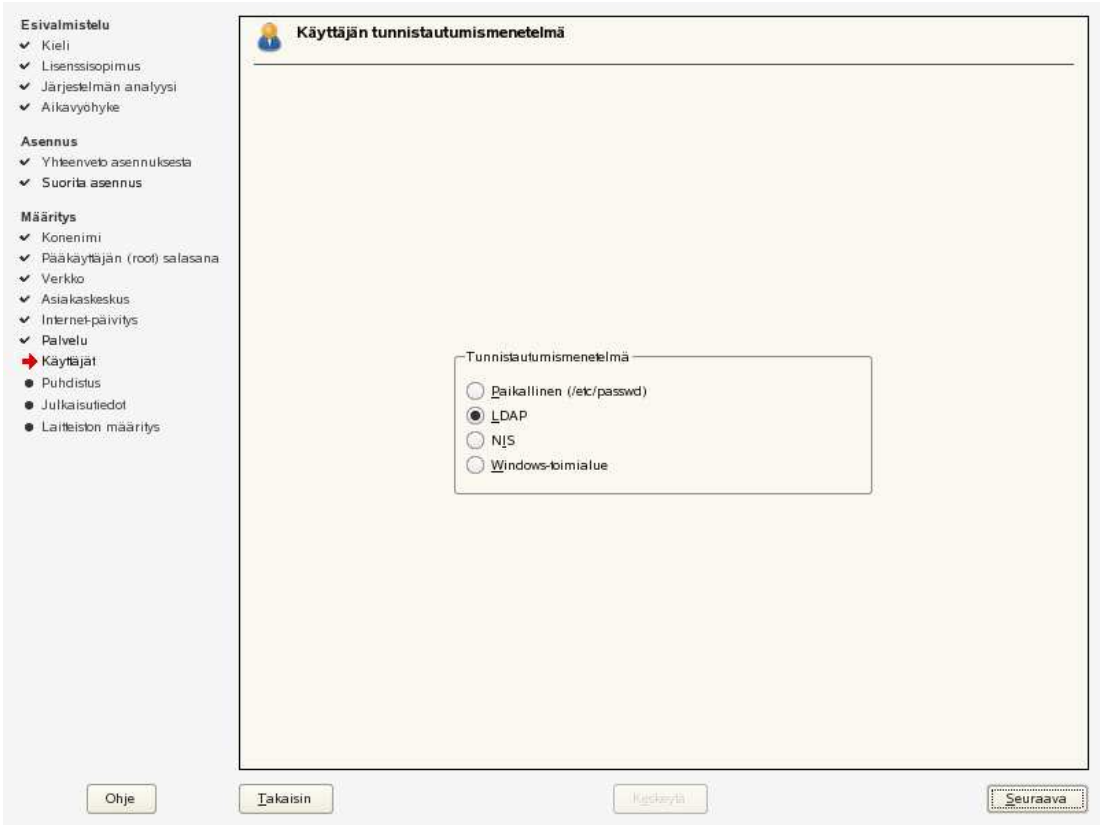
LDAP Salasana. Pääkäyttäjän salasana..

Tietokanta hakemisto. Polku hakemistoon jossa tieto kanta sijaitsee.

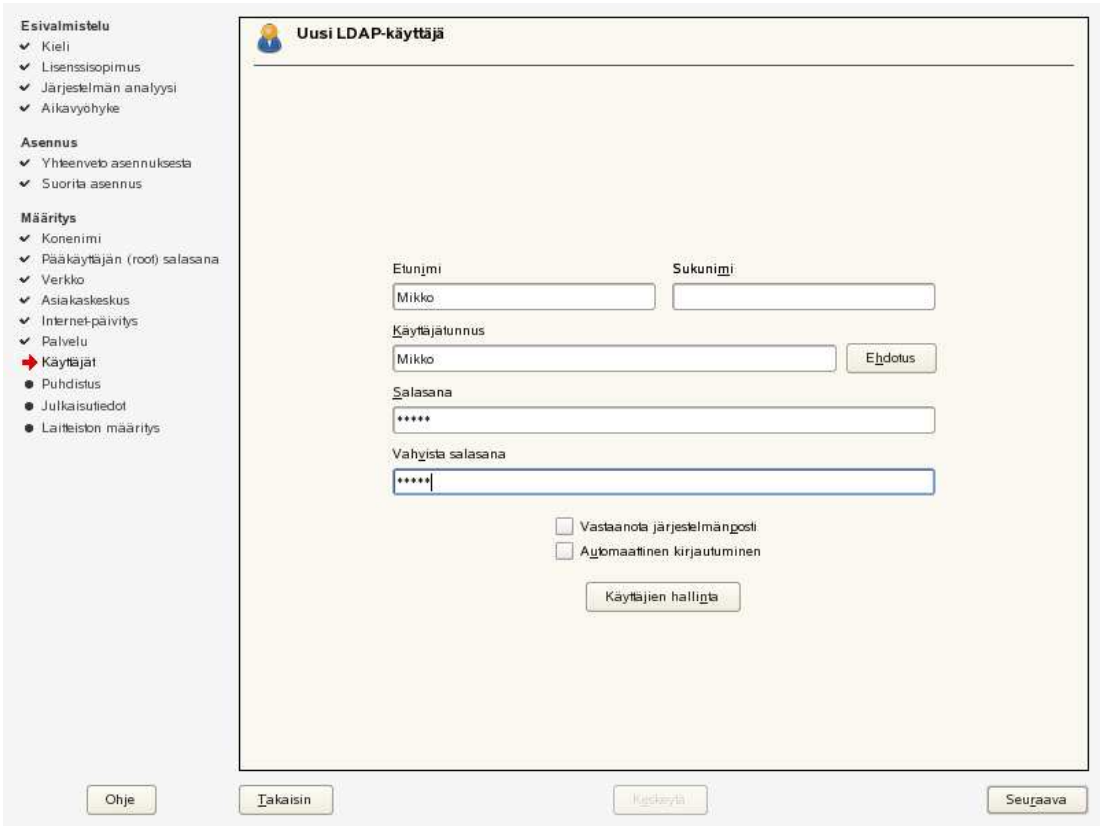
Kuva 5.7 Asetuksen määritykset



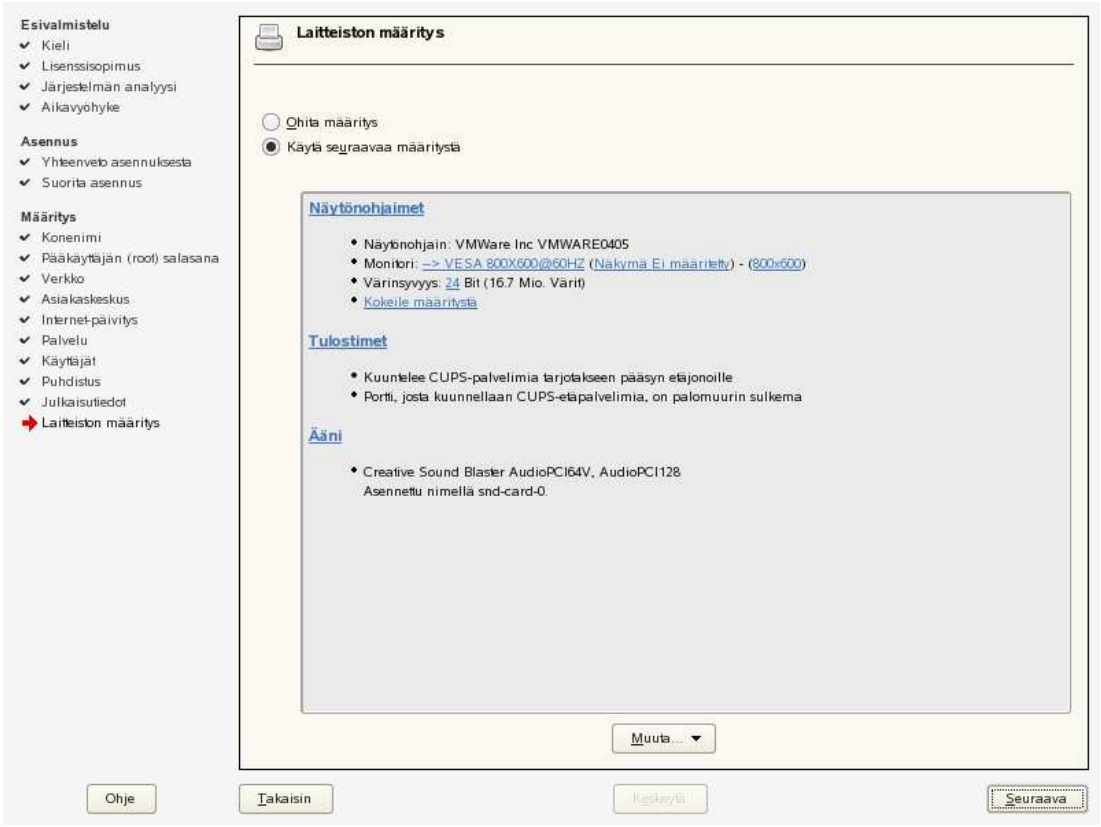
Kuva 5.8 Tunistusmenetelmät



Kuva 5.9 Käyttäjän luonti

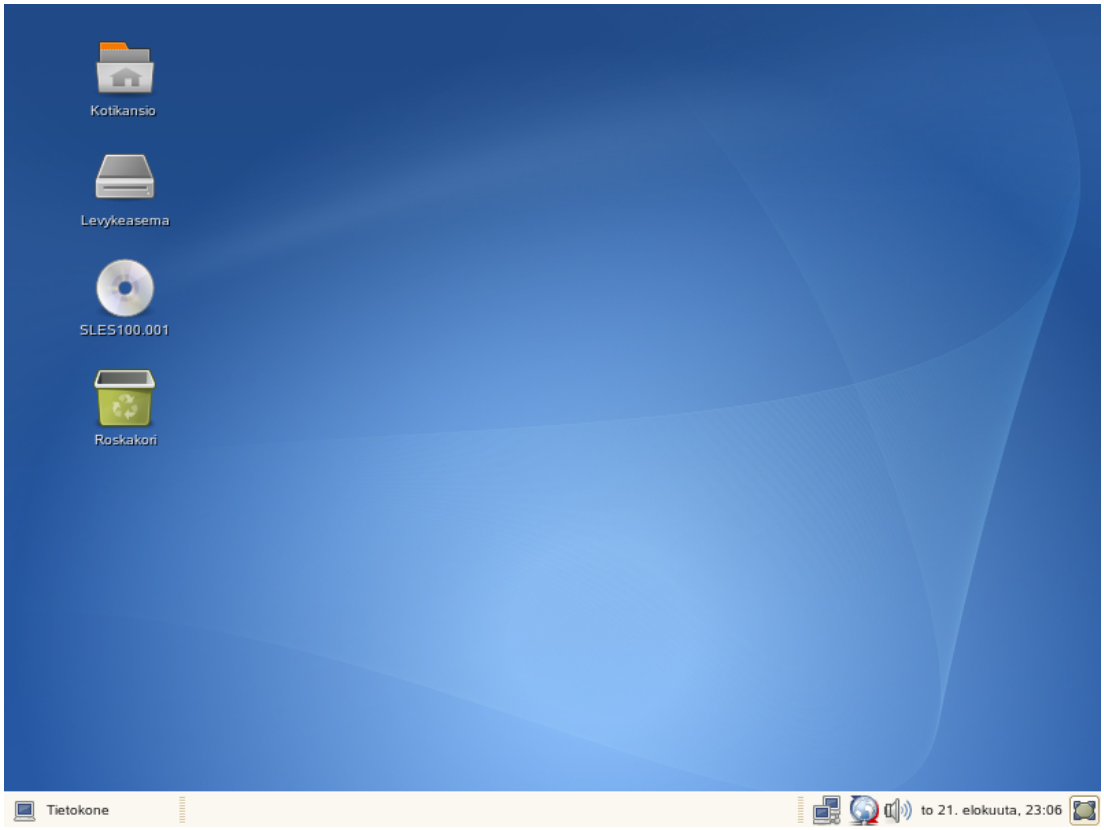


Kuva 5.10 Luodut määritykset



Lopuksi näemme laitteestoon liittyviä määrityksiä. LDAP:n kanssa tarvitaan kolme pakettia: openldap2, pam_ldap ja mss_ldap. Tämän jälkeen asennus viimeistellään käyttö valmiiksi.

Kuva 5.11 Työpöytä



5.2 FreeRADIUS

Paketin haku ja asennus koneelle.

cd /usr/src/packages/

2.wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.0.5.tar.gz

3. tar –zxf freeradius-server-2.0.5.tar.gz

4. asennus komennolla ./configure

5. make

6. make install

Jos ./configure-komennolla tulee virhe. Voi virheen tuottaa mm.puuttuvat kirjasto-paketit jotka saadaan hakemalla paketinhallinta ohjelmmalla kuten Yast.

Konfigurointi:

Kaikki konfiguroitavat tiedostot ovat hakemistossa /etc/raddb.
Konfiguroitavat tiedostot ovat: clients.conf, radiusd.conf, ldap

Muita tiedostoja jotka ovat tärkeitä:

- users
  - tiedostossa on kaikki tunnistukseen liittyvät turvallisuustiedot jokaiselle järjestelmään liittyvälle asiakkaalle.
  - jokaisella asiakkaalla on oma osio, jossa määritellään käyttäjänimi, tunnistukseen liittyviä muuttujia, kuten salasana ja porttinumero.

- hints
  - tiedosto sisältää tiedot kuinka FreeRADIUS palvelee asiakasta käyttäjänimen perusteella. Jos esimerkiksi käyttäjänimi on user ja asiakas on määritetty käyttämään rlogin-yhteyttä voi käyttäjä kirjautua sisään esimerkiksi käyttäjänimellä Puser ja saada PPP-yhteyden.

- huntgroups
  - tiedostossa on erilaisia joukkoja, jotka sisältävät tiedot eri porteista tai muista asiakkaan kommunikointikanavista.
  - Jos käyttäjällä on salasana johonkin huntgoupiin, hän voi saada esimerkiksi kiinteän IP-osoitteen.

5.2.1 clients.conf

/usr/local/etc/raddb/clients.conf
Sisältää tiedot asiakkaista jotka ovat valtuutettuja ottamaan yhteyden FreeRADIUS-palvelimelle. Clients.conf-tiedostossa on jo valmiiksi joitain esimerkkiasiakkaita, kuten localhost ja joitain DEFAULT-määrityksiä.

Aseta jaettu salaisuus ja nimi jokaiselle Radiuksen asiakkaalle jotka ovat tarkoitettu ottamaan yhteyttä serveriin. Voi myös numeroida jokaisen käyttäjän erikseen tai voi käyttää ”globaalia” salausta kaikissa laitteissa.

Esimerkiksi seuraavasti:

Single Client:
client 180.44.200.9 {
{
Secret = hpsecret
Shortname = nm4104_SNPW2
}
Network Global:
client 180.44.200.0/24
{
secret = hpsecret
shortname = nirvana
}

5.2.2 radiusd.conf

/usr/local/etc/raddb/radiusd.conf

Tiedosto sisältää lähes kaikki RADIUS-palvelimen perustoimintoihin liittyvät optiot ja toimintaohjeet.
RADIUS-palvelimen keskeisin konfigurointi-tiedosto ja muistuttaa Apachen httpd.conf-tiedostoa.
Tiedostossa on oletuksena kommentoitu pois käytöstä järjestelmän salasanojen sijainnit. FreeRADIUS tarvitsee näitä tiedostoja käynnistyksessä joten ne otettiin käyttöön poistamalla kommentointi kohdista:

passwd = etc/passwd

shadow = etc/shadow
group = etc/group

5.2.3 ldap

Ldap alueen asetuksilla voidaa yhdistyä suoraan eDirectory serveriin. Muuntamalla seuraavia parametrejä.

server = "AITTATEAMI"

Tämä nimi on serverin nimi ja sen pitäisi olla yhdenmukainen nimen kanssa joka lähetetään todistuksena eteen pain. Jotta ne voidaan tunnistaa yhdeksi ja samaksi

identity = "dn=AITTATEAMI,cn=Administrator"

Tässä pitäisi olla sisältö administrator-käyttäjän tiedoista eDirectory:lla. Käytetään työssä seuraavia

dn= AITTATEAMI, cn=Administrator**.**
password = *********

Tähän kohtaan laitetaan administrator-käyttäjän salasana.

basedn = " AITTATEAMI "

Näillä tiedoilla FreeRADIUS etsii autentikoivaa käyttäjää. Tarkoittaen että serveri etsii näillä tiedoilla tunnistettavaa käyttäjää joka yrittää langattomasti päästa verkkoon.

start_tls = no

Laitetaan vaihtoehto kylle(yes) equal:tille. Tarkoittaen että tämä kertoo RADIUS serverille että käyttää turvattua liikenneyhteyttä LDAP serveriin(eDirectory).

tls_cacertfile = /path/to/cacert.pem

Tähän laitetaan ROOT CA tunnistaumis tiedoston osoite Root CA. Käytämme osoitetta: /etc/raddb/certs/rootcert.pem

access_attr = "dialupAccess"

Vaihdetaan tähän wirelessAccess eli langaton pääsy. Tämä atribuutti etsii käyttäjiä joilla on oikeus päästä läpi.

password_attribute = nspmPassword

Nämä tiedot ldap alueelle. Tässä yksityiskohtaisesti eritellään LDAP attribuutti jossa salasanat on varastoitu.

```
ldap {
        server = "192.168.20.11"
        identity = "cn=Administrator"
        password = pass
        basedn = " dn=AITTATEAMI "
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        start_tls = yes
        tls_cacertfile    = /etc/raddb/certs/rootcert.pem
        access_attr = "wirelessAccess1"
        password_attribute = nspmPassword
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        ldap_connections_number = 5
        timeout = 4
        timelimit = 3
        net_timeout = 1
        }
```

Muutetaan tiedostoa osoitteessa /etc/raddb/users.

Tarkoitus on tyhjentää tiedosto koska käytetää LDAP hakemistoa tämän sijasta.
Mutta jos ei tahdo tyhjentää sitä voi korvata seuraavan lauseen:
DEFAULT Auth-Type = System
Lauseella:
DEFAULT Auth-Type = LDAP

5.3 eDirectory 8.8: asennus

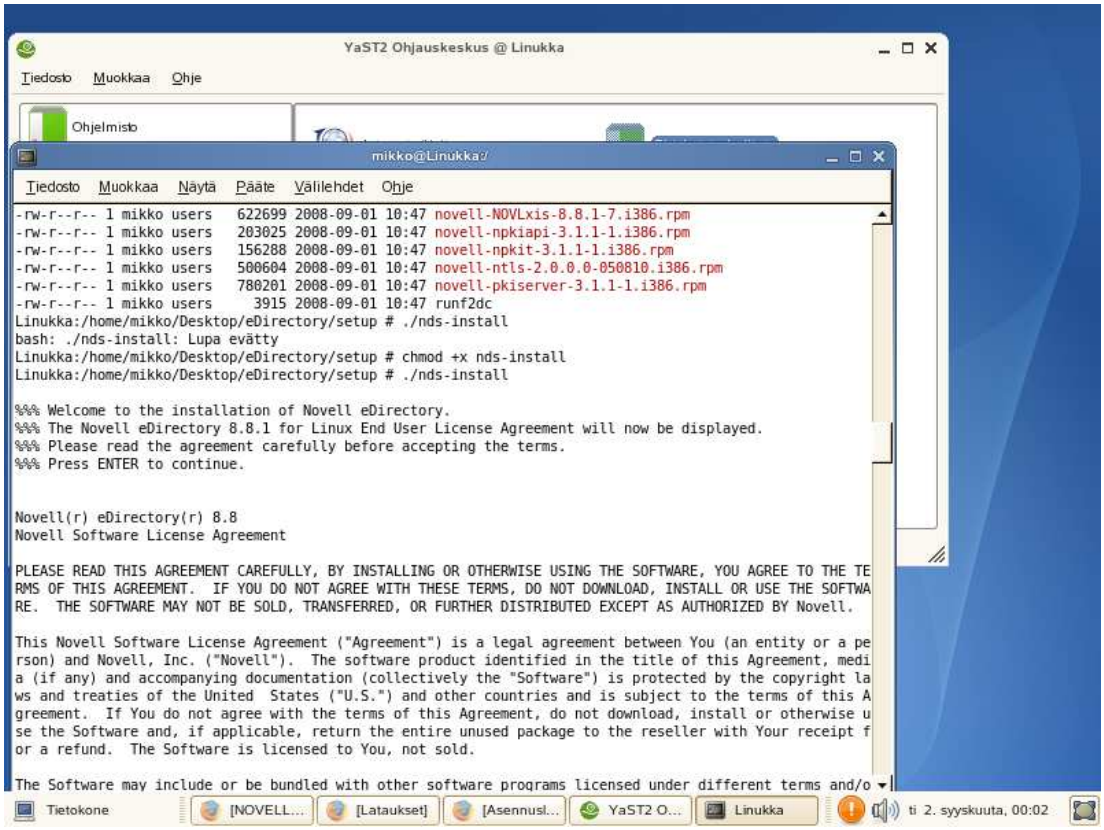
Ohjelmat saa kirjautumalla download.novell.com sivulle ja sieltä etsimällä eDirectory.

http://download.novell.com/sendredirect?target=%2Fprot%2FWfdwR1NwYBg%7E%2F20060526_0800_Linux_88-SP1_FINAL.iso&buildid=WfdwR1NwYBg~&fileid=mPGY7myYFI4~&mirror=AkamaiHost&nohost=false

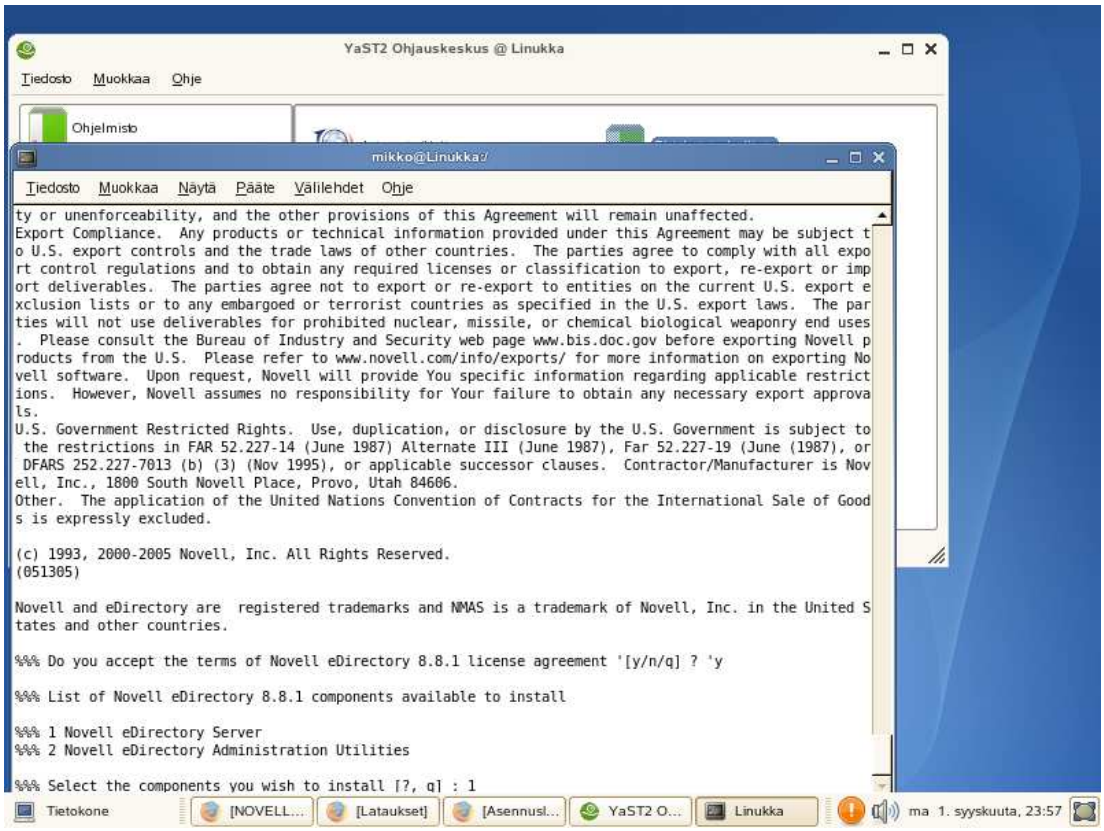
eDirectory oli image muodossa. Puretun ohjelman jälkeen päästään käsiksi Setup kansioon jossa sijaitsee nds-install.
Jos komennolla ./nds-install tulee ilmoitus ”Lupa evätty”.

Komennoilla “chmod +x nds-install” pääkäyttäjä tilassa annettan oikeudet tälle ohjelmalle. Tämän jälkeen ”./nds-install” jonka jälkeen asennus alkaan.

Kuva 5.11 eDirectory:n asennus



Kuva 5.12 Työssä käytetään Palvelin osaa.



5.4 Freeradiuksen asetukset eDirectory:n kanssa

Seuraavassa ldap alue tiedostosta radiusd.conf.

```
ldap {
#
# Note that this needs to match the name in the LDAP
# server certificate, if you're using ldaps.
server = "AITTATEAMI"
port = 636
identity = "cn=Administrator"
password = *******
basedn = " dn=AITTATEAMI "
filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
base_filter = "(objectclass=radiusprofile)"
# How many connections to keep open to the LDAP server.
# This saves time over opening a new LDAP socket for
# every authentication request.
ldap_connections_number = 5

# seconds to wait for LDAP query to finish. default: 20
timeout = 4

# seconds LDAP server has to process the query (server-side
# time limit). default: 20
#
# LDAP_OPT_TIMELIMIT is set to this value.
timelimit = 3

#
# seconds to wait for response of the server. (network
# failures) default: 10
#
# LDAP_OPT_NETWORK_TIMEOUT is set to this value.
net_timeout = 1

#
# This subsection configures the tls related items
# that control how FreeRADIUS connects to an LDAP
```

```
# server. It contains all of the "tls_*" configuration
# entries used in older versions of FreeRADIUS. Those
# configuration entries can still be used, but we recommend
# using these.
#
tls {
# Set this to 'yes' to use TLS encrypted connections
# to the LDAP database by using the StartTLS extended
# operation.
#
# The StartTLS operation is supposed to be
# used with normal ldap connections instead of
# using ldaps (port 636) connections
start_tls = no

cacertfile = /etc/raddb/certs/MY-TREE_CA.b64
# cacertdir = /path/to/ca/dir/
# certfile = /path/to/radius.crt
# keyfile = /path/to/radius.key
# randfile = /path/to/rnd

# Certificate Verification requirements. Can be:
# "never" (don't even bother trying)
# "allow" (try, but don't fail if the cerificate
# can't be verified)
# "demand" (fail if the certificate doesn't verify.)
#
# The default is "allow"
require_cert = "allow"
}

default_profile = "cn=default_radius_profile,o=acme"
profile_attribute = "radiusProfileDn"
access_attr = "dialupAccess"

# Mapping of RADIUS dictionary attributes to LDAP
# directory attributes.
dictionary_mapping = ${confdir}/ldap.attrmap
```

```
# Set password_attribute = nspmPassword to get the
# user's password from a Novell eDirectory
# backend. This will work ONLY IF FreeRADIUS has been
# built with the --with-edir configure option.
#
# See also the following links:
#

# Novell may require TLS encrypted sessions before returning
# the user's password.
#
password_attribute = nspmPassword

# Un-comment the following to disable Novell
# eDirectory account policy check and intruder
# detection. This will work *only if* FreeRADIUS is
# configured to build with --with-edir option.
#
edir_account_policy_check = yes

#
# Group membership checking. Disabled by default.
#
# groupname_attribute = cn
# groupmembership_filter =
"(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=3DGroupOfUniqueNames)(uniq uemem-
ber=%{Ldap-UserDn})))"
# groupmembership_attribute = radiusGroupName

# compare_check_items = yes
# do_xlat = yes
# access_attr_used_for_allow = yes

#
# By default, if the packet contains a User-Password,
# and no other module is configured to handle the
```

```
# authentication, the LDAP module sets itself to do
# LDAP bind for authentication.
#

#
# You can disable this behavior by setting the following
# configuration entry to "no".
#
# allowed values: {no, yes}
set_auth_type = no

# ldap_debug: debug flag for LDAP SDK
# (see OpenLDAP documentation). Set this to enable
# huge amounts of LDAP debugging on the screen.
# You should only use this if you are an LDAP expert.
#
# default: 0x0000 (no debugging messages)
# Example:(LDAP_DEBUG_FILTER+LDAP_DEBUG_CONNS)
ldap_debug = 0x0028
}
```

5.4.1 authorize

“authorize” eli valtuutetut alueelta poistetaan seuraavasti kommentti kentät(eli poistetaan #-merkit).

Ennen:

```
  #
  #  The ldap module will set Auth-Type to LDAP if it has not
  #  already been set
  # ldap
```

Jälkeen:

```
        #
        #  The ldap module will set Auth-Type to LDAP if it has not
        #  already been set
        ldap
```

5.4.2 authenticate

Autentikointi alueelta poistetaan kommentti kentät seuraavasti

Ennen:

```
#       Auth-Type LDAP {
#               ldap
#       }
```

Jälkeen:

```
        Auth-Type LDAP {
                ldap
        }
```

post-auth

Post-auth alueelta täytyy poistaa kommentti kentät ldap and chage the Post-Auth-Type.Seuraavasti

Ennen:

```
#       ldap
        #
        #  Access-Reject packets are sent through the REJECT sub-section of the
        #  post-auth section.
        #  Uncomment the following and set the module name to the ldap instance
        #  name if you have set 'edir_account_policy_check = yes' in the ldap
        #  module sub-section of the 'modules' section.
        #
```

```
#       Post-Auth-Type REJECT {
#               insert-module-name-here
#       }
```

Jälkeen:

```
        ldap
        #
        #  Access-Reject packets are sent through the REJECT sub-section of the
        #  post-auth section.
        #  Uncomment the following and set the module name to the ldap instance
        #  name if you have set 'edir_account_policy_check = yes' in the ldap
        #  module sub-section of the 'modules' section.
        #
        Post-Auth-Type REJECT {
                ldap
        }
```

5.4.3 eap.conf

Tämä tiedosto pitaä sisällään EAP:n eli Extensible Authentication Protocol asetukset. Tarkoittaa protokollaa joka kommunikoi autentikoinnin yhteydessä. Käytetään projektissa TLS konjuktiota EAP purun kanssa.

5.4.4 eap

Eap alueella muutetaan default_eap_type:n.
Ennen se näytti tältä
default_eap_type = md5
muutettiin se:
default_eap_type = peap

5.4.5 tls

Tls-alueelta ensiksi poistettaan kommentti osuudet kentästä. Eli poistetaan # ennen tls { ja sen loppu sulun jälkeen }. Jonka jälkeen muutetaan muutamia parametrejä

private_key_password = whatever

Muutetaan salasana omaksi yksityisavaimeksi.

private_key_file = ${raddbdir}/certs/cert-srv.pem

Asetettiin tähän osoite jossa sijaitsee tiedosto joka sisältää luodun yksityisen avaimen eli private_key:n.

Tiedosto siirrettiin on osoitteeseen

/etc/raddb/certs/servercert.pem.

certificate_file = ${raddbdir}/certs/cert-srv.pem

Laitetaan tähän sama kuin yläpuolella koska pyritään laittamaan varmistus ja yksityinen avain samaan tiedostoon. Käytetään tässä osoitetta:
/etc/raddb/certs/servercert.pem.

CA_file = ${raddbdir}/certs/demoCA/cacert.pem

Set this to the file that contains the Root CA’s certificate. We exported this from

YasT to **/etc/raddb/certs/rootcert.pem**.

#dh_file = ${raddbdir}/certs/dh
#random_file = ${raddbdir}/certs/random
Poistetaan kommentti merkit. Tls näyttää seuraavanlaiselta:

```
tls {
        private_key_password = pass
        private_key_file = /etc/raddb/certs/servercert.pem

        #  Jos Private key sekä Certificate sijaitsevat samassa
        #  tiedostossa, niin private_key_file ja
        #  certificate_file täytyy olla sama nimi

        certificate_file = /etc/raddb/certs/servercert.pem

        #  Luotettava eli Trusted pääkäyttäjän “Root” CA lista
        CA_file = /etc/raddb/certs/rootcert.pem

        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
    }
```

5.4.6 peap

Peap alueelta poistetaan kommentti merkit ainoastaan kentän aloitus ja lopetus {} suluista sekä default_eap_type kohdasta.

Ennen:

```
    # peap {
        #  The tunneled EAP session needs a default
        #  EAP type which is separate from the one for
        #  the non-tunneled EAP module.  Inside of the
        #  PEAP tunnel, we recommend using MS-CHAPv2,
        #  as that is the default type supported by
        #  Windows clients.
        #default_eap_type = mschapv2
    #}
```

Jälkeen:

```
peap {
        #  The tunneled EAP session needs a default
        #  EAP type which is separate from the one for
        #  the non-tunneled EAP module.  Inside of the
        #  PEAP tunnel, we recommend using MS-CHAPv2,
        #  as that is the default type supported by
        #  Windows clients.
        default_eap_type = mschapv2
}
```

Käynnistetään RADIUS-palvelin

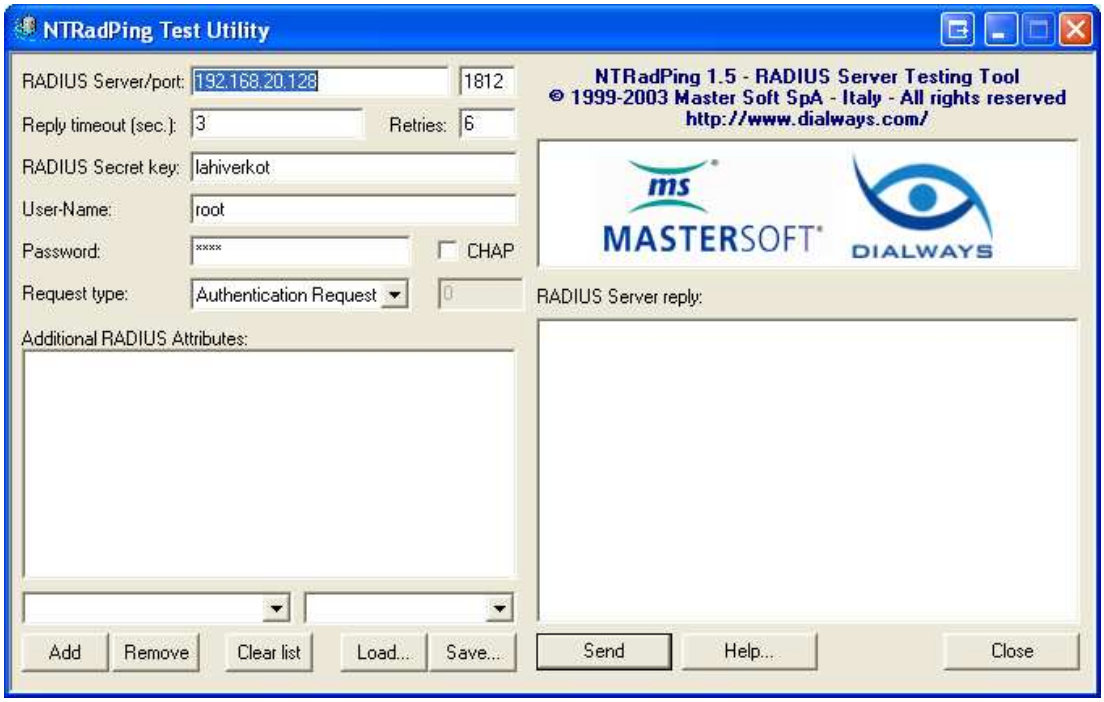
Radiusd

Palvelimen toiminta testattiin radtest-ohjelmalla käytteäen seuraavia asetuksia.

radtest root 6218lahiverkot localhost 0 6218lahiverkot, missä
root – käyttäjätunnus,
6218lahiverkot – salasana,
localhost – testiä varten määritetty asiakas ja
6218lahiverkot – jaettu salaisuus.
Vastauksena Access-Accept

Testattiin myös NTRadPing-ohjelmalla.

Kuva 5.13 NTRadPing



6 YHTEENVETO

Projektin asetukset testattiin virtuaalisesti. Työ aloitettiin tutustumalla tarvittaviin työkaluihin ja ympäristöön. Koska työkalut olivat ennestään tuntemattomia. Linux-ympäristön heikko tuntemus tuotti alussa vaikeuksia. Siihen tutustuminen ja materiaalin laaja valikoima helpotti järjestelmän oppimista. Virtuaalinen työympäristö auttoi testauksessa paljon. Näin saatiin tietoa asetuksista ja työn kuluessa näin parantamaan niitä.

Nakkilan taide ja käsityö koulu otti käyttöön koko uuden järjestelmän joka piti itsessään sisällä langattoman käyttäjän autentikoinnin. Tehty projekti jäi uuden järjestelmän ulkopuolelle. Koko uuden järjestelmän käyttöön otto yksinkertaistaa sen sisäisten asetuksien muokkaamista ja näin vähentää eri ohjelmistojen konflikteja.

Vaikka yksittäisten ohjelmien sulauttaminen suurempaan voisi helpottaa tiettyjen yksittäisten asetusten muokkaamista, mutta näin myös aiheuttaa enemmän virheitä. Tulevaisuutta ajatellen, Linux-ympäristön vapaa lähdekoodi-periaate antaa hyvät mahdollisuudet laajentaa ohjelmistoa erikouluissa. Huomioon ottaen myös taloudelliset säästöt verrattavissa kaupallisiin järjestelmiin.

LÄHTEET

[1] RADIUS,Jonathan Hassell,O'Reilly,October 2002

[2] Authentication HOW TO (http://www.tldp.org/HOWTO/8021X-HOWTO/)

[3] HOW TO: EAP/TLS Setup for FreeRADIUS and Windows XP Supplicant

(http://www.freeradius.org/doc/EAPTLS.pdf)

[4] Authentication Setup

(http://text.dslreports.com/forum/remark,9286052~mode=flat)

[5] Information on security in wireless networks. (http://www.sans.org/rr/whitepapers/wireless/171.php)

[6] IS IEEE 802.1X Ready for General Deployment?

(http://www.sans.org/rr/whitepapers/casestudies/709.php)

[7] An Initial Security Analysis of the IEEE 802.1X Standard

(http://www.funk.com/radius/Solns/umdresp_wp.asp)

[8]IEEE 802.1X For Wireless LANs

(http://www.ieee802.org/1/files/public/docs2000/ieee_plenary.PDF)

[9] 802.1X Still Evolving as a Standard

(http://www.mtghouse.com/8021X.pdf)

[10] http://freeradius.org/

[11]http://en.wikipedia.org/wiki/FreeRADIUS

[12] http://vuksan.com/linux/dot1x/802-1x-LDAP.html

[13] http://www.ietf.org/rfc/rfc3078.txt

[14]http://fi.wikipedia.org/wiki/Novell_eDirectory

[15] http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[16] LDAP-autentikointi eri käyttöjärjestelmissä / Tomi Nordberg.2008

[17] LDAP Directories Explained: An Introduction and Analysis. Brian Arkills,2003

[18] LDAP System Administration, Gerald Carter,2003

[19] Hassell, J. 2002. RADIUS. O'Reilly & Associates.

[20] Wahl, M. et. al.: Lightweight Directory Access Protocol (v3), RFC

2251, The Internet Society, 1997.

[21] RFC 3580 Authentication Dial In User Service (RADIUS),2003

[22] Integrating Novell eDirectory with FreeRADIUS Administration Guide10, 2005

[23] Linux-Serveri, Pekka Riikonen ja Janne Rotko,1999

[24] THE BOOK OF VMware,2002, Brian Ward.

[25] www.novell.com

[26] AAA AND NETWORK SECURITY FOR MOBILE ACCESS RADIUS, Madjid and Mahsa Nakhjiri, 2005

[27] http://fi.wikipedia.org/wiki/Novell