SAVONIA

Langaton vierailijaverkko

Veli-Matti Strengell

Opinnäytetyö

___. ___. _____ _____

Ammattikorkeakoulututkinto

SAVONIA-AMMATTIKORKEAKOULU **OPINNÄYTETYÖ**
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Veli-Matti Strengell	
Työn nimi Langaton vierailijaverkko	
Päiväys 4.6.2012	Sivumäärä/Liitteet 44/3
Ohjaaja(t) Matti Kuosmanen, Tietohallintopäällikkö	
Toimeksiantaja/Yhteistyökumppani(t) Kuopion ev.lut. seurakuntayhtymä	

Tiivistelmä

Tässä työssä selvitettiin, miten yritykseen voidaan suunnitella ja toteuttaa vierailijaverkko yrityksen oman sisäverkon rinnalle. Työ tehtiin Kuopion ev.lut. seurakuntayhtymälle.

Työssä tutustuttiin erilaisiin tekniikoihin, joita langattomat lähiverkot käyttävät sekä vierailijaverkon perusideaan. Selvitettiin mitä kaikkea langattoman vierailijaverkon suunnitteluvaiheessa tuli ottaa huomioon. Lisäksi vertailtiin hieman kolmea eri toteutustapaa, joilla työ olisi voitu toteuttaa.

Työ toteutettiin vapaaseen lähdekoodiin perustuvaa Captive Portal -ratkaisua käyttäen. Työ oli kokeiluluontoinen projekti, joten tästä syystä kustannustehokas ratkaisu nähtiin parhaimmaksi vaihtoehdoksi. Lisäksi työssä apuna käytettiin Captive portal -ohjelmiston keskustelupalstoja, joista tietoa löytyi niukasti. Työn lopputuloksena saatiin toteutettua toimiva vierailijaverkko Kuopion ev.lut. seurakuntayhtymän toimitiloihin.

Avainsanat
Vierailijaverkko, WLAN, CoovaChilli,Linux

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Veli-Matti Strengell			
Title of Thesis Wireless guest WLAN			
Date	4 June 2012	Pages/Appendices	44/3
Supervisor(s) Mr Matti Kuosmanen, IT Manager			
Client Organisation /Partners The Evangelical Lutheran Church of Kuopio			

Abstract

The purpose of this study was to examine how to purchase a guest access network to a company's infrastructure. This study was made for The Evangelical Lutheran Church of Kuopio.

First, the techniques that wireless local area networks use were introduced. Also the basic idea of a visitor network was explained. Then, the means of designing and implementing a visitor network were shown.The work was done using an open source based captive portal-solution. The task was an experimental project and because of this, the cost efficient solution was the best choice. A captive portal-sofware forum was used as an additional source for aid.

As a result, the thesis was successfully completed. The Evangelical Lutheran Church of Kuopio now has a wireless visitor access network in their facilities.

Keywords
Guest WLAN, CoovaChilli, Linux

SISÄLTÖ

LIITTEET

Liite 1 Vierailijaverkon palvelimen ohje

TERMIT JA LYHENTEET

3G	Third Generation, Lyhenne kolmannen sukupolven matkapuhelinteknologioille.
ADSL	Asymmetric Digital Subscriber Line, Modeemitekniikka.
AES	Advanced Encryption Standard, Lohkosalausmenetelmä.
CCK	Complementary Code Keying, Langattomassa lähiverkossa käytetty modulaatio kaava.
CCMP	Counter Mode with CBC-MAC Protocol, Langattomien lähiverkkojen salausprotokolla liikennöitävän tiedon suojaamiseen.
DHCP	Dynamic Host Configuration Protocol, Verkkoprotokolla, jonka tehtävä on jakaa IP-osoitteita uusille lähiverkkoon kytkeytyville laitteille.
IEEE	Institute of Electrical and Electronics Engineers, Kansainvälinen tekniikanalanjärjestö.
IR	Infrared, Infrapunavalo.
ISM	Industrial, Scientific and Medical, ISM-tajuusalue on maailmanlaajuinen radiotaajuuskaista.
LAN	Local Area Network, Lähiverkko.
LINUX	Moniajoa tukeva käyttöjärjestelmä.
MAC	Yksilöllinen tunniste verkkokortilla.
MYSQL	Tietokanta järjestelmä.
NAT	Network Address Translation, Osoitteenmuunnos.
OFDM	Orthogonal Frequency Division Multiplexing, Modulointi, jota käytetään useissa erilaisissa tiedonsiirtojärjestelmissä.
PSK	PreShared Key, Termi, jota käytetään, kun määritellään miten salausavain jaetaan käyttäjille.
QoS	Quality of Service, Termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia.
RADIUS	Remote Authentication Dial In User Service, Tunnistukseen ja valtuutuksien määrittelyyn käytettävä protokolla.
RF	Radio Frequency, Radiotaajuudet.
TKIP	Temporal Key Integrity Protocol, Langattomien lähiverkkojen tietoturvaprotokolla.
WEP	Wired Equivalent Privacy, Langattomien lähiverkkojen tietoturvaprotokolla.

Wi-Fi	Wireless Fidelity, Toinen sana WLAN:lle.
WLAN	Wireless Local Area Network, Langaton lähiverkko.
WPA	Wi-Fi Protected Access, Välivaiheen tietoturvatekniikka.

1 JOHDANTO

Tässä opinnäytetyössä tutkitaan ja selvitetään, kuinka voidaan luoda yritykselle turvallinen ja helppokäyttöinen langaton vierailijaverkko sekä mitä kaikkea on otettava huomioon langatonta vierailijaverkkoa luotaessa. Työ on toteutettu Kuopion ev.lut. seurakuntayhtymälle, joten Kuopion ev.lut. seurakuntayhtymä käytetään opinnäytetyössä esimerkkinä. Kaikki tehdyt toteutukset perustuvat seurakuntayhtymän tarpeisiin.

Seurakuntayhtymä hoitaa kaikkien seurakuntien tehtäviä, jotka on määritetty seurakuntayhtymän perussäännöissä. Näihin tehtäviin kuuluvat aina vähintään taloushallinto ja henkilöstöhallinto. Lisäksi seurakunnat voivat antaa muitakin tehtäviä seurakuntayhtymän hoidettavaksi.

Kuopion ev.lut. seurakuntayhtymän tiloissa vierailee viikoittain paljon asiakkaita ja yrityskäynnillä olevia henkilöitä, joten tarve päästä Internetiin kasvaa jatkuvasti. Näin ollen Kuopion ev.lut. seurakuntayhtymän tiloissa olisi tarpeen tarjota mahdollisuus päästä käyttämään internetiä, millä ei kuitenkaan vaarannettaisi seurakuntayhtymän oman sisäverkon tietoturvaa.

Seuraavissa luvuissa käydään läpi WLAN-tekniikoita ja -protokollia sekä tutustutaan hallittavaan todentamis- ja kirjautumistekniikkaan. Tämän jälkeen esitellään vierailijaverkon normaaleja vaatimuksia ja asioita, joita vierailijaverkossa tulisi ottaa huomioon. Viimeisenä esitellään esimerkki siitä, kuinka vierailijaverkko asennetaan ja otetaan käyttöön.

2 TEKNIIKKA

2.1 WLAN

Langaton lähiverkko eli WLAN (Wireless Local Area Network) tarkoittaa tekniikkaa, jota käytetään langattomissa lähiverkoissa. WLAN:n avulla voidaan erilaisia verkkolaitteita yhdistää toisiinsa langattomasti eikä näin ollen tarvitse käyttää kaapeleita laitteiden yhdistämiseen. WLAN-termiä on totuttu käyttämään, kun puhutaan eniten yleistyneestä langattomasta IEEE 802.11 -standardista.

Langattomia lähiverkkostandardeja on olemassa useampiakin. Esimerkiksi ETSI (European Telecommunications Standards Institute) on kehittänyt oman langattoman lähiverkkostandardin, jota kutsutaan HiperLAN-standardiksi. HiperLAN-standardin versiot eivät kuitenkaan ole yleistyneet. Tästä syystä yleisessä kielenkäytössä termit WLAN, 802.11 ja Wi-Fi tarkoittavat samaa asiaa, eli 802.11-standardiin pohjautuvaa langatonta lähiverkkoa. Suosituin käytössä oleva versio tällä hetkellä on 802.11g, jonka suurin teoreettinen tiedonsiirtonopeus on 54 Mbps. Nykypäivänä myös versio 802.11n on yleistynyt, koska lähes jokainen uusi langattoman lähiverkon laite tukee 802.11n-versiota, jonka suurin teoreettinen tiedonsiirtonopeus on 600 Mbps. (Wikipedia, WLAN.)

Langattomia lähiverkkoja käytetään paljon kotitalouksissa. Nykyisin uusiin kiinteistöihin rakennetaan myös huoneistokohtaiset sisäverkot, mutta vanhemmissa kiinteistöissä ei välttämättä ole omaa sisäverkkoa. Jotta erillistä sisäverkkoa ei tarvitsisi kaapeloida, käytetään usein langatonta verkkotekniikkaa jakamaan langallista Internet-yhteyttä. Kotitalouteen tulevaan kiinteään Internet-yhteyteen kytkettyyn modeemiin liitetään langaton tukiasema (access point). Jotta yhteys tukiaseman ja tietokoneen välille voidaan muodostaa, tarvitaan tietokoneeseen lähetin-vastaanotin, joka toimii radioteitse tukiaseman kanssa. Langattomat verkkolaitteet hyödyntävät lisenssivapaita radiotaajuuksia. Pöytäkoneeseen voidaan liittää langaton PCI-verkkokortti tai USB-porttiin tuleva lähetin-vastaanotin. Kannettaviin tietokoneisiin voidaan myös liittää USB -porttiin lähetin-vastaanotin tai liittää PCMCIA-porttiin langaton PCMCIA-verkkokortti. Nykyisissä sekä myös hieman vanhemmissa kannettavissa löytyy sisäänrakennettu langaton lähetin-vastaanotin. Myös useilla modeemeilla, jotka kytketään Internet-yhteyteen, on WLAN valmius. (Wikipedia 2011a.)

Langattomien verkkolaitteiden ohella myös monet muut kotitaloudesta löytyvät laitteet hyödyntävät lisenssivapaita radiotaajuuksia tiedonsiirrossa. Jos käytetään maantieteellisesti lähekkäin samaa radiotaajuusaluetta olevaa fyysistä laitetta, synnyttävät ne toisilleen häiriötä tai pahimmassa tapauksessa estävät toistensa toiminnan. Tällaisia laitteita ovat esimerkiksi erilaiset langattomat multimedialaitteet, kuten langattomat kuulokkeet tai televisiokuvan langattomat siirtolaitteet. (Wikipedia, WLAN.)

Langattoman lähiverkon toteuttaminen kiinteän tietoliikenneverkon rinnalle on pääpiirteittään hyvin yksinkertaista ja jopa edullista. Tästä syystä monet elinkeinoharjoittajat, esimerkiksi lentokentät, kahvilat, hotellit ja ravintolat, tarjoavat mahdollisuutta käyttää langatonta lähiverkkoa. Myös monessa kunnassa on otettu kokeiluun tai on jo käytössä toimiva langaton verkko, joka voi kattaa suuren alueen kaupungin keskustasta, jollei koko keskustan aluetta niin ainakin tärkeimmät kunnan tarjoamat palvelut, kuten kirjastot ja koulut. Tällaisia paikkoja, joissa tarjotaan langatonta verkkoa ilmaiseksi tai maksua vastaan, kutsutaan langattoman verkon kuumiksi pisteiksi (WLAN -hotspot) tai vierailijaverkoiksi. Vierailijaverkkojen tarjoaminen on lisääntynyt jatkuvasti ja tarjonta on laajentunut jopa julkisiin kulkuneuvoihin. (Wikipedia 2011a.)

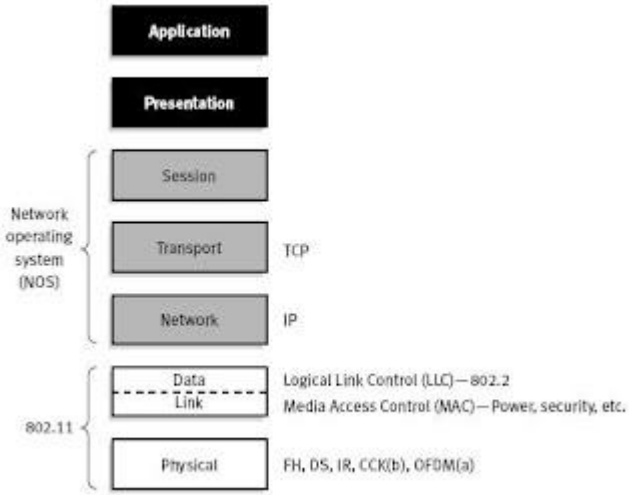
Kokonaiskustannuksissa langattoman verkon verkkolaitteiden osuus on pääsääntöisesti pieni. Kustannuksissa voidaan säästää, kun kiinnitetään huomiota verkon tarkkaan suunnitteluun, tarpeiden kartoittamiseen sekä oikeaoppiseen verkon rakentamiseen. Langattomien verkkojen kattavuus, nopeus, luotettavuus ja tietoturva saattaavat vaihdella, joten tarkka suunnittelu on tärkeää. (Wikipedia 2011a.)

2.2 IEEE 802.11 -standardi

Kansainvälinen tekniikan alan järjestö IEEE (Institute of Electrical and Electronics Engineers) on kehittänyt langattomalle WLAN-lähiverkkotekniikalle IEEE 802.11-standardin. Tämä tekniikka on läheistä sukua Ethernetille (802.3), minkä vuoksi WLAN-tekniikkaa kutsuttiin alkuaikoina langattomaksi Ethernetiksi. Nykyään tekniikkaa markkinoidaan nimellä Wi-Fi. (Wikipedia 2011b.)

Ajan saatossa standartista on kehittynyt useita versioita, joista jokaista versiota kehittämässä on ollut oma työryhmänsä. Jokainen työryhmä on keskittynyt erilaisiin piirteisiin standardeissa. Eri standardi versioita kuvataan tietyllä kirjaimella normaalin 802.11-standardin nimen perässä. Standardiversiot kuvataan nopeusjärjestyksessä,

mutta nimeäminen ei ole aina looginen. Esimerkiksi standardi 802.11a on kehittynyt 802.11b standardin jälkeen. (Wikipedia 2011b.)

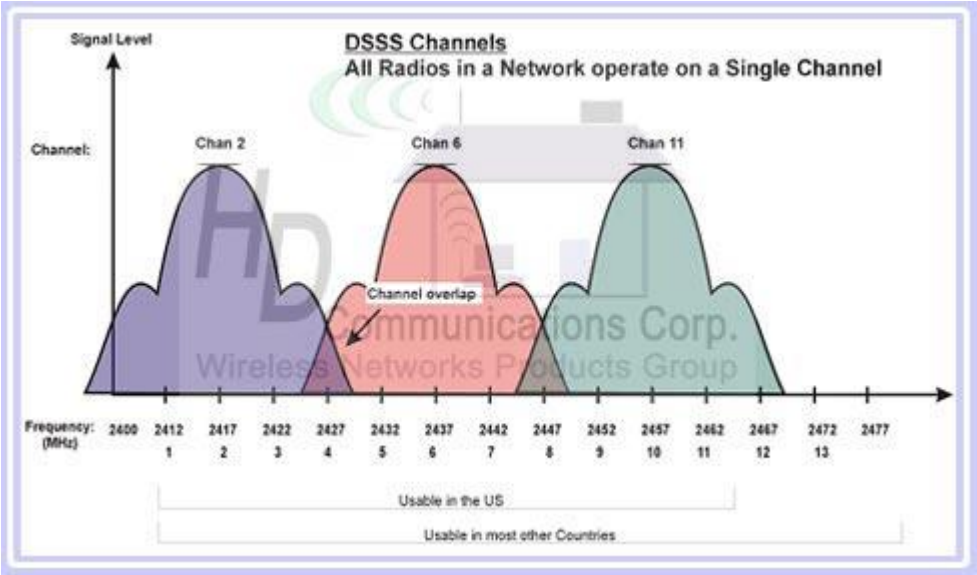


KUVIO 1: 802.11 ja OSI-malli.(IEEE 802.11b 2012. Wireless LAN)

Ensimmäinen WLAN-tekniikka tunnetaan nimellä 802.11. IEEE julkaisi tämän tekniikan 26.7.1997. IEEE esitteli standardin ensimmäisen version jo vuonna 1990, mutta virallinen versio kehittyi kuuden aikaisemman version pohjalta vasta vuonna 1997. standardi 802.11 määrittää pääsääntöisesti OSI -mallin (kuvio 1) alimman kerroksen eli fyysisen kerroksen ja toisen kerroksen eli siirtokerroksen alemman osan. Tämä alue tunnetaan nimellä MAC (Media Access Control). Kyseisen standardin määrittelemät verkkoyhteyksien nopeudet ovat 1 Mbps ja 2 Mbps ja se toimii vapaalla ISM -taajuusalueella, jonka taajuudet ovat 2,4 - 2,4835 Gigahertsiä.

Standardin määrittelemät välitystekniikat ovat infrapuna ja radiotiet. Käytössä olevat radiotaajuustekniikat ovat suorasekvensointi eli DSSS (Direct Sequence Spread Spectrum) (kuvio 2) ja taajuushyppely eli FHSS (Frequency Hopping Spread Spectrum). DSSS-tekniikassa tiedonsiirto toteutetaan lähettämällä tieto 11-bitin sarjoina (Barkerin sarja) verkkolaitteiden välillä.

802.11 standardiin on määritelty kaksi verkkotopologiaa. Ensimmäinen on AdHoc-verkko eli verkko, jossa langattomat laitteet ovat suoraan yhteydessä toisiinsa. Toinen verkkotopologia on infrastruktuuri eli verkko, jossa langattomat laitteet ovat yhteydessä tukiasemiin. (Wikipedia 2011b.)



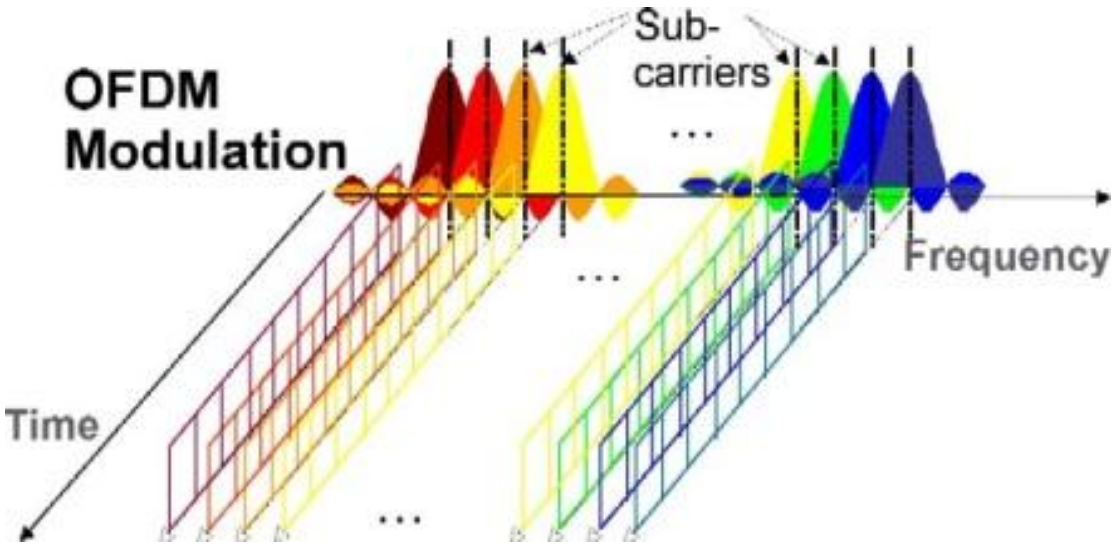
KUVIO 2: DSSS-taajuuskanavat 2,4 GHz (Wireless Technical Fundementals)

Langattomat verkot saivat nopeasti suuren suosion ja koko ajan kehittyvien verkkosovellusten takia ne laajenivat. Nopeudet, jotka oli määritelty 802.11-standardiin, alkoivat käydä liian hitaiksi jonka vuoksi tarvittiin uusi ja nopea standardi, joka vastaisi uusiin vaatimuksiin. (Wikipedia 2011b.)

Vuonna 1999 IEEE julkaisi uuden standardin, joka tunnetaan nimellä 802.11b, mutta siitä käytetään myös nimeä 802.11hr (high rate). Verkkoyhteyden nopeudeksi tässä standardissa on määritelty 5,5 Mbps ja 11 Mbps. Tämä tarkoittaa, että uusi standardi on huomattavasti nopeampi kuin edeltäjänsä 802.11. Standardi 802.11b käyttää edelleen samaa 2,4 GHz:n taajuutta, mutta tiedonsiirtotekniikka DSSS- ja FHSS-tekniikoiden sijasta käytössä on CCK-tekniikka (Complemet Code Keying). Kyseisessä tekniikassa tieto lähetetään 8-bittisenä koodisanoina 64 kappaleen sarjoissa. Jokaisella 8-bittisellä koodisanalla on oma matemaattinen merkitys. Toinen 802.11b-standardiin määritelty tiedonsiirtotekniikka on PBCC -tekniikka (Packet Binary Convolutional Coding), joka tukee 802.11-standardissa käytettyä DSSS -tekniikkaa.

802.11a -standardi julkaistiin myös vuonna 1999 IEEE:n toimesta. Uusi standardi on hyvin samanlaista tekniikkaa kuin aikaisempi 802.11b, mutta toimii korkeammalla taajuusalueella. Uusi 802.11a-standardi toimii 5,150 - 5,350 ja 5,475 - 5725 GHz:n taajuusalueella. Tämä ylemmän taajuusalueen käyttäminen mahdollisti useamman kuin kolmen toisiaan häiritsemättömän kanavan käytön. Suurin syy taajuusalueen nostamiseen oli kuitenkin tarve kasvattaa verkkoyhteyksien kaistaa, jotta tiedonsiirtonopeuksia pystyttäisiin kasvattamaan suuremmiksi.

802.11a-standardi määritteli käytettäväksi myös uuden tiedonsiirtotekniikan, jota aikaisimmissa versioissakin oli käytetty. Uusi tiedonsiirtotekniikka on OFDM-tekniikka (Orthogonal Frequency Division Multiplexing) (kuvio 3), jonka toimintaperiaate on jakaa signaali pienempiin alasignaaleihin. Pienempien alasignaalien lähettäminen yhtäaikaisesti toisilleen häiriöttömillä eri taajuuksilla mahdollistaa jopa teoreettisesti 54 Mbps -nopeuden verkkoyhteyksissä. (Wikipedia 2011b.)



KUVIO 3: OFDM-tekniikan alisignaalit (Building future networks with MIMO and OFDM.)

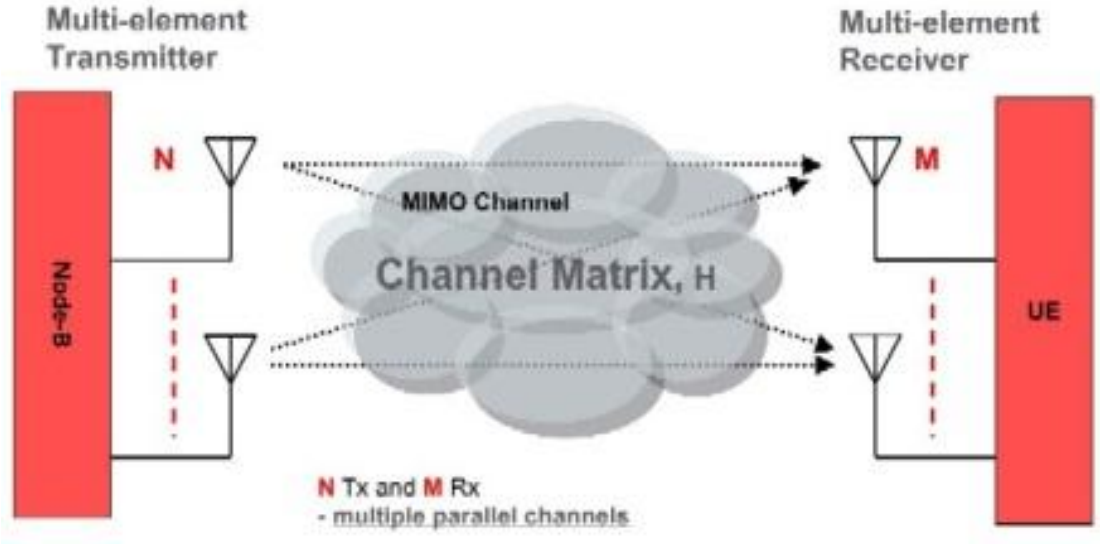
Huomattavista eduista huolimatta 802.11a-standardi ei ole saavuttanut yhtä suurta suosiota kuin minkä 802.11b saavutti. Suurimmat syyt tähän olivat kalliimmat verkkolaitteet sekä langattoman verkon kantaman pieneneminen, joka aiheutuu 802.11a-standardin korkeammasta taajuudesta. (Wikipedia 2011b.)

Vuonna 2003 IEEE julkaisi uuden standardin 802.11g, jonka kehitys aloitettiin jo vuonna 2000. Tällöin uutta standardia varten perustettiin uusi työryhmä, joka kolmessa vuodessa kehitti nykypäivänäkin suositun 802.11g-standardin. 802.11g -standardi perustuu 802.11a- ja 802.11b-standardeihin. Tämä standardi käyttää 802.11b:stä tuttua CCK-tekniikkaa sekä 802.11a:sta tuttua OFDM-tekniikkaa eli CCK-OFDM -tekniikkaa. 802.11g-standardin käyttämä toinen tiedonsiirtotekniikka on PBCC. Standardin määrittelyssä radiotaajuustekniikoita ovat DSSS-, HR-DSSS- ja OFDM-tekniikat. 802.11g-standardi liikennöi nopeuksilla 11 Mbps ja 54 Mbps. (Wikipedia 2011b.)

Suuremman nopeuden ansiosta 802.11g-standardi on syrjäyttänyt 802.11b-standardin yleisessä käytössä. 802.11g toimii myös vapailla IMS -taajuusalueilla, eli käyttää 2,4 Gigahertsin taajuuksia. Tästä syystä 802.11g on yhteensopiva aikaisemman 802.11b:n kanssa. 802.11g -standardilla siis päästään samaan nopeuteen kuin 802.11a:lla, mutta saadaan langattomalle verkolle suurempi kantavuusalue. (Wikipedia 2011b.)

802.11n on niin sanottu lisäominaisuusstandardi, jonka IEEE julkaisi vuonna 2009, ja jolla voidaan parantaa langattoman verkon suorituskykyä verrattuna aiempiin 802.11a- ja 802.11g-standardeihin. Tämä lisäominaisuus, jota kutsutaan myös laajennukseksi, on yhteensopiva taajuuksiltaan 802.11a:n 5 Gigahertsin sekä 802.11g:n 2,4 Gigahertsin taajuusalueita käyttävien standardien kanssa. Yhteensopivuustilassa aikaisempien standardien kanssa 802.11n-standardi pystyy hyödyntämään ainoastaan vanhemman standardin nopeutta. (Wikipedia 2011b.)

Uusi lisäominaisuusstandardi määrittää teoreettiseksi maksiminopeudeksi 600 Mbps. Teoreettisiin nopeuksiin ei normaali käytössä koskaan päästä, joten realistinen nopeus on johon uudella laajennuksella voidaan päästä, on noin 100–200 Mbps. Aikaisempiin standardeihin verrattuna, joiden teoreettinen maksimi nopeus oli 54 Mbps, on 802.11n laajennuksen tuoma lisänopeus huomattava. 802.11n laajennus tukee MIMO-tekniikkaa (Multiple-input Multipe-output) (kuva 4), joka perustuu useamman antennin sekä useamman ilmatien kanavan käyttöön. Tämän ansiosta päästäänkin paljon suurempiin tiedonsiirtonopeuksiin sekä tasaisempaan kantamaan, kuin aikaisimmilla standardeilla. (Wikipedia 2011b.)



KUVIO 4: MIMO -tekniikan periaate (Building future networks with MIMO and OFDM.)

2.3 Tietoturva

Langattoman verkon suunnittelussa ja toteutuksessa on olemassa muutamia menetelmiä, jotka vaikuttavat tiedonsiirron, kirjautumisen sekä langattoman verkon käytön turvallisuuteen. Tällaisia menetelmiä ovat esimerkiksi erilaiset salaukset, käyttäjien autentikointi, pääsylistat, langattoman verkon mainostaminen sekä tukiaseman lähetysteho.

2.3.1 SSID

Langattoman verkon tukiasemat mainostavat itseään. Eli tukiasema lähettää SSID (Service Set ID) -tietoa itsestään koko ajan, jotta käyttäjät voisivat helposti kirjautua langattomaan verkkoon. Näin ollen käyttäjien ei tarvitse muistaa sen langattoman verkon nimeä, johon haluavat liittyä. Uudet tukiasemat ovat yleensä määritetyt mainostamaan omaa SSID:tään. Useimmat tukiasemat voidaan asettaa myös sellaiseen tilaan, että ne ei jaa julkisesti omaa SSID:tään Tällä ominaisuudella jo sellaisenaan voidaan karsia asiattomien henkilöiden pääsyä langattomaan verkkoon. On kuitenkin otettava huomioon, että tämä toimenpide ei sinänsä vaikeuta verkkoon pääsyä, vaan pääsääntöisesti karsii satunnaisia verkon väärinkäyttäjiä. SSID-tieto kulkee tukiaseman ja asiakkaan välillä salaamattomana, joten kun asiakkaan ja tukiaseman välistä liikennettä kuunnellaan tarpeeksi kauan, voidaan piilotettu SSID murtaa. SSID:n piilottaminen ei hidasta henkilöä, joka haluaa murtautua langattoman verkkoon. SSID:n piilottaminen ei siis ole mikään suojaus- tai tunnistusmenetelmä. (Wikipedia 2011c.)

2.3.2 Pääsylista

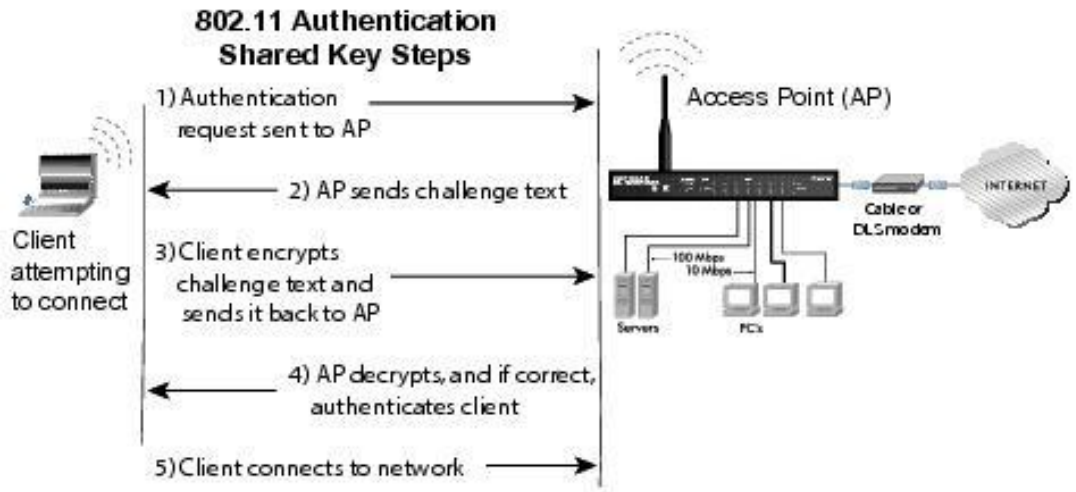
Langattomaan verkkoon pääsyä voidaan rajoittaa monella eri tavalla. Yksi keino on esimerkiksi pääsylistojen käyttäminen. Pääsylistojen (Access List) ideana on pitää listaa asiakaslaitteiden MAC-osoitteista (Media Access Control). Lista sisältää tiedon osoitteista, mitkä omaavat pääsyn verkkoon. Tämä tapa ei ole kovin hyvä, varsinkaan suuremmissa ympäristöissä, koska se lisää ylläpitäjän työmäärää huomattavasti. Jokainen MAC-osoite olisi lisättävä manuaalisesti verkon jokaiseen tukiasemaan. Jotkin laitevalmistajat tarjoavat tuotteita, joista löytyy ohjelmistoja, joilla voidaan hallita pääsylistoja koostetusti. Tämä ei silti poista manuaalista MAC-osoitteiden syöttämistä. Pääsylistojen käyttöä ei pidetä tehokkaana tapana suodattaa käyttäjien pääsyä verkkoon, koska MAC-osoitteita ei salata millään tavalla, vaikka itse data niissä olisikin salakirjoitettu. Verkkoon murtautuja pystyy siis kuuntelemaan erilaisilla verkon kuunteluohjelmilla verkkoliikennettä ja näin selvittämään verkossa käytössä olevan

MAC -osoitteen. Kun MAC-osoite on selvillä, voi hän muuttaa oman verkkokorttinsa vastaamaan kyseistä MAC-osoitetta. (Wikipedia 2011c.)

2.3.3 Autentikointi

Toinen tapa, jolla saadaan rajattua käyttäjien pääsyä langattomaan verkkoon, on käyttäjien tunnistautuminen eli autentikointi. Tunnistautumiseen voidaan käyttää muutamaa eri teknikkaa, kuten WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA-PSK (Pre-shared Key), WPA2 (Wi-Fi Protected Access II) ja WPA2-PSK.

WEP-autentikoinnissa on kaksi tapaa, avoin autentikointi sekä autentikointi, joka käyttää jaettua avainta. Avoimessa autentikoinnissa käyttäjän ei tarvitse syöttää minkäänlaisia tunnuksia tai salasanoja tukiasemalle. Tästä syystä kuka tahansa käyttäjä voikin yhdistäytyä langattomaan verkkoon, eli toisin sanoen minkäänlaista autentikaatiota ei tapahdu. Niin sanotun autentikaation ja yhdistämisen jälkeen WEP-tekniikka voidaan käyttää verkossa liikkuvan datan salaukseen. Toinen toimintaperiaate, jota WEP käyttää on autentikointi jaetulla WEP-avaimella, joka on tukiaseman tiedossa sekä käyttäjän tiedossa. Tässä menetelmässä on neljä vaihetta ennen kuin käyttäjä voi käyttää verkkoa. Ensimmäiseksi asiakaslaite ottaa yhteyttä tukiasemaan ja lähettää tunnistautumispyynnön. Tämän jälkeen tukiasema lähettää asiakaslaitteelle selkokielisen viestin. Asiakaslaiteen täytyy tämän jälkeen salata viesti käyttäen WEP-avainta ja lähettää se salattuna takaisin tukiasemalle. Lopuksi tukiasema purkaa viestin, jonka asiakaslaite on lähettänyt, ja jos se täsmää alkuperäiseen viestiin, jonka tukiasema lähetti on asiakas tämän jälkeen tunnistettu ja pystyy käyttämään yhteyttä, jossa on WEP-salaus (Kuvio 1). (Wikipedia 2011c.)



KUVIO 5: WEP -autentikoinnin vaiheet (NetGear, WEP Shared Key Authentication).

WPA ja WPA2 autentikointitekniikkaa käytettään pääsääntöisesti suurissa verkkoympäristöissä, kuten suurissa yrityksissä, jossa on monta langattoman verkon käyttäjää. WPA ja WPA2 tunnetaan myös nimillä WPA-enterprise ja WPA2-enterprise. WPA2-tekniikka on paranneltu versio WPA-tekniikasta. WPA ja WPA2 tekniikoissa tunnistautumiseen käytetään IEEE 802.1X / EAP-rajapintaa sekä autentikointipalveluprotokollaa (AAA -Protocol, Authentication, Authorization and Accounting). Tunnetuin protokolla on RADIUS (Remote Authentication Dial-In User Service), jonka pääideana on yksi keskitetty tietokanta, josta kaikki verkon käyttäjät voidaan turvallisesti tunnistaa kaikissa olosuhteissa, joissa autentikointiliikenne kuljetetaan autentikointipalvelimelle. (Hovatta 2005, 29.)

Autentikointipalvelimen hyväksyttyä käyttäjän tämä liitetään langattomaan verkkoon. Jos kuitenkin tunnistautuminen epäonnistuu, käyttäjä pysyy eristettynä verkkoon pääsystä. Kun asiakas autentikoidaan, palvelin ja asiakaslaite muodostavat samanaikaisesti PMK (Pairwise Master Key) -avainparin. (Wikipedia 2011c.)

Kun autentikointipalvelin on tunnistanut käyttäjän verkon käyttäjäksi, saatetaan kirjautuminen loppuun käyttäjän ja tukiaseman välillä. Kirjautumiseen tukiaseman ja käyttäjän välillä kuuluu salausavainten muodostaminen ja asentaminen käyttäjälle. Tähän käytetään WPA-tekniikassa TKIP (Temporal Key Integrity Protocol) -protokollaa ja WPA2-tekniikassa AES (Advanced Encryption Standard) -protokollaa, WPA2-tekniikka tukee myös vanhempaa TKIP-protokollaa. (Wikipedia 2011c.)

WPA-PSK- ja WPA2-PSK-autentikointitekniikka on tarkoitettu kotikäyttöön tai pienemmille yrityksille, joissa ei ole osaamista, tarvetta tai varaa monimutkaiselle 802.1X-rajapintaa käyttävälle tunnistautumispalvelimelle. PSK-tekniikka tunnetaan myös nimellä WPA/WPA2 -personal. PSK-tekniikka perustuu esijaettuun avaimeen, joka on siis myös käytössä WEP-tekniikassa. Tukiasemaan on määritetty esijaettu avain, joka jaetaan sitten käyttäjille, jotka halutaan sallia langattoman verkon käyttäjiksi. (Wikipedia 2011c.)

2.3.4 Salaus

Ensimmäinen salausprotokolla, joka WLAN-tekniikalle julkaistiin, oli WEP, joka käyttää 40-, 104-, tai 232 -bittistä salausta. WEP protokollassa käytetään RC4-salausprotokollaa, joka sisältää puutteita, kuten tiettyjen bittien salauksen puute. WEP jättää salaamatta joidenkin pakettien alustusvektoreita, joiden perusteella salausavain voidaan helposti selvittää Internetistä löytyvillä nuuskintaohjelmilla. Salausavain voidaan selvittää sitä nopeammin, mitä enemmän verkossa on tietoliikennettä. WEP-salausta ei ole suositeltavaa, koska se on purettavissa hyvinkin nopeasti esimerkiksi tavallisella työasema koneella. (Hovatta. 2005, 28)

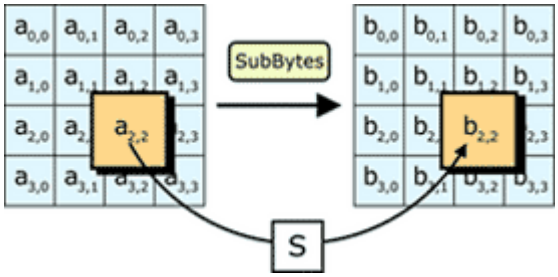
WPA tunnistautumisen yhteydessä kehitettiin uusi TKIP-salausprotokolla, kun WEP salauksessa huomattiin puutteita. TKIP-salauksella pystytään poistamaan WEP-salauksen tunnetut ongelmakohdat, jotka muodostuivat salauksessa käytetyistä staattisista salausavaimista. TKIP käyttää 128 bittistä pakettikohtaista salausavainta WEP:n käyttämän 40-bittisen manuaalisesti syötetyn avainparin sijaan. TKIP-salausavainta käytettäessä poistuu sen ennustettavuus, jota WEP-salauksessa esiintyi, koska nyt avainparit muodostetaan dynaamisesti jokaista pakettia kohti. WPA-tunnistautumisessa käytetään myös MIC (Message Integrity Check) -toimintoa, joka valvoo pakettien eheyttä. Tästä johtuen mahdollinen verkkoon murtautuja ei pysty kaappaamaan mitään paketteja tai muuttamaan pakettien sisältämää tietoa. Vaikka WPA:n käyttämä TKIP-salausprotokolla on hyvin vaikea murtaa, on sekin onnistuttu murtamaan jo nykyään. (Wikipedia 2011c.)

Uusin salausmenetelmä on AES (Advanced Encryption Standard), joka otettiin käyttöön WPA2-tunnistautumisen yhteydessä. AES -salausmekanismin kehitti belgialaiset John Daemen ja Vincent Rijmen. AES-salauksesta saatetaankin käyttää myös nimitystä Rijndael. (Wikipedia 2011d.)

Algoritmi, jota AES käyttää salaukseen, eroaa huomattavasti RC4-algoritmista, jota WEP ja WPA käyttävät. Tämä algoritmi vaatii hieman enemmän laskentatehoa prosessorilta. AES -salausmenetelmä voi käyttää erimittaisia salausavaimia, salausavainten joiden mahdolliset avainpituudet ovat 128, 192, ja 256-bittiä. AES-salaus toimii neljässä eri vaiheessa. (Wikipedia 2011d.)

VAIHE 1: SubBytes

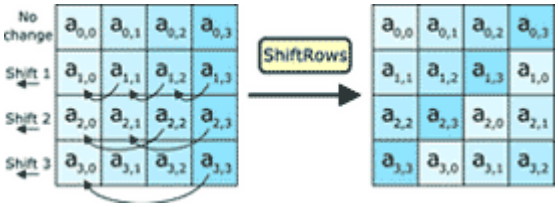
Ensimmäisessä vaiheessa jokainen taulukon tavu päivitetään pysyvän 8-bittisen korvauslokeron avulla (kuvio 6).



KUVIO 6: SubBytes (Wikipedia 2011d).

VAIHE 2: ShiftRows

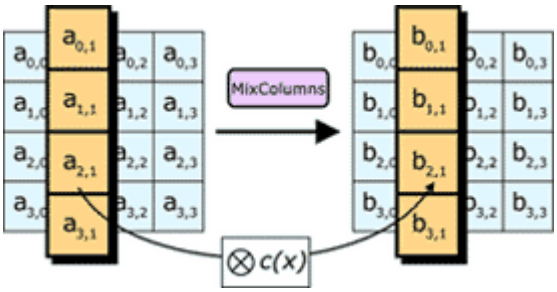
Toisessa vaiheessa rivit siirretään standardissa määritetyllä offset-arvolla. Ensimmäistä riviä ei siirretä, toisen rivin tavuja siirretään kerran vasemmalle eli yhden tavun verran. Kolmannen rivin tavuja siirretään kahden tavun verran vasemmalle, ja niin edelleen (kuvio 7).



KUVIO 7: SiftRows (Wikipedia 2011d).

VAIHE 3: MixColums

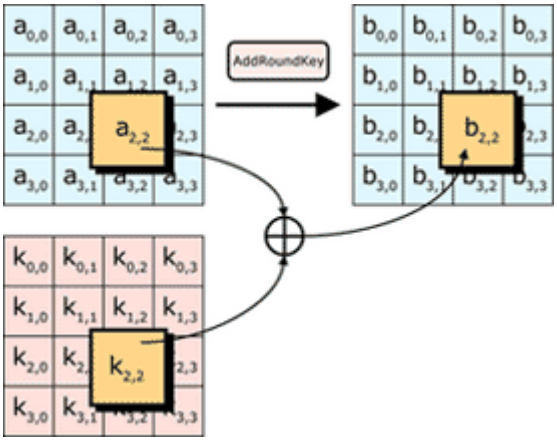
Kolmannessa vaiheessa jokaisen tilan neljä tavua, jotka ovat pystysarakkeissa, yhdistetään käännettävän lineaarimuutoksen kautta (kuvio 8).



Kuvio 8: MixColums (Wikipedia 2011d).

VAIHE 4: AddRoundKey

Neljännessä vaiheessa jokainen tavu yhdistetään kierrosavaimeen XOR-funktiolla (kuvio 9).



Kuvio 9: AddRoundKey (Wikipedia 2011d).

AES-salausmenetelmää vastaan ei tiedetä yhtään onnistunutta murtautumista. Amerikkalainen NSA (National Security Agency) on myös todennut tämän salausmenetelmän tarpeeksi turvalliseksi, jotta Yhdysvaltojen hallitus voi käyttää sitä luokittelemattoman materiaalin salaamisessa. (Wikipedia, Advanced Encryption System.)

2.4 Captive Portal

Captive portal eli vapaasti suomennettuna kaappaava WWW-palvelin, joka estää kaiken TCP/IP liikenteen verkossa, kunnes asiakas avaa WWW-selaimen. Tämän jälkeen Captive portal ohjaa verkossa olevan asiakkaan tietylle Internet sivulle. Syötetystä URL-osoitteesta (Uniform Resource Locator) iippumatta sivu, jolle asiakas ohjataan, on yleensä kirjautumissivu, jota käytettään jonkinlaiseen asiakkaan autentikointiin. Captive portal -tekniikkaa käytetään yleensä langattomien vierailijaverkkojen yhteydessä ja kyseistä tekniikkaa voidaan käyttää langattomissa verkoissa sekä kaapeloidussa verkossa. (Wikipedia 2011e.)

Captive portal -kirjautumissivun sijainnilla ei ole merkitystä, se voi sijaita joko erillisellä WWW-palvelimella, Internetissä, tukiasemassa tai samalla palvelimella, jossa Captive portal sijaitsee. Internetissä tai erillisellä WWW-palvelimella sijaitseva kirjautumissivu tulee kuitenkin muistaa sallia eli lisätä osoitelistalle kyseisen kirjautumissivun osoite, jonne asiakkaalla on pääsy ilman hyväksyttyä autentkointia. Tälle osoitelistalle voidaan myös lisätä muitakin Internet-osoitteita, esimerkiksi sen yrityksen kotisivut, joka kyseistä palvelua tarjoaa. Captive portal -asetuksiin voidaan myös tehdä muita listoja joilla voidaan sallia tietystä TCP-portista tuleva liikenne tai tietystä MAC -osoitteesta tuleva liikenne. (Wikipedia 2011e.)

Captive portal voidaan toteuttaa usealla eri tavalla, kuten HTTP-, IP-, tai DNS-uudelleenohjauksella. Jokainen toteutustapa toimii samalla periaatteella, jolla kirjautuminen on suoritettu. Asiakkaan langattomassa verkossa toimiva laitteen MAC-osoite ja IP-osoite tallennetaan Captive portal -palvelimelle ja laitteelle sallitaan verkon käyttö. Tällä periaatteella toimivissa ratkaisuissa on kuitenkin havaittu haavoittuvuus, jos ei ole käytössä minkäänlaista salausta, jolla MAC-otsikkotiedot voitaisiin salata. Salaamattomasta tietoliikenteestä on helppo saada selville IP-osoite sekä MAC-osoite käyttäen siihen tarkoitettua yksinkertaista ohjelmaa. Väärentämällä autentikoimattomalle tietokoneelle kyseiset osoitteet voidaan huijata Captive portal -palvelinta ja päästä käyttämään verkkoa ilman tunnuksia. Tätä ongelmaa on todella vaikea huomata. Siihen on olemassa ratkaisu, joka voidaan toteuttaa käyttämällä aikakatkaisumäärityksiä, joilla autentikointi vanhenee tietyssä ajassa ja käyttäjä kirjataan ulos verkosta. Uloskirjautumisen jälkeen mahdollinen osoitteiden väärentäjä ei pysty käyttämään verkkoa ilman tunnuksia. (Wikipedia 2011e.)

2.4.1 HTTP-uudelleenohjaus

HTTP-uudelleenohjauksen toimintaperiaate on seuraavanlainen: Jos autentikoimaton asiakas yrittää avata jotain Internet-sivua selaimella, asiakkaan selain tekee DNS-pyyntö (Domain Name System) kyselyn ja IP-osoitteen selvityksen normaalin tapaan. Seuraavaksi kun avattavan sivun osoite on selvillä, selain lähettää kyseiseen IP-osoitteeseen HTTP-pyynnön (Hyper Transfer Protocol). Tämän jälkeen Captive portal palvelimen palomuuri pysäyttää kyseisen pyynnön ja lähettää HTTP-vastauksen, joka sisältää HTTP-tilakoodin 302. Tämä kertoo selaimelle, että kyseinen sivu on siirretty toiselle palvelimelle, tässä tapauksessa kyseessä on Captive portal -palvelin malli. (Wikipedia 2011e.)

2.4.2 IP-uudelleenohjaus

Uudelleenohjaus voidaan myös toteuttaa IP-uudelleenohjauksella käyttäen OSI-mallin kolmatta tasoa. Tämän tavan huono puoli on se, että asiakkaalle tarjottu sivusto ei vastaa syötetyn Internet-sivuston sisältöä. (Wikipedia 2011e.)

2.4.3 DNS-uudelleenohjaus

Kun autentikoimattoman asiakaan WWW-selain tekee DNS-pyynnön, Captive portal -palvelimen palomuuri vastaa kaikkiin DNS-pyyntöihin antamalla Captive portal -kirjautumissivun IP-osoitteen. Captive portal -palvelimen palomuurin tulee ohjata kaikki tulevat DNS-pyynnöt yhdelle DNS-palvelimelle, jonka DHCP-palvelin on määrittänyt. On suositeltavaa, että käytetään palomuurin sisäistä DNS-palvelinta. Huomioitavaa tässä menetelmässä on myös se, että palomuuriin on määritetty, ettei muita DNS-palvelimia pystytä käyttämään. Jos tätä määritystä ei ole toteutettu, voidaan Captive portal -kirjautumissivu ohittaa helposti määrittelemällä tietokone käyttämään jotain muuta DNS-palvelinta. (Wikipedia 2011e.)

2.5 ADSL

ADSL on epäsymmetrinen tiedonsiirtotekniikka, jota käyttäen voidaan muodostaa jopa 8 Mbps nopeus normaalia puhelinlinjaa hyödyntäen. Kyseisen tekniikan viimeisin versio on ADSL2+, joka mahdollistaa suuremman jopa 24 Mbps nopeuden hyödyntäen vain yhtä puhelinparia. ADSL käyttää tiedonsiirrossa korkeita taajuuksia. Normaalin modeemin taajuuskaista on 300–3400 Hz kun taas ADSL:n taajuuskaista on 23 000–1 100 000 Hz:n taajuusalueella. (Wikipedia, ADSL.)

ADSL tunnistetaan epäsymmetrisestä tiedonsiirtonopeudesta. ADSL kykenee laskevassa suunnassa 8Mbps nopeuteen, kun taas nousevassa suunnassa jää nopeus 800kbps tasolle. Tästä syystä ADSL-yhteyksiä suositaan kuluttaja yhteyksinä, kun pääpaino on tiedon siirtäminen verkosta kotikoneelle. (Wikipedia 2011f.)

2.6 ADSL2+

ADSL2+ on uudempi tiedonsiirtotekniikka, jota käytetään eniten kuluttajayhteyksissä. ADSL2+ toimii laskevassa suunnassa teoriassa jopa nopeudella 24 Mbps ja nousevassa suunnassa päästään nopeuteen 1 Mbps. ADSL2+ yhteyksiin on kehitetty Annex L- M- ja J -tekniikat, joilla nouseva nopeus voidaan nostaa teoriassa jopa 3,5 Mbps tasolle. Uudella ADSL2+ -tekniikalla pystytään toimittamaan yhteyksiä vanhan ADSL:n puolentoista kilometrin sijaan jopa yhdeksän kilometrin päähän keskittimeltä. (Wikipedia, ADSL2+.)

Uusimmalla ADSL2+ G Bond -tekniikalla voidaan yhdistää kahden Annex-linjan kapasiteetti. Tällä tekniikalla voidaan siis saavuttaa teoriassa jopa nopeus 48 Mbps laskevassa sunnassa ja nopeus 6 Mbps nousevassa suunnassa. Kyseisen tekniikka perustuu kahteen puhelinkaapeliparii. (Wikipedia 2011g.)

2.7 Linux

Linux on monen käyttäjän moniajokäyttöjärjestelmä, jonka ohjelmarajapinta noudattaa useita UNIX-versioille kehitettyjä standardeja. Linux toimii Intelin 80386SX- tai paremmalla prosessorilla varustetussa tietokoneissa. Linux on syntynyt harrastelijavoimin. Näitä harrastelijoita on totuttu nimittämään hakkereiksi, ja sanan alkuperäinen merkitys sopiikin varsin hyvin Linux kehittelijöihin. Rikollisuuteen liittyvät painotukset sanan merkityksessä ovat myöhäisempää perua. (Koski. 2008, 5-11)

Linuxin lähdekoodia suojataan ns. GNU copyleftillä. Lyhyesti kerrottuna tämä tarkoittaa, että ohjelmaa suojaa tekijän omistama tekijänoikeus, mutta tätä oikeutta käytettään vain suojaamaan ohjelman vapaata levitystä. Jokainen ohjelma, mikä on suojattu GNU:lla, on vapaasti saatavilla lähdekoodeineen. Halukkaat voivat ladata ohjelma lähdekoodin ja tehdä siihen muutoksia tarvittaessa, mutta muutettua versiota ei saa hyödyntää kaupallisesti. Muutettujen versioiden täytyy myös olla vapaasti saatavissa olevia versioita. Muutoksia sisältävää versiota ei kuitenkaan ole pakko levittää. (Koski. 2008, 5-11)

Kehitystyö, jota Linuxille tehdään, tapahtuu internetissä olevien yhteisöjen välityksellä. Mitään virallista organisaatiota tätä varten ei ole olemassa, tästä johtuen laadunvalvonta ja versiokontrolli ovat kevyempiä. Kaupallista käyttöjärjestelmää tehtäessä vastaava käytäntö ei tulisi kuuloonkaan. Ilmaisella käyttöjärjestelmällä on kuitenkin runsaasti vapaaehtoisia testaajia ja kehittäjiä, näin ollen Internetin kautta ohjelmakehittäjät voivat vastaan ottaa palautettua käyttöjärjestelmästä, tehdä vaaditut korjaukset ja levittää korjatut versiot uudelleen testattaviksi. (Koski. 2008, 5-11)

2.8 Debian GNU/Linux

Debian GNU/Linux on vapaa käyttöjärjestelmä, jonka on valmistunut Debian-projektiin kuuluvat yksilöt sekä yhteisöt. Käyttöjärjestelmä sisältää valikoiman ohjelmia sekä työkaluja. Tärkein osa käyttöjärjestelmässä on kernel, jonka avulla voidaan jakaa järjestelmän resursseja ja mahdollistaa muiden ohjelmien ajamisen yhtäaikaisesti. Debian järjestelmät käyttävät Linux-ydintä. Linux on Linus Torvaldsin kehittämä ohjelmisto, jota kehitetään ja ylläpidetään jatkuvasti tuhansien ohjelmoijien toimesta.

Perusidea käyttöjärjestelmässä on neljään tasoon jakautuva perusperiaate. Alimmaisena tasona toimii Ydin. Seuraavassa kerroksessa toimii kaikki vaadittavat työkalut. Tämän yläpuolella käytössä ovat ohjelmistot, joita käytetään arkipäivän tehtävissä.

Päällimmäisenä toimii Debian, joka varmistaa ja sovittaa yhtenäisen toimivuuden. (Debian, Tietoa Debianista.)

2.9 Coovachilli

Coovachilli on Linuxille suunniteltu pääsynvalvontaohjelmisto, jossa mukana on Captive portal ominaisuus. Se on suunniteltu käytettäväksi langattomiin vierailijaverkkoihin. Se tukee kahta erilaista tapaa autentikoida asiakas vierailijaverkon käyttäjäksi: UAM (Universal Access Method) autentikointia, sekä WPA autentikointia. Coovachilli on jatkokehitetty ohjelmasta nimeltä ChilliSpot, jota nykyään ei enää kehitetä. (Coovachilli, ManPages.)

Coovachilli:ssä on kolme verkkoa. Sisäverkko, jossa kaikki vierailijaverkon asiakaskoneet ovat, Radius -verkko autentikointia varten sekä ulkoverkko, joka ohjaa liikenteen muihin verkkoihin. (Coovachilli, ManPages.)

Asiakaskoneiden autentikointi suoritetaan erillisellä radius palvelimella, joka voi sijaita samalla fyysisellä palvelimella kuin itse Coovachilli. UAM tapaa käyttäessä on CHAP-Chalenge ja CHAP-password määritetty standardin RFC 2865 mukaan. WPA tapaa käyttäessä radius EAP-Message on määritetty RFC 2869 standardin mukaan. Viestiattribuutit, jotka on kuvailtu RFC 2548 standardissa, on käytössä salattujen avaimien siirtämisessä radius palvelimelta CoovaChilli -palvelimelle. (Coovachilli, ManPages.)

Coovachilli:n sisäverkko hyväksyy DHCP- ja ARP-pyyntöjä asiakaskoneilta. Asiakaskone voi olla kahdessa eri tilassa, joko autentikoimattomassa tilassa tai autentkoidussa tilassa. Autentikoimattomassa tilassa http-pyynnöt asiakaskoneelta uudelleen ohjataan vierailijaverkon kirjautumissivulle. Kirjautumissivulla käyttäjää pyydetään syöttämään käyttäjätunnus ja salasana. Web-palvelin ohjaa syötetyt käyttäjätiedot coovachilli -palvelimelle. Tämän jälkeen Coovachilli ohjaa syötetyt tunnukset radius -palvelimelle. Jos käyttäjätunnukset löytyvät radius -palvelimen tietokannasta, asiakaskoneen tila muutetaan autentikoimattomasta tilasta autentikoituun tilaan. Tämä tunnetaan nimellä UAM. (Coovachilli, ManPages.)

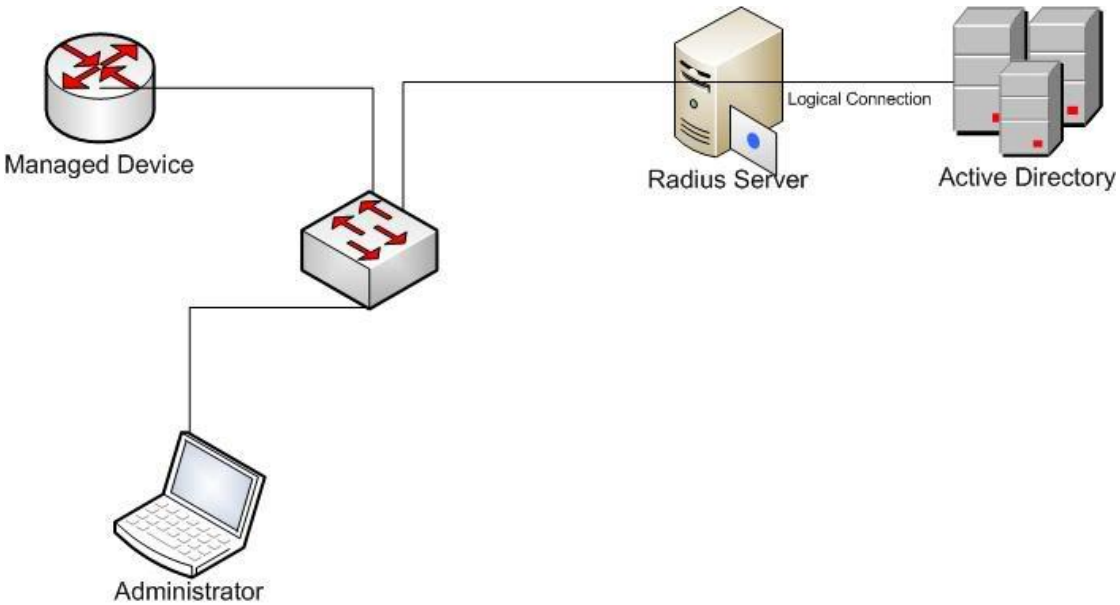
Vaihtoehtoisesti UAM tavan sijaan voidaan asiakaskoneet autentikoida WPA tekniikalla. Tässä tapauksessa WPA autentikointitiedot välitetään langattomalta tukiasemalta Coovachilli-palvelimelle, josta ne ohjataan radius -palvelimelle. (Coovachilli, ManPages.)

2.10 Radius

Radius (Remote Authentication Dial In User Service) suunniteltiin tunnistusmenetelmään, jota käytetään sisäänsoitto -palveluissa, jossa se on tänä päivänä laajassa käytössä. Radius -protokollaa käytetään yleisemmin operaattoreiden omissa sisäisissä verkoissa, näin ollen verkkoa voidaan pitää todella luotettavana. (Wikipedia 2011h.)

Autentikoinnin käyttämiseen lähiverkossa vaaditaan Radius-palvelin, johon verkkolaitteet ottavat yhteyden, joko suoraan tai erinäisten verkkolaitteiden avulla, esim. langattoman tukiaseman kautta. (Wikipedia 2011h.)

Radius – palvelin voi sisältää tai käyttää erillistä tietokantapalvelinta, jossa käyttäjätunnukset ja salasanat sijaitsevat. Radius-palvelin pystyy myös hyödyntämään olemassa olevaa NT4-toimialueen ohjauskonetta, Windows Active Directorya, Novell eDirectorya tai ylipäätään lähes kaikkia käyttäjätunnustietokantoja. (Wikipedia 2011h.)



KUVIO 10: Radius -palvelimen käyttö käyttäjän todentamiseen (KpJungle, Authentication by radius).

2.11 MySQL

MySQL on paljon suosiota saanut SQL -tietokantajärjestelmä. MySQL tietokantajärjestelmää kehittää ruotsalainen yritys MYSQL AB. Kyseisen yrityksen osti Sun Microsystems vuonna 2008, jonka jälkeen vuonna 2009 Oracle Corporation osti Sun Microsystems yrityksen itselleen. Samalla MySQL:n omistus siirtyi uudelle omistajalleen. MySQL säilyi kuitenkin vapaan GNU GPL -lisenssin alla, mutta siitä tuli tarjolle myös kaupallinen versio. (Wikipedia 2011i.)

Erona kaupallisiin tietokantajärjestelmiin MySQL-tietokantajärjestelmää hallitaan komentoriviltä tai tekstipohjaisella asiakasohjelmalla. MySQL-tietokantajärjestelmään on saatavilla myös valmistajan sivuilta graafiset käyttöliittymät MySQL Administrator ja MySQL Query Browser. Vaihtoehtoisesti graafiseen hallintaan on myös tarjolla ilmainen phpMyAdmin. (Wikipedia 2011i.)

MySQL -tietokannan kehitti suomalainen Michael Widenius vuonna 1995 yhteistyössä ruotsalaisen David Axmarkin kanssa. Ensimmäinen versio MySQL-tietokantajärjestelmästä julkaistiin 1996. (Wikipedia 2011i.)

MySQL-tietokantajärjestelmää käyttävä järjestelmä toteutetaan yleensä PHP, Python tai Perl-ohjelmointikielellä ja julkaisujärjestelmänä käytetään Apache-ohjelmistoa, joka toimii Linux-käyttöjärjestelmän päällä. Tätä yhdistelmää kutsutaan LAMP -ympäristöksi. MySQL-tietokantajärjestelmää voidaan myös käyttää muilla ohjelmointikielillä. MySQL-tietokantajärjestelmä sisältää rajapinnat seuraaviin ohjelmointikieliin: C, C++, C#, Smaltalk, Java, Ruby ja TLC. (Wikipedia 2011i.)

2.12 Wlan-tukiasema

Fyysistä tiedonsiirtoverkkoa voidaan jatkaa langattomilla tukiasemilla. Tukiasemat toimivat radiotaajuuksilla, joilla ne muodostavat yhteyden päätelaitteisiin. Tukiaseman tehtävänä on toimia lähettimenä sekä vastaanottimena halutussa tilassa. Langattomat tukiasemat voivat toimia verkossa, joko sillatussa tilassa, jolloin tieto kulkee tukiaseman läpi, tai tukiasema voi toimia myös reitittimenä.

Kun halutaan saavuttaa suurempi langattomanverkon kattavuusalue, tarvitaan useita yhteyspisteitä, jotka voidaan liittää toisiinsa jakelujärjestelmällä. Jos käytössä on useampi yhteyspiste, muodostuu päällekkäisiä peittoalueita. Päällekkäiset peittoalueet voidaan estää käyttämällä tukiasemissa, jotka muodostavat toistensa kanssa päällekkäisen kattavuusalueen, eri radiokanavia, jotka eivät häiritse toisiaan. 802.11g:n kanssa riittää käytettäväksi kolme eri radiokanavaa, joidenka taajuudet eivät mene päällekkäin. Työssä käytetään Linksys E2000 tukiasemia (kuva 1) (Puska. 2005, 131)

KUVA 1: Työssä käytettävät tukiasemat (Cisco, Advanced Wireless-N Router E2000)

WLAN-teknikkaa käytetään monenlaisissa ympäristöissä ja monenlaisiin käyttötarkoituksiin, joten WLAN-tukiasemien ominaisuudet vaihtelevat suuresti. WLAN-tukiasemia käytetään kodeissa ja yrityksissä, sisä- ja ulkotiloissa, muutaman metrin tai jopa kilometrien kantamilla, joten verkkototeutukseen kustannuksien sekä luotettavan ja tehokkaan toiminnan kannalta on tärkeää valita oikeanlainen laite kuhunkin käyttöympäristöön. (Hovatta 2005, 13.)

3 VIERAILIJAVERKKO

Nykyisin yhä useammalla on laite, jolla pääsee internetiin, joko käyttämällä 3G-, 4G- tai WLAN-yhteyksiä. Nykyisin lähes kaikissa matkapuhelimissa on internetselain. Matkapuhelimien lisäksi taulutietokoneiden käyttö on yleistynyt ja kannettavien tietokoneiden määrä kasvaa. Tästä syystä langattomille verkoille on paljon kysyntää. Langattomalla internetyhteydellä voidaan turvata varma ja nopeasti toimiva verkkoyhteys. Tästä syystä halutaan, että langaton verkko olisi helposti saavutettavissa useassa paikassa. Vastaavasti taas langattomia vierailijaverkkoja tarjoavat tahot haluavat, että verkko olisi helppo toteuttaa ja eikä sitä käytettäisi väärin.

Vierailijaverkko ei tekniikaltaan eroa normaalista verkosta. Nimi tulee vain siitä, että halutaan tarjota verkkoyhteys, joka ei ole yrityksen omassa verkossa, vaan tarkoitettu juuri vieraita varten. Vierailijaverkon voi toteuttaa monella tavalla. Yksinkertaisin ratkaisu on hankkia internetyhteys, jonka mukana tulee WLAN ominaisuutta tukeva modeemi. Langattoman verkon voi jättää suojaamatta, jolloin verkko on kaikkien käytettävissä. Tämä ei kuitenkaan ole suositeltavaa väärinkäytön vuoksi. Turvallisen vierailijaverkon toteutus vaatii joko salauksen tai käyttäjien todennuksen. Yksinkertaisella tukiasemalla voidaan määrittää verkkoon salausavain, jolloin käyttäjiä voidaan rajata. Ongelmana on kuitenkin salausavain, joka tulisi vaihtaa viikoittain tai jopa päivittäin verkon väärinkäytön estämiseksi.

Paras tapa toteuttaa vierailijaverkko on käyttää jonkinlaista käyttäjien todennusta. Yksi tapa toteuttaa todentaminen on käyttää esimerkiksi Captive portal -tyyppistä ratkaisua, joka käyttää todennukseen vaikkapa Radius-palvelinta.

4 SUUNNITTELU

Suunnittelu aloitetaan vaatimusten määrittämisellä. Tässä työssä oli saatava käyttöön WLAN-verkko, jota seurakuntayhtymässä vierailevat henkilöt voisivat käyttää. Tärkeintä työssä oli ottaa huomioon, että WLAN-verkkon tuli olla kokonaan erillinen ja irrallaan yrityksen omasta tietoverkosta. Normaalisti kyseisen verkon voisi toteuttaa myös yrityksen olemassa olevaan verkkoon tai tämän rinnalle käyttäen jo olemassa olevaa tietoliikenneyhteyttä. Tällä kertaa kyseinen järjestely ei ollut mahdollinen suuren tietoturvahaitan vuoksi.

Suunnittelussa tuli ottaa huomioon myös vierailijaverkon helppo käytettävyys, eli tavoitteena oli, että käyttäjän kirjautuminen vierailijaverkkoon olisi helppoa. Suurin osa kannettavia tietokoneita tai älypuhelimia käyttävistä ihmisistä osaa yhdistää laitteensa suojaamattomaan tai suojattuun verkkoon. Seurakuntayhtymän sijainnin takia suojaamatonta verkkoa ei voi käyttää, koska tällöin verkkoa olisi liian helppo käyttää väärin. Normaalissa salasanalla suojatussa verkossa taas ongelmaksi muodostuisivat tukiasemien salasanojen vaihto-ongelmat lisäksi jos samaa salasanaa käytetään vaihtamatta koskaan, kasvaa verkon väärinkäytön riski huomattavasti. Näin ollen parhaimmaksi vaihtoehdoksi jää Captive portal -tyyppinen hallittava WLAN-verkko.

Tärkeänä osana suunnitteluun vaikuttaa myös vierailijaverkon kattavuusalue. Jos on tarve kattaa vain esimerkiksi yksi neuvottelutila, voi hankinta olla suhteellisen pieni. Jos tavoitellaan suurta kattavuusaluetta, joudutaan tällöin suunnittelemaan tukiasemien sijoituspisteet sekä kattavuusalueet huomattavasti tarkemmin. Suurella alueella tulee ottaa huomioon myös seinien paksuudet sekä materiaalit.

Seurakuntayhtymän tiloissa tarkoituksena oli kattaa ensisijaisesti neuvotteluhuoneet sekä yhteiset tilat, mutta samalla pyrittiin myös rakentamaan mahdollisimman laajasti kattava vierailijaverkko. Neuvotteluhuoneet sijaitsevat monessa eri kerroksessa, joten päämääränä ei kuitenkaan ole mahdollisimman suuri yhtenäinen kattavuusalue.

4.1 Verkonsuunnittelu

Ensimmäisenä selvitettiin voisiko vierailijaverkkoon käyttää jo olemassa olevia kytkimiä virtuaaliverkkoja hyödyntäen (VLAN) tai onko mahdollista vaihtoehtoisesti käyttää kokonaan omaa verkkoa talon sisällä. Yksi vaihtoehto myös olisi ollut käyttää WDS (wireless distribution system) -tekniikkaa. Selvitysten myötä päädyttiin käyttämään kokonaan erillistä verkkoa. Tämä ratkaisu oli paras, koska näin saadaan käyttöön paras tietoturva, kun verkot ovat fyysisesti eri verkkoja. WDS-tekniikka olisi myös ollut oikein hyvä vaihtoehto, mutta tämä tekniikka puolittaa verkon nopeuden aina kun lisätään tukiasemia, joten yhteysnopeudet olisivat jääneet huomattavasti hitaimmiksi.

Langallisen lähiverkon suunnittelussa tuli ottaa huomioon, että se saataisiin vietyä tukiasemien suunniteltuihin sijoituspaikkoihin. Rakennuksen kerrosten välisiin kytkentäkaappeihin täytyi sijoittaa omat kytkimet, jotta vierailijaverkko olisi fyysisesti erillään nykyisestä sisäverkosta. Kytkentäkaapissa vierailijaverkko merkittiin selvästi erivärisillä verkkokaapeleilla, jotta jatkossa jo yleissilmäyksellä nähdään, mitkä kytkennät liittyvät vierailijaverkkoon.

Tukiasemien sijoittaminen täytyi suunnitella niin, että ne olivat helposti asennettavissa jo olemassa olevien verkkorasioiden läheisyyteen. Tukiasemat täytyi sijoittaa joko suoraan neuvotteluhuoneisiin, joihin langaton vierailijaverkko halutaan pääsääntöisesti toteuttaa, tai niiden läheisyyteen silmällä pitäen myös mahdollisimman suurta langattoman verkon kattavuusaluetta koko rakennuksessa. Tukiasemien lopullista sijaintia mitattiin kannettavalle tietokoneelle asennettavalla langattoman verkonmittaus ohjelmalla.

4.2 Laitehankintojen suunnittelu

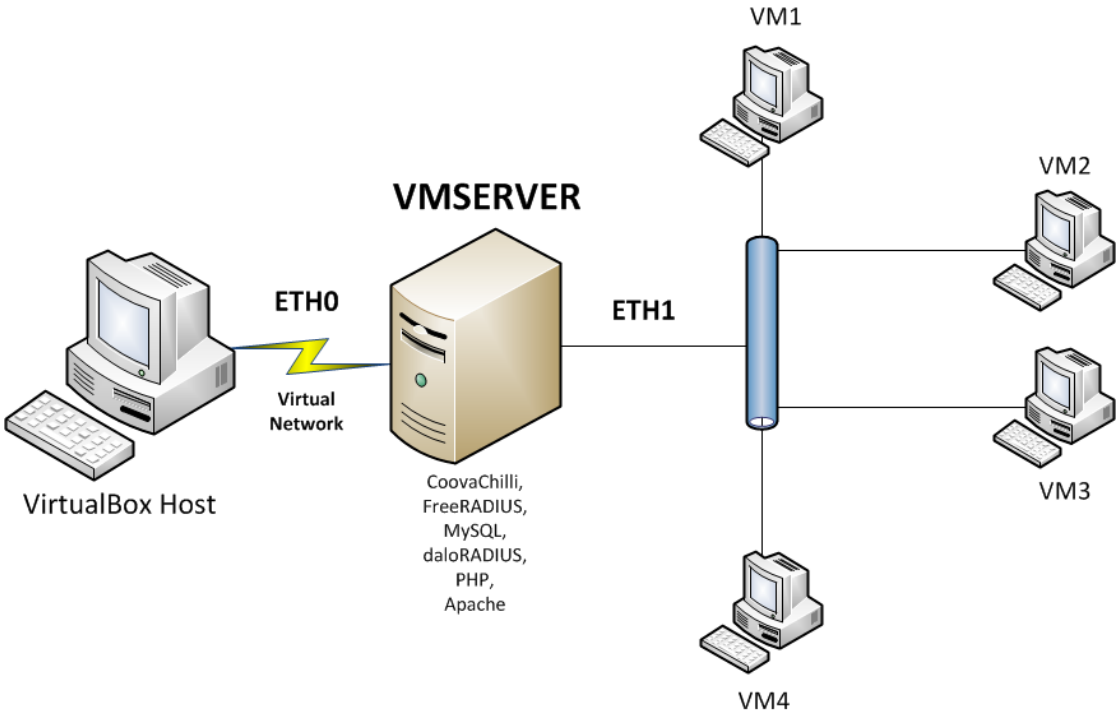
Laitehankintojen suunnittelussa oli kolme lähtökohtaa. Yksi vaihtoehto oli hankkia Ciscon tukiasemat sekä laite, jolla näitä voitaisiin hallita keskitetysti yhdestä järjestelmästä. Toisena vaihtoehtona oli Helwett-Packardin valmistama WLAN-kontrolleri, johon olisi voitu kytkeä joko erikseen hankittavia tukiasemia tai jo olemassa olevia tukiasemia. Kolmas vaihtoehto perustui keskitetyn hallittavuuden osalta täysin ilmaiseen Linux-käyttöjärjestelmän päälle asennettavaan Captive portal -ratkaisuun, jolloin kustannuksia kertyisi vain hankittavista tukiasemista sekä ADSL-yhteydestä.

Koska työ oli täysin kokeiluluontoinen projekti, vaikutti suhteellisen edullinen ratkaisu parhaimmalta ratkaisulta. Jos projekti epäonnistuisi täysin, ei tällöin muodostuisi turhia ja kalliita kustannuksia. Myös Teknisten määritysten myötä edullinen vaihtoehto vaikutti parhaimmalta. Tällä ratkaisulla pystyttäisiin rakentamaan tarpeeksi kattava, mutta myös samalla hallittava vierailijaverkko, jonka kattavuus aluetta voitaisiin kuitenkin kasvattaa jatkossa lisäämällä tukiasemien määrää.

Vierailijaverkkoa varten tarvittiin myös oma ADSL-yhteys, jotta vierailijaverkko ei käytäisi seurakuntayhtymän omaa kirkkoverkkoyhteyttä. Seurakuntayhtymällä oli voimassa oleva sopimus tietyn operaattorin kanssa, joka on juuri kilpailutettu, joten yhteys päädyttiin valitsemaan kyseiseltä operaattorilta. Vierailijaverkon vienti palvelimelta tukiasemille vaatii monta nousua rakennuksen kerrosten välillä, joten kerroskytkimien rinnalle tulee hankkia omat verkkokytkimet vierailijaverkkoa varten. Lisäksi tarpeeksi suuren kattavuusalueen saavuttamiseksi tarvittaisiin neljä tukiasemaa.

4.3 Testiympäristö

Ennen lopullista päätöstä ja laitehankintoja suunniteltiin ja toteutettiin lopullista ympäristöä vastaava ympäristö. Testiympäristö toteutettiin aluksi täysin virtuaalisena (kuvio 11), minkä jälkeen se vielä toteutettiin myös fyysisesti. Testiympäristön pystyi toteuttamaan vanhalla työasemalla, johon asennettiin Debian -käyttöjärjestelmän ja tämän lisäksi CoovaChilli ohjelmisto ja sen vaatimat ohjelmistot. Tukiasemana testiympäristössä käytettiin jo ennestään käytöstä poistettua tukiasemaa.



KUVIO 11: Virtuaalinen testiympäristö.

5 TOTEUTUS

Työn toteutus aloitettiin, kun kaikki tarvittavat laite- sekä laajakaistahankinnat oli hankittu ja toimitettu sekä kun testiympäristö oli suunniteltu ja toteutettu onnistuneesti. Testiympäristön toteutuksessa vastaan tuli suuria ongelmia, jotka johtuivat vapaata lähdekoodia käyttävästä ohjelmistosta. Kun olemassa ei ollut mitään virallista tukea, löytyi tietoa vain kyseisen ohjelmiston foorumeilta, jossa kaikki ratkaisut eivät aina olleet paikkaansa pitäviä. Tämä viivästytti projektia huomattavasti, kun tärkeimpien asetuksien ratkaisut löytyivät testaamalla ohjelmiston eri konfiguraatioita.

5.1 Laitteiden asentaminen

Laitteiden asentaminen aloitettiin tukiasemista. Tukiasemat sijoitettiin neuvotteluhuoneiden välittömään läheisyyteen, mutta samalla silmällä pitäen mahdollisimman suurta verkon kattavuusaluetta koko rakennuksessa. Tukiasemat asennettiin viisikerroksisessa rakennuksessa kolmeen eri kerrokseen, koska näin kattavuutta saatiin vielä suuremmaksi.

ADLS -yhteyden palveluntarjoava yhtiö toimitti ja asensi vierailijaverkkoa varten hankitun yhteyden palvelinsalin yhteyteen, jossa muutkin yhteydet sijaitsivat. Verkkokytkimet, jotka hankittiin kerrosten välisiin kytkentäkaappeihin, asennettiin tarvittaviin kerroksiin ja kytkettiin samaan verkkoon vierailijaverkon palvelimen kanssa.

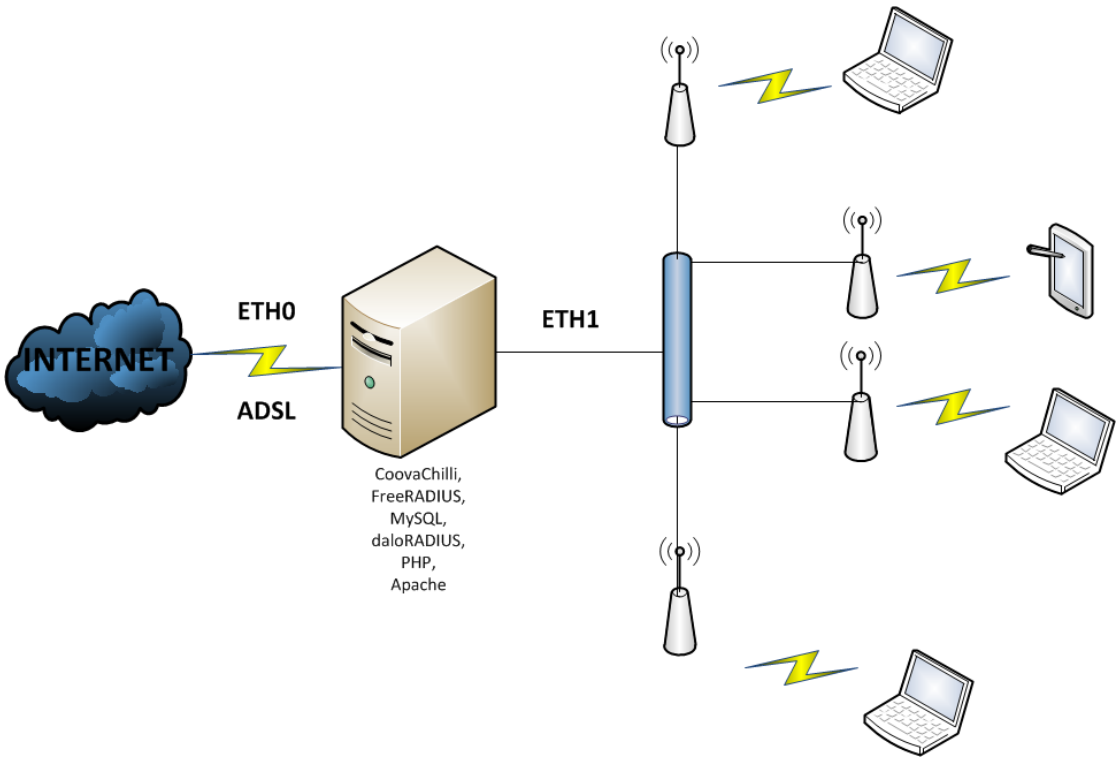
Työasema joka toimii palvelimena, sijoitettiin samaan tilaan muiden seurakuntayhtymän palvelimien kanssa. Palvelinhuone, johon kyseinen palvelin asennettiin, oli erikseen jäähdytetty, jolloin turvattiin vielä vierailijaverkon toimivuutta laiterikkojen varalta.

5.2 Asetusten määrittäminen

5.2.1 Palvelin

Kyseiseen palvelimeen asennettiin Debian Linux-käyttöjärjestelmä. En käy tässä työssä läpi sen tarkemmin kyseisen käyttöjärjestelmän asennusta. Palvelimeen kuitenkin jouduttiin asentamaan muutamia ohjelmistoja, jotta vierailijaverkon tarvitsema captive portal -tyyppinen ratkaisu voitiin toteuttaa. Ohjelmistot, joita tarvittiin, olivat seuraavat: CoovaChilli, FreeRadius, MySQL, PHP, daloRADIUS ja Apache.

Palvelimen tuli myös toimia DHCP palvelimena, jotta verkkoa käyttäville laitteille voidaan jakaa IP-osoitteita, joten palvelimelle asennettiin myös DHCP-palvelu. Tietoturvasyistä en voi julkaista salasanoja tai käyttäjätunnuksia. Palvelin tarvitsee kaksi verkkokorttia, jotta voi toimia captive portal -palvelimena. Ensimmäinen verkkokortti ETH0 on kytketty ADSL linjasta tulevaan yhteyteen. Toinen verkkokortti ETH1 on määritetty jakamaan IP-osoitteita vierailijaverkkoon (kuvio 12).



KUVIO 12: Vierailijaverkon palvelimen rooli.

Vierailijaverkon toteutusta varten palvelimelle asennettiin Radius-ohjelmisto. Tässä työssä Radius palvelimena käytettiin vapaata lähdekoodia käyttävää. FreeRadius ohjelmistoa. FreeRadius ohjelmistoon täytyi määrittää /etc/freeradius/clients.conf -tiedostoon tieto siitä, millä salasanalla daloRADIUS-ohjelmisto voi käyttää FreeRadius-ohjelmistoa.

```
client 127.0.0.1 {
 secret     = mysecret
}
```

Lisäksi FreeRadiukseen määritettiin asetukset MySQL-ohjelmistoa varten. Tarvittavat määritykset tehtiin /etc/freeradius/sql.conf -tiedostoon, jonne tuli määrittää MySQL-palvelimen osoite, tunnus sekä salasana, joilla MySQL-kantaa voidaan käyttää. Palvelimen osoitteeksi määritettiin localhost, koska tässä tapauksessa MySQL-kanta sijaitsee samalla palvelimella.

```
server = "localhost"
login = "yyyyyy"
password = "xxxx"
```

FreeRadius -ohjelmaan täytyi määrittää asetukset niin, että käytössä tulee olla SQL todennus ja, että käyttäjätunnukset sijaitsevat MySQL-kannassa. Kyseiset asetukset saatiin käyttöön muokkaamalla /etc/freeradius/sites-available/default -tiedostoa. Alkuperäisillä asetuksilla nämä toiminnot ovat vain kommentteina kyseisessä tiedostossa.

```
authorize {
        sql
}
accounting {
       sql
}
```

Viimeisenä toimintona määritettiin, että FreeRadius käyttää jo aikaisemmin muokattua /etc/freeradius/sql.conf -tiedostoa. Kyseinen määritys tehtiin muokkaamalla /etc/freeradius/radiusd.conf -tiedostoa, josta alkuperäisissä asetuksissa kommenttina oleva asetus otettiin käyttöön.

```
$INCLUDE sql.conf
```

Kun FreeRadius-ohjelmiston asetukset oli määritetty, voitiin siirtyä MySQL-ohjelmiston asetusten määrittämiseen. Ensin käynnistettiin MySQL-ohjelmisto halutulla tunnuksella sekä salasanalla, joita daloRADIUS-ohjelmisto tulisi käyttämään. Samalla luotiin myös tietokanta, jota vasten vierailijaverkkoa käyttävät todennetaan.

mysql -u yyyyyy --password=xxxx
mysql> CREATE DATABASE radius;
mysql> exit

Tietokannan lisäämisen jälkeen lisättiin siihen vielä tarvittavat taulut aikaisemmin määritetyllä käyttäjätunnuksella ja salasanalla. Valmiit tietokannan mallitaulut sijaitsivat /var/www/daloradius/contrib/db-tiedostossa daloRADIUS-ohjelmiston asennuksen jälkeen.

mysql -u yyyyyy --password=xxxx radius < /var/www/daloradius/contrib/db/fr2-mysql-daloradius-and-freeradius.sql

FreeRadius-ohjelmistoa varten asennettiin daloRADIUS-ohjelmisto, jota käytetään internetselaimella FreeRadius-ohjelmiston hallintaan. DaloRADIUS määritettiin käyttämään aikaisemmin asennettuja FreeRADIUS- ja MySQL-ohjelmistoja niitä vastaavilla käyttäjätunnuksilla sekä tietokantamäärityksillä. Määritykset tehtiin seuraaviin tiedostoihin: /var/www/daloradius/library/daloradius.conf.php, /var/www/signup-*/library/daloradius.conf.php ja /var/www/signup*/index.php.

$configValues['CONFIG_DB_PASS'] = 'xxxx';
$configValues['CONFIG_MAINT_TEST_USER_RADIUSSECRET'] = 'mysecret';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';

$configValues['CONFIG_DB_PASS'] = 'xxxx';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
*$configValues['CONFIG_SIGNUP_SUCCESS_MSG_LOGIN_LINK'] = "
Paina tästä" " palataksesi kirjautumissivulle ja aloittaaksesi internetin käytön

";*

$sql = "INSERT INTO ".$configValues['CONFIG_DB_TBL_RADCHECK']." (id, Username, Attribute, op, Value) ".

" VALUES (0, '$username', 'Cleartext-Password', ':=', '$password')";

Viimeisenä vaiheena palvelimen asetusten määrittämisessä konfiguroitiin CoovaChilli-ohjelmisto vastaamaan muiden aikaisemmin asennettujen ohjelmistojen määrityksiä sekä lisättiin verkkoalueet, joita CoovaChilli käyttää. Määritykset tehtiin /etc/chilli/defaults -tiedostoon, jonka asetukset CoovaChilli ottaa käyttöönsä käynnistyessään.

HS_NETWORK=192.168.10.0
HS_UAMLISTEN=192.168.10.1

HS_RADSECRET=xxyyxxyy
HS_UAMSECRET=yyxxyyxx
HS_UAMFORMAT=https://\$HS_UAMLISTEN/hotspotlogin/hotspotlogin.php
HS_UAMHOMEPAGE=https://\$HS_UAMLISTEN

Kun kaikkien tarvittavien ohjelmistojen määritykset olivat valmiit, voitiin CoovaChilli-ohjelmisto käynnistää ja todeta kaiken toimivan halutulla tavalla. Palvelimen uudelleenkäynnistyksen yhteydessä haluttiin vielä varmistua siitä, että vierailijaverkko käynnistyisi automaattisesti. Tämä voitiin varmistaa määrittämällä /etc/default/chilli -tiedostoon kyseinen asetus.

START_CHILLI=1

5.2.2 Tukiasemat

Tukiasemiin asennettiin oman ohjelmiston tilalle dd-wrt-ohjelmisto, jolloin tukiasemista saatiin enemmän ominaisuuksia käyttöön. Kun ohjelmistot oli jokaiseen tukiasemaan asennettu, määritettiin niihin seuraavanlaiset asetukset (taulukko 1).

TAULUKKO 1. Tukiasemien asetukset.

Tukiasema	MAC-osoite	IP-osoite	Taajuuskanava	Tila
1	00:25:9C:5C:8D:0C	192.168.10.2	1	Sillattu
2	00:25:9C:5C:60:9F	192.168.10.3	6	Sillattu
3	00:25:9C:5C:8D:15	192.168.10.4	11	Sillattu
4	00:25:9C:5C:5F:97	192.168.10.5	1	Sillattu

Jokainen tukiasema toimii hyvin yksinkertaisilla asetuksilla. Tukiasemaan määritettiin vain IP-osoite 192.168.10.0 verkkoalueelta ja toimimaan sillatussa tilassa. Näin ollen tukiasema vain muodostaa yhteyden langattoman laitteen ja itsensä välille, jolloin laite saa IP-osoitteen DHCP-palvelimelta ja ohjaa selaimen avattua kirjautumissivulle. Tukiasemien MAC-osoitteet lisättiin vielä CoovaChilli-ohjelmiston sallittuihin MAC-osoitteisiin, jotta tukiasemien ja palvelimen välinen tietoliikenne ei estyisi.

Tukiasemiin määritettiin myös taajuuskanavat. Taajuuskanavina käytettiin kanavia 1, 6, 11, jotta mahdolliset häiriöt, joita samalla taajuusalueella toimivat tukiasemat voivat aiheuttaa, jäisivät keskenään mahdollisimman pieniksi. Kyseiset taajuuskanavat eivät mene taajuusalueeltaan toistensa päälle. Seurakuntayhtymän sijainnin takia täysin häiriötöntä verkkoa ei voinut toteuttaa, koska ympärillä sijaitsee paljon asuinrakennuksia, joissa olevat langattomat verkot käyttävät samoja tai päällekkäisyyksiä aiheuttavia taajuuskanavia.

6 JOHTOPÄÄTÖKSET

Tässä työssä tutkittiin kuinka yritykseen voidaan suunnitella ja toteuttaa vierailijaverkko hyvin pienillä kustannuksilla. Työ toteutettiin Kuopion ev.lut. seurakuntayhtymälle, koska erillisen langattoman vierailijaverkon tarve oli todella suuri.

Vierailijaverkko toteutettiin mahdollisimman erilleen olemassa olevasta sisäverkosta, jonne ulkopuolisten käyttäjien pääsy on suuri tietoturvariski. Käyttämällä erillistä Internet yhteyttä toteutettiin samalla myös varayhteys, jos normaali yhteys olisi poissa käytöstä vikatilanteen vuoksi.

Vierailijaverkko on ollut Kuopion ev.lut. seurakuntayhtymän tiloissa käytössä kohta noin kaksi vuotta. Tänä aikana se on toiminut halutulla tavalla ja luotettavasti. Huomattavasti edullisempana toteutuksena ratkaisu on ollut hyvä ja järkevä verrattuna kalliimpiin järjestelmiin.

Työn suunnittelu ja toteutus onnistui hyvin, vaikkakin vapaata lähdekoodia käyttävien ohjelmistojen ohjeet ja dokumentit olivat puutteellisia tai niitä ei ollut olemassa. Tästä huolimatta työhön ei tarvinnut käyttää juurikaan ylimääräisiä resursseja tai lisäbudjettia. Langatonta vierailijaverkkoa suunniteltiin ja toteutettiin normaalin työn ohessa kokeiluluontoisena projektina.

Avointa lähdekoodia käyttävä ratkaisu voi siis olla usein toimiva, mutta päätyisin silti jatkossa käyttämään tunnetun laitevalmistajan tarjoamia laitteita. Näin voidaan varmistua hyvistä ja luotettavista ohjeista ja dokumenteista ja parhaassa tapauksessa voi laitevalmistaja tarjota suoraa tukea ongelmatilanteissa.

LÄHTEET

Hovatta, T. 2005. *Wlan-tekniikat ja -käyttösovellukset toimitilakiinteistöissä*. Espoo: Sähköinfo.

Koski, R. 2008. *Linuxin perusteet*. Helsinki: Readme.fi

Puska, M 2005. *Langattomat lähiverkot*. Helsinki: Talentum

Debian 2011. *Tietoa Debianista* [viitattu 24.5.2011]. Saatavissa: http://www.debian.org/intro/about

Cisco 2012. *Advanced Wireless-N Router E2000* [viitattu 19.5.2012]. Saatavissa: http://homesupport.cisco.com/en-us/support/routers/E2000

CoovaChilli 2011. *CoovaChilli ManPages* [viitattu 26.3.2011]. Saatavissa: http://www.coova.org/CoovaChilli/chilli

IEEE 802.11b 2012. *Wireless LAN: The IEEE* [viitattu 28.5.2012]. Saatavissa: http://www.ieee80211b.blogspot.com/

Kirkkolaki 26.11.1993/1054. Finlex. Lainsäädäntö [viitattu 26.5.2012]. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1993/19931054#L11

KpJungle 2012. *Authentication by radius* [viittattu 28.5.2012]. Saatavissa: http://kpjungle.wordpress.com/2009/08/18/authentication-by-radius-on-a-cisco-device/

NetGear 2012. *WEP Shared Key Authentication* [viitattu 28.5.2012] Saatavissa: http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-09.html

Telephony Online 2012. *Building future networks with MIMO and OFDM* [viitattu: 28.5.2012]. Saatavissa: http://connectedplanetonline.com/wireless/technology/mimo_ofdm_091905/

Wikipedia 2011a. *WLAN* [viitattu 19.3.2011]. Saatavissa: http://fi.wikipedia.org/wiki/WLAN

Wikipedia 2011b. *IEEE 802.11* [viitattu 19.3.2011]. Saatavissa: http://fi.wikipedia.org/wiki/IEEE_802.11

Wikipedia 2011c. *Langattoman lähiverkon tietoturva* [viitattu 22.3.2011]. Saatavissa: http://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva

Wikipedia 2011d. *Advanced Encryption Standard* [viitattu 19.3.2011]. Saatavissa: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Wikipedia 2011e. *Captive portal* [viitattu 23.3.2011]. Saatavissa: http://en.wikipedia.org/wiki/Captive_portal

Wikipedia 2011f. *ADLS* [viitattu 22.5.2012]. Saatavissa: http://fi.wikipedia.org/wiki/ADSL

Wikipedia 2011g. *ADLS2+* [viitattu 22.5.2012]. Saatavissa: http://fi.wikipedia.org/wiki/ADSL2%2B

Wikipedia 2011h. *RADIUS* [viitattu 26.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/RADIUS

Wikipedia 2011i. *MySQL* [viitattu 26.5.2011]. Saatavissa: http://fi.wikipedia.org/wiki/MySQL

Wireless network product 2012. *Wireless Technical Fundamentals* [viitattu 28.5.2012]. Saatavissa: http://www.wirelessnetworkproducts.com/wifitechfundamentals.aspx

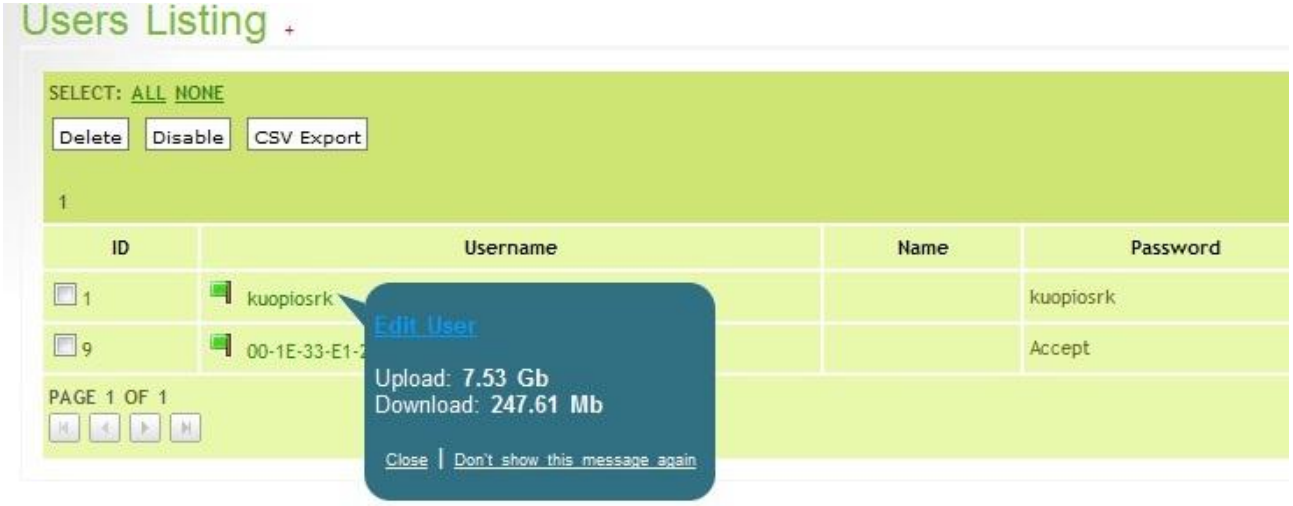
VIERAILIJAVERKON PALVELIMEN OHJE

Käyttäjätunnuksen vaihtaminen

Mene osoitteeseen http://84.250.200.47/daloradius/login.php (HUOM! Jos palvelimen IP on muuttunut joudut menemään vierailijaverkon kautta hallintasivuille. http://192.168.10.1/daloradius/login.php).

Kirjaudu seuraavilla tunnuksilla: Username: administrator Password: radius

Valitse välilehti Management -> List Users -> klikkaa hiirellä käyttäjää jonka tietoja haluat muuttaa ja valitse Edit User.

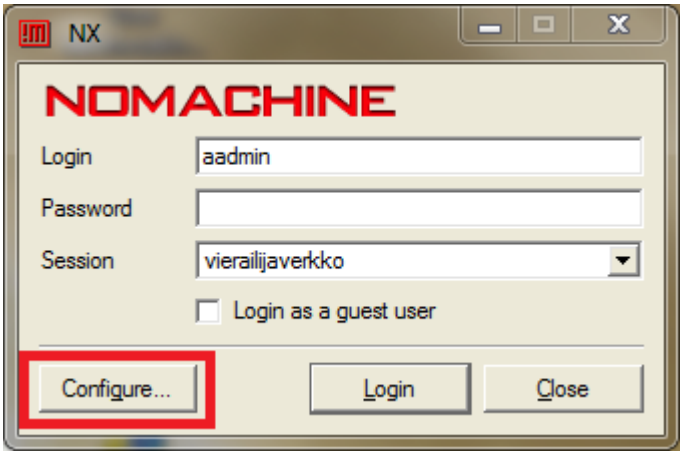


Uuden salasanan voit syöttää sivulle olevaan kenttään ja hyväksyä muutokset valitsemalla Apply. (Älä muuta muita asetuksia).

Etäyhteys vierailijaverkko palvelimelle

Etäyhteys palvelimeen otetaan NXclient ohjelmalla. Ohjelman löydät osoitteesta: http://www.nomachine.com/download-client-windows.php

Avaa NXclient, valitse Configure.



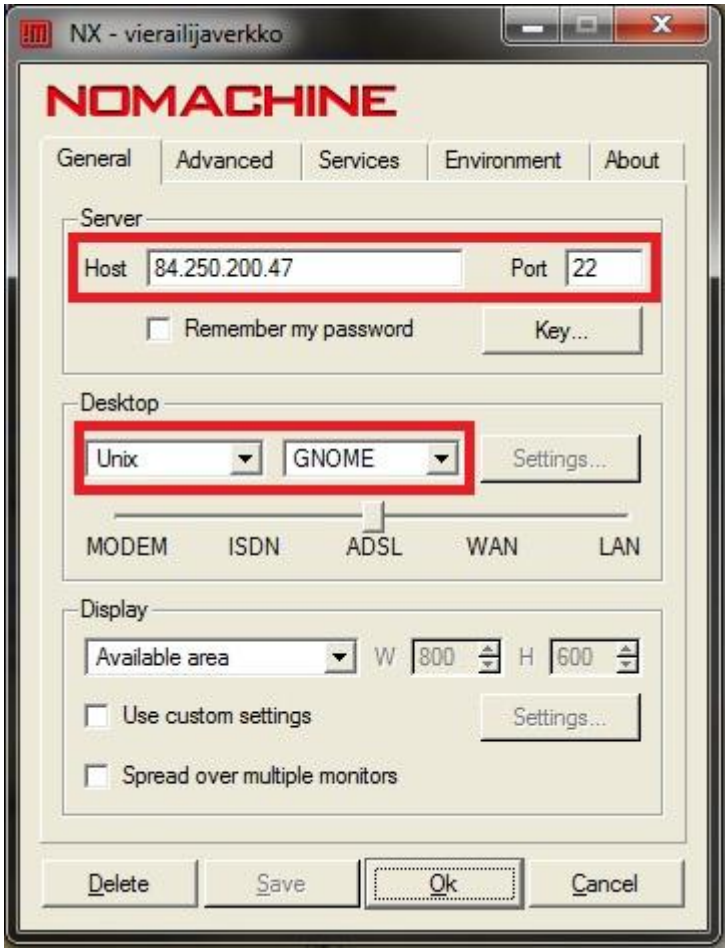
Syötä seuraavat tiedot General välilehdelle:

Host: 84.250.200.47

Port: 22

Desktop: UNIX ja GNOME

Valitse OK



Syötä seuraavat tunnukset kirjautumis ikkunaan:

Login: xxxxxx

Password: xxxxxxxx

Session: Voit itse keksiä, nxclient muistaa seuraavalla kerralla tämän session asetukset automaattisesti.

Valitse Login, jolloin etäyhteys palvelimeen tulisi aueta.


SAVONIA