TURUN AMMATTIKORKEAKOULU
ÅBO YRKESHÖGSKOLA

Opinnäytetyö

LANGATTOMAT VERKOT: OPENSPARK JA SPARKNET

Mikko Hartman

Tietojenkäsittely
Uusikaupunki
2009

TURUN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Koulutusohjelma: Tietojenkäsittely	
Tekijä: Mikko Hartman	
Työn nimi: Langattomat verkot: Openspark ja Sparknet	
Suuntautumisvaihtoehto: **Lähiverkkopalvelut**	**Ohjaaja:** **Kari Kouhia**
Opinnäytetyön valmistumisajankohta:	**Sivumäärä:** **58**

Tutkimuksessa käydään läpi erilaiset langattomat verkot. Tutkimustyö painottuu erityisesti langattomien verkkojen tietoturvaan johtuen Openspark- ja Sparknet-verkkosovelluksista, jotka ovat avoimia langattomia verkkoja.

Tutkimus tehdään useilla eri tietokoneilla, joissa kytkettynä Masterplanetin ohjelmiston sisältävä Buffalo AirStation Turbo G, langaton verkkopäätelaite.

Työhön kuuluu myös kattava ohjeistus oman Openspark- tukiaseman asentamiseen, käyttötilien luomiseen ja yhteyden muodostamiseen.

Openspark – tukiaseman käyttäjiin kuuluvat yksityiset ihmiset, jotka haluavat kokea langattomuuden vapauden kotonaan. Tukiaseman kantavuus riittää koko kotiin, joten erillisiä tukiasemia ei tarvita.

Työssä käytetään lähteenä pääasiassa Jim Geierin Langattomat verkot – kirjaa, josta asiat löytyvät parhaiten.

Hakusanat: Langattomat verkot, Openspark, Sparknet

Säilytyspaikka: Turun ammattikorkeakoulun kirjasto

TURKU POLYTECHNIC ABSTRACT

Degree Programme: Data Processing	
Author: Mikko Hartman	
Title: Openspark and SparkNet	
Specialization line: LAN services	**Instructor: Kari Kouhia**
Date: 19.11.08	**Total number of pages: 58**

This research deals with various wireless networks. It emphasizes especially the data security of wireless networks because of the Openspark and Sparknet network applications which are open wireless networks.

The research was conducted with several computers in which had the wireless network equipment, Buffalo Airstation G54 router, containing the software developed by Masterplanet.

Complete instructions are also included on how to install and configure a Buffalo Airstation G54 router, create an Openspark account and establish a connection.

Keywords: Wireless networks, Openspark, Sparknet

Deposit at: Turku University of Applied Science Library

SISÄLLYS

KUVAT

1 JOHDANTO

Työ toteutetaan Atk-Palvelu Mikrolalle. Työssä tutkitaan MP-Masteplanet Oy:n kehittämää langatonta Sparknet & Openspark verkkoyhteisöä.

Työssä käsitellään erilaisia langattomia verkkoja ja niiden tietoturvaa, keskittyen erityisesti avoimiin Openspark ja Sparknet – verkkosovelluksiin. Työssä käydään läpi langattomien verkkojen tietoturva, Sparknetin ja Opensparkin toimintaperiaate, erilaiset ominaisuudet ja käyttö. Työn tavoitteena on tutustua erilaisiin langattomiin verkkoihin, niiden rakenteisiin ja tietoturvaan. Työssä myös tutustutaan Openspark ja Sparknet – verkkosovelluksiin, käyttöönottoon ja käyttöön. Työ aihe on valittu sen kiinnostavuuden ja nykyaikaisuuden mukaan. Tänä päivänä lähes kaikessa elektroniikassa langaton on päivän sana. Itse olen kiinnostunut langattomasta tekniikasta, joten aihevalinta oli helppo

Tapasin Masterplanetin edustajan ollessani työharjoittelussa ja hänen kanssaan keskustellessani päätin valita kyseisen aiheen. Valitsin aiheen myös sen takia, että mielenkiintoista materiaalia oli saatavilla tarpeeksi.

Työhön kuuluu myös Buffalo -tukiaseman konfigurointiopas omaa OpensPark – yhteyden luontia varten.
Työ on aloitettu heinäkuussa 2007.

2 YRITYSESITTELY

2.1 Atk-Palvelu Mikrola

Atk - Palvelu Mikrola on vuonna 2000 perustettu atk-alan palveluyritys. Yrityksen kotipaikka on Naantali ja se toimii Turun talousalueella. Yrityksen asiakaskuntaan kuuluu pienet ja keskisuuret yritykset, yhdistykset ja yhteisöt sekä yksityishenkilöt.

Atk - Palvelu Mikrola tarjoaa seuraavia palveluita:

- tietokoneiden ja oheislaitteiden asennus ja huolto
- ohjelmistojen asennus ja alustava käytön opastus
- verkon asennus, palvelimen asennus ja liittäminen työasemiin sekä oheislaitteisiin
- virustorjunta- ennaltaehkäisy (F-Secure) ja viruksen konkreettinen poisto, ohjelmiston käytön opastus
- Internet- sivujen valmistus sekä päivitys
- DNA - laajakaistan jälleenmyynti
- yksityisopetus (Word, Excel, Power Point, HTML)

Yrityksen toimintaperiaatteena on asiakassuuntautunut toiminta, palvelu aloitetaan asiakkaan tilauksesta samana päivänä tai viimeistään seuraavana arkipäivänä asiakkaan niin halutessa.(www.mikrola.fi[viitattu 4.6.2008])

2.2 MP-Masterplanet Oy

MP -MasterPlanet Oy on lähiverkkoihin erikoistunut informaatio - teknologian ammattilainen. Yrityksen palvelu kattaa verkon koko elinkaaren: se kartoittaa asiakasyrityksen tarpeet sekä suunnittelee ja toteuttaa tietojärjestelmät. Palveluihin kuuluvat lisäksi verkon ylläpito, mikrotuki, konsultointi ja monipuoliset Internet-palvelut.

MP-Masterplanet Oy hallitsee sekä Windows -että Linux-ympäristöt. Yrityksen erikoisalaa ovat Microsoft BackOffice, Linux, verkkoprotokollat sekä tietoturvaratkaisut.

Osaamisesta on takeena Microsoft Certified Partner (MCP) - sertifikaatti, joten Windows - asennukset suorittavat Microsoftin hyväksymät asiantuntijat.

MP-Masterplanet tarjoaa yrityksille kokonaisvaltaisia verkkopalveluita, joihin kuuluvat verkon fyysinen asentaminen sekä verkon ylläpitoon tarvittavat toimenpiteet.

- kaapelointi
- lähiverkot: lähiverkkokeskittimet, kytkimet
- reititinverkot: reititysprotokollat ja osoitteistus, runkoreitittimet
- verkon käytettävyyden parantaminen
- järjestelmien ylläpito ja mikrotuki
- verkkojen tietoturva ja palomuurit
- verkon- ja järjestelmänhallinta
- yksilölliset Internet-palvelut
- verkon etäkäyttö ja VLAN
- konsultointi .

(www.mp-masterplanet.fi[viitattu 8.3.2009)

3 LANGATTOMAT VERKOT

Langattomilla verkoilla on nykyisin tärkeä rooli ihmisten elämässä niin työpaikalla, kotona kuin julkisissa tiloissakin. Vaikka langattoman verkon yksinkertaisena perustarkoituksena on tarjota käyttäjien ja tiedonlähteiden välille langattomat yhteydet, on tarpeellista tuntea langattomien verkkojen tärkeimmät käsitteet.

3.1 Langattoman verkon määritelmä

Langattoman verkon avulla ihmiset voivat viestiä keskenään ja olla yhteydessä sovelluksiin ja tietoon ilman fyysistä tietoverkkoa. Tämä mahdollistaa liikkumisen vapauden. Langattoman verkon avulla sovellukset toimivat lähes missä tahansa. Esimerkiksi kotonaan Internetiä käyttävät ihmiset voivat olla rauhallisessa paikassa loitolla melusta ja häiriötekijöistä. Langattomien verkkojen avulla ihmiset voivat käyttää Internetiä lähes missä tahansa. (Geier 2005, 3-5; Puska 2000, 12)

Langattomia viestintäjärjestelmiä on useita erilaisia, mutta langattoman verkon erottaa muista se, että siinä on kysymys kahden tietokonelaitteen välisestä viestinnästä. Näihin laitteisiin sisältyvät kämmentietokoneet, kannettavat tietokoneet, henkilökohtaiset tietokoneet, palvelimet ja tulostimet. Tietokonelaitteessa on prosessori, muistia ja liitäntä jonkin tyyppiseen verkkoon. Perinteisesti matkapuhelinten ei ole katsottu kuuluvan tietokonelaitteisiin. Kuitenkin uusimmissa puhelimissa ja kuulokkeissa on nykyisin kyky käsitellä tietoa ja puhelimet sisältävät verkkosovittimen. (Geier 2005, 3-5; Puska 2000, 12)

Langallisten, kupariin tai optiseen kuituun perustuvien verkkojen lailla langattomat verkot siirtävät tietoa tietokonelaitteiden välillä. Tieto voi olla sähköpostiviestejä, web-sivuja, tiedostoja, videota tai ääntä. Useimmiten langattomissa verkoissa siirretään tietoa, kuten sähköpostiviestejä ja tiedostoja, mutta langattomien verkkojen suorituskyvyn kehittyminen tekee tänä päivän mahdolliseksi myös video- ja puhesovelluksien siirtämisen.. (Geier 2005, 3-5; Puska 2000, 12)

Langattomat verkot voidaan jakaa useaan eri ryhmään sen perusteella, kuinka laajan fyysisen alueen ne peittävät. Seuraavat langattomien verkkojen tyypit vastaavat erilaisiin käyttäjien tarpeisiin:

- langaton henkilökohtainen lähiverkko (PAN)
- langaton lähiverkko (LAN)
- langaton kaupunkiverkko (MAN)
- langaton laajaverkko (WAN)

Langattomien verkkotyyppien vertailua

Tyyppi	**Peittoalue**	**Suorituskyky**	**Standardit**	**Sovellukset**
Langaton henkilökohtainen lähiverkko (PAN)	Henkilön lähiympäristö	Keskinkertainen	Bluetooth, IEEE 802.15 ja IrDa	Oheislaitekaapelien korvaaminen
Langaton lähiverkko (LAN)	Rakennus tai rakennusalue	Korkea	IEEE 802.11, Wi-Fi	Lankaverkkojen laajentaminen
Langaton kaupunkiverkko (MAN)	Kaupungin alue	Korkea	Valmistaja-kohtaiset, IEEE 802.16 ja WIMAX	Kiinteät langattomat yhteydet kotien ja yritysten sekä Internetin välillä
Langaton laajaverkko (WAN)	Maailmanlaajuinen	Alhainen	CDPD ja 2G, 2,5G ja 3G	Mobiilit yhteydet Internetiin ulkotiloista

3.2 Langattomat henkilökohtaiset lähiverkot (PAN)

Langattomien henkilökohtaisten lähiverkkojen kantama on nykypäivänä 15 – 200 metriä, riippuen siitä, onko yhteys avoin vai onko tiellä metsää, rakennuksia tai muita yhteyttä haittaavia tekijöitä. Yhteydet ovat parhaimmillaan pienessä huoneessa, asunnossa ja henkilön lähiympäristössä. Langattomien henkilökohtaisten verkkojen suorituskyky vastaa tänä päivänä laajakaistanopeuksia. Tällä hetkellä niiden tiedonsiirtonopeus on noin 54 Mbps. Nämä ominaisuudet ovat täysin riittävät korvaamaan kaapeliyhteyden. (Geier 2005, 7; Jaakonhuhta 2002, 4)

Useimpien langattomien henkilökohtaisten lähiverkkojen tiedonsiirto perustuu radioaaltojen käyttöön. Esimerkiksi Bluetooth – verkko toimii 2,4 GHz:n taajuuskaistalla, toimintasäde on 10 - 100 metriä. Toimintasäde riippuu lähetystehosta ja radiotien esteistä. Lisäksi Institute of Electronic Engineers – organisaation eli IEEE:n standardi 802.15 sisältää Bluetooth-spesifikaation langattomia henkilökohtaisia lähiverkkoja varten. (Geier 2005, 7; Jaakohuhta 2002, 4; Jaakohuhta 2001, 58)

Jotkut langattomat henkilökohtaiset lähiverkot käyttävät kahden pisteen väliseen siirtoon infrapunavaloa. Infrared Associationin eli IrDa:n spesifikaatio määrittelee suorien infrapunasäteiden käytön. Niiden kantama on enintään muutaman metrin ja tiedonsiirtonopeus 4 Mbps. Infrapunavalon etuna on vapaus radiotaajuuden häiriöistä, mutta langattomien rakenneosien sijoittelua rajoittaa näköyhteyden vaatimus laitteiden välillä. (Geier 2005, 7; Jaakohuhta 2002, 4)

3.3 Langattomat lähiverkot (WLAN)

Langattomat lähiverkot tarjoavat korkean suorituskyvyn toimisto- ja tehdasrakennuksissa sekä kodeissa. Näissä tiloissa käyttäjien laitteisto muodostuu tehokkaista kannettavista tietokoneista, työasemista ja kämmentietokoneista. Langaton lähiverkko täyttää hyvin tällaisten tietokonelaitteiden yhteystarpeet.

Langattomat lähiverkot kykenevät helposti siirtämään tehokkaiden sovellusten vaatiman suuren tietomäärän. Langattoman lähiverkon tiedonsiirtonopeus voi olla jopa 108 tai 125 Mbps, joka riittää lähes kaikkien toimisto- ja kotiverkkosovellusten tarpeisiin.

Langattomat lähiverkot muistuttavat suorituskykynsä, kustannustensa ja toimintansa suhteen perinteisiä langallisia Ethernet – lähiverkkoja. (Geier 2005, 8-9; Jaakohuhta 2002, 4)

IEEE 802.11 on vallitsevin langattomien lähiverkkojen standardi, ja sen versiot toimivat 2,4 GHz:n ja 5 GHz:n taajuuskaistoilla. 802.11:n ongelmana on, että standardin eri versioiden keskinäisessä sopivuudessa on rajoituksia. Vaikka 802.11a–version mukaiset laitteet eivät kykene muodostamaan yhteyttä laitteeseen, jossa on käytössä 802.11b-versio, ongelma ei ole suuri koska 802.11a-standardi on käytössä Euroopassa ja 802.11b-versio Yhdysvalloissa. Lisäksi 802.11–standardi on tietoturvaominaisuuksiltaan puutteellinen. (Geier 2005, 8-9; Jaakohuhta 2002, 4)

802.11 – standardin puutteiden korjaamiseksi Wi-Fi Alliance – valmistajayhteenliittymä on sisällyttänyt 802.11:n valikoituja toimintoja standardiin, josta se käyttää nimitystä Wireless Fidelity eli Wi-Fi. Jos langaton lähiverkkotuote on Wi-Fi -yhteensopiva, sen toimivuus muiden Wi-Fi – laitteiden kanssa on taattu. Wi-Fin avoimuudella on pyritty takaamaan se, että erilaiset käyttäjät voivat toimia samassa langattomassa lähiverkossa. Avoimuus on tärkeä julkisissa langattomissa lähiverkoissa. (Geier 2005, 8-9; Jaakohuhta 2002, 4)

3.4 Langattomat kaupunkiverkot (MAN)

Langattomat kaupunkiverkot ovat laajuudeltaan kaupunkialueiden laajuisia, ja niitä käytetään kiinteiden yhteyksien dataverkkoina. Myös jotkut mobiilisovellukset pystyvät hyödyntämään niitä. Esimerkiksi sairaalat voivat käyttää langatonta kaupunkiverkkoa sairaaloiden väliseen tietoliikenneyhteyteen. Langaton kaupunkiverkko yhdistää olemassa olevat verkot toisiinsa tai tarjoaa liikkuville käyttäjille yhteydet jo olemassa olevaan verkkoon. (Geier 2005, 9–11; Jaakohuhta 2002, 4)

Langattomien Internet-palvelujen tarjoajat omistavat langattomia kaupunkiverkkoja kaupungeissa ja niiden ulkopuolella. Näin ne voivat tarjota langattomia yhteyksiä kodeille ja yrityksille laajalla alueella. Langaton kaupunkiverkko tarjoaa merkittäviä

etuja silloin, kun perinteisiä lankayhteyksiä ei ole mahdollista käyttää. Langattomat kaupunkiverkot ovat tehokkaita varsinkin silloin, kun perinteisen verkon rakentaminen on hankalaa tai kallista. (Geier 2005, 9–11; Jaakohuhta 2002, 4)

Markkinoilla on useita valmistajakohtaisia langattomia kaupunkiverkkoratkaisuja, mutta eri standardeihin perustuvat ratkaisut yleistyvät nopeasti. Jotkut valmistajat hyödyntävät langattomien kaupunkiverkkojen perustana IEEE 802.11 – standardia. 802.11 – järjestelmät sopivat rakennusten sisäiseen käyttöön, niillä voidaan myös yhdistää kaupunkialueen sisällä sijaitsevia rakennuksia signaalien lähetys- ja vastaanottosuuntauksen keskittävillä antenneilla. (Geier 2005, 9–11; Jaakohuhta 2002, 4)

”Kasvava joukko yrityksiä on alkanut ottaa käyttöön IEEE 802.16 – pohjaisia ratkaisuja. Kyseessä on melko uusi standardi. Se mahdollistaa tehokkaiden langattomien kaupunkiverkkojen toteuttamisen, ja sillä saavutetaan useiden megabittien nopeus pitkilläkin etäisyyksillä. 802.16 – standardi tulee todennäköisesti muodostumaan langattomien kaupunkiverkkojen perusratkaisuksi.” (Geier 2005, 9–11; Jaakohuhta 2002, 4)

3.5 Langattomat laajaverkot (WAN)

Langattomat laajaverkot tarjoavat mahdollisuuden mobiilisovellusten käyttöön laajoilla, kokonaisen maan tai maanosan suuruisilla alueilla. Tällöin palveluille voidaan saada suuri asiakaskunta, mikä mahdollistaa melko kalliin verkkoinfrastruksuurin käytön. Käyttökustannukset pysyvät kohtuullisina, koska käyttäjiä on paljon.

Langattomat laajaverkot voivat kattaa lähes koko maapallon, jos eri operaattorit tekevät yhteistyötä. Operaattoreiden väliset vakiintuneet verkkovierailu- eli roaming-sopimukset mahdollistavat nopean langattoman dataliikenteen tarvitsemat jatkuvat yhteydet. Käyttäjä voi saada rajoitetut Internet-palvelut langattoman laajaverkon kautta lähes missä tahansa, vaikka on vain yhden operaattorin asiakas.

Langattomien laajaverkkojen suorituskyky on ollut melko alhainen aina viime aikoihin saakka. Siirtonopeudet ovat vastanneet tasoltaan modeemien suorituskykyä.

Nykyaikaisten 3G-järjestelmien tiedonsiirtonopeudet voivat olla useita megabittejä sekunnissa.

Langattomat laajaverkot eivät toimi sisätiloissa, sillä niiden tekniikka on suunniteltu avonaiseen maastoon. Verkkoa ei voi käyttää toimistoissa, lentoasemilla ja vastaavissa paikoissa, koska verkon perustana olevat radiosignaalit menettävät sisätiloihin saapuessaan valtaosan tehostaan. Niinpä langattomien laajaverkkojen käyttäjien yhteyksien suorituskyky heikkenee tai he eivät saa siihen yhteyttä lainkaan. Jotkut teleoperaattorit asentavat rakennuksiin toistimia parantaakseen verkkojen kattavuutta, mutta tämä on kallista eikä useissa tapauksissa lainkaan mahdollista. Teleoperaattorit käyttävät yhdistämisessä ATM-, Frame Relay- tai kiinteitä reititinverkkoyhteyksiä. (Geier 2005, 11-13; Jaakohuhta 2002, 4)

4 LANGATTOMIEN VERKKOJEN HYÖDYT

Ihmiset ympäri maailman ovat havainneet langattomuuden tarjoamat hyödyt. Tuotteet, joissa on langaton liitäntä, mahdollistavat ihmisten työskentelyn ja viihdepalvelujen käytön olinpaikastaan riippumatta. Langaton verkko tekee tarpeettomaksi johdot tietokonelaitteiden ja olemassa olevien verkkojen välillä. Näin tietokonelaitteet ja käyttäjät voivat liikkua vapaasti ja pysyä samalla kuitenkin yhteydessä Internetiin ja yrityksen sovelluksiin. Yhteys voidaan säilyttää, oli käyttäjä sitten missä tahansa.

4.1 Tehokkuuden ja tarkkuuden paraneminen

Yksi houkuttelevimmista perusteista langattomien verkkojen asentamiseen on parantuva tuottavuus. Langaton verkko on hyödyllinen, mikäli sen tuomat säästöt ylittävät asennuksesta ja tuesta syntyvät kustannukset. Positiivinen tuotto sijoitetulle pääomalle kannustaa käyttämään uusia järjestelmiä.

Tuottavuuden paranemisen lisäksi langattomat verkot tarjoavat toimistoympäristössä seuraavia hyötyjä:

- Käyttäjät voivat käyttää verkkoa vaikka yrityksen toimitiloissa tehtäisiin muutoksia rakenteisiin, esimerkiksi väliseinien siirtoa.
- Vierailevat työntekijät voivat käyttää helposti yrityksen verkkopalvelimia ja sovelluksia.
- Yritys voi kustannuksia säästääkseen ottaa käyttöön langattomia lisäsovelluksia, kuten matkapuhelimet.

4.2 Luotettavuuden paraneminen

Epäluotettavuus on kaapeleille uhka, kaapelit kuluvat ja niitä voidaan helposti käsitellä väärin. Huonosti tehty asennus ja kaapelien vaurioituminen ovat suurimpia syitä lankaverkkojen vikaantumiseen. Puhelinasentaja voi esimerkiksi puhelinjärjestelmän vikaa korjatessaan katkaista vahingossa tietoverkkokaapelin. Tästä seuraa järjestelmän toimintakatkos, jolloin verkkovastaavan täytyy selvittää, mistä vika johtuu.

Langaton verkko vähentää fyysisistä vaurioista johtuvia ongelmia. Järjestelmän käytettävyys paranee, ja käyttäjillä on verkkoyhteys suuremman osan aikaa. Lankaverkko voi olla välttämätön, mikäli langaton verkko ei pysty vastaamaan asetettuihin suorituskykyvaatimuksiin, mutta langatonta verkkoa voidaan käyttää varmistusratkaisuna. Langallisen ja langattoman yhteyden yhdistelmä rakennusten välillä tekee järjestelmästä sekä suorituskykyisen että luotettavan.

Toki täytyy aina ottaa huomioon, että tietoturvallisuutta ajatellen kaapeli on varmempi ratkaisu, koska siihen eivät luvattomat käyttäjät pääse käsiksi. Langattomia verkkoja käytettäessä onkin aina varmistettava yhteyden riittävä suojaus ja se, että tietokoneen virustorjunta ja palomuuri ovat ajan tasalla.

5 LANGATTOMIEN VERKKOJEN TIETOTURVA

Tietoturva on elintärkeää langattomille verkoille, koska viestisignaalit ovat avoimesti tavoitettavissa niiden edetessä ilmassa. Langattomia verkkoja käyttävien yritysten ja henkilöiden on oltava tietoisia mahdollisista ongelmista ja riskeistä sekä niihin liittyvistä vastatoimista. Hakkerien mahdollisuus tarkkailla verkon liikennettä, päästä luvattomasti arvokkaisiin tietoihin ja suorittaa palvelunestohyökkäyksiä ovat ongelmia, joihin langattomissa verkoissa on kiinnitettävä huomiota. Uhkia on mahdollista vähentää merkittävästi tehokkaan salausjärjestelmän käytöllä. On kuitenkin syytä muistaa, että tietoturvan tarvittava taso riippuu vaatimuksista. Kotisovellusten hyväksyttävä turvataso on paljon alhaisempi kuin yrityksen vastaava turvataso. (Geier 2005, 171-172)

5.1 Tietoturvauhat

Langattomiin verkkoihin kohdistuu monenlaisia tietoturvauhkia. Esimerkiksi hakkerit voivat varastaa yritykseltä tietoja, hankkia luvattoman pääsyn sovelluksiin ja jopa keskeyttää verkon toiminnan.

5.1.1 Liikenteen tarkkailu

Kokenut hakkeri tai jopa satunnainen ”nuuskija” voi helposti tarkkailla salaamattomia ilmateitse kulkevia datapaketteja hakkerointityökaluilla, joita ovat esimerkiksi AirMagnet ja AiroPeek. Ne näyttävät sellaisenaan datapakettien sisällön. Hakkerit voivat esimerkiksi seurata kaikkia kyseisessä verkossa tapahtuvaa liikennettä satojen metrien päässä rakennuksesta, jossa langaton lähiverkko sijaitsee. Tällöin kuka tahansa voi periaatteessa hankkia tietoonsa käyttäjätunnuksia, salasanoja tai luottokorttinumeroita. Esimerkkinä tästä ovat niin sanotut war driverit, jotka ajavat autolla ympäriinsä etsien suojaamattomia langattomia lähiverkkoja ja laittavat vain huvin vuoksi löytönsä esille web-sivustoille. (Geier 2005, 171-172)

Ratkaisuna ongelmaan on, että langattomassa yhteydessä käytetään salausta. Salaus koodaa databitit salaisen avaimen avulla. Koska avain on salainen, hakkeri ei pysty purkamaan salausta. Ainoastaan tehokkaiden ja tarpeeksi monimutkaisten salausmekanismien käyttö turvaa datan yksityisyyden ja langattoman verkon turvallisuuden. (Geier 2005, 171-172)

5.1.2 Luvaton pääsy

Langattoman sovelluksen tarkkailu on helppoa. On myös vaivatonta päästä ulkopuolelta yrityksen langattomaan verkkoon, mikäli suojaustoimenpiteisiin ei ole ryhdytty. Valitettavasti monet yritykset ottavat langattomat verkkonsa käyttöön oletusarvoisilla, turvattomilla salaustoimenpiteillä. Tämä tekee kenelle tahansa mahdolliseksi muodostaa yhteys yrityksen palvelimiin. Näin voi käydä myös kodeissa ulkopuolisen tunkeutuessa käyttäjän langattomaan tukiasemaan. Tutkimusten mukaan keskivertokaupungin langattomista tukiasemista 30 prosenttia on täysin vailla tietoturvaa.

Windows XP – käyttöjärjestelmä tekee yhteydenmuodostuksen langattomiin verkkoihin helpoksi. Tämä koskee erityisesti julkisia langattomia lähiverkkoja. Kun kannettava kytkeytyy langattomaan lähiverkkoon, käyttäjä voi navigoida mihin tahansa samaan langattomaan lähiverkkoon kytkeytyneeseen toiseen kannettavaan. Ilman henkilökohtaisen palomuurin tarjoamaa tietoturvaa ulkopuolisen on mahdollista päästä käsiksi käyttäjän koneen luottamuksellisiin tiedostoihin. Luvaton käyttäjä voi myös käyttää konetta rikoksentekovälineenä koneen omistaja ollessa täysin tietämätön tapahtuneesta.

Vaikka tukiasemissa olisi otettu käyttöön kaikki tietoturvasuojaukset, voi vakavan uhan muodostaa niin sanottu rosvotukiasema. Se on verkossa oleva luvaton tukiasema. Työntekijä voi hankkia tukiaseman ja asentaa sen toimistoonsa tuntematta tämän seurausvaikutuksia tietoturvalle. Myös hakkeri voi asentaa yrityksen tiloihin rosvotukiaseman liittämällä tarkoituksella suojaamattoman tukiaseman yrityksen verkkoon. Rosvotukiasemaa voidaan käyttää, koska siinä yhteys on todennäköisesti salaamaton. Tämä tarjoaa avoimen oven, jonka kautta yrityksen verkkoon on helppo päästä tilojen ulkopuolelta. Yritysten tulisikin jatkuvasti tarkkailla verkkoaan

rosvotukiasemien varalta. Täytyy myös muistaa, että tällainen vihamielinen tukiasema on ongelma, oli yrityksessä sitten langaton verkko tai ei. Rosvotukiasema voidaan asentaa myös langalliseen verkkoon, jossa ei ennestään ole yhtään langatonta komponenttia.

Luvattoman pääsyn estämiseksi langattomassa verkossa tulisi olla yhtenäinen kaksisuuntainen todennus asiakaslaitteiden ja tukiasemien välillä. Todennus on tunnistustoiminto, jossa henkilö tai laite tunnistetaan. Langattomassa verkossa tulisi käyttää menetelmiä, joissa asiakaslaitteet todennetaan tukiasemissa ja päinvastoin. Tämä varmistaa käyttäjän turvallisuuden ja sen, että yhteys muodostetaan luvalliseen tukiasemaan. Lisäksi tukiasemien täytyy todentaa itsensä kytkimille, millä estetään rosvotukiaseman liittäminen verkkoon. (Geier 2005, 172-174)

5.1.3 Välistävetohyökkäykset

Salaus- ja todennustekniikoiden käyttö parantaa langattoman verkon tietoturvaa. Taitavat hakkerit pystyvät silti löytämään verkosta heikkouksia, jotka johtuvat verkkoprotokollien toiminnasta. Selvä heikkous ovat välistävetohyökkäykset, joissa hakkerit laittavat valelaitteen käyttäjien ja langattoman verkon väliin. Tyypillinen välistävetohyökkäys käyttää hyväkseen yleistä ARP – protokollaa, jota kaikki TCP/IP – verkot käyttävät. Hakkeri voi käyttää ARP – protokollaa hyödykseen ja ottaa langattoman verkon hallintaansa.

ARP on tärkeä toiminto, jota lähettävä langaton tai langallinen verkkokortti käyttää selvittääkseen kohdeverkkokortin fyysisen osoitteen eli MAC – osoitteen. Lähettävän verkkokortin lähettävän verkkokortin on tiedettävä kohteen MAC – osoite. Verkkokortti ymmärtää ja vastaa ainoastaan fyysiseen MAC – osoitteeseen.

Datan lähettävällä sovelluksella on kohteen IP – osoite, mutta lähettävän verkkokortin on käytettävä ARP:tä saadakseen selville sitä vastaavan fyysisen osoitteen. Verkkokortti saa osoitteen lähettämällä yleislähetyksenä ARP – pyyntöpaketin, joka sisältää kohdeverkkokortin IP – osoitteen. Kaikki asemat kuulevat tämän pyynnön, ja oikean IP-

osoitteen omaava asema palauttaa ARP – vastauspaketin, joka sisältää sen MAC – osoitteen ja IP – osoitteen.

Lähettävä asema laittaa sitten tämän MAC – osoitteen lähetettävän kehyksen kohdeosoitteeksi. Lähettävä asema myös tallentaa tämän IP – osoitteen ja sitä vastaavan MAC – osoitteen erilliseen tauluun määräajaksi tai siksi, kunnes asema vastaanottaa uuden ARP – vastauksen kyseisen IP – osoitteen omaavalta asemalta.

ARP:n ongelmana on sen synnyttämä tietoturvariski, joka johtuu ARP spoofing – toiminnosta. Hakkeri voi huiputtaa tukiasemaa lähettämällä rosvotukiasemalta valheellisen ARP – vastauksen, joka sisältää luvallisen verkkolaitteen IP – osoitteen ja rosvolaitteen MAC – osoitteen. Tästä seuraa, että kaikki luvalliset verkon asemat päivittävät automaattisesti ARP – taulunsa väärillä tiedoilla. Nämä laitteet lähettävät edelleen kaikki tulevat paketit rosvolaitteelle eivätkä oikealle ja lailliselle tukiasemalle tai reitittimelle. Tämä on klassinen välistävetohyökkäys, jolla hakkeri voi manipuloida käyttäjäistuntoja. Seurauksena hakkeri voi saada haltuunsa salasanoja, siepata arkaluontoista dataa tai muodostaa yhteyden yrityksen palvelimiin samalla tavalla kuin luvallinen käyttäjä.

Jotkut valmistajat estävät ARP spoofing – toimintoon perustuvat välistävetohyökkäykset käyttämällä Secure ARP:tä eli SARP:tä. Tämä ARP:n laajennus tarjoaa erityisen turvatunnelin jokaisen asiakkaan ja langattoman tukiaseman tai reitittimen välille. Tätä tekniikkaa käyttävät laitteet jättävät huomioimatta kaikki ARP – vastaukset, jotka eivät liity tunnelin toisessa päässä oleviin asiakkaisiin. Tällöin ARP – tauluja päivitetään vain laillisten vastausten perusteella ja SARP:tä käyttävät asemat eivät joudu osoitemanipuloinnin kohteiksi.

SARP:n käyttö edellyttää kuitenkin erikoisohjelmistojen asentamista kaikkiin laitteisiin. Siksi SARP ei myöskään ole käyttökelpoinen julkisilla langattomilla palvelualueilla. Yritykset voivat kuitenkin asentaa SARP:n ja vapautua lähes kokonaan välistävetohyökkäyksiltä. (Geier 2005, 175)

5.1.4 Palvelunesto (DoS)

Palvelunestohyökkäys voi estää tai kaataa langattoman verkon. Kaikkien langattomia verkkoja käyttävien tulee ottaa huomioon tällaisen hyökkäyksen mahdollisuus. Palvelunestohyökkäyksen vakavuus riippuu siitä, millaisia seurauksia langattoman verkon toimintakyvyttömyydestä aiheutuu. Hakkeri voi esimerkiksi kaataa langattoman kotilähiverkon, mutta seurauksena on vain hieman hankaluuksia kotikäyttäjälle. Palvelunestohyökkäys, joka sulkee yrityksen langattoman varastohallintajärjestelmän, voi kuitenkin aiheuttaa paljon suurempia taloudellisia tappioita.

Yksi palvelinestohyökkäysten muoto on väsytyshyökkäys. Tällainen on esimerkiksi hyökkäys, jossa verkko rampautetaan valtavalla määrällä paketteja. Valtava liikenne kuluttaa verkon kaikki resurssit, ja seurauksena on verkon kaatuminen. Internetissä on työkaluja, joilla hakkerit voivat rampauttaa langattoman verkon. Hakkeri voi suorittaa hyökkäyksen lähettämällä hyödyttömiä paketteja palvelimelle verkon muilta tietokoneilta. Tämä kasvattaa verkonrasitetta ja vie kaistaa luvallisilta käyttäjiltä.

Jotkin tietoturvamekanismit ovat palvelunestohyökkäysten keskeisiä kohteita. Esim. Wi-Fi Protected Access eli WPA on haavoittuvainen tietyntyyppiselle palvelunestohyökkäykselle. WPA käyttää matemaattisia algoritmeja verkon käyttäjien todennuksessa. Jos käyttäjä yrittää päästä verkkoon ja lähettää kaksi valtuuttamatonta pakettia sekunnin sisällä, WPA olettaa joutuneensa hyökkäyksen kohteeksi ja sulkee verkon.

Ainoa täysin tehokas tapa suojautua palvelunestohyökkäyksiltä on eristää tietokone ja kytkeä se irti kaikista verkoista. Viranomaiset käyttävät tätä menetelmää suojatakseen kaikkein arkaluontoisimmat tietonsa, mutta ratkaisu ei ole käyttökelpoinen yritys- tai kotikäyttäjän kannalta. Palvelunestohyökkäyksiä estetään parhaiten kehittämällä ja pitämällä yllä vahvoja tietoturvakäytäntöjä. Palomuurien käytön ja päivitysten, virussuojauksen ylläpidon, ajan tasalla olevien tietoturvapäivitysten asentamisen ja vahvojen salasanojen käytön tulisi olla rutiinia kaikissa yrityksissä ja kodeissa. Verkkolaitteet tulisi myös sammuttaa silloin, kun niitä ei tarvita.

Langattoman lähiverkon voi suojata palvelunestohyökkäyksiltä tekemällä rakennuksesta mahdollisimman vastustuskykyisen sisään tulevia radiosignaaleja vastaan esimerkiksi seuraavin toimenpitein:

- Jos sisäseinissä käytetään metallisia tukirakenteita, on varmistettava, että ne on maadoitettu.
- Ikkunoiden tulee olla kuparilämpöeristettyjä tai metallikalvopohjaisia ja metallivärjättyjä.
- Lähettimen teho tulee asettaa siten, että vuoto ehkäistään tai se laskee tasolle, jolla hakkerin paikallistaminen on helppoa.
- Suunnattavat tukiasema-antennit tulee kohdistaa rakennuksen sisäosan suuntaan.

Koska kaikilta hyökkäystyypeiltä ei ole mahdollista suojautua täydellisesti, on syytä laatia toimintasuunnitelma siltä varalta, että palvelunestohyökkäys aiheuttaisi merkittävää vahinkoa. (Geier 2005, 171-178)

5.2 Salaus

Salaus muuntaa datapaketin bittejä tietyllä menetelmällä. Jos salakuuntelija saa tiedot käsiinsä, tavoitteena on, että hän ei pysty tulkitsemaan viestiä. Ennen salausta datan sanotaan olevan selväkielistä. Salaus muuttaa tuotetun tekstin salatuksi, jolloin se voidaan purkaa vain oikealla salaisella avaimella.

WEP on symmetrinen salausmenetelmä eli salauksen purkamiseen käytetään samaa avainta, jolla se on tehty. Jotta symmetrinen salaus olisi riittävän tehokasta, on salausavainten uudelleen käyttäminen estettävä muuttamalla niitä usein. Tämä lyhentää hakkerin aikaa verkkoon murtautumiseen ja tekee verkon tietoturvan murtamisen hankalaksi, ellei mahdottomaksi. Siksi symmetrisissä salausmekanismeissa täytyy olla tehokkaat avaintenjakelumenetelmät.

Julkisen avaimen salauksessa käytetään epäsymmetrisiä avaimia, yksityistä ja julkista. Tämä mahdollistaa tehokkaammat salaus- ja todennusmenetelmät, koska se yksinkertaistaa avainten jakelua. Julkisen avaimen salauksen tärkeä vaatimus on salausten toisiaan vastaavuus salauksen näkökulmasta. Lähettävä asema voi esimerkiksi

salata datan julkisella avaimella ja vastaanottaja käyttää yksityistä avainta purkaakseen salauksen tai päinvastoin.

5.2.1 WEP

WEP on 802.11:n salaus- ja todennusstandardi. Se on toteutettu MAC – kerroksessa, ja sitä tukevat useimmat radioverkkokorttien ja tukiasemien valmistajat. Langatonta verkkoa toteutettaessa on tarpeen ymmärtää, millä tavalla WEP pystyy parantamaan tietoturvaa.

Käyttäjän aktivoidessa WEP:n, verkkokortti salaa ennen lähettämistä jokaisen 802.11 – kehyksen hyötykuorman käyttäen RSA:n RC4-vuosalausta. Vastaanottava asema, kuten tukiasema tai toinen verkkokortti, purkaa kehyksen saavuttua sen salauksen. 802.11 WEP salaa siis datan ainoastaan 802.11 – asemien välillä.

”Osana salausprosessia WEP valmistelee avainaikataulun tai juuren linkittämällä lähettävän aseman valmistajan tarjoaman jaetun salaisen avaimen satunnaisesti luotuun 24-bittiseen alustusvektoriin. Alustusvektori pidentää salaisen avaimen elinaikaa, koska asema voi muuttaa sitä jokaisen kehyksen lähettämisen kohdalla. WEP syöttää tuloksena olevan juuren näennäiseen satunnaislukugeneraattoriin, tämä tuottaa avainmerkkijonon, joka vastaa kehyksen hyötykuorman ja 32-bittisen eheystarkisteen pituutta. Eheystarkiste on tarkistussumma, jonka vastaanottava asema laskee uudelleen. Se vertaa saamaansa tulosta lähettävältä asemalta saamaansa tarkistukseen. Vertailun perusteella se päättelee, onko lähetettyä dataa peukaloitu tiedonsiirron aikana.

WEP määrittelee datan salaukseen ja salauksen purkamiseen jaetun salaisen avaimen. Vastaanottavan aseman on käytettävä samaa avainta salauksen purkamiseen. Siksi jokainen radioverkkokortti ja tukiasema on konfiguroitava käsin käyttämään samaa avainta. Ennen lähetystä WEP yhdistää avainmerkkijonon ja hyötykuorman sekä eheystarkisteen bittitason XOR - prosessilla, joka tuottaa salatun tekstin. WEP sisällyttää alustusvektorin selväkielisenä kehysrungon muutamaan ensimmäiseen tavuun. Vastaanottava asema käyttää tätä alustusvektoria yhdessä käyttäjän antaman jaetun salaisen avaimen kanssa purkaakseen kehysrungon hyötykuormaosan salauksen.

Yleensä lähettävä asema käyttää kussakin kehyksessä eri alustusvektoria. Tätä ei tosin edellytetä 802.11 – standardissa. Kun asema lähettää viestejä joilla on sama alkuosa, kunkin salatun hyötykuorman alkuosa on sama, kun käytetään samaa avainta. Kun data on salattu, kehyksen alkuosa olisi sama, mikä tarjoaisi toistuvan mallin, jota hakkerit voisivat käyttää salausalgoritmin murtamiseen. Koska useimmissa kehyksissä on eri alustusvektori, WEP tarjoaa suojan tämänkaltaista hyökkäystä vastaan. Alustusvektorin usein toistuva vaihtaminen parantaa myös WEPin kykyä suojata dataa murtamisyrityksiltä.” (Geier, 181-182)

5.2.2 WEPin ongelmia

WEP in alustusvektorit ovat melko lyhyitä ja avaimet ovat kiinteitä mistä johtuu se, että WEP on haavoittuva. WEPin ongelmat eivät itse asiassa juurikaan liity salausalgoritmiin. WEP on vain 24 – bittinen, joten se käyttää tietyn ajan kuluttua uudelleen samaa alustusvektoria eri datapaketissa. Suuressa verkossa sama alustusvektori voi toistua suhteellisen lyhyessä ajassa. Tästä seuraa, että lähetettävien kehysten avainmerkkijonot ovat liian samanlaisia. Jos hakkerilla on hallussaan riittävä määrä kehyksiä, hän voi päätellä jaetun salaisen avaimen. Tämä johtaa siihen, että hakkeri pystyy purkamaan minkä tahansa 802.11-kehyksen salauksen.

Jaettujen salaisten avaimien kiinteys vahvistaa ongelmaa. 802.11 ei tarjoa toimintoja, jotka tukisivat avainten vaihtoa asemien kesken. Siksi järjestelmänhaltijat ja käyttäjät käyttävät yleensä samoja avaimia pitkiä aikoja. Tämä tarjoaa asiaan kuulumattomille henkilöille runsaasti aikaa seurata WEP:iä käyttäviä verkkoja. (Geier 2005, 183)

5.2.3 Wi-Fi Protected Access

Wi-Fi Protected Access eli WPA – standardi on WEP:n päivitys, joka tarjoaa dynaamisen avaimen salauksen ja kaksisuuntaisen todennuksen. Useimmat langattomien laitteiden valmistajat tukevat WPA:ta. WPA - asiakkaat käyttävät ajoittain vaihtuvia salausavaimia. Tämä tekee salauksen murtamisen vaikeammaksi. WPA 1.0 on käytännössä yhteenveto nykyisestä 802.11i:stä, joka sisältää TKIP ja 802.1x-mekanismit. Näiden kahden mekanismin yhdistelmä tarjoaa dynaamisen avaimen salauksen ja kaksisuuntaisen todennuksen, joita langattomissa lähiverkoissa tarvitaan.

WPA 2.0 tarjoaa täyden yhteensopivuuden 802.11 – standardin kanssa. (Geier 2005, 184-185)

5.3 Todennus

Kaksisuuntaisen todennuksen käyttö on langattomassa verkossa tärkeää. Se toimii suojana tietoturvauhkia vastaan. Kaksisuuntaisessa todennuksessa langattoman asiakkaan ja langattoman verkon tulee tunnistautua toisilleen. Tässä tapahtumassa käytetään todennuspalvelinta, kuten Remote Authentication Dial-In User Service eli Radius, joka suorittaa todennuksen.

5.3.1 802.11 – todennuksen haavoittuvuuksia

WEP tarjoaa ainoastaan menetelmän, jolla radioverkkokortit voidaan tunnistaa tukiasemien suuntaan, mutta ei toisin päin. Siksi hakkeri voi reitittää datan uudelleen luvattoman polun kautta, joka välttää muut tietoturvamekanismit. Tämän ongelman välttämiseksi langattomissa verkoissa on käytettävä kaksisuuntaista todennusta.

”Kun langaton asiakas aktivoituu, se etsii siirtotiestä tukiasemien lähettämiä beacon-viestejä. Oletusarvona tukiasema lähettää beacon – viestejä, jotka sisältävät tukiaseman SSID – tunnisteen ja muita parametreja. Tukiasema sallii yhteyden vain, jos asiakkaan SSID vastaa sen SSID:tä. Tämä prosessi tarjoaa perustasoisen, mutta sangen heikon todennuksen muodon.

Haavoittuvuus piilee ensi sijassa siinä, että SSID lähetetään salaamattomana, mikä tekee siitä näkyvän langattomien verkkojen ”pakettinuuskimille”. Siksi hakkeri voi helposti tunnistaa beacon – kehyksessä olevan SSID:n ja todentaa itsensä langattomaan verkkoon. Vaikka tukiaseman SSID – lähetys olisi kytketty pois käytöstä, ”nuuskimet” voivat silti saada tietoonsa SSID:n yhteyspyyntökehyksistä, joita asiakaslaitteet lähettävät tukiasemalle. (Geier 2005, 187)

802.11 tarjoaa oletuksena avoimen todennuksen. Tässä tilassa tukiasema takaa hyväksynnän kaikille todennuspyynnöille. Asiakas vain lähettää todennuspyyntökehyksen, ja tukiasema vastaa hyväksynnällä. Näin kuka tahansa, jolla on oikea SSID, voi kytkeytyä tukiasemaan.” (Geier 2005, 187)

802.11 – standardi sisältää myös jaetun avaimen todennuksen, joka on valinnainen, kehittyneempi todennuksen muoto. Prosessi on nelivaiheinen:

- Asiakas lähettää todennuspyyntökehyksen.
- Tukiasema vastaa kehyksellä, joka sisältää haasteeksi kutsutun merkkijonon.
- Seuraavaksi asiakas salaa haasteen käyttäen tavallista WEP – salausavainta. Asiakas lähettää salatun haasteen takaisin tukiasemalle, joka purkaa salauksen yhteisellä avaimella ja vertaa tulosta alun perin lähetettyyn tekstiin.
- Jos vastaavuus löytyy, tukiasema todentaa asiakkaan.

Tämänlaisessa todennuksessa on ongelmana se, että jaetun avaimen todennus vain todistaa, että asiakkaalla on oikea WEP – avain. (Geier 2005, 187)

5.3.2 MAC – suodattimet

Langattomat tukiasemat tarjoavat MAC – suodatuksen. Tämä tarkoittaa sitä, että tukiasema tutkii jokaisen saapuvan kehyksen lähdeosoitteen. Suodatus hylkää kehykset, joiden MAC – osoitetta ei löydy järjestelmävalvojan ohjelmoimasta listasta. Siten MAC- suodatus on yksikertainen menetelmä todennukseen. (Geier 2005, 187)

MAC – suodatuksessa on kuitenkin eräitä heikkouksia. WEP – salaus esimerkiksi ei salaa kehyksen MAC – osoitekenttää. Näin ollen hakkeri voi helposti tutkia kehyslähetyksiä ja saada selville oikeita MAC – osoitteita. Hakkeri voi muuttaa vapaasti saatavilla olevilla ohjelmilla radioverkkokorttien MAC – osoitteet vastaamaan oikeita MAC – osoitteita. MAC – osoitteen voi muuttaa Windows – käyttöjärjestelmässä rekisteristä ja Linux – käyttöjärjestelmästä ifconfig – käskyllä. Esimerkiksi MAC Address Changer – ohjelma muuttaa MAC – osoitteita. Tällaiset keinot mahdollistavat sen, että hakkeri voi naamioitua sallituksi käyttäjäksi ja huiputtaa tukiasemaa, kun oikea käyttäjä ei ole läsnä verkossa. (Geier 2005, 187)

Lisäksi MAC – suodatuksen hallinta on raskasta laajassa verkossa, jossa on paljon käyttäjiä. Järjestelmävalvojan täytyy syöttää jokaisen käyttäjän MAC – osoite tauluun ja tehdä tarvittavat muutokset aina, kun verkkoon tulee uusia käyttäjiä. MAC –

osoitesuodatus voi riittää koti- ja pientoimistosovelluksiin, mutta soveltuu huonosti laajoihin langattomiin yritysverkkoihin. (Geier 2005, 187)

5.3.3 Julkisen avaimen salaukseen perustuva todennus

Asemat voivat suojata tietojaan hakkereilta ja sen lisäksi käyttää julkisen avaimen salausta todentaakseen itsensä toisille asemille ja tukiasemille. Tämä voi olla välttämätöntä, ennen kuin tukiasema tai ohjain sallii tietyn aseman muodostaa yhteyden verkon suojattuun osaan. Myös asiakas voi todentaa tukiaseman samalla tavalla.

Asema todentaa itsensä salaamalla paketin sisällä olevan merkkijonon yksityisellä avaimellaan. Vastaanottava asema purkaa salauksen lähettävän aseman julkisella avaimella. Jos tämä teksti vastaa jotakin ennalta määriteltyä tekstiä, kuten aseman nimeä, vastaanottava asema tietää että lähettävä asema on oikea. Tietyn tekstijonon salaus toimii tässä tapauksessa sähköisenä allekirjoituksena.

5.3.4 802.1x

”802.1x:n käyttö tarjoaa tehokkaan kehyksen suojattuun verkkoon suuntautuvan käyttäjäliikenteen automaattiseen todennukseen ja valvontaan. Se tarjoaa myös dynaamisen salausavainten muuttamisen. 802.1x yhdistää Extensible Authentication Protocol- eli EAP – protokollan sekä lanka- että langattomaan verkkosiirtotiehen ja tukee useita todennusmenetelmiä kuten Kerberos, kertakäyttöiset salasanat, varmenteet ja julkisen avaimen todennus.

802.1x-liikenne käynnistyy, kun todentamaton langaton asiakaslaite yrittää muodostaa yhteyden langattomaan tukiasemaan. Tukiasema vastaa avaamalla portin, jossa hallitaan vain EAP – paketit asiakkaalta todennuspalvelimelle, joka sijaitsee tukiaseman langallisella puolella. Tukiasema estää kaiken muun liikenteen, kuten http, DHCP ja POP3 – paketit, kunnes tukiasema voi varmentaa asiakkaan identiteetin todennuspalvelimen, kuten RADIUS – palvelimen avulla. Kun asiakas on todennettu, tukiasema avaa tämän portin muunkin tyyppiselle liikenteelle todennuspalvelimen ilmoittamien oikeuksien mukaisesti.” (Geier 2005, 189)

5.4 Tietoturvakäytännöt

Kun langaton verkko on otettu käyttöön, on käyttöönotossa tehtävä arviointi, jolla varmistetaan, että langaton lähiverkko noudattaa määriteltyjä tietoturvakäytäntöjä. Useimmissa tapauksissa tämä on välttämätöntä, jotta verkko noudattaa tehokkaita tietoturvamekanismeja. Järjestelmän rakenteen varaan ei voi pelkästään turvautua, vaan on testata, että verkko on riittävästi varmistettu. Tällöin yrityksen resurssit on suojattu niitä vastaan hyökkääviltä luvattomilta henkilöiltä. Tietoturvatarkastuksia tulisi tehdä säännöllisesti, jotta varmistetaan, että langattomaan lähiverkkoon tehdyt muutokset eivät tee järjestelmää haavoittuvaiseksi.

5.4.1 Tehokkaan salauksen käyttäminen

Taitavat hakkerit osaavat murtaa WEP – pohjaisen verkon vapaasti saatavana olevilla työkaluilla. WEP toimii kuitenkin hyvin kotien ja yritysten verkkojen suojaamisessa suurelta yleisöltä. WEPin murtaminen edellyttää monimutkaisten työkalujen käyttöä ja suuren verkkopakettimäärän sieppaamista. Tätä useimmat eivät vaivaudu tekemään, elleivät verkon resurssit ole todella arvokkaita. Standardin 802.11 WEPin käyttäminen alhaisen hyökkäysriskin verkoissa on tietoturvakäytännön vähimmäistaso.

Jos langaton verkko tukee jotakin salausmuotoa kuten WPA:ta, jossa avaimia muutetaan usein, sitä kannattaa käyttää. Tämä ratkaisu on paljon turvallisempi kuin kiinteiden menetelmien, kuten WEPin käyttö. (Geier 2005, 198)

5.4.2 Laiteohjelmien päivitys

Valmistajat tarjoavat tukiasemiin ja verkkokortteihin usein ohjelmistopäivityksiä, jotka korjaavat tietoturvaongelmia. Tukiaseman laiteohjelmisto kannattaa päivittää heti ensimmäisen käyttöönoton yhteydessä. Kannattaa myös tarkistaa ajoittain, että kaikissa laitteissa on viimeisin laiteohjelmistoversio, jotta laitteen tietoturvataso on ajan tasalla. (Geier 2005, 198)

5.4.3 Vahvojen salasanojen käyttö

Tukiasemissa koskaan käyttää oletussalasanoja. Oletussalasanat ovat hyvin tunnettuja, ja tämä tekee kenelle tahansa helpoksi tukiaseman parametrien muuttamisen mielensä

mukaiseksi. Sen sijaan tulee käyttää vaikeasti arvattavia salasanoja. Niissä käytetään sekaisin isoja ja pieniä kirjaimia sekä erikoismerkkejä. Salasanat on syytä vaihtaa säännöllisesti. Ne tulee myös salata ennen verkossa lähettämistä. (Geier 2005, 198)

5.4.4 SSID – lähetysten estäminen

SSID:n ominaisuuden ollessa käytössä voidaan välttää se, että käyttäjälaitteet ”nuuskisivat” automaattisesti langattoman lähiverkon tukiaseman käyttämän SSID:n. Windows XP ja muut monitorointityökalut nuuskivat automaattisesti 802.11:n beacon – kehyksiä saadakseen tietoonsa SSID:n. Jos SSID- lähetys on kytketty pois päältä, tukiasema ei sisällytä SSID:tä beacon – kehykseen, mikä tekee useimmista ”nuuskintatyökaluista” hyödyttömiä. Tämän lisäksi Windows – käyttäjät eivät näe langatonta lähiverkkoa. (Geier 2005, 197)

5.4.5 Radioaaltojen leviämisen rajoittaminen

Radioaaltojen levittäminen voidaan rajoittaa tietylle alueelle suunnattuja antenneja käyttämällä. Langaton verkko voidaan esimerkiksi suunnitella siten, että antennien tehovahvistus ja suuntaus vähentää radioaaltojen vuotoa rakennuksen seinien ulkopuolelle. Tämä takaa parhaimman peiton ja lisäksi minimoi ”nuuskijan” mahdollisuuksia salakuunnella käyttäjäsignaalien lähetyksiä tai muodostaa yhteys yrityksen verkkoon tukiaseman kautta. (Geier 2005, 195 -199)

5.4.6 Henkilökohtaiset palomuurit

Jos hakkeri onnistuu kytkeytymään tukiasemaan, hän pääsee helposti käsiksi muissa samaan langattoman lähiverkkoon liitettyyn tukiasemaan kytkeytyneissä käyttäjätileissä oleviin tiedostoihin. Siksi on erittäin tärkeää, että kaikki käyttäjät estävät kaikkien kansioiden tiedostojen jakamisen ja käyttävät henkilökohtaisia palomuureja. Tämä on todella tärkeää silloin, kun käyttäjät toimivat julkisissa tiloissa. (Geier 2005, 195-199)

5.4.7 Konfiguraatioiden tarkkailu

Yritysten tulee käyttää tukityökaluja verkkoa tarkkaillakseen ja estääkseen tukiasemat, jotka eivät noudata annettuja konfiguraatiokäytäntöjä. Jos tukiaseman tietoturva – asetukset eivät vastaa ohjeita, on todennäköistä, että se on asetettu uudelleen alkuasetuksiin tai se on rosvotukiasema. (Geier 2005, 195)

Tukiasemiin, joissa on väärät asetukset, on palautettava oikeat asetukset. Hallintaliikenne pitää salata Simple Network Management Protocol- eli SNMP – protokollan turvallisella versiolla. Esimerkiksi SNMP:n versio 1 lähettää kaiken selväkielisenä. Verkossa voidaan myös käyttää tunkeutumisen havaitsemisen tunnistimia, joita jotkut tukityökalut sisältävät. Niillä voidaan löytää vääriä MAC – osoitteita käyttävät hakkerit. Ne perustuvat settä epäilyttävän käyttäytymien aikaansaamaan hälytykseen. (Geier 2005, 195-196)

5.4.8 Toteutusten valvonta

Yrityksen tulee varmistaa, että lähiverkkoja asentaessaan kaikki sen työntekijät ja organisaatiot toimivat yhdessä. Esimerkiksi luvattomien tukiasemien käyttö on kiellettävä. Kun sopivat tietoturvamenettelyt on tarkistettu, voidaan sallia hyväksyttyjen valmistajien tuotteiden hankinta. (Geier 2005, 196)

Yrityksen kannattaa pitää yllä luetteloa valtuutettujen verkkokorttien ja tukiasemien MAC – osoitteista. Tätä luetteloa voidaan käyttää perustana etsittäessä rosvotukiasemia. Lisäksi tulee ottaa käyttöön hallintatyökalut, jotka pakottavat tukiasemat noudattamaan yrityksen tietoturvakäytäntöjä. (Geier 2005, 197-198)

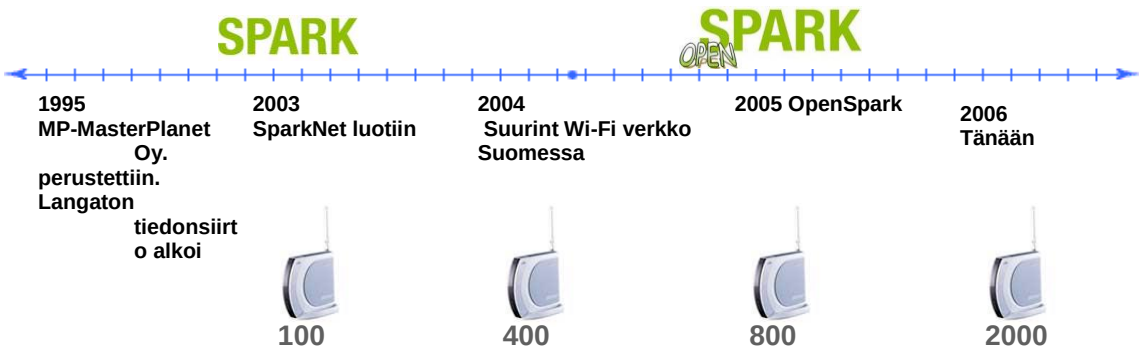
Näillä suosituksilla voidaan rakentaa vankka tietoturvakäytäntö. Tekniikoita valittaessa on kuitenkin pidettävä mielessä sopivat tietoturvatarpeet. WEP voi esimerkiksi olla riittävä ratkaisu kotien ja pientoimistojen langattomiin lähiverkkoihin. Jos kyseessä on suuri yritys, joka siirtää arkaluontoista dataa, täytyy käyttää jotain vahvempaa menetelmää, kuten WPA tai AES. (Geier 2005, 199)

6 OPENSPARK

6.1 Openspark yleisesti

Langaton kotikäyttäjille suunnattu OpenSpark – verkko lanseerattiin maaliskuussa 2005. OpenSpark on MP-Masterplanet Oy:n perustama ja ylläpitämä langattomien verkkokäyttäjien yhteisö. OpenSpark-yhteisön jäseneksi liitytään tuomalla oma langaton tukiasema yhteisön käyttöön. OpenSpark-yhteisön jäsen saa käyttöönsä yhden OpenSpark käyttäjätunnuksen. OpenSparkin käyttö on yhteisön jäsenille veloituksetonta. Perusajatuksena on, että yhteisön jäsenet antavat toistensa käyttää omaa yhteyttään ja saavat oman tukiaseman jakamalla käyttöoikeuden toisten jäsenten tukiasemaan. Kaikessa OpenSpark – ja SparkNet -toiminnassa on pyritty välttämään kustannuksia, koska asiakas ne tulee loppujen lopuksi maksamaan. Tämän takia OpenSparkia ja SparkNettiä ei ole markkinoitu rahallisesti ollenkaan. Ilmaista näkyvyyttä yhteisöt saavat lehtiartikkeleissa, web-sivuilla ja uusien kuntien liittyessä yhteisöihin. SparkNetin toimintaan palaan myöhemmin.

OpenSpark -käyttäjätunnuksella voidaan käyttää Internet-yhteyttä kaikista OpenSpark- ja Sparknet-toiminnan piirissä olevista tukiasemista. Myös kaikki SparkNet-käyttäjät voivat käyttää OpenSpark-toiminnan piirissä olevia tukiasemia. OpenSpark ja Sparknet-tukiasemia on tällä hetkellä yhteensä 2255 kpl.



Kuva 1. OpenSparkin toiminta.

OpenSpark on MP-Masterplanet Oy:n perustama ja ylläpitämä langattomien verkkokäyttäjien yhteisö. Yhteisöön liittyminen ei maksa mitään ja OpenSpark-ohjelmiston saa ladattua ilmaiseksi Internetistä. Yhteisön jäsenet liittävät oman OpenSpark -ohjelmistolla varustetun tukiaseman omaan laajakaistayhteyteensä ja jakavat näin oman yhteytensä koko yhteisön kesken. Yhteisöön liittynyt saa yhden OpenSpark - käyttäjätunnuksen, jolla hän voi käyttää koko OpenSpark - verkkoa veloituksetta aina kun liittyjän oma tukiasema on yhteisön käytettävissä. Oman tukiaseman lokitieto taltioidaan ja mikäli käyttäjän oma tukiasema on poistettu yhteisön verkosta, kyseiset tunnukset eivät toimi missään tukiasemassa ennen kuin kyseisen tunnuksen omaava tukiasema liitetään uudelleen OpenSpark - verkkoyhteisöön.

OpenSpark -verkkoa voi käyttää myös SparkNet - tunnuksilla ja myös toisin päin. SparkNet - verkkoon pääsee kirjautumaan OpenSpark - käyttäjätunnuksilla. Tällä tavalla kansalaiset rakentavat langattoman tietoyhteiskunnan itse ilman verorahojen käyttöä tai päätöksien odottamista.

5.2 Ominaisuudet ja vaatimukset

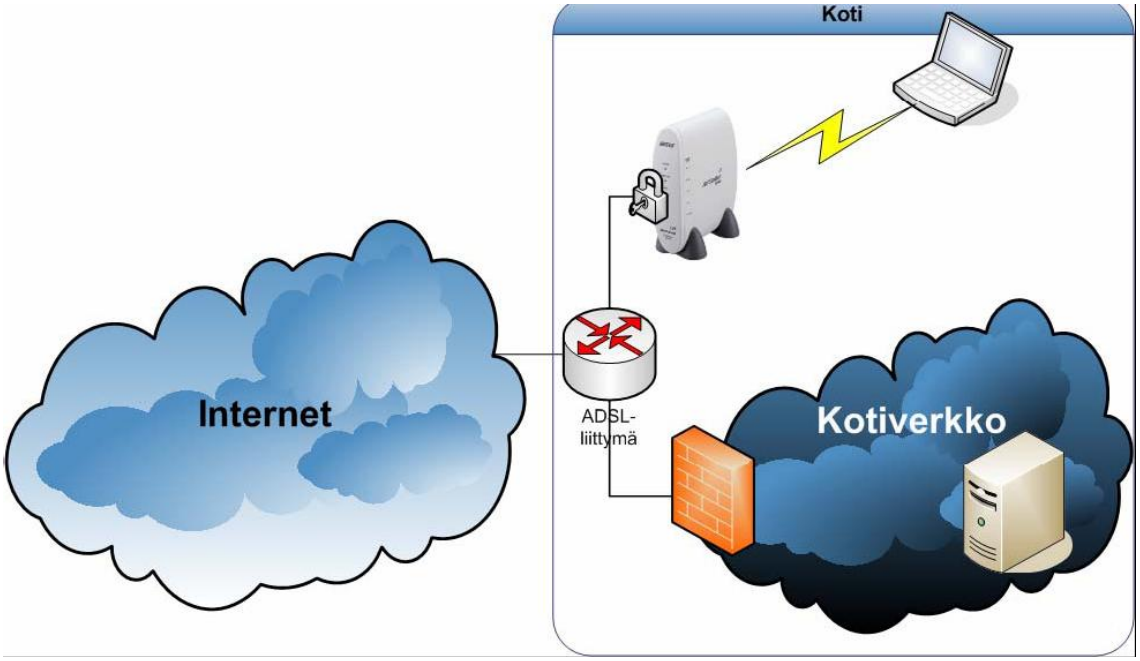
OpenSpark – tukiaseman asentaminen on helppoa. OpenSpark – tukiasemalla langattomat langattomat verkkopalvelut tuotetaan aina yhdenmukaisina, jolloin käyttäjän tuntuma langattomaan verkkoon on paikasta riippumatta aina sama. Muita tukiaseman ominaisuuksia ovat mm.

- helppo pnp – käyttöönotto
- käyttäjätunnistus käyttäen SSL – suojattua www-yhteyttä
- www – pohjainen hallinta
- paikallinen käyttäjätietokanta, jossa on mahdollista luoda lisää käyttäjätunnuksia vieraita ja perheenjäseniä varten
- ”dead link detection” – linjakatkosten havainnointi
- LAN – porttiin kytkettyjen laitteiden käyttäjätunnistus voidaan ohittaa MAC – sulkulistoilla

OpenSpark – tukiasemat hyödyntävät aina olemassa olevaa internet- liittymää. Internet-liittymälle asetetaan seuraavat vaatimukset:

- aito IP – osoite
- IP – osoite voi olla kiinteä tai dynaaminen
- liittymän liikennettä ei ole rajoitettu

Kaikki operaattorit eivät salli tietoyhteiskunnan rakentamista näin ja OpenSpark – tukiaseman liittämistä oman verkkonsa yhteyteen. Varsinkin Telia – Sonera on ottanut kielteisen kannan. Sen sijaan Elisa ja sen tytäryhtiö Lounet sallivat OpenSpark-tukiaseman liittämisen omaan verkkoonsa. Tähän samaan ryhmään kuuluvat myös Lännen Puhelimen DNA-laajakaistaliittymät.



Kuva 2. Verkon toimintamalli (Tuomas Saarinen 23.5.2006)

6 SPARKNET

6.1 Sparknet yleisesti

SparkNet on Suomen laajin langaton verkkototeutus. SparkNetissä on yli 100 000 käyttäjätunnusta, yli 10 000 aktiivista käyttäjää ja tukiasemia oli vuoden 2006 alussa yli 1200 kappaletta. Toimintamalli on varsin edistyksellinen ja mukautuva. SparkNet on monipuolinen toteutus, joka soveltuu niin pienen yrityksen kuin suurenkin julkisen konsernin langattoman verkon pohjaksi. SparkNet on käytännössä olemassa olevia verkkoresursseja hyödyntävä langaton verkkopalvelu. Sen sijaan, että yritykset investoisivat suuren määrän rahaa rakentaakseen tietoturvallisen langattoman verkon vain omaan käyttöönsä, SparkNet tarjoaa tietoturvallisen tavan rakentaa verkko myös vieraiden käyttöön ilman suuria investointeja. Verkkototeutus erotetaan yrityksen olemassa olevasta sisäverkosta tietoturvan maksimoimiseksi.

SparkNetin avulla verkko on käytettävissä myös työpaikan ulkopuolella, ravintoloissa, elokuvateattereissa sekä lukemattomissa muissa julkisissa paikoissa. SparkNettiin investoimalla asiakas saa huomattavasti suuremman hyödyn verrattuna itse rakennettuun langattomaan verkkoon. SparkNetin palvelut toimivat kaikkialla samalla tavalla riippumatta siitä onko käyttäjä omassa toimistossa, kauppakeskuksessa tai ulkomailla. SparkNet laajenee nopeasti sekä Suomessa että ulkomailla.. SparkNetin avulla on mahdollista käyttää myös lukuisia mobiilisovelluksia. VoIP –ohjelmat, dokumentinjako – ohjelmat sekä WebTV toimivat SparkNetissä mobiilisti.(Tuomas Saarinen 23.5.2006)

6.2 SparkNetin historia

SparkNet syntyi huhtikuussa vuonna 2003 Turun Yliopiston ja MP-Masterplanet Oy:n yhdistäessä omat Vlan – segmenttinsä luodakseen pohjan wlan – toteutukselle. Ensimmäiset tukiasemat kytkettiin verkkoon toukokuussa 2003 ja SparkNet - verkko aloitti toimintansa. SparkNet yhteistoimintasopimus allekirjoitettiin Turun Yliopiston, MP-MasterPlanet Oy:n, ICT Turku Oy:n, Turun kauppakorkeakoulun sekä Åbo

Akademin välille kesäkuun alussa. Turun kaupunki ja monet muut julkisen sektorin toimijat liittyivät mukaan SparkNet - toimintaan. MP-MasterPlanet Oy yhdessä ICT Turku Oy:n kanssa vastaa verkon kehittämisestä, ylläpidosta ja kaupallisesta toiminnasta. SparkNet - toiminnan laajetessa Masterplanet Oy kehitti keväällä 2004 uusia konsepteja erikokoisille toimijoille. Muun muassa SpakNet Enterprise, Business Solution, Business Center ja SparkNet SoHo- konseptit lanseerattiin. (Kuosmanen 16.2.2006)

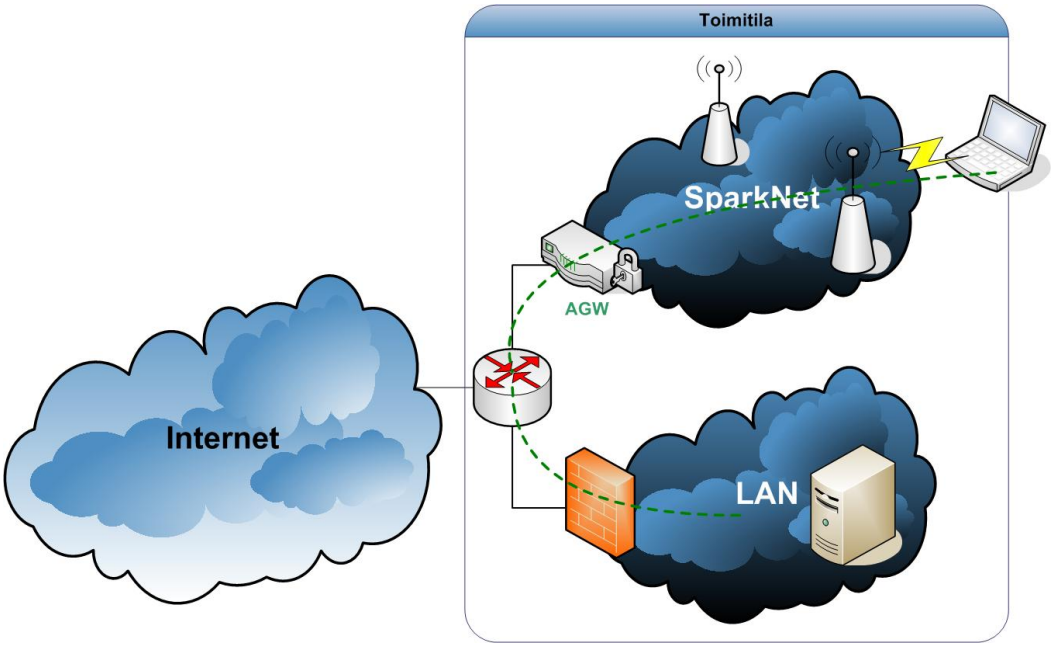
6.2.1 SparkNet – spotti

SparkNet – spotti muodostuu seuraavista osista:

- Autentikointipalvelimesta, joka sisältää muun muassa käyttäjähallinnan. Palvelimen tehtävänä on autentikoida eli tunnistaa käyttäjät.
- Langattomista tukiasemista. Tukiasemina käytetään Buffalon tuotteita, joihin on asennettu MAsterPlanetin valmistama erikoisohjelmisto (Kuosmanen 16.2.2008)

6.2.2 SparkNet Business Solution

SparkNet Business Solution on hyvin skaalautuva pienten ja keskisuurten yritysten langaton verkkoratkaisu. Ratkaisu perustuu olemassa olevien verkkoresurssien hyödyntämiseen verkkototeutuksessa. Toimitilaratkaisujen toteutuksen hoitavat asiantuntijat, jotka yhdessä asiakkaan kanssa suunnittelevat langattoman verkon. Suunnitteluvaiheessa määritellään tavoitteellinen langattoman verkon peittoalue. Suunnitelman perusteella asiakas saa toimitilaratkaisun toteutustarjouksen.



Kuva 3. Toimitilaratkaisun toteutus.(Tuomas Saarinen 23.5.2006)

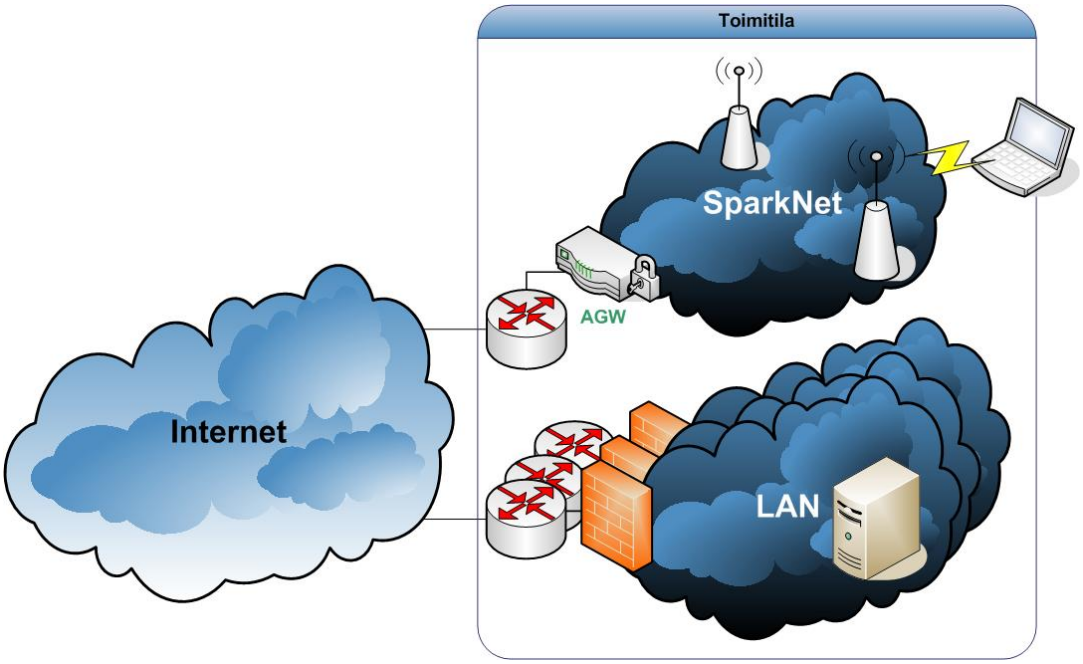
Toimitilaratkaisun hankkineet organisaatiot voivat veloituksetta käyttää paikallista verkkoaluetta. Myös paikallisten veloituksettomien vierailijatunnusten hallinnointi on mahdollista. Tunnusten hallinnointi mahdollistetaan kehittyneillä hallintatyökaluilla. Peruslaitteisto sisältää autentikointipalvelimen sekä yhden sisäantennilla varustetun tukiasemalaitteen. Toteutuksen kokonaishinta määritellään asiakaskohtaisella tarjouksella. Toteutuksen käytöstä ei aiheudu kuukausikustannuksia. Verkon ylläpito hoidetaan veloituksetta ja SparkNet – verkon komponentit jäävät SparkNet – ryhmän hallintaan.

SparkNet on tietoturvallinen ratkaisu. Verkkoalue toteutetaan aina yritysten sisäverkoista erotettuna ratkaisuna, joten SparkNet – toteutus ei uhkaa yrityksen sisäverkon tietoturvaa. SparkNet –liittymä on Internet –liittymä, joten liittymän käyttäjän on otettava yleiset Internetin tietoturvanäkökohdat huomioon.

6.3 SparkNet Business Center

SparkNet -toimitilaratkaisu on kehitetty palvelemaan yrityksiä ja yhteisöjä, joiden toimitiloihin SparkNetin yleinen ”yritysspotti” -konsepti ei sellaisenaan sovellu.

SparkNet -toimitilaratkaisu soveltuu erinomaisesti esimerkiksi toimistohotellien ja muiden suurten toimitilakokonaisuuksien käyttöön.

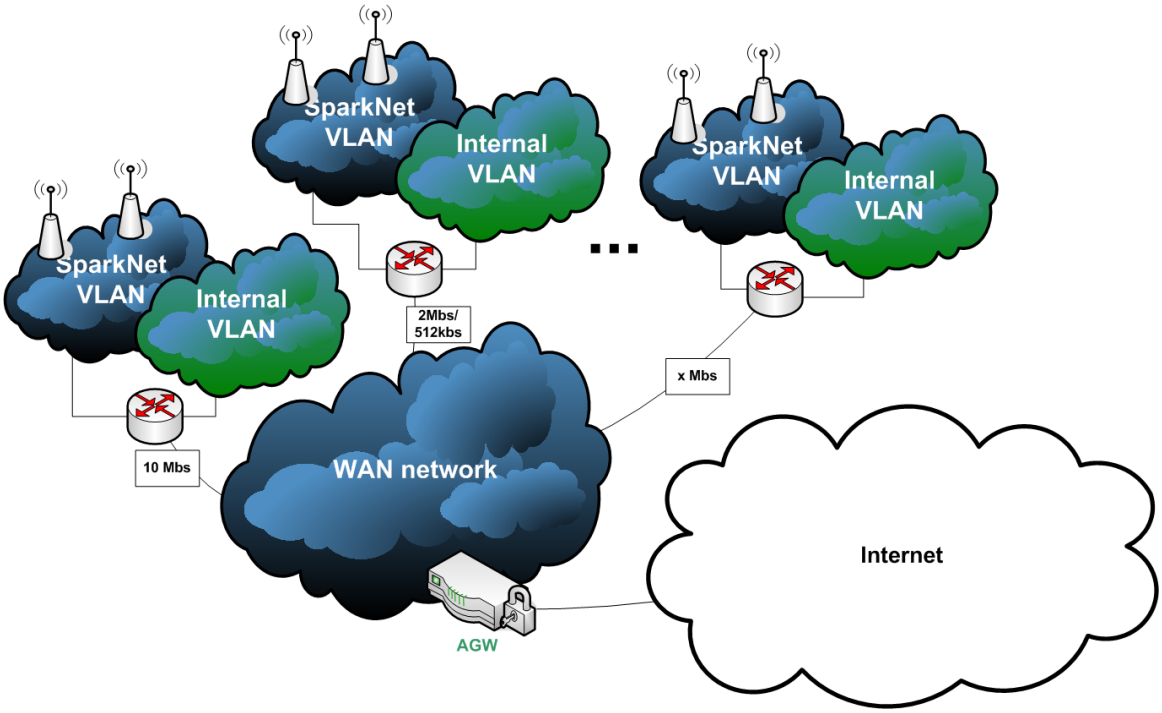


Kuva 4. Toimitilaratkaisun toteutus. .(Tuomas Saarinen 23.5.2006)

Toimitilaratkaisun hankkineet organisaatiot voivat veloituksetta käyttää paikallista verkkoaluetta. Koko toimitilaratkaisun toteutus vastaa SparkNet Business Solutionia. Ainoastaan palvelun hinnoittelu on erilainen.

6.4 SparkNet Enterprise

SparkNet Enterprise - ratkaisu on erittäin skaalautuva suurten yritysten langaton verkkoratkaisu. Ratkaisu soveltuu esimerkiksi WAN – ratkaisuksi. Toteutus voi perustua esimerkiksi VLAN – teknologian hyödyntämiseen. Internet – liittymänä voidaan käyttää yrityksen olemassa olevaa Internet – liittymää. Myös SparkNet Enterprise toimitilaratkaisussa pätevät samat toteutussuunnitelmat kuin kahdessa edellä mainitussa. Ainoastaan kustannukset eroavat eri palveluissa.



Kuva 5. Toimitilaratkaisun toteutus. .(Tuomas Saarinen 23.5.2006)

7 OpenSpark – asennus

7.1 Tukiaseman kytkentä

ADSL – liittymä kytketään tukiaseman mukana toimitettavalla kaapelilla tukiaseman AN – porttiin. Buffalon WBR2- ja WHR – malleissa on viisi ethernet – porttia. Neljä ylintä porttia muodostaa 10/100 Mbs sisäverkon ja alin portti on WAN – portti, johon ADSL – yhteys kytketään.

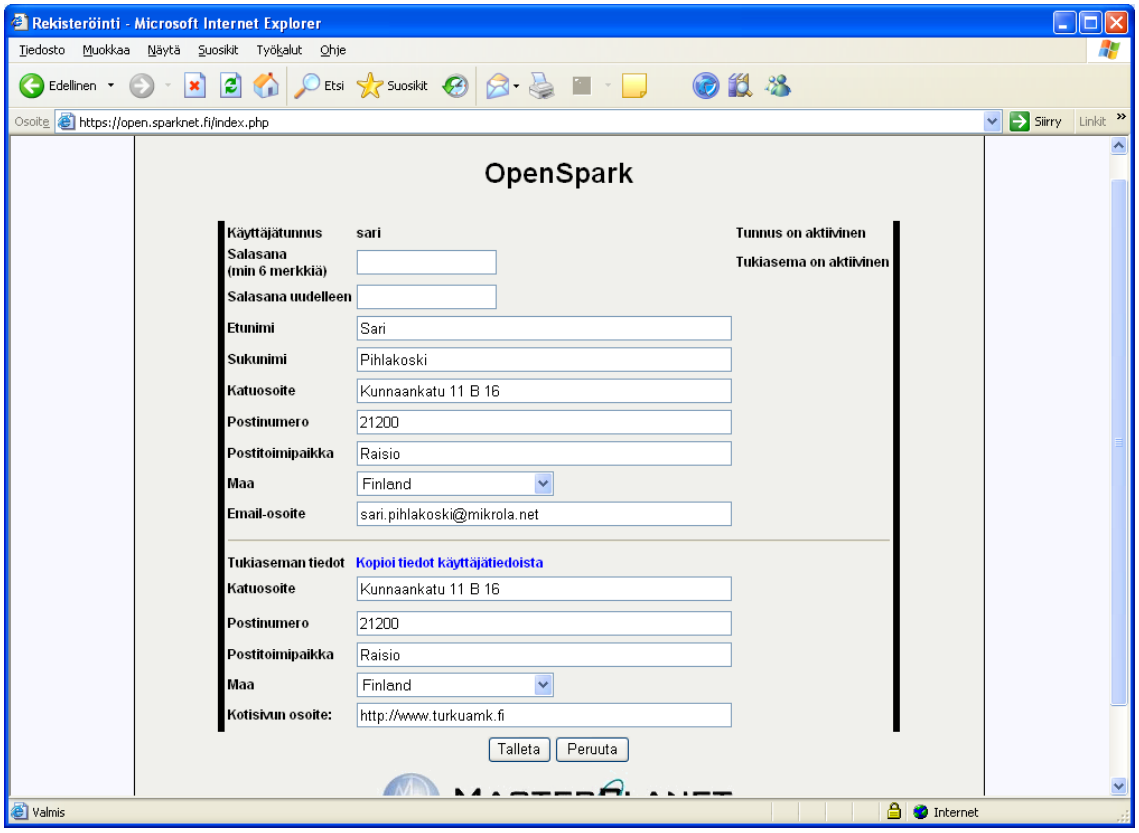
7.2 Salasanan vaihto

Tietoturvasyistä uuden tukiaseman hallintatunnuksen salasana pitää aina vaihtaa. Tukiaseman hallinta tapahtuu www – selaimella osoitteessa http://10.51.0.254:8080.

7.3 Tukiaseman rekisteröinti ja OpenSpark – käyttäjätunnuksen luonti

Kytketään tietokone OpenSpark – tukiasemaan. Avaa www – selaimella sivu: **http://10.51.0.254/register.html.** Paina register – valintaruutua.

Syötetään www – lomakkeelle käyttäjätiedot ja rekisteröintiin käyttämän tukiaseman tiedot. Tämän jälkeen valitaan Talleta – valintaruutu.



Kuva 6. Opensparkin rekisteröinti.

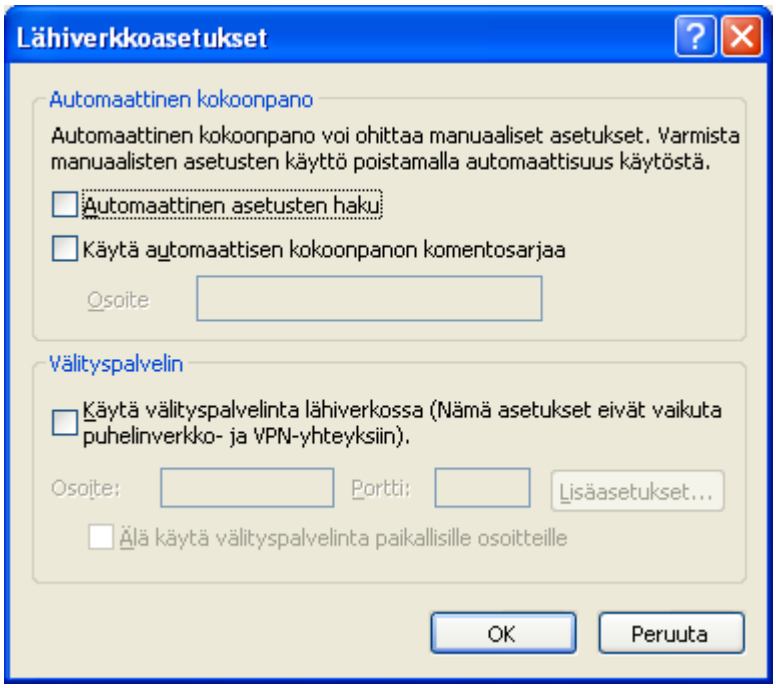
Rekisteröimisen viimeinen vaihe suoritetaan sähköpostivarmenteella. Sähköpostiin tulee viesti, jonka sisältämällä linkillä OpenSpark – tunnus aktivoidaan. Aktivoitunutta käyttäjätunnusta voidaan käyttää kaikissa OpenSpark – tukiasemissa. OpenSpark – tunnuksia käytetään aina muodossa ”käyttäjätunnus@opensparknet”.

7.4 Yhteyden avaaminen

Internet – yhteys tukiaseman kautta avataan seuraavasti:

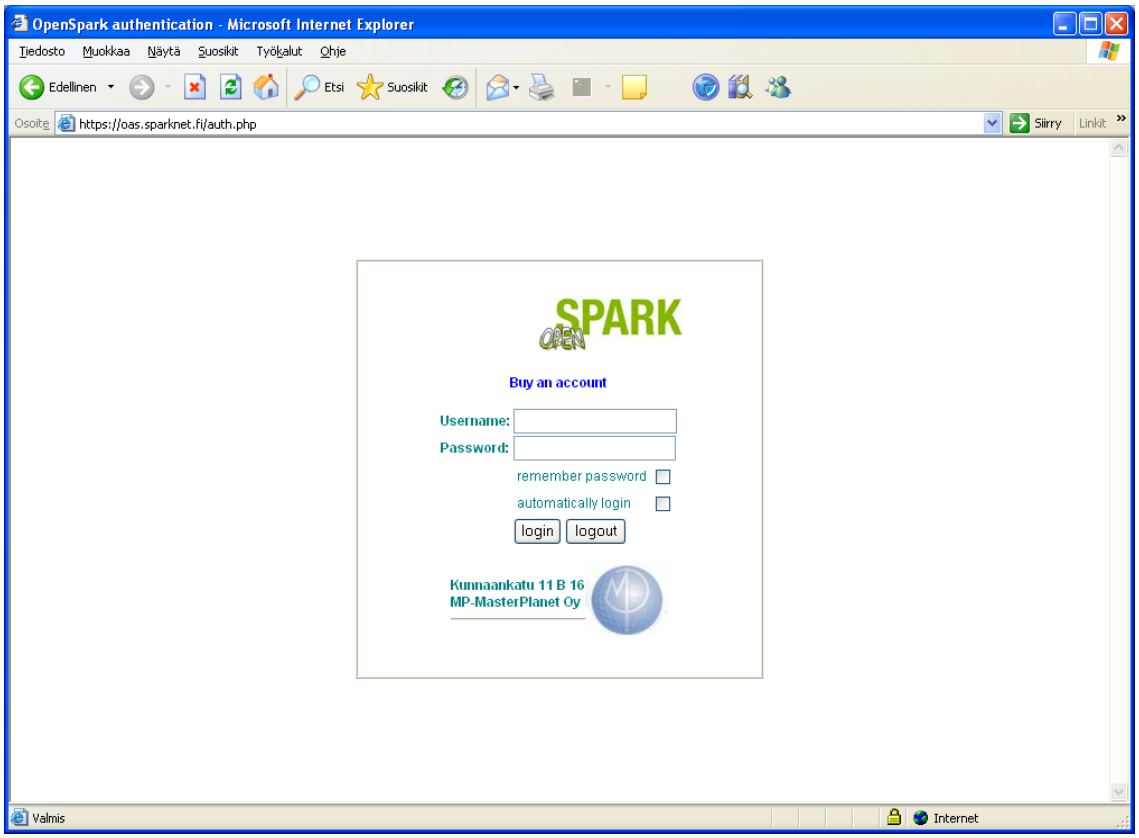
Yhdistä koneesi tukiasemaan.

Avaa mikä tahansa olemassa oleva www – sivusto. Huomaa, että Internet – selaimen proxy – asetukset on otettava OpenSpark – käytössä pois päältä. Proxy- asetukset voit tarkistaa seuraavasti. Avaa selaimessa Työkalut → Internet-asetukset → Yhteydet → Lähiverkko. Lähiverkkoasetuksista tarkista, että Välityspalvelin – kohtaa ”Käytä välityspalvelinta lähiverkossa” ei ole valittu.



Kuva 7. Välityspalvelimen käytöstä poisto

Internet – selain esittää autentikointiruudun.

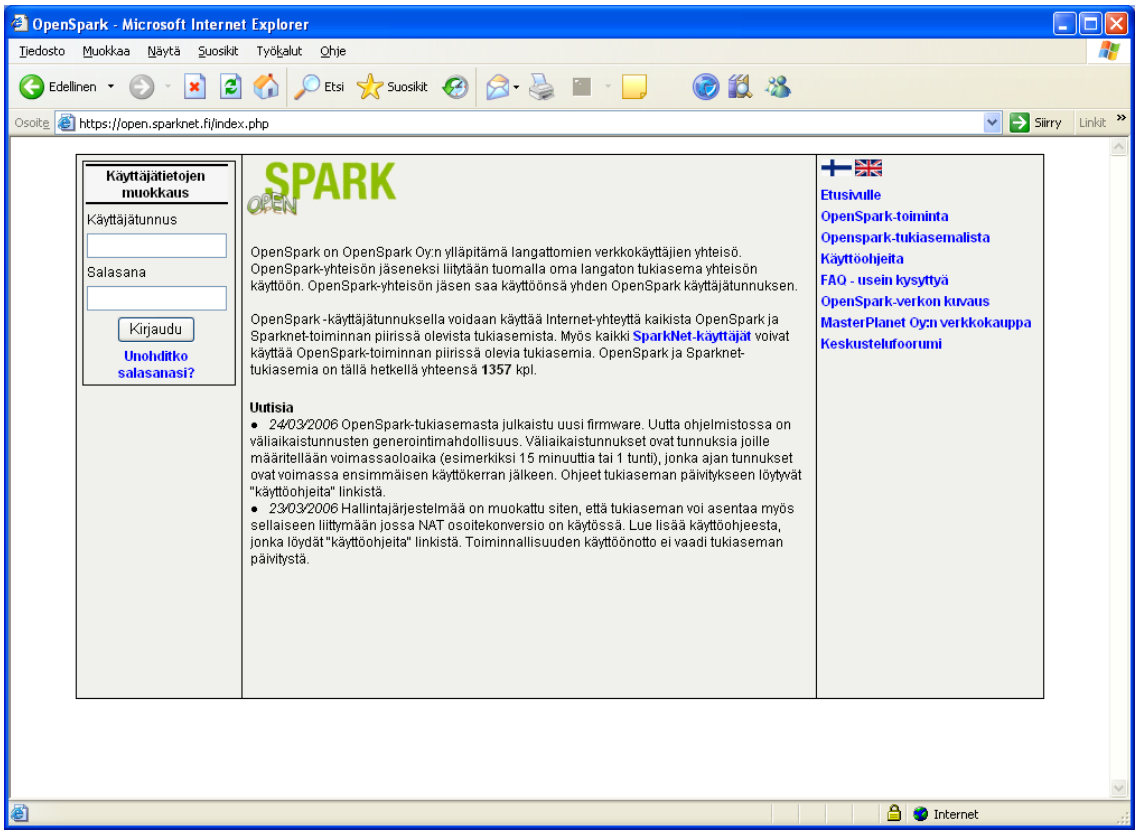


Kuva 8. Autentikointiruutu

Voit kirjautua käyttäen OpenSpark – tunnustasi muodossa: tunnus@openspark, tai paikallista käyttäjätunnusta käyttäen muodossa: tunnus@local

7.5 OpenSpark – rekisteröintitietojen muokkaus

Kirjautumisen jälkeen voit muokata OpenSpark – rekisteröintitietoja http://open.sparknet.fi – sivuilla. Sivuston kautta pääset muokkaamaan sekä tukiaseman että henkilökohtaisia rekisteröintitietoja. Myös OpenSpark – tunnuksen salasanan voit vaihtaa tällä sivustolla.

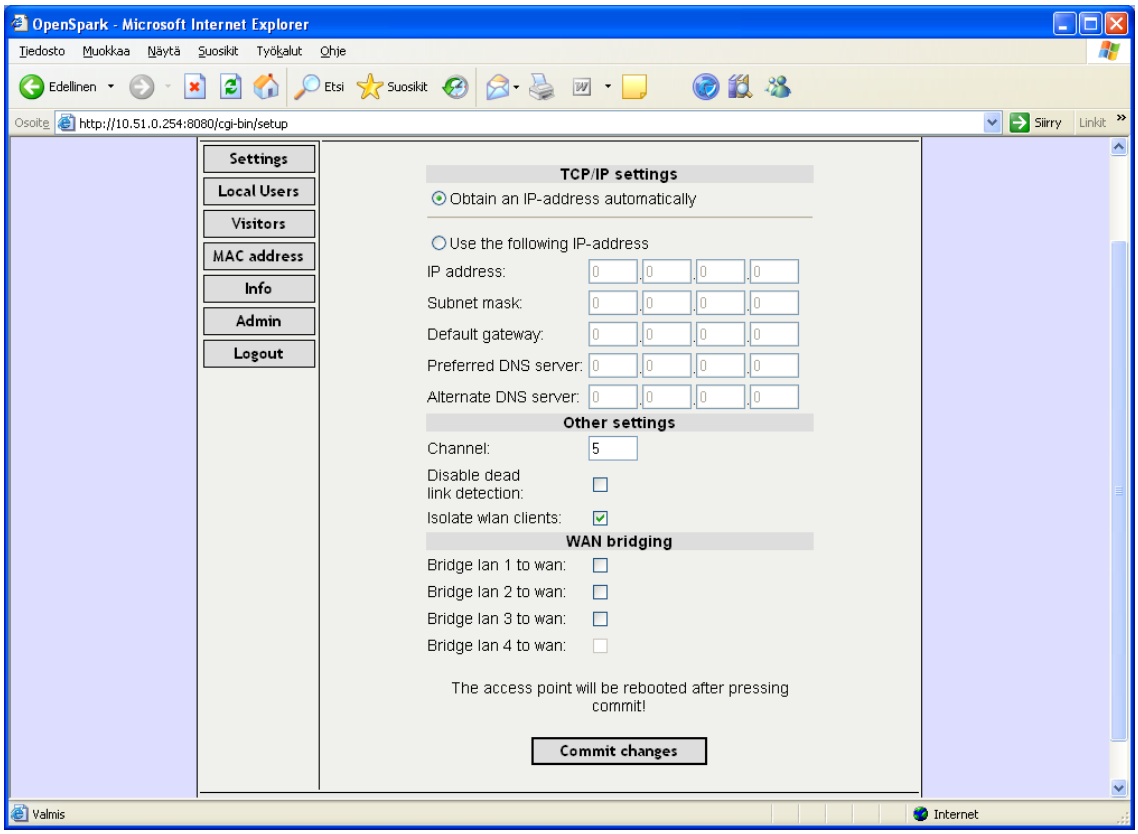


Kuva 9. Käyttäjätietojen muokkaus

7.6 Tukiaseman hallinta

Kytkeydy tukiasemaan joko langallisesti tai langattomasti. Avaa www – selaimellasi tukiaseman hallintayhteys osoitteessa http://10.51.0.254:8080. Syötä tukiaseman salasana password – ruutuun ja valitse ”login” painonappi. Kun käytät hallintasovellusta ensimmäisen kerran, tukiasema pakottaa sinua asettamaan salasanan.

7.7 Tukiaseman asetustoiminnot



Kuva 10. Asetustoiminnot.

7.7.1 Settings

Toiminnolla voidaan muokata tukiaseman IP – asetuksia, sekä määritellä langattoman tukiaseman käyttämän radiokanavan. Asetukset tallennetaan ”commit changes” – painonapilla. Asetusten tallennuksen yhteydessä tukiasema uudelleenkäynnistetään aina.

7.7.2 Disable dead link detection

Aktivoimalla ”Disable dead link detection” – valintaruutu tukiaseman automaattinen yhteyskatkon havannointitoiminto voidaan haluttaessa kytkeä pois päältä.

7.7.3 Isolate WLAN clients

Tukiasema oletusarvoisesti estää tukiasemaa käyttävien päätelaitteiden suoran kommunikoinnin toistensa kanssa. Tällä asetuksella tämä toiminto voidaan kytkeä pois päältä.

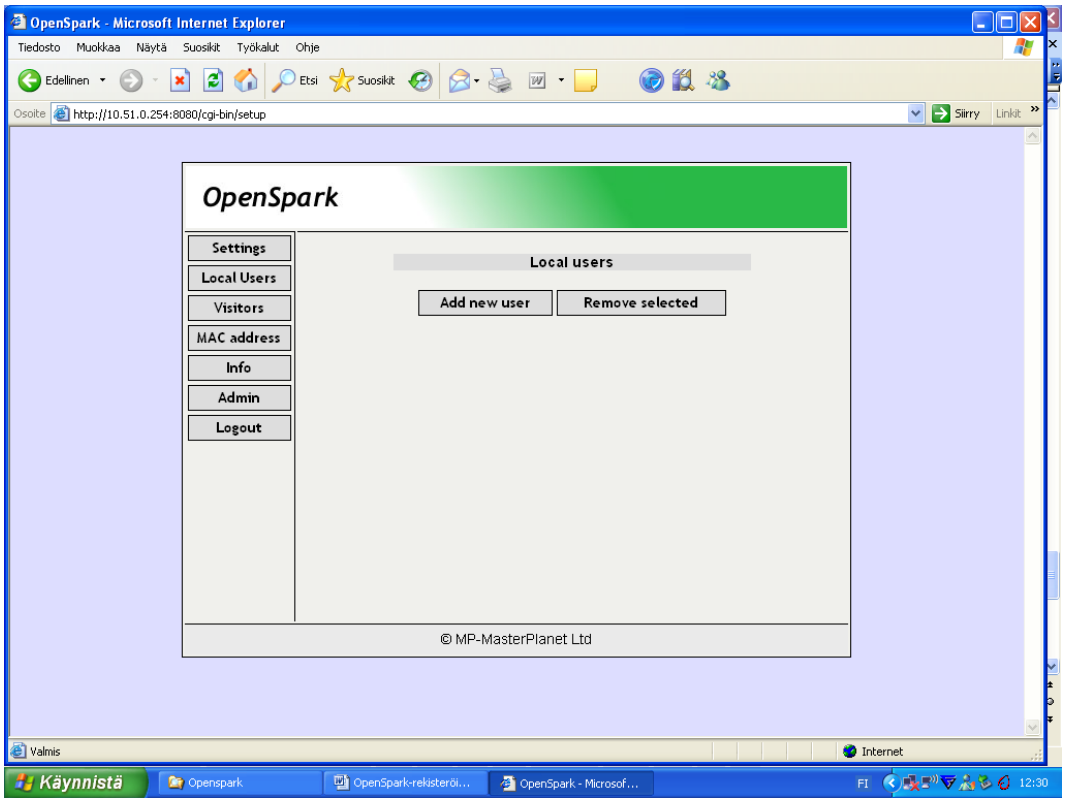
7.7.4 WAN bridging

Toiminto on käytössä sellaisissa tukiasemissa, joissa LAN – porttien kytkin on hallittava (esimerkiksi Buffalon WHR – mallin tukiasemat). Toiminnolla tukiaseman LAN – portteja voidaan hyödyntää perinteisen verkkokytkimen portteina siltaamaan WAN – portin liikenne suoraan valittuihin LAN – portteihin.
Toimintoa käytetään, kun kotityöasema halutaan kytkeä suoraan ADSL – liittymään OpenSpark – tukiaseman ohi, esimerkiksi silloin kun ADSL - päätelaitteessa ei enää ole vapaita kytkentäportteja.

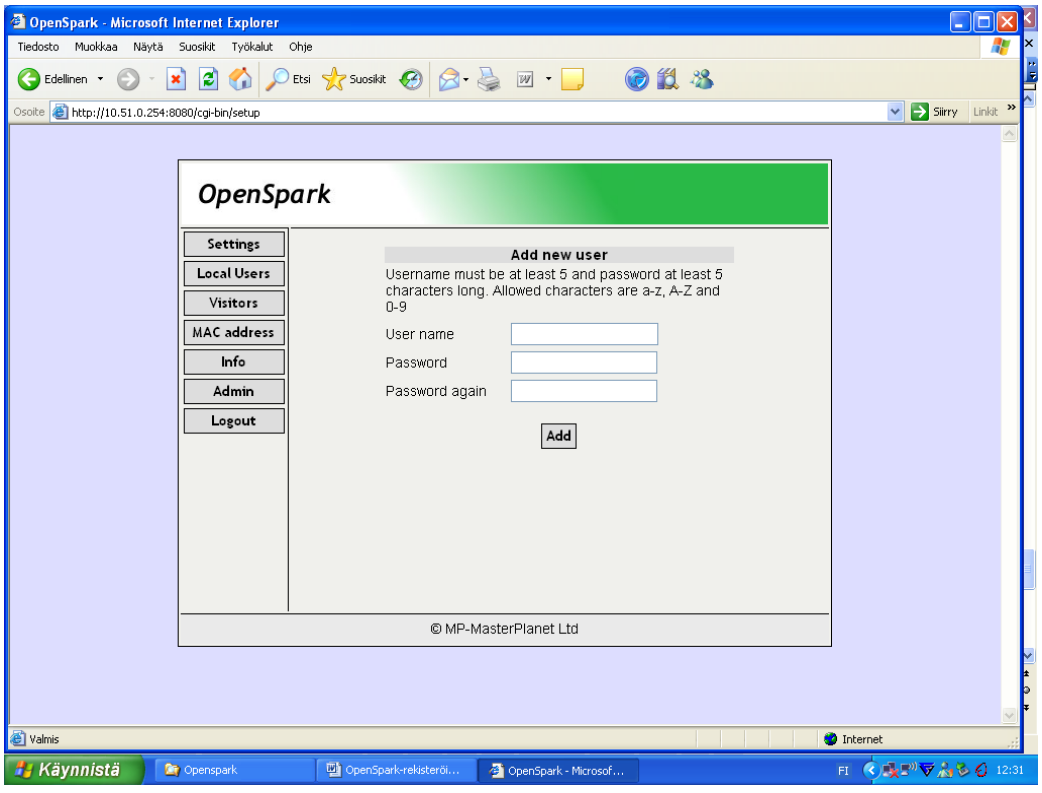
7.7.5 Local users

Toiminnolla voidaan lisätä, muokata ja poistaa tukiaseman paikallisia käyttäjätunnuksia. Näitä käyttäjätunnuksia käytetään tukiasemaan kirjautumiseen lisäämällä kirjautumisvaiheessa tunnuksen perään ”@local” – määrite.

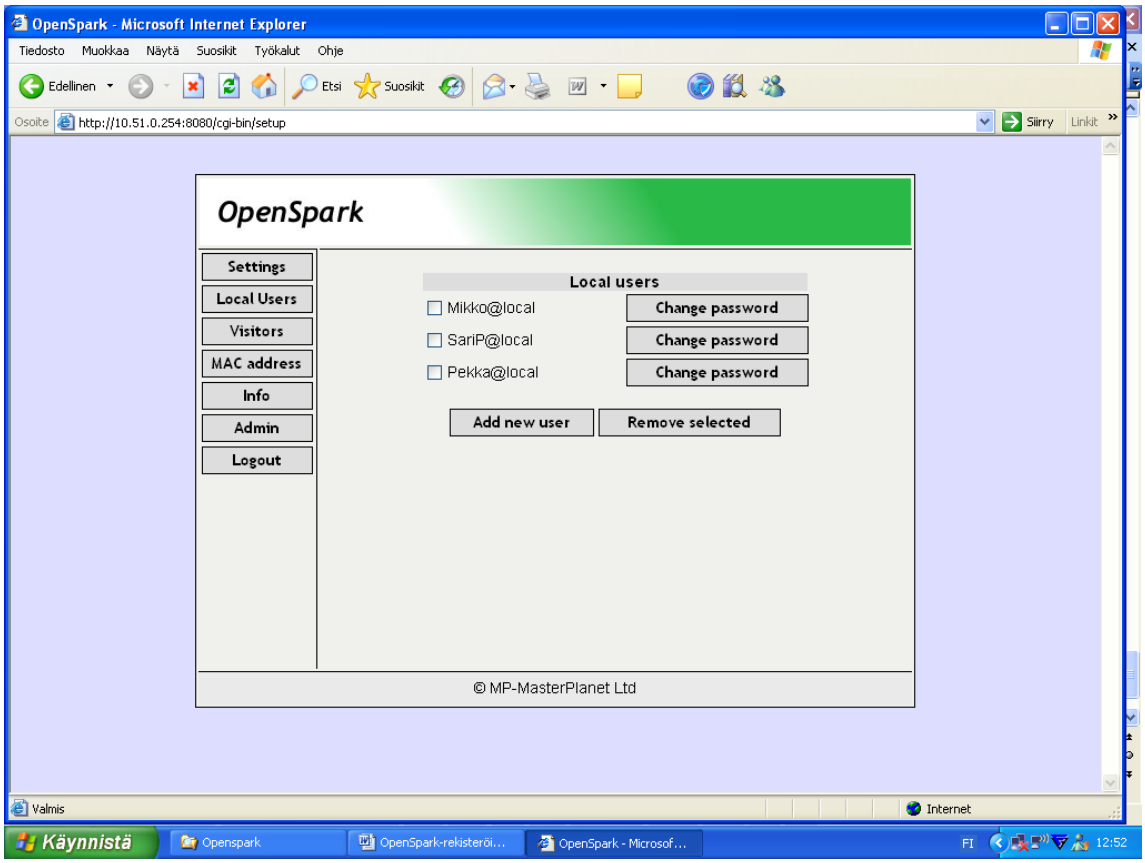
Paikalliset käyttäjätunnukset toimivat vain silloin, kun OpenSpark – tukiasema on kontrolliyhteydessä OpenSparkin keskitettyyn hallintajärjestelmään.



Kuva 11. Paikallisten käyttäjätunnusten luonti.



Kuva 12. Uuden käyttäjän lisäys.

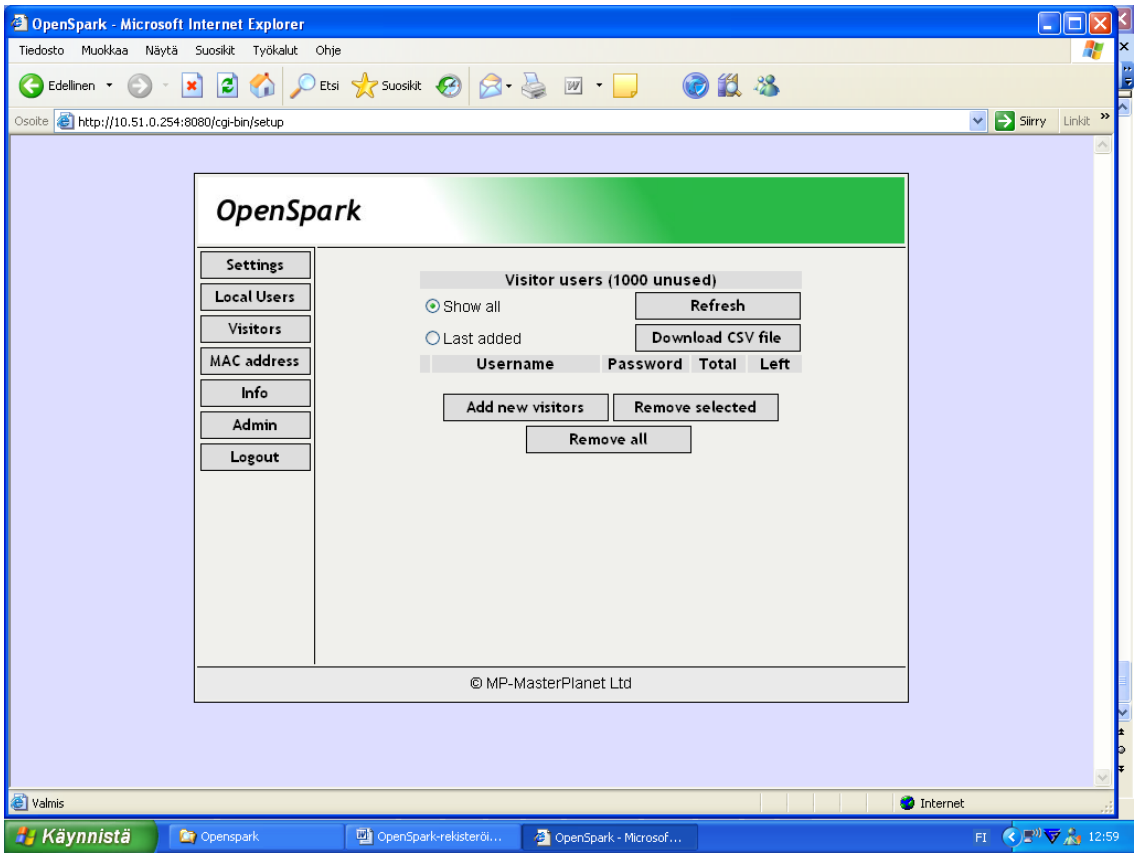


Kuva 13. Paikallisten käyttäjätilien hallinta.

7.7.6 Visitors

Toiminnolla voidaan käsitellä vierailijatunnuksia. OpenSpark – tukiaseman vierailijatunnukset toimivat vain paikallisesti kussakin tukiasemassa. Vierailijatunnuksille määritellään tunnuksen voimassaoloaika, jonka ajan tunnukset ovat voimassa ensimmäisen käyttökerran jälkeen. Toiminnolla voidaan luoda useita väliaikaistunnuksia kerrallaan, ja luodut tunnukset voidaan ladata tukiasemalta taulukkotiedostona csv – formaatissa..

Aktiivisia väliaikaistunnuksia voi olla kerrallaan 1000 kappaletta. Jo käytetyt tunnukset korvataan automaattisesti uusilla tunnuksilla tunnuksia lisättäessä.



Kuva 14. Visitor- tilien lisäys

7.7.7 Add new visitors

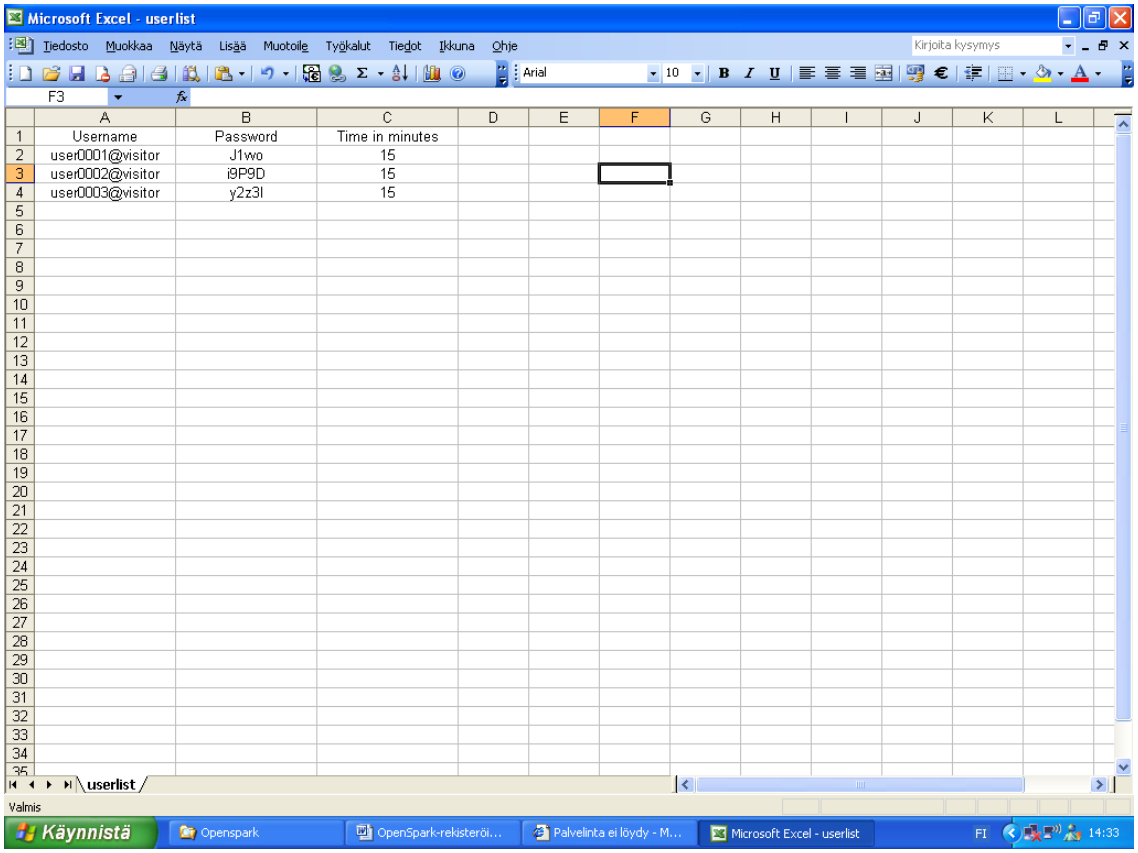
Toiminnolla lisätään vapaavalintainen määrä tunnuksia, maksimissaan 1000. Lisättävien tunnusten lukumäärä syötetään ”number of accounts” – kenttään. Tunnusten voimassaoloaika määritellään valitsemalla sopiva aikavaihtoehto.

7.7.8 Remove selected, Remove all

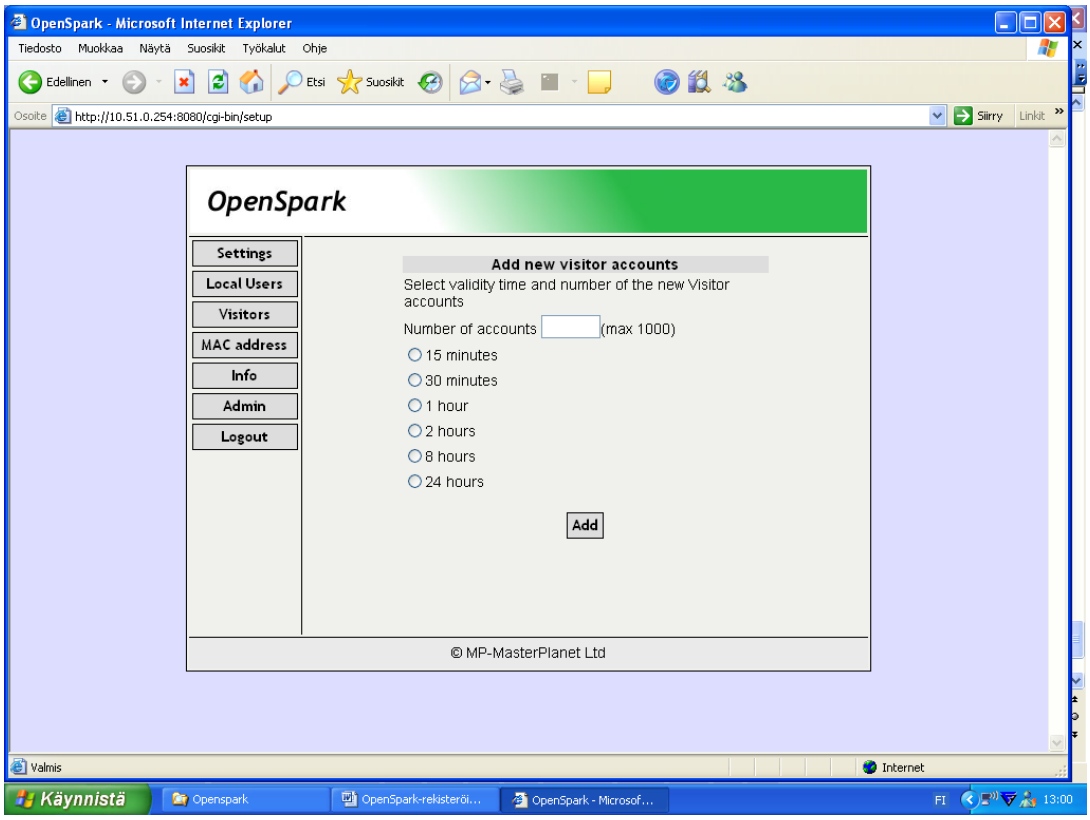
”Remove all” – toiminnolla poistetaan kaikki tukiasemaan määritellyt väliaikaistunnukset. ”Remove selected” – toiminnolla poistetaan ne tunnukset, joiden eteen on määritetty ”valittu” – merkki.

7.7.9 Download CSV file

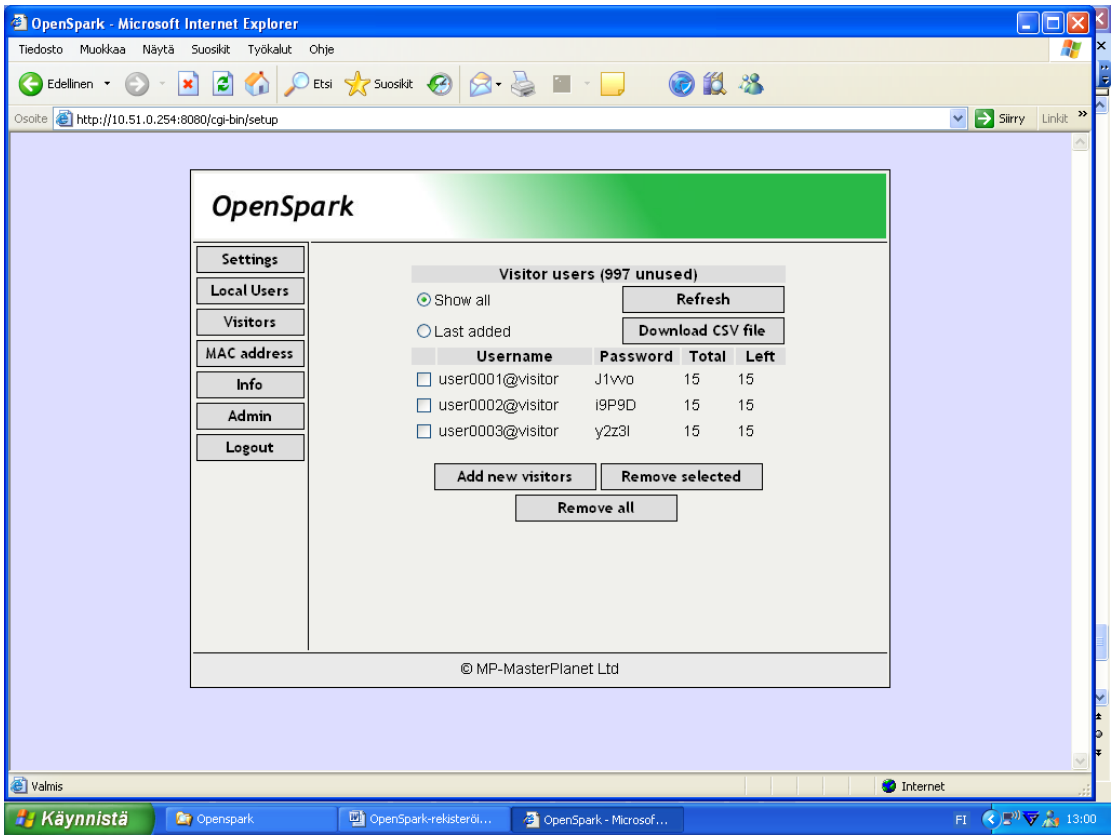
Toiminnolla ladataan viimeksi luodut tunnukset taulukkomuotoisena csv – formaatissa. Taulukkotiedostoa voidaan käsitellä suoraan yleisimmillä taulukkolaskentaohjelmilla.



Kuva 15. CSV - tiedosto



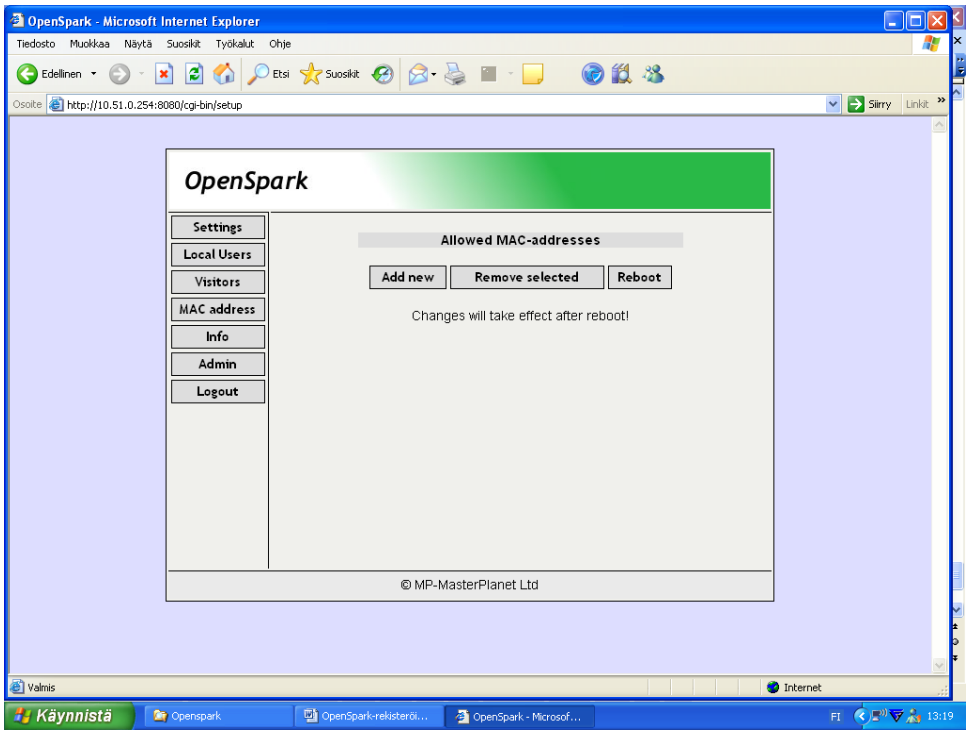
Kuva 16. Uuden visitor- tunnuksen ajan määrittely.



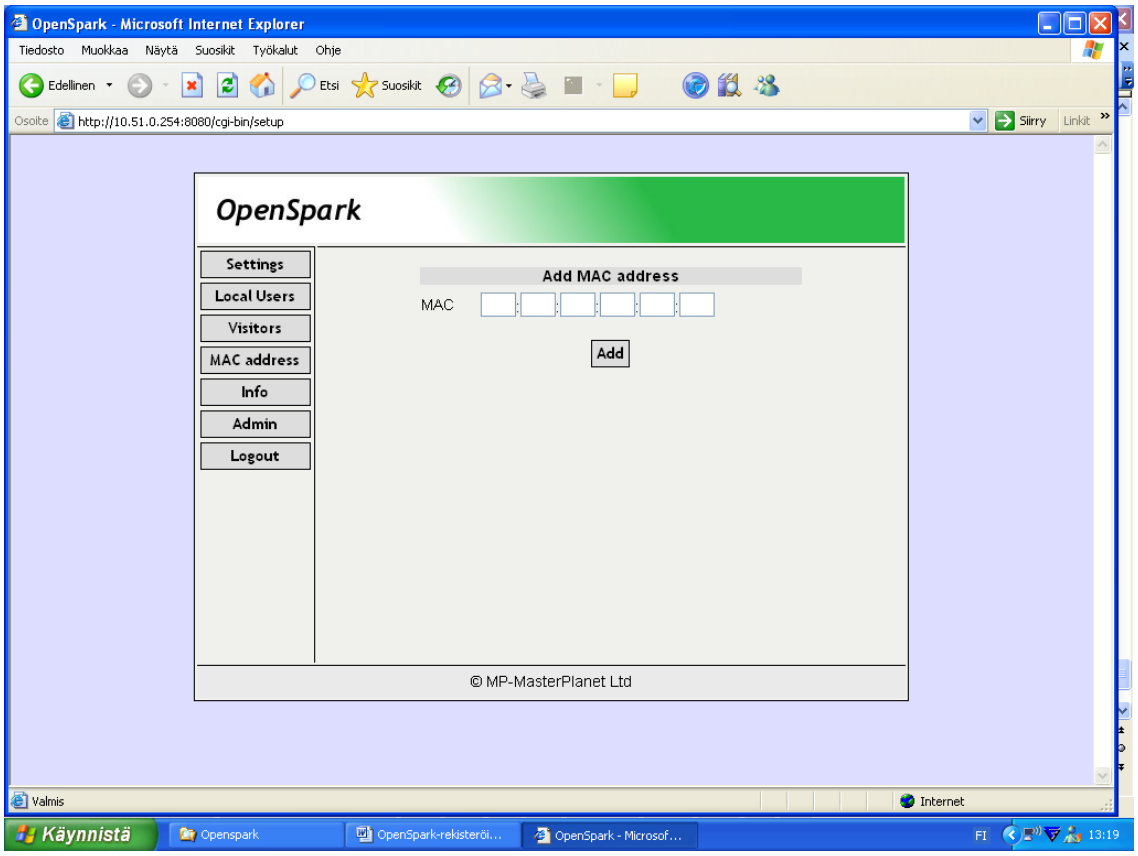
Kuva 17. Visitor- tunnusten hallinta

7.7.10 MAC address

Esimerkiksi kotona käytettävän pöytäkoneen voidaan haluta muodostavan Internet – yhteys ilman käyttäjätunnistusta. Allow MAC – address – toiminnolla käyttäjä voi määritellä niiden tietokoneiden verkkokorttien MAC – osoitteet, joiden koneiden yhteys halutaan sallia ilman käyttäjätunnistusta.



Kuva 18. MAC – osotteiden hallinta

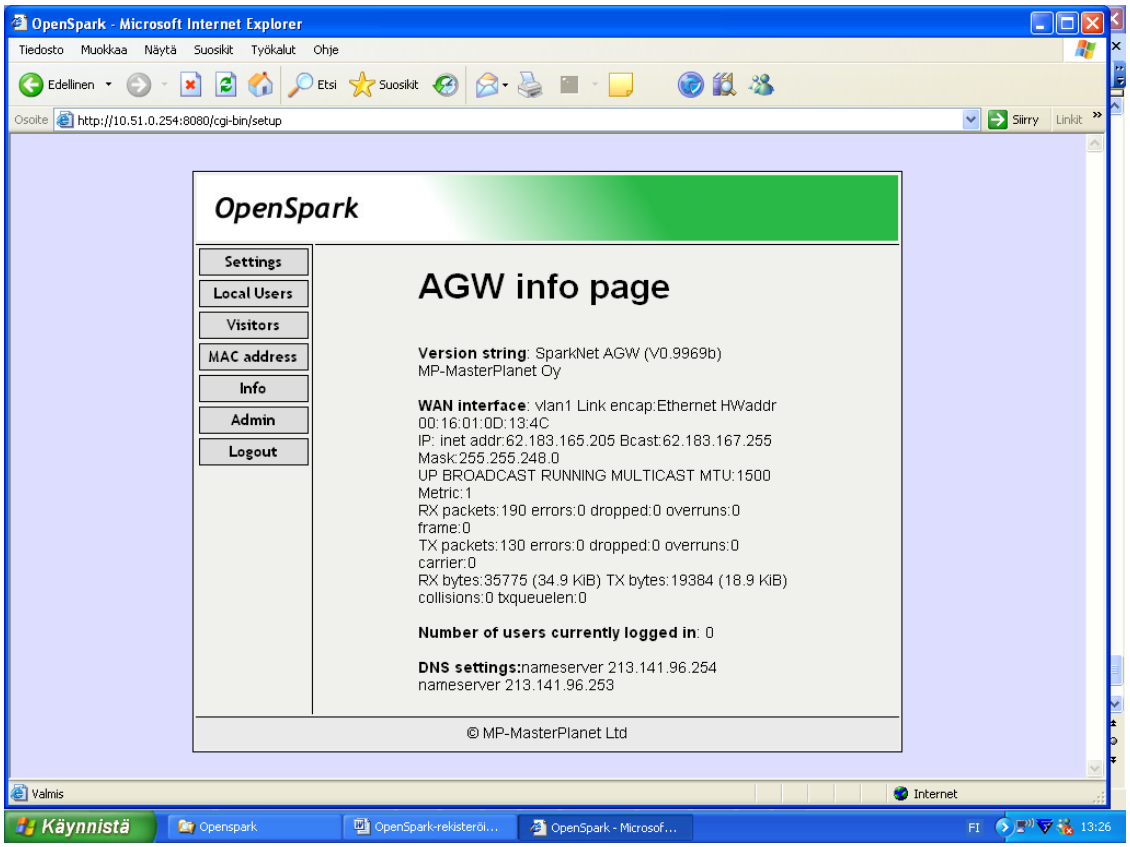


Kuva 19. MAC – osotteiden lisäys

Tietoturvan maksimoimiseksi toiminnolla syötetyt MAC – osoitteet voivat muodostaa yhteyden vain tukiaseman LAN – portteihin liitettyinä. On tärkeää muistaa, että tietokoneiden verkkokorttien MAC – osoite on helppo väärentää, ja toimintoa käyttäessä tulee olla aina kontrolli siihen keitä tukiaseman LAN – porttiin kytkeytyy. Toimintoa ei pidä käyttää esimerkiksi silloin, jos kytket toisen langattoman tukiaseman tukiasemasi LAN – porttiin.

7.7.11 Info

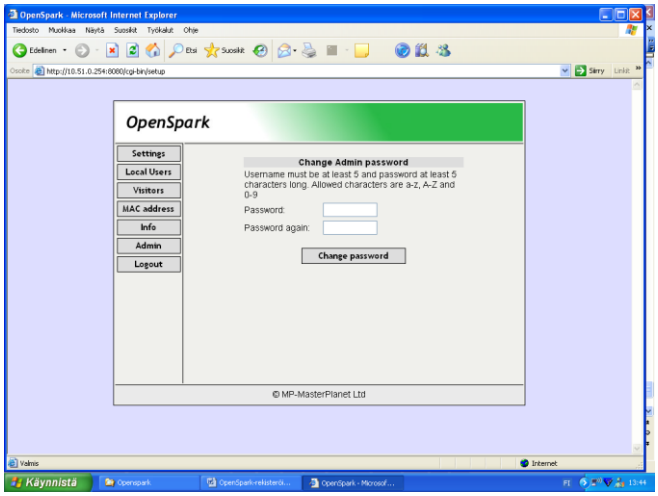
Info - toiminnolla näet muun muassa tukiaseman käyttämän WAN – liittymän IP – osoitteen, tukiaseman versiotiedot ja tukiasemaan kirjautuneiden käyttäjien määrän.



Kuva 20. Info – sivu.

7.7.12 Admin

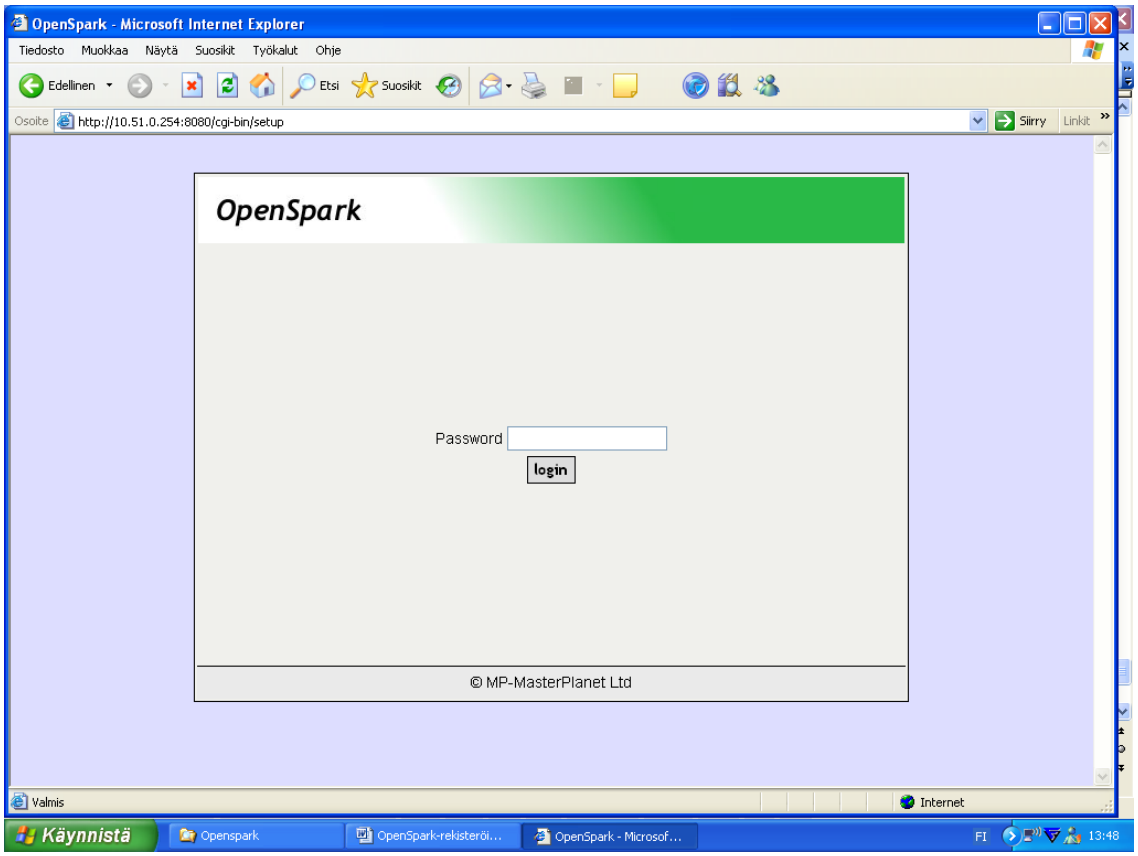
Tukiaseman hallintasalasana vaihdetaan admin - toiminnolla. Salasanan on oltava vähintään viisi merkkiä pitkä.



Kuva 21. Tukiaseman hallintasalasanan vaihto

7.7.13 Logout

Toiminnolla poistutaan hallintaohjelmasta. Logoutin jälkeen avautuu ruutu, josta on mahdollista yhdistää uudestaan OpenSparkiin.



Kuva 22. Opensparkin sisäänkirjautuminen

7.8 OpenSparkin käyttö

Voit käyttää rekisteröinnin aika luotua käyttäjätunnusta Internet – yhteyden avaamiseen kaikissa OpenSpark – yhteisön tukiasemissa.

OpenSparkin käyttö edellyttää aina yhteyden avaamista sisäänkirjautumalla. Sisäänkirjautuminen käynnistetään avaamalla mikä tahansa www – sivu Internet – selaimella. Mikäli yhteytesi ei jo ole auki, OpenSpark esittää käyttäjän www – selaimessa sisäänkirjautumissivun, johon käyttäjä syöttää käyttäjätunnuksen ja salasanan. Muista lisätä @openspark – liite omaan OpenSpark – käyttäjätunnukseesi.

7.9 Ongelmatilanteet

7.9.1 Ongelmat Internet - yhteyden avauksessa

OpenSparkin keskitetyn hallinnan ja tukiaseman välillä täytyy olla rajoittamaton Internet – yhteys. Tukiasema ei voi sijaita NAT – osoitekonversion takana, tai liittymän sisään tulevan TCP – portin 22 liikenne on ohjattava OpenSpark – tukiasemalle.

7.9.2 Ongelmatilanteissa

Tukiaseman tietojen katselutoiminto saattaa olla hyödyllinen ongelmatilanteissa (http://10.51.0.254/info.html). Esimerkiksi, kun Internet – liittymässäsi on käytössä dynaamiset IP – osoitteet, voit selvittää tämän toiminnon kautta tukiasemasi saaman IP – osoitteen. WWW–selaimen .proxy – asetukset täytyy ottaa OpenSpark – käytössä pois päältä.

7.9.3 Tukiaseman automaattinen vianetsintä

Toiminto on käytössä ohjelmistoversiosta V.9921b alkaen. Toiminto on mahdollista kytkeä pois päältä tukiaseman hallinnan ”settings” – toiminnolla.

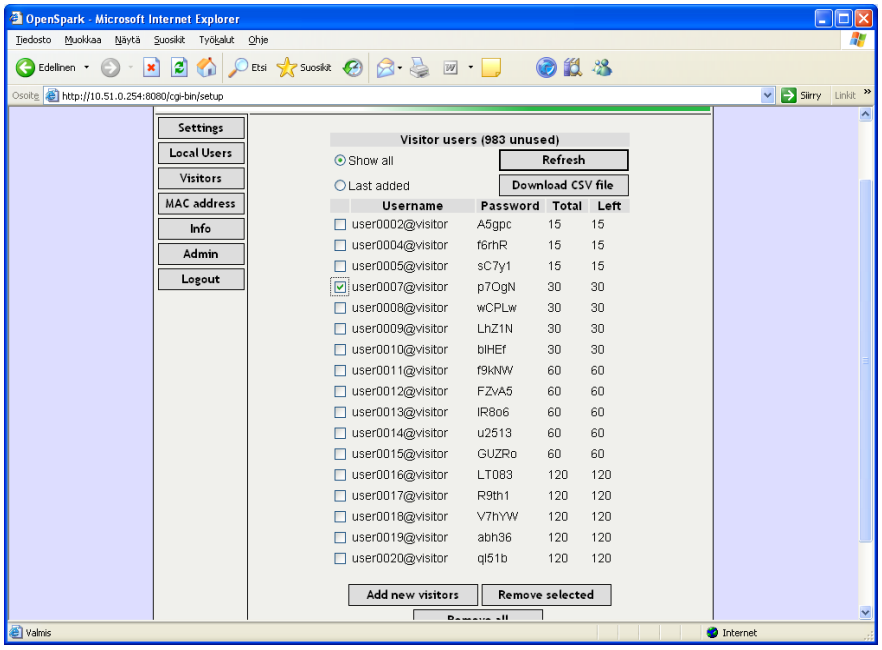
Mikäli tukiasema havaitsee Internet – yhteyden olevan katkennut se ohjaa kaikki www – sivupyynnöt yllä olevalle sivulle. Tällöin tukiasema toimii normaalisti, ja käyttäjä voi alkaa etsiä yhteysongelmaa esimerkiksi ADSL – liittymästään.

Kun haluat testata onko ongelma poistunut, sulje www-selain ja käynnistä selain uudelleen ja avaa yhteys johonkin www-sivustoon.

7.10 Asiakkaalle myytävä visitor – tunnus

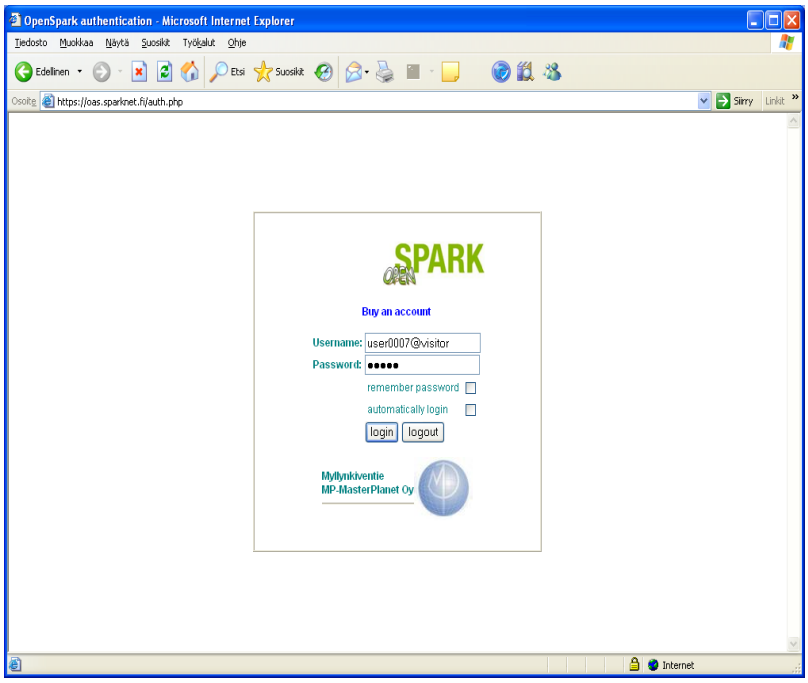
Asiakkaalle annetaan visitor – tunnus, joka on luotu tukiaseman asetustoimintojen visitors – sivulle. Asiakas saa käyttäjätunnuksen ja salasanan, joka on voimassa asiakkaan haluaman ajan.

Esimerkki: Asiakas haluaa tunnuksen, joka sallii 30 minuutin käytön Internetiin OpenSparkin kautta. Listasta valitaan sopiva tunnus. Visitor – tunnukset toimivat ainoastaan sen päätelaitteen kantavuusalueella, jolla visitor – tunnus on alun perin luotu.

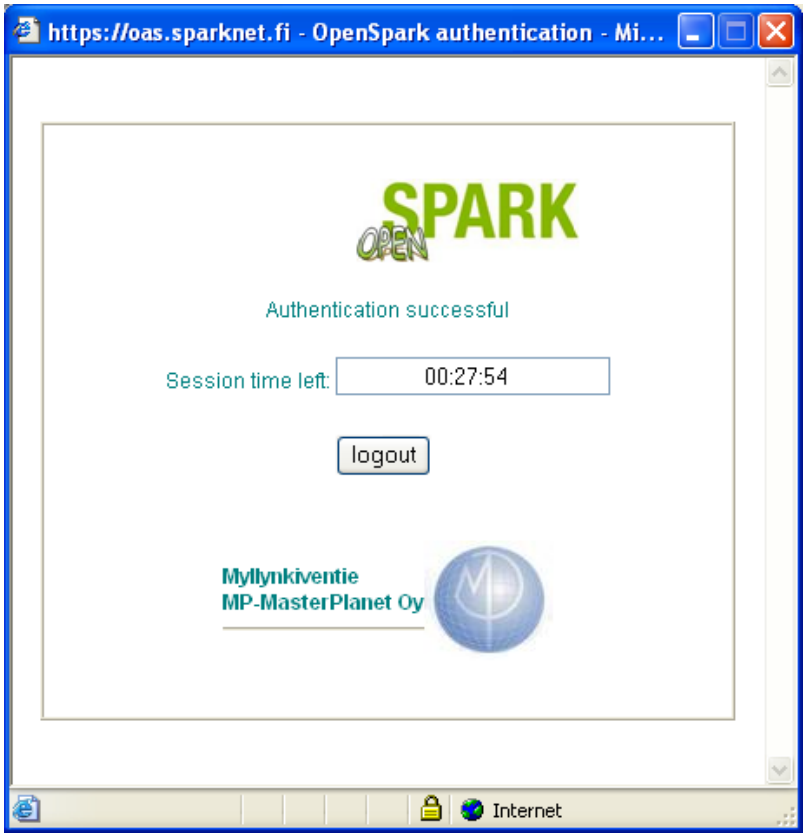


Kuva 23. Vierailija – käyttäjätilit

Asiakas saa käyttäjätunnuksen ja salasanan. Seuraavaksi asiakas avaa selaimella osoitteen http://oas2.sparknet.fi/, jolloin selain avaa rekisteröintisivun, johon saatu tunnus ja salasana syötetään, jonka jälkeen laskuri lähtee käyntiin. Asiakas voi milloin tahansa katkaista yhteyden ja kirjautua uudelleen niin kauan kuin kyseessä olevalla visitor – tunnuksella on käyttöaikaa jäljellä. Visitor – tunnukset toimivat ainoastaan sen päätelaitteen kantavuusalueella, jolla kyseinen visitor – tunnus on alun perin luotu.

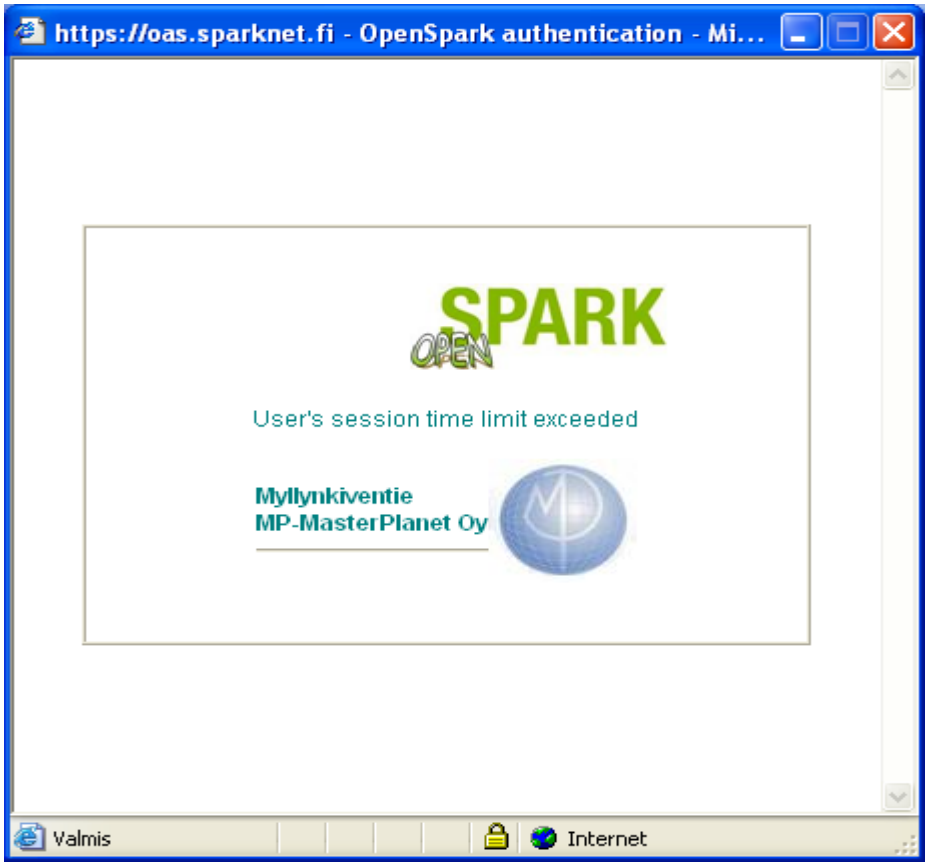


Kuva 24. Visitor- tilin sisäänkirjaus



Kuva 25. Visitor-tunnuksen jäljellä oleva käyttöaika

Kun tunnuksen käyttöaika on loppunut, selain ilmoittaa seuraavaa:



Kuva 26. Käyttöaika käytetty loppuun.

7.11 Local user – tunnus

Tukiasemaan on mahdollista luoda myös local user – tunnuksia, joiden avulla voidaan ottaa yhteys Internetiin OpenSparkin kautta ilman erikseen määrättyä aikarajoitusta.. Local user – tunnuksilla pääsee ainoastaan Internetiin. Tunnuksilla ei pääse muokkaamaan tukiaseman asetustoimintoja, vaan siihen on oikeus ainoastaan tukiaseman omistavalla henkilöllä.

8 YHTEENVETO

Langattomia verkkoja on infrastruktuuriltaan erilaisia, ja ne luokitellaan yleensä kantavuuden laajuuden mukaan. Tänä päivänä niin yksityinen henkilö kuin julkinenkin sektori löytää helposti itselle sopivan langattoman verkkoratkaisun

Langattomista verkoista puhuttaessa on ensiarvoisen tärkeää huolehtia riittävästä salauksesta ja riittävästä tietoturvan tasosta. Suojamaton langaton verkko on täysin avoin hyökkäyksille koko verkon kantoalueella. Langattoman verkon laajuudesta riippuen suojaamattomaan langattomaan verkkoon on täysi pääsy sadoilla tai jopa tuhansilla ihmisillä.

Openspark ja Sparknet ovat suojaamattomia langattomia verkkoyhteisöjä. Tämä tarkoittaa, että liittämällä oman Openspark – tukiasemansa verkkoon käyttäjä saa oikeuden käyttää muiden tukiasemaa. Koska kyseessä on suojaamaton langaton verkko, on ensiarvoisen tärkeää, että omassa tietokoneessa on riittävä palomuuri ja virustentorjunta- ohjelmisto.

Sparknet ja Openspark muodostavat Suomen laajimman langattoman verkkototeutuksen.. Sparknet on käytössä niin julkisella kuin yksityisellä sektorilla ja se palvelee noin 100 000 käyttäjää. SparkNet on käyttäjilleen täysin ilmainen. Ainoa käyttövaatimus on oman langattoman tukiaseman liittäminen yhteisön toisten jäsenten käyttöön. Openspark - tunnukset toimivat myös Sparknet tukiasemissa ja päinvastoin.

Openspark - verkkoyhteys on tarkoitettu yksityisille henkilöille. Omaan tukiasemaan on helppo luoda käyttäjätunnukset jokaiselle perheenjäsenelle ilman, että kaikilla olisi pääsy tukiaseman asetustietoihin. Tukiasemaan voidaan luoda käyttäjätunnukset tuhannelle käyttäjälle Tämä vähentää vahinkojen määrää ja parantaa tietoturvaa.

Sparknet on yhteisöille ja yrityksille tarkoitettu verkkosovellus. Sparknet - tukiasemiin luodaan käyttäjätunnukset aivan samoin kuin Opensparkin puolellakin. Sparknet - lisenssi maksaa 500 €, jolla asiakas saa oikeuden käyttää Sparknettiä liiketoimintaan.

Tukiasemaan voidaan luoda visitor - käyttäjätunnuksia, jotka ovat voimassa ennalta määrätyn ajan. Esimerkiksi kahvilan omistaja voi kaupata surffausaikaa ja veloittaa siitä esimerkiksi tuntihinnan.

Openspark- ja Sparknet- tukiasemia on tällä hetkellä käytössä noin 2500 kappaletta, mikä mahdollistaa yhteyden lähes missä tahansa Turun keskustan alueella ja lähiseuduilla.

LÄHTEET

Kirjat

Geier, Jim 2005, Langattomat verkot – perusteet. Helsinki : Edita Oy

Jaakohuhta, Hannu 2001, IT Ensyklopedia: Edita Oy

Jaakohuhta, Hannu 2002, Lähiverkot – Ethernet: Edita Oy

Puska, Matti 2005. Langattomat lähiverkot. Helsinki: Talentum

Puska, Matti 2000, Lähiverkkojen tekniikka: Pro Training: Helsinki: Satka

Artikkelit

Anttila, Timo 2006 Openspark teki Turusta langattomuuden pääkaupungin. Turun Sanomat (3.62006)

Hamilo, Marko 2005, Turussa verkkoja jaetaan talkooperiaatteella. Helsingin Sanomat (29.5.2005)

Elektroniset lähteet

Sparknet 2006,viitattu 4.4.2008 (https://open.sparknet.fi/index.php?page=openspark)

Sparknet 2006,viitattu 4.4.2009 (https://open.sparknet.fi, viitattu 4.4.2008)

Sparknet 2006,viitattu 8.4.2009 (https://open.sparknet.fi/index.php?page=openspark)

Sparknet 2006,viitattu 8.4.2009 (http://www.sparknet.fi/fi/About.html)

Sparknet 2006,viitattu 8.4.2009 (https://open.sparknet.fi/index.php?page=openspark)

Sparknet 2006,viitattu 8.4.2009 (http://www.sparknet.fi/fi/History.html)

Sparknet 2006,viitattu 8.4.2009 (https://open.sparknet.fi, viitattu 4.4.2008)