Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2011

Rami Ruohola

LANGATTOMAN LÄHIVERKON TURVALLINEN KOTIKÄYTTÖ

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Joulukuu 2011 | 47 sivua

Esko Vainikka

Rami Ruohola

LANGATTOMAN LÄHIVERKON TURVALLINEN KOTIKÄYTTÖ

Opinnäytetyön tavoitteena on luoda suojattu ja toimiva langaton lähiverkkokotioloissa. Ensimmäinen ongelma on lähiverkon kuuluvuus kaikille lähiverkossa oleville käyttäjille. Toinen ongelma on lähiverkon toimivuus erilaisten salausten ollessa päällä. Työssä tutkitaan tukiaseman kuuluvuutta lähiverkon muille käyttäjille sekä mahdollisuuksia parantaa ja vahvistaa kuuluvuutta. Lähiverkon käyttäjillä on suuria laite- ja ohjelmistoeroja, työssä tutkitaan myös näiden vaikutusta toimivuuteen.

Langaton lähiverkko eli Wireless Local Area Network mahdollistaa verkkoyhteyden toisiin tietokoneisiin, verkkolaitteisiin ja Internetiin ilman kaapeleita. Langaton lähiverkko vaatii sopivan WLAN-verkko-ohjaimen jokaiseen verkkoon yhdistyvään laitteeseen. Yhdessä tukiasemassa voi olla yhteydessä useita langattomia laitteita ja käyttäjiä.

Langattomat lähiverkot käyttävät tiedonsiirrossaan radioaaltoja. Radioaaltoja on helpompi vakoilla kuin kiinteää lankaverkkoa, joka käyttää tiedonsiirrossaan kaapelointia. Langattomalle lähiverkolle on onneksi olemassa erilaisia salausmenetelmiä ja muita suojausmenetelmiä. Langattoman lähiverkon suurin haittapuoli on silti sen turvattomuus. Kuka tahansa voi päästä verkkoon, jos on lähiverkon signaalin kantaman sisällä. Salakuuntelemalla verkkoa ja sen tietoliikennettä voidaan yrittää selvittää esimerkiksi verkossa käytettävää WEP/WPA-salausavainta ja MAC-osoitteita.

Työssä tutkittavana oleva langatonlähiverkko koostuu A-Linkin tukiasemasta, kahdesta pöytäkoneesta ja kahdesta kannettavasta tietokoneesta. Tukiasemaan on jouduttu hankkimaan A-Linkin oma tehokkaampi sisäantenni sekä parantamaan langattoman lähiverkon kuuluvuutta talon sisällä. Työssä käytettävä langaton lähiverkko on nimeltään Poeniweb. Poeniweb koostuu neljästä käyttäjästä, eli tilaajasta. Kaksi näistä tilaajasta on kiinteitä pöytäkoneita ja toiset kaksi ovat liikkuvia tilaajia eli kannettavia tietokoneita.

Vertailtaessa kahta salausmenetelmää WEP ja WPA, WEP toimi moitteettomasti kaikilla käyttäjillä, mutta se ei ole enää kovinkaan turvallinen. WPA toimi melkein kaikilla käyttäjillä, yhden käyttäjän laitteisto oli liian vanha toimiakseen. Ongelmia työssä aiheutti saman käyttäjän WLAN-sovitin. Muiden tilaajien laitteet tai ohjelmistot eivät aiheuttaneet ongelmia missään vaiheessa työtä.

ASIASANAT:

WLAN, langaton lähiverkko, IEEE 802.11x, salaus, suojaus, WEP, WPA, SSID.

BACHELOR´S THESIS | ABSTRACT

UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communication

December 2011 | 47 pages

Esko Vainikka

Rami Ruohola

THE SAFE USE OF WIRELESS LOCAL AREA NETWORK AT HOME

This thesis aims to establish a secure and efficient wireless local area network at home. The problem is that the reception of the WLAN does not reach all users of the local area network. Previously, the problem has been WLANs functionality of the various encryptions. This thesis examines the Access Points coverage to other network users, as well as opportunities to improve and strengthen Access Points signal. Local Area Network users have large hardware and software differences; the impact of these is examined in this thesis.

Wireless Local Area Network or WLAN allows network connection to other computers, network devices and the Internet without cables. Wireless local area network requires a suitable WLAN controller in each network, connecting with the device. Multiple wireless devices and users can be connected to a single Access Point.

WLANs use radio waves for communications. Radio waves are easier to spy than fixed wire network, which uses cables for data transfers. Fortunately, WLAN has different methods of encryption and other security methods. WLANs main drawback is still the lack of security. Anyone can access the network, if you are in the range of WLANs signal. Taping to the network and its data traffic one can try to figure out, for example WEP / WPA encryption key and MAC addresses of the network they spy.

My home WLAN consists of A-Links Access Point, two desktop computers and of two laptops. Access Point has been fitted with A-Link's own powerful internal antenna to improve WLANs coverage inside the house. I named my WLAN Poeniweb. Poeniweb consists of four computers. Two of these computers are desktop computers and the other two are laptops.

When choosing from two types of encryption method, WEP or WPA. WEP functioned properly for all users, but it is not very safe to use anymore. WPA encryption worked in almost all users; one user's hardware was too old to work properly. Problems in the thesis were caused by the same user's WLAN-adapter, the other user’s devices or software applications did not cause problems at any stage of work.

KEYWORDS:

WLAN, Wireless local area network, IEEE 802.11x, encryption, protection, WEP, WPA, SSID.

SISÄLTÖ

KUVAT

1 JOHDANTO

WLAN-verkko eli langaton lähiverkko on radioaaltoihin perustuva lähiverkko, johon tarvitaan lähetinantenni ja vastaanotin. Nykyään monilla on kotikäytössä langattomia lähiverkkoja. Ne ovat nykyään helppoja asentaa ja käyttää, mutta niiden tietoturvallisuus on vähintäänkin kyseenalainen. Langattomalle lähiverkolle on olemassa hyviä salausmenetelmiä, mutta niitä ei löydy muista kuin uusimmista WLAN-modeemeista ja sovittimista.

Työssäni lähden tutkimaan, miten saisin kotiverkkoni toimimaan mahdollisimman luotettavasti ja turvallisesti. Tällä hetkellä langattomassa lähiverkossani ei ole kytkettynä muita suojauksia kuin MAC-osoitteen varmennus. Tämä johtuu siitä, että yhteys ei kuulu muiden suojauksien ollessa käytössä. Työssäni tulen selvittämään, miten paljon ADSL-modeemin ja WLAN-verkkokortin välinen etäisyys ja sen välissä olevat esteet hidastavat signaalin kuuluvuutta. Tavoitteeni on luoda kotiini turvallinen ja toimiva langaton lähiverkko, mihin voi myöhemmin lisätä uusia laitteita. Testiryhmääni on mahdollista vielä lisätä toinen pöytäkone ja kaksi kannettavaa tietokonetta, jolloin nämä lisäykset tekevät langattoman lähiverkon mittauksesta vielä vakuuttavamman ja tarkemman.

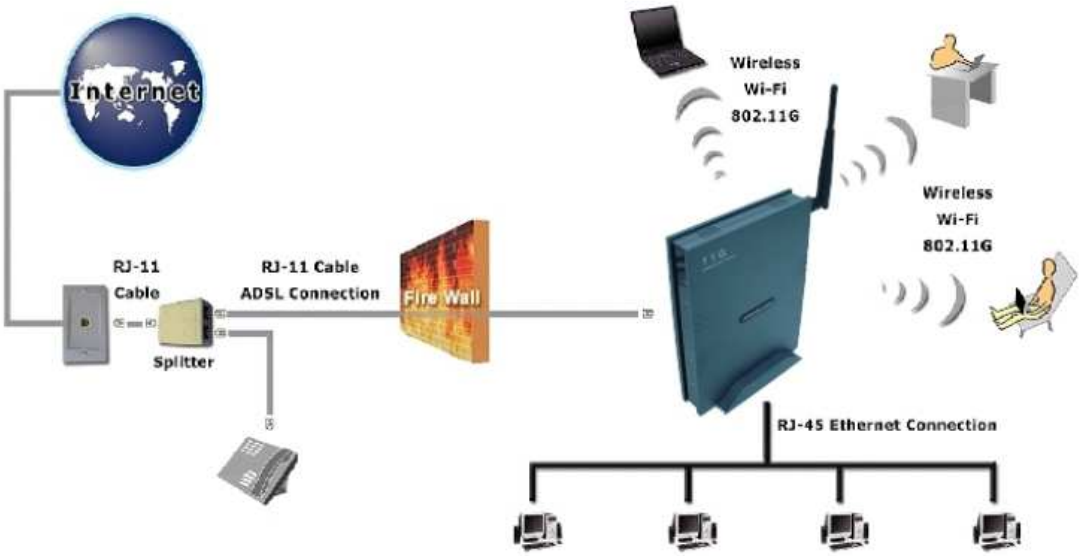
Teoreettisessa viitekehyksessä olen perehtynyt kirjoihin, jotka käsittelevät langatonta lähiverkkoa yleisesti ja varsinkin niiden salausmenetelmiä. Olen myös tutkinut muutamia opinnäytetöitä, jotka käsittelevät langattomia lähiverkkoja ja niiden mittauksia. Olen perehtynyt myös muutamaan vakuuttavaan internet-lähteeseen, jotka käsittelivät valitsemaani aihetta hyvin. Selvennän työtäni talon pohjapiirustuksella, jossa on merkittyinä lähiverkon kaikki laitteet.

Empiiriseen osioon lähden toteuttamaan ja testaamaan erilaistenverkko-laitteiden yhdistelmiä. Testaan eri suojaukset ja niitä yhdistelemällä rakennan toimivan ja turvallinen kokonaisuuden. WLANin kattavuuden mittaamiseksi tarvitsen kannettavan tietokoneen, joka näyttää verkonkuuluvuuden.

2 LANGATTOMAN LÄHIVERKON PERUSTEET

Langaton lähiverkko eli Wireless Local Area Network (WLAN) mahdollistaa verkkoyhteyden toisiin tietokoneisiin, verkkolaitteisiin ja Internetiin ilman kaapeleita. Langattoman lähiverkon helppo ja kustannustehokas rakentaminen ja käyttö on tehnyt tästä äärimmäisen suositun nykyaikana. Koska langaton lähiverkko ei tarvitse kaapelia muuta kuin tukiaseman ja Internetin väliin, on se mahdollista rakentaa paikkaan, jossa kaapelointi on mahdotonta.

Langaton lähiverkko vaatii sopivan WLAN-verkko-ohjaimen jokaiseen verkkoon yhdistyvään laitteeseen. Yhdessä tukiasemassa voi olla yhteydessä useita langattomia laitteita ja käyttäjiä (kuva 1).



Kuva1. Tyypillinen langaton lähiverkko (RoadRunner, 2011).

2.1 IEEE 802.11 –standardikokoelma

IEEE 802.11 on kokoelma eri standardeja, joilla määritellään langattoman lähiverkon yhteydet taajuuksilla 2.4, 3.6 ja 5GHz. IEEE LAN/MAN-standardikomitea on luonut nämä ja se ylläpitää sekä valvoo näiden käyttöä.

802.11 on ensimmäinen langattoman lähiverkon standardi, se on luotu 1997 ja nykypäivänä se on äärimmäisen harvinainen. Sen nimellisnopeus on 1 tai 2 megabittiä sekunnissa. 802.11 toimii 2.4GHz:n taajuudella ja sen välitystekniikoiksi on määritelty infrapuna ja radiotiet. Nopeuksien moduloinnissa käytetään Baker-sekvenssiä eli tieto lähetetään 11-bittisinä sarjoina. (IEEE 802.11, 2011.)

802.11a julkaistiin vuonna 1999. Taajuuden 2.4GHz ruuhkautuessa otti 802.11a käyttöön 5GHz taajuuden. Taajuuden korkeus mahdollisti myös nopeamman liikenteen, standardin nimellisnopeus on 54 megabittiä sekunnissa. 802.11a:ssa otettiin käyttöön OFDM-tekniikka (orthogonal frequency division multiplexing), joka jakaa signaalin alasignaaleihin ja lähettää niitä yhtäjaksoisesti eri taajuuksilla. OFDM-tekniikka mahdollisti 54Mbit/s nopeuden, mutta se oli laitteistoltaan kallis ja siitä ei koskaan tullut kovinkaan suosittua. (IEEE 802.11, 2011.)

802.11b–standardi julkaistiin myös vuonna 1999. Sen nimellisnopeus oli 11 megabittiä sekunnissa ja se jatkoi toimintaa 2.4GHz taajuudella. 802.11b tukee nopeuksia 1 ja 2 megabittiä sekunnissa sekä lisäksi nopeuksia 5.5 megabittiä ja 11 megabittiä sekunnissa. Alemmilla nopeuksilla käytetään Baker-sekvenssiä, mutta suurimmilla nopeuksilla käytetään CCK-modulointia (Complementary Code Keying). CCK-tekniikassa tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. (Granlund, 2007, 301.)

802.11g –standardi on otettu käyttöön vuonna 2003. Se toimii 54Mbit/s siirtonopeudella, mutta se toimii 2.4GHz taajuudella. 802.11g mahdollisti nopeuksien nostamisen vaihtamatta taajuutta, jolloin yhteensopivuus versioiden b ja g välillä voitiin säilyttää. 802.11g on tällä hetkellä suosituin standardi ja se on käytännössä katsoen syrjäyttänyt 802.11b –standardin.(IEEE 802.11, 2011.)

802.11n–standardi on otettu käyttöön vuonna 2009. Se käyttää MIMO-tekniikkaa (multiple-input, multiple-output), jossa käytetään useampaa antennia ja useampaa ilmatietä. 802.11n:n nopeudeksi on määritetty 600Mbit/s, mutta sen todellinen nopeus on 100-200 Mbit/s. Se käyttää hyväkseen 5MHz ja

2.4MHz taajuuksia. Lähetyksen kaistan leveys on joko 20 tai 40 MHz, tämä mahdollistaa paremman kuuluvuuden verrattuna aikaisempiin standardeihin(kuva 2). (IEEE 802.11, 2011.)

Langaton verkko

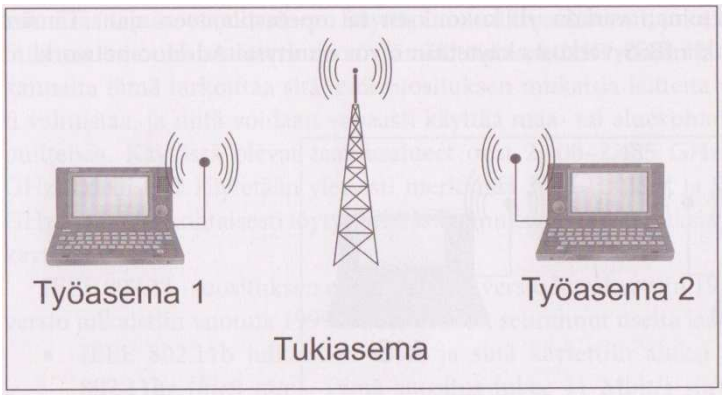
Standardi	Suurin nopeus	Taajuus	Toiminta	Yhteensopivuus
IEEE 802.11a	54 Mb/s	5,0 GHz	Usean verkkolaitteen välillä tukiaseman avulla	Toimii IEEE 802.11n:n kanssa
IEEE 802.11b	11 Mb/s	2,4 GHz	Usean verkkolaitteen välillä tukiaseman avulla	Toimii IEEE 802.11g:n kanssa
IEEE 802.11g	54 Mb/s	2,4 GHz	Usean verkkolaitteen välillä tukiaseman avulla	Toimii IEEE 802.11b:n kanssa
IEEE 802.11n	600 Mb/s	2,4 ja 5,0 GHz	Usean verkkolaitteen välillä tukiaseman avulla	Toimii IEEE 802.11g:n ja IEEE 802.11a:n kanssa
Bluetooth 1.2	728 kb/s	2,4 GHz	Kahden verkkolaitteen välillä	Ei toimi muiden kanssa erilaisen rakenteen takia
Bluetooth 2.0 + EDR	2,1 Mb/s	2,4 GHz	Kahden verkkolaitteen välillä	Ei toimi muiden kanssa erilaisen rakenteen takia

Kuva2. 802.11 –standardien yleistiedot (Flyktman, 2010, 330).

2.2 Langattoman lähiverkon topologiat.

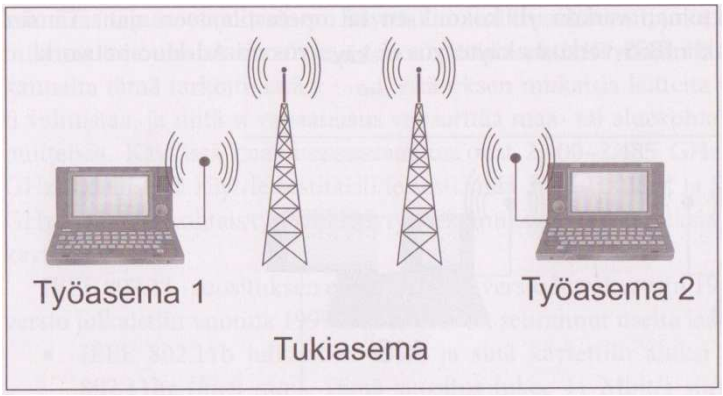
IEEE 802.11 määrittelee kolme tapaa kytkeä laitteet langattomasti toisiinsa. Perusarkkitehtuuria kutsutaan BSS:ksi (Basic Service Set). Tämä koostuu laitteista, jotka kykenevät kommunikoimaan keskenään. (Granlund, 2007, 294.)

BSS-lähiverkko muodostuu tukiasemasta ja siihen liitetyistä langattomista tietokoneista. Tietokoneiden välinen liikenne verkossa käydään tukiaseman kautta. Tämäntapainen langaton lähiverkko on yleisimmin kotikäytössä (kuva3). (Granlund, 2007, 295.)



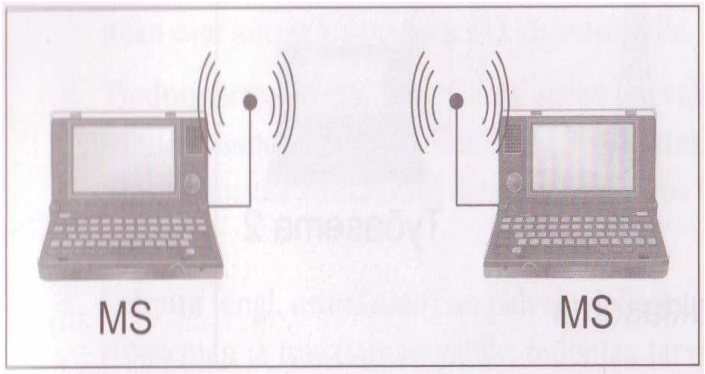
Kuva3. BSS-lähiverkko (Granlund, 2007, 296).

BSS-lähiverkkoa voidaan laajentaa käyttämällä useampia tukiasemia, jotka kytketään samaan runkoverkkoon. Useammalla tukiasemalla varustettua langatontalähiverkkoa kutsutaan ESS:ksi (Extended Service Set), mitä runkoverkkon suositus kutsuu DS:ksi (Distribution System). Tämä tapa on yleisin tapa muodostaa langaton lähiverkko, jos yhdellä tukiasemalla ei saada tarpeeksi kattavaa lähiverkkoa (kuva4). (Granlund, 2007, 295.)



Kuva4. ESS – DS lähiverkko.

Kolmas tapa kytkeytyä langattomaan lähiverkkoon on IBSS (Independet Basic Service Set) eli Ad-Hoc. Tämä tarkoittaa kahden tietokoneen välistä langatonta yhteyttä ilman tukiasemaa. Ad-Hoc -tilaa käytetään pääasiassa tiedon siirtämiseen koneelta toiselle. IBSS-tilan ollessa käytössä tietokone ei voi olla yhteydessä mihinkään muuhun langattomaan lähiverkkoon (kuva5).



Kuva5. IBSS lähiverkko (Granlund, 2007, 295).

3 LANGATTOMAN VERKON SALAUS JA SUOJAUS

Langattomat lähiverkot käyttävät tiedonsiirrossaan radioaaltoja. Radioaaltoja on helpompi vakoilla kuin kiinteää lankaverkkoa, joka käyttää tiedonsiirrossaan kaapelointia. Langattomaan lähiverkkoon on myös helpompi kytkeytyä kuin kaapeleita käyttävään verkkoon. (Hakala, ym 2006, 296.)

IEEE 802.11 –suositus pyrki tietoturvallaan luomaan saman tasoisen suojauksen kuin perinteisellä kiinteällä lähiverkolla. Tämä suojaus keskittyi radiotiellä siirtyvään tietoon, suojausmenetelmästä käytettiin nimitystä WEP (Wired Equivalent Privacy). WEP havaittiin nopeasti haavoittuvaksi, ja WiFI-allianssi korjasi sen puutteita suosituksella WPA (Wifi Protected Access). IEEE:n802.11-verkon tietoturvatyöryhmä julkaisi vuonna 2004 suosituksen 802.11i, josta WiFi-allianssi käyttää nimitystä WPA2. (Granlund 2007,317.)

Langattoman lähiverkon suurin haittapuoli on silti sen turvattomuus. Kuka tahansa voi päästä verkkoon, jos on lähiverkon signaalin kantaman sisällä. Salakuuntelemalla verkkoa ja sen tietoliikennettä voidaan yrittää selvittää esimerkiksi verkossa käytettävää WEP/WPA-salausavainta ja MAC-osoitteita. (Flyktman 2010, 333.)

Seuraavaksi käsittelen muutamia menetelmiä, joilla voi oikeastaan vain hidastaa verkon salauksen murtamista. Langattomaan lähiverkkoon murtautuminen ei vaadi kuin tietotaitoa ja oikeat välineet. Onkin kysymys siitä, onko lähiverkkoon murtautuminen vaivan arvoista?

3.1 Hidden SSID

Verkkonimi (SSID, Service Set Indentification) voidaan piilottaa, jolloin se ei näy verkkoja selatessa. Vaikka verkkonimi on piilotettu, siihen voidaan ottaa yhteys yhdenmukaistamalla asetukset manuaalisesti. Todellista murtautujaa verkkonimen piilottaminen ei pidättele. Muiden suojauksien käyttäminen verkkonimen piilottamisen lisäksi parantaa huomattavasti lähiverkon suojauksen tasoa. (Flyktman 2010, 334.)

3.2 WEP-salaus

Wired Equivalent Privacy –protokolla (WEP) on suojausmekanismi, jonka avulla pyritään turvaamaan tietoliikenteen luottamuksellisuus. WEP perustuu tukiasemiin ja verkkokortteihin määriteltyihin salausavaimiin. Avaimen vähimmäispituus on 64 bittiä ja enimmäispituus 128 bittiä, joidenkin laitevalmistajien sovittimet tukevat 256-bittistä avainta. Tukiasemat ja verkkokortit mahdollistavat usean salausavaimen käyttämisen, mutta ei ole olemassa mekanismia avainten automaattiseen vaihtoon. Koska salausavain pysyy pitkiä aikoja samana, helpottaa tämä salauksen murtamista huomattavasti. (Hakala, ym 2006, 296.)

64 bitin salasanan pituus ASCII-merkistöllä on 5 merkkiä. Usein WEP-avaimessa käytetään kuitenkin hexadesimaalilukuihin (0-9, A-F) 10 merkin sarjaa. 128-bittiseen avaimeen tulee vastaavasti 13 ja 26 merkkiä. (Flyktman 2010, 335.)

WEP-avaimet jakautuvat kahteen järjestelmään. Ensimmäinen on Open System eli kaikille avoin pääsy verkkoon. Sovitin ei autentikoi kirjautuneita käyttäjiä, koska salausavaimet autentikoidaan laitetasolla. Käyttäjällä kuitenkin tulee olla tiedossa salausavaimet tätä varten. Autentikoinnin jälkeen tieto Gatewayn ja laitteen välillä kryptataan. Avointa verkkoa ei suositella, jos lähiverkossa liikkuu yksityistä tietoa. (RoadRunner, 2011.)

Toinen järjestelmä on Shared Key Authentication eli yhteiseen salattuun avaimeen perustuva autentikointi. Tässä WEP-avainta käytetään neljän kohdan haaste-vaste –kättelyssä.:

1. Tilaaja lähettää sovittimelle pyynnön autentikointiin.
2. Sovitin vastaa lähettämällä nonssin, tämä on yhdistelmä sekalaisia lukuja ja kirjaimia.
3. Tilaaja salakirjoittaa WEP-avaimellaan tämän ja lähettää sen takaisin sovittimelle.
4. Sovitin purkaa vastauksen ja jos tämä vastaa nonssia, päästää sovitin tilaajan verkkoon.

Autentikoinnin jälkeen WEP-avainta käytetään vielä liikenteen salaamiseksi, aivan kuin avoimen pääsyn verkolla. (WEP, 2011.)

3.3 WPA-salaus

WPA-salausprotokolla on WiFi-allianssin kehittämä WEP-salauksen korvaava langattoman lähiverkon salausmenetelmä. WPA vaihtaa salausavaimen 10 000 paketin välein, WEP ei vaihtanut salausavainta kertaakaan. WPA käyttää myös pakettikohtaisia salausavaimia sekä korjaa muitakin WEP:ssä olleita turvallisuusongelmia.(Hakala, ym 2006, 297.)

WPA sisältää myös MIC-protokollan (message integrity check), joka on suunniteltu estämään mahdollista hyökkääjää kaappaamasta tai muuttamasta suojatun verkkoliikenteen sisällä kulkevia paketteja. MIC käyttää algoritmia tarkastaessaan pakettien eheyttä. Jos se ei voi todentaa eheyttä, paketti pudotetaan pois. (WPA, 2011.)WPA protokolla hyödyntää kahta muuta protokollaa, WPA-TKIPiä ja WPA-EAPia.

WPA-TKIP (Temporal Key Integrity Protocol) huolehtii lähetettävien tietojen salauksesta. WPA-TKIP on WPA salauksen heikoin lenkki, sillä se käyttää samaa RC4-salausalgoritmiä kuin WEP.

WPA-EAP (Extensible Authentication Protocol) mahdollistaa käyttäjien luotettavan tunnistamisen.

WPA-suojausta voidaan käyttää kahdessa eri tilassa. WPA-Personal-tila on perustila, joka on tarkoitettu pääsosin pienille langattomille lähiverkoille ja kotikäyttöön. WPA-Personal käyttää PSK-tunnistusta (Pre Shared Key) eli verkkosovittimella ja tilaajilla tulee olla sama salasana. Salasanan pituus on 8-63 merkkiä, suositeltava salasanan pituus on 20 merkkiä ja siinä tulisi käyttää isoja ja pieniä kirjaimia sekä lukuja. PSK-tunnistus käyttää samaa neljän kohdan haaste-vaste kättelyä kuin WEP-shared autentikointi. (Flyktman 2010, 336.) WPA-Enterprise-tila tarvitsee toimiakseen RADIUS-palvelimen, joka jakaa käyttäjilleen oman uniikin avaimen.

3.4 WPA2-salaus

WPA ei pohjautunut mihinkään standardiin, vaan se oli periaatteessa paranneltu WEP. WPA oli mahdollista päivittää vanhempiin verkkosovittimiin, WPA2 vaatii jo oman laitteiston, jota ei löydy vanhemmista verkkosovittimista. WPA2 on standardisoitu IEEE-802.11isalausmetodi. WPA2 käyttää CCMP-salausmekanismia (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), joka on vahvempi salaus kuin TKIP. CCMP tunnetaan myös lyhenteellä AES (Advanced Encryption Standard). (IEEE 802.11i, 2011.)

3.5 802.1x -todennus

802.1x –todennus suunniteltiin alun perin käytettäväksi kaikissa IEEE 802 –lähiverkoissa. Se määrittelee porttiperusteisen verkkoonpääsymenettelyn (Port Based Network Access Control), jossa tilaajan verkon käyttöä rajoitetaan langattoman lähiverkon loogisten porttien ja todennuspalvelimen avulla.

802.1x mahdollistaa paremman ja laajemman suojauksen kuin lähiverkoissa yleisesti käytetyt käyttäjienhallintatekniikat, jotka rajoittavat käytännössä lähinnä palvelimiin ja toisiin työasemiin pääsyä. Käyttäjien todennuksessa käytetään yleensä RADIUS-palvelimia (Remote Authentication Dial-In User Service). RADIUS-palvelimet hoitavat käyttäjien tunnistamisen, määrittelevät käyttäjän oikeudet lähiverkossa ja ylläpitävät verkonhallinnan tietokantoja. (Hakala, ym 2006, 298.)

3.6 Access List

MAC-osoite on jokaisen verkkokortin yksilöllinen osoite. Verkkosovittimessa on pääsylista, jolle on mahdollista lisätä tiedettyjen käyttäjien MAC-osoite. Verkkosovitin suodattaa verkkoon pyrkijöiden joukosta sallitut käyttäjät ja pitää ei toivotut ulkona. MAC-osoite on mahdollista kaapata, joten pääsylistaa on hyvä käyttää muiden salausten kanssa. (Flyktman 2010, 333.)

4 VERKON LAITTEET JA TILAAJAT

Kotonani oleva langatonlähiverkko koostuu A-Linkin tukiasemasta, kahdesta pöytäkoneesta ja kahdesta kannettavasta tietokoneesta. Tukiasemaan on jouduttu hankkimaan A-Linkin oma tehokkaampi sisäantenni parantamaan langattoman lähiverkon kuuluvuutta talon sisällä. Langaton lähiverkko on käytössä pääosin kahden pöytäkoneen vuoksi, kannettavat tietokoneet ovat tulleet kuvioihin myöhemmin.

Työstä teki haastavan tietokoneiden laitteistojen ja ohjelmistojen erot, verkkokortteja oli monelta eri valmistajalta ja niiden yhteensopivuuden kanssa oli hetkittäin pienoisia ongelmia. Molemmat pöytäkoneet ovat itse rakennettuja AMD-pohjaisia koneita, kannettavat ovat Hewlett-Packard Pavillion ja Acer Aspire.

Työtä varten olen nimennyt verkkoa käyttävät tietokoneet seuraavanlaisesti:

- Tilaaja1: Pöytäkone1, Windows 7 + D-link DWL-G122 DWA-110
- Tilaaja2: Pöytäkone2, Windows Xp + ZyXEL G-360 WH
- Tilaaja3: Kannettava1, Windows Vista + Atheros AR5007 802.11b/g
- Tilaaja4: Kannettava2, Windows 7 + Atheros AR5B95 WNA

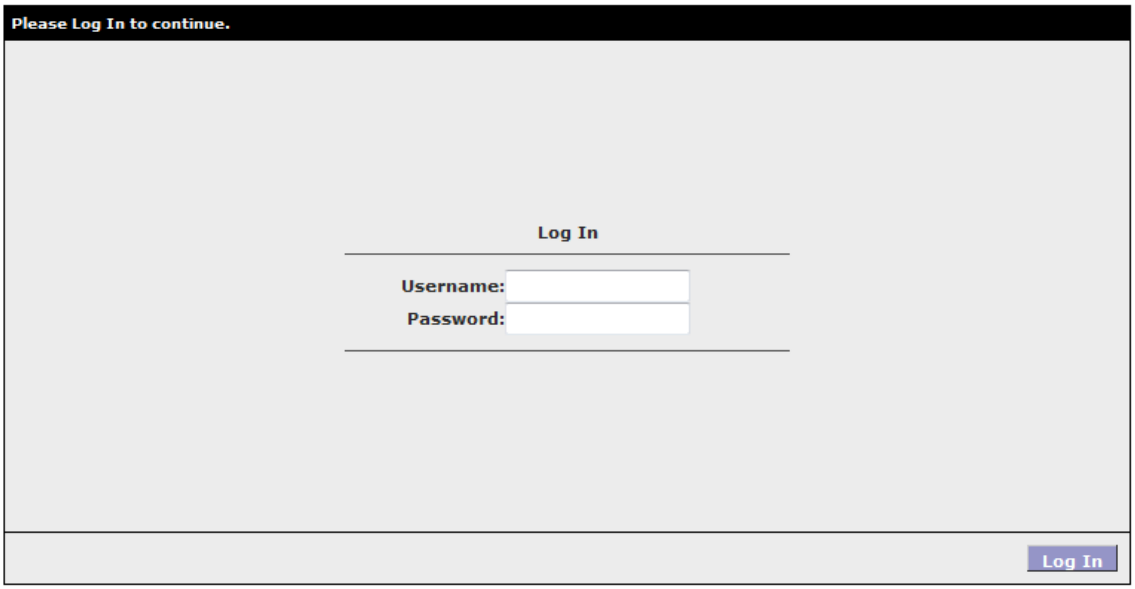
4.1 Tukiasema - Access Point (AP).

WLAN-tukiasema välittää lähiverkossa olevien tietokoneiden välisen verkkoliikenteen. (Flyktman 2010, 329.) Langattomanlähiverkkoni tukiasema (AP) on A-LINKin RoadRunner 24AP (kuva 6). Se on 4-porttinen verkkokytkin, jossa on myös 54Mb WLAN-tukiasema. Tukiasema käyttää 802.11b- ja802.11g-standardeja. Salauksessa tukiasema käyttää WEP/WPA salausta sekä MAC-suodatusta ja SSID:n piilotusta. IEEE 802.11g WLAN toimii taajuuksilla 2.412GHZ ~ 2.484GHZ 2,5dBi antennilla. (RoadRunner 2011.)

Kuva6.A-LINK RoadRunner 24AP (RoadRunner, 2011).

Tukiasemaan on jouduttu hankkimaan tehokkaampi sisäantenni, sillä tukiaseman oman antennin signaali ei kuulunut tarpeeksi kauas tai tarpeeksi vahvasti. Tukiasemaan on kytketty suunnattava A-LINKin A6IN WLAN-antenni, joka toimii 6dBi:n voimalla. A6IN-antennin johto on noin puolimetriä pitkä, tämä helpottaa suuresti antennin sijoittamista ja suuntausta. Antenni on ympärisäteilevä, mutta sen vahvimman keilan voi suunnata haluamaansa suuntaan (kuva7).

Kuva7. A-LINK A6IN sisätila-antenni (A6IN, 2011).



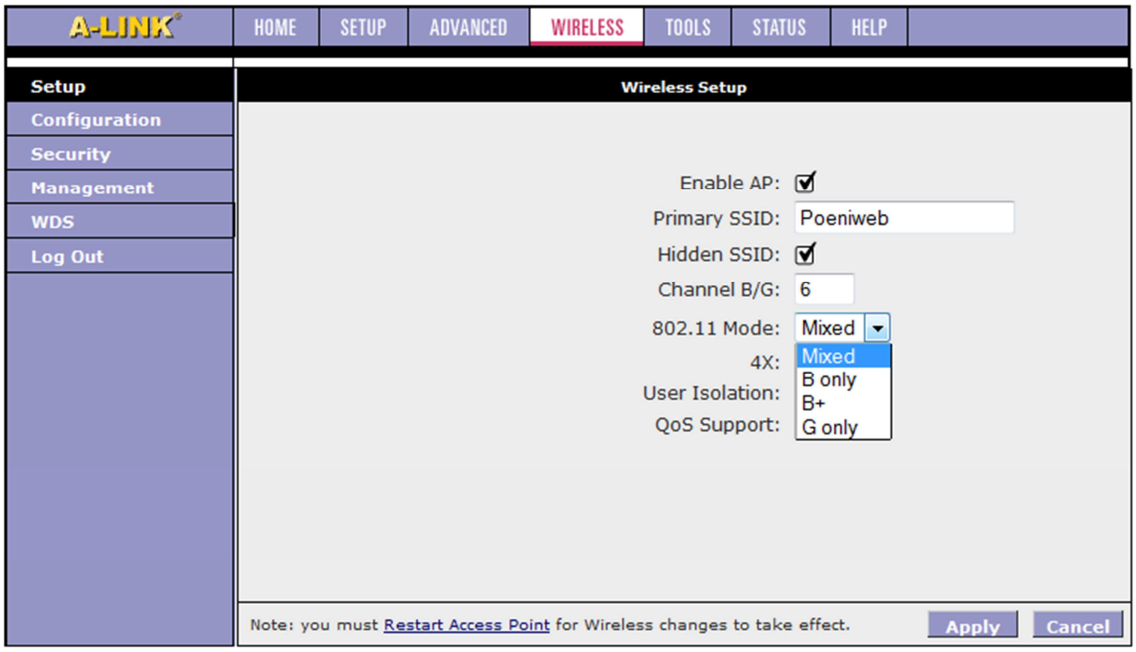
Kuva8. Tukiaseman kirjautumissivu.

Tukiasemaan kirjaudutaan selaimen kautta. Käyttäjän tulee olla kirjautunut tukiaseman langattomaan verkkoon tai olla yhteydessä tukiasemaan kaapelin kautta. Tukiasemaan pääsee kirjautumaan osoitteella http://10.0.0.2 ja syöttämällä järjestelmänvalvojan tunnuksen ja salasanan (kuva8).

Tukiaseman pääsivu kertoo tärkeimmät tiedot yhteyden tilasta. Se kertoo langattoman verkon nimen sekä sen, kuinka kauan yhteys on ollut kytkettynä (kuva9).

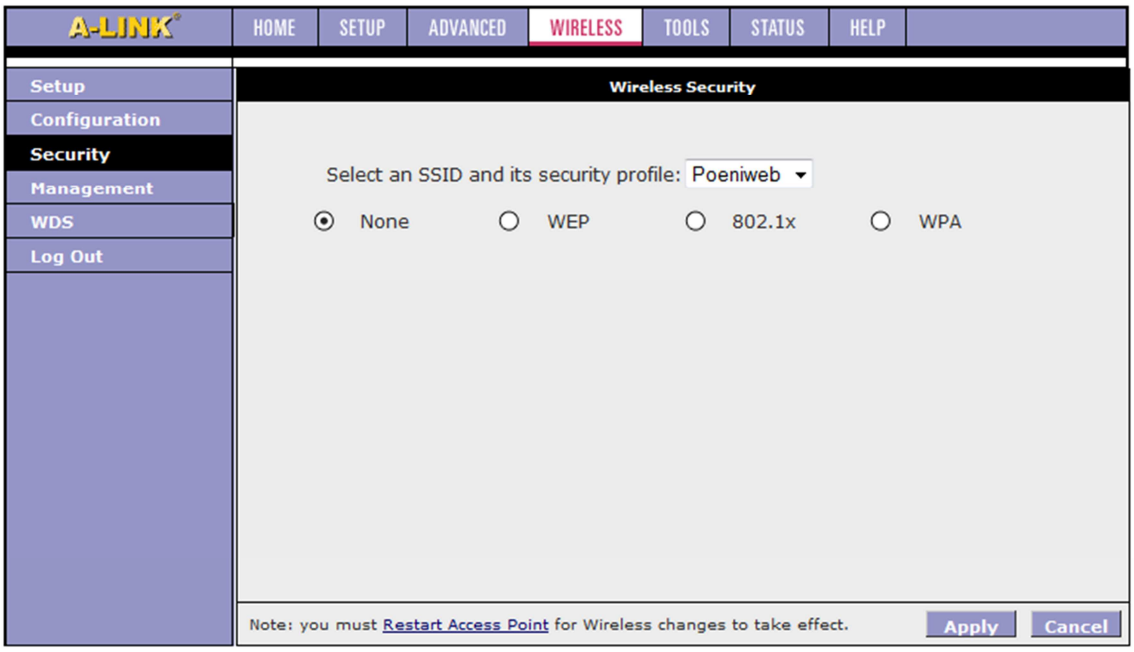
Kuva9. Tukiaseman pääsivu.

Setup-osiosta pystyy määrittelemään, onko tukiasema toiminnassa, eli lähettääkö tukiasema langattoman verkon signaalia ympäristöön. Osiossa määritellään myös langattoman verkon nimi sekä se, näkyykö nimi julkisesti. Osiossa pääsee myös määrittelemään, käyttääkö tukiasema IEEE-802.11b-, IEEE-802.11g-standardia vai molempia verkkostandardeja (kuva10).



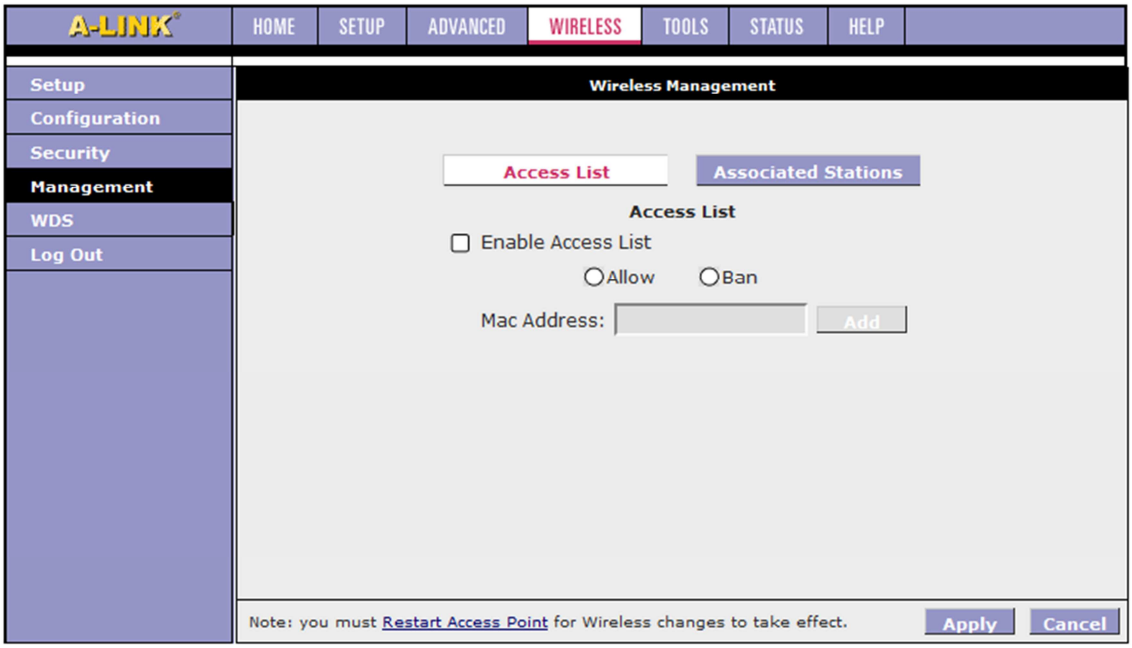
Kuva10. Langattoman osion keskeisimmät asetukset.

Security-osiosta asetetaan langattoman verkon salaus. Saatavilla olevat suojausmenetelmät ovat WEP- tai WPA-salaus. Valitsemalla 802.1x-suojauksen pääsee määrittelemään RADIUS-salauksen. On mahdollista jättää lähiverkko suojaamatta valitsemalla None vaihtoehdon (kuva11).



Kuva11. Langattoman osion turvallisuusasetukset.

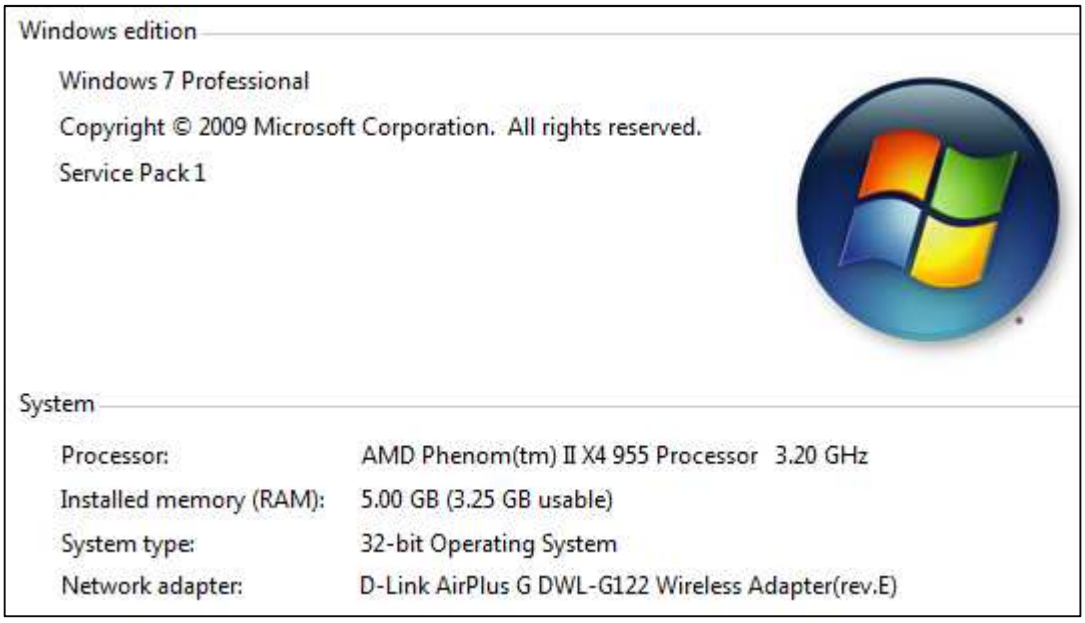
Management-osiosta pääsee asettamaan käyttäjien MAC-osoitteita, jolloin tukiasemaan pääsevät kirjautumaan tilaajat, joiden uniikki MAC-osoite on lisätty access listiin (kuva12).



Kuva12. Langattoman osion hallinta-asetukset.

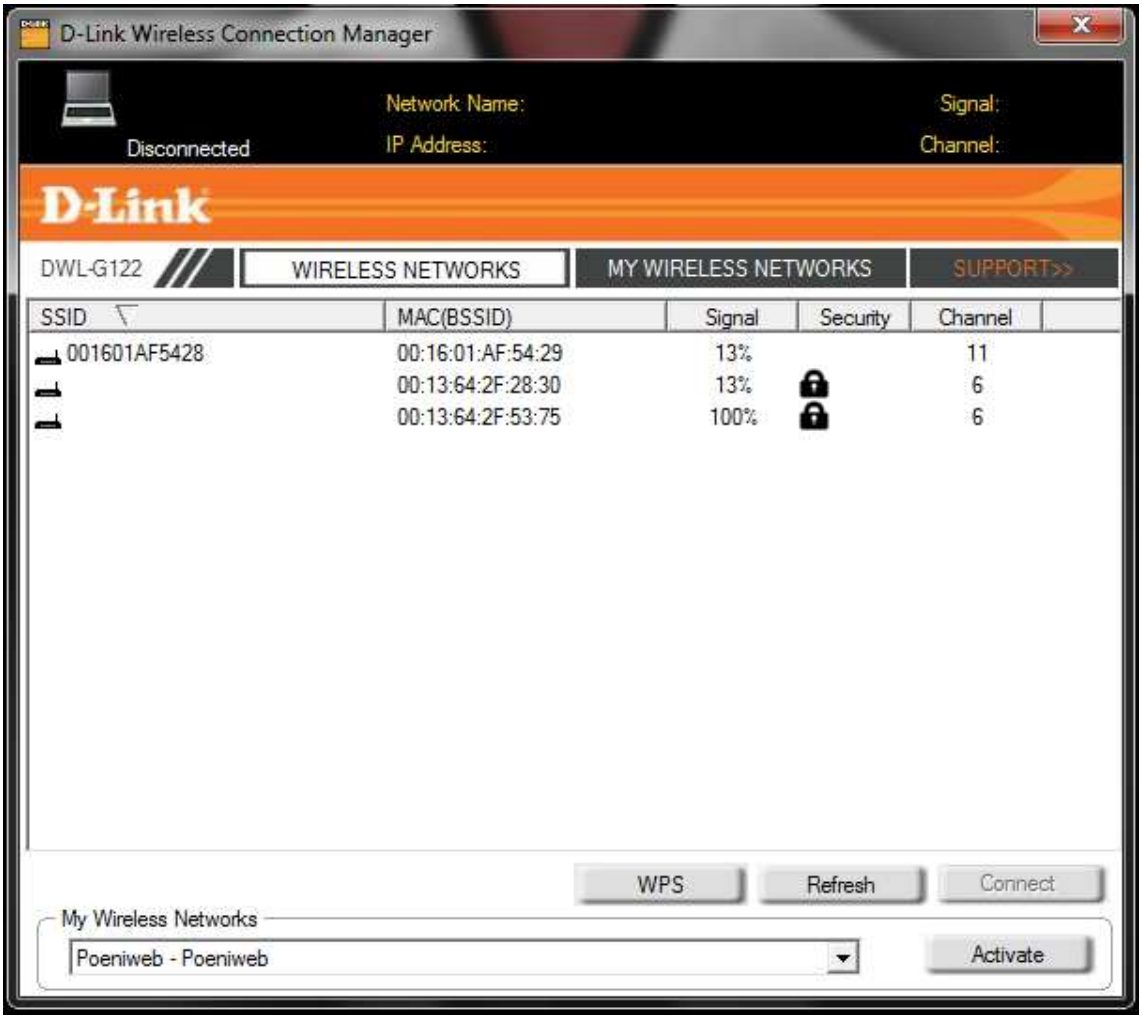
4.2 Tilaaja1

Tilaaja1 on verkon tehokkain tietokone ja varustettu Windows 7:llä. Yleensä se on kaapelin kanssa kiinni tukiasemassa, mutta kesällä tapahtuneen ukkosmyrskyn jälkeen olen hankkinut siihen D-Linkin DWL-G122 USB2.0 WLAN-sovittimen. Sovittimen voi kytkeä suoraan USB-porttiin, mutta keskusyksikköni ollessa sen verran matalalla käytän sovittimen mukana tullutta telakkaa. Telakassa on pitkä johto, joka mahdollistaa sovittimen sijoittamisen korkeammalle ja näin taata esteetön signaalin kulku. DWL-G122 on verkkoni uusin WLAN-sovitin. Se sisältää WEP, WPA- ja WPA2- salaukset ja se on äärimmäisen helppokäyttöinen. Tukiaseman kantama sisätilassa on noin 100m ja siinä on perus 2dBi lähetin/vastaanotin (kuva13). (D-Link, 2011.)



Kuva13. Tilaaja1:n tiedot.

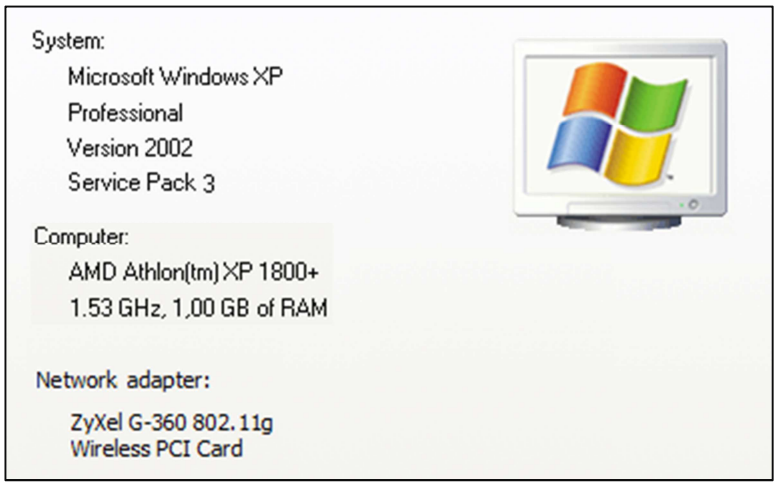
Wireless Networks -osiosta näkee kaikki sovittimen löytämät langattomat verkot. My Wireless Networks näyttää käyttäjän omat verkot, jos sinne on ne valmiiksi asettanut. D-Link Wireless Connection Manager on todella selkeä ja helppokäyttöinen hallintaohjelma (kuva14).



Kuva14. Perusnäkymä D-Linkistä.

4.3 Tilaaja2

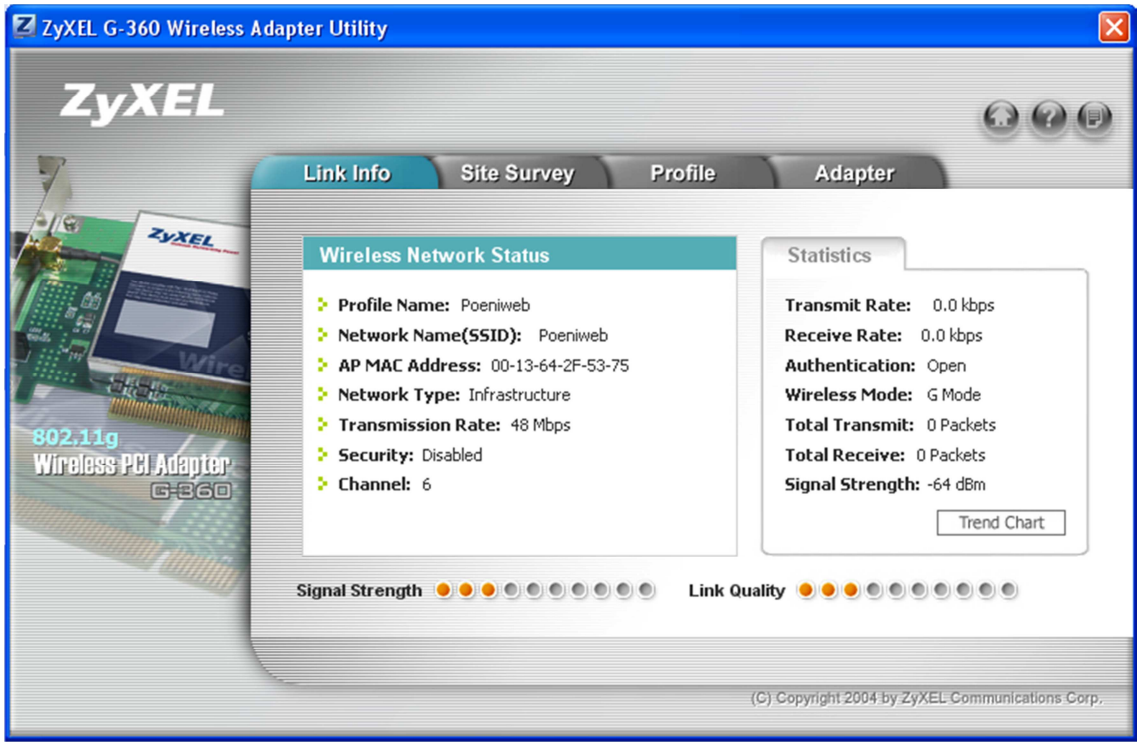
Tilaaja2 on koko opinnäytetyön alkuunpanija. Se on verkon vanhin tietokone ja käyttäjäjärjestelmänä siinä on Windows XP. Tilaaja2:lle ei ollut mahdollista rakentaa kaapeliyhteyttä, joten minun piti hankkia siihen WLAN-sovitin. Tukiaseman ja Tilaaja2:n välillä oli kuitenkin sen verran matkaa ja rakenteellisia esteitä, että signaali ei kuulunut tarpeeksi vahvasti. Signaali kuului heikosti, kun tukiasemassa ei ollut mitään salauksia tai suojauksia. Kun suojaukset laitettiin päälle, Tilaaja2 ei enää löytänyt verkkoa. Tästä johtuen jouduin hankkimaan vahvemman sisäantennin, mikä helpotti tilannetta hetken. Uuden antennin asentamisen jälkeen signaalin laatu nousi huomattavasti. Kun salaus otettiin käyttöön WLA-sovitin löysi verkon, mutta yhteys siihen ei ollut kovin vakaa (kuva15).



Kuva15. Tilaaja2:n tiedot.

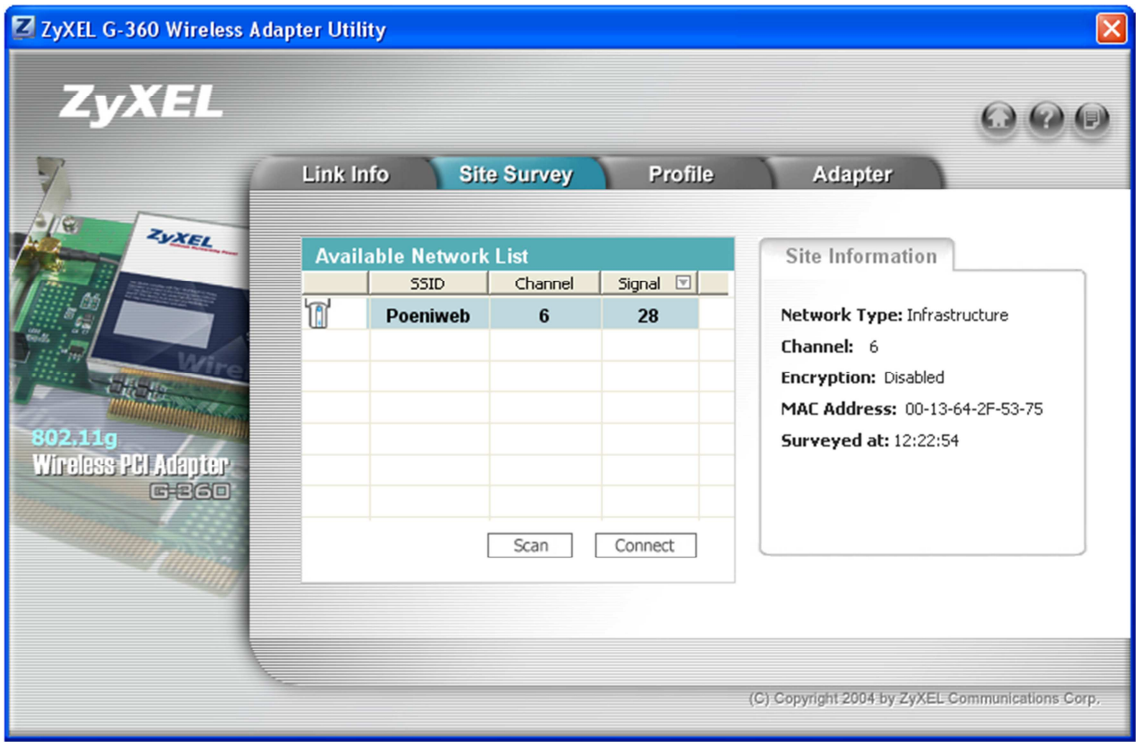
Tilaaja2:lla on ZyXel G-360 802.11g PCI-verkkokortti. Kortti on huomattavasti vanhempi kuin verkon muut WLAN-sovittimet, mutta päivittämällä siitä tuli yhteensopiva muiden kanssa.

Link Info-osiosta näkyy käytössä oleva verkko sekä yhteyden tekniset tiedot. Statistiikasta näkee yhteyden nopeuden ja liikenteen määrän (kuva16).



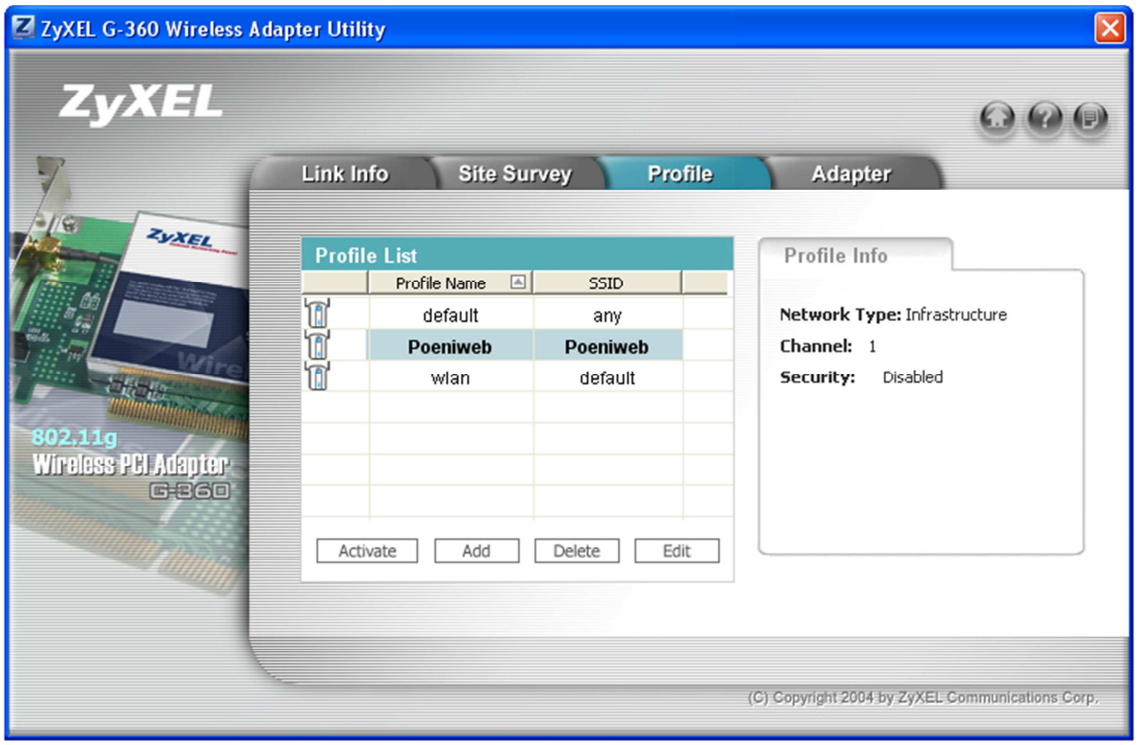
Kuva16. ZyXel Link Info.

Site Survey skannaa aktiivisesti verkkoa ja ilmoittaa löytyneet langattomat tukiasemat. Ainoa listassa näkyvä tukiasema on Poeniweb. Alueella on muitakin tukiasemia, mutta tässä kohdassa kuuluvuus on huono (kuva17).



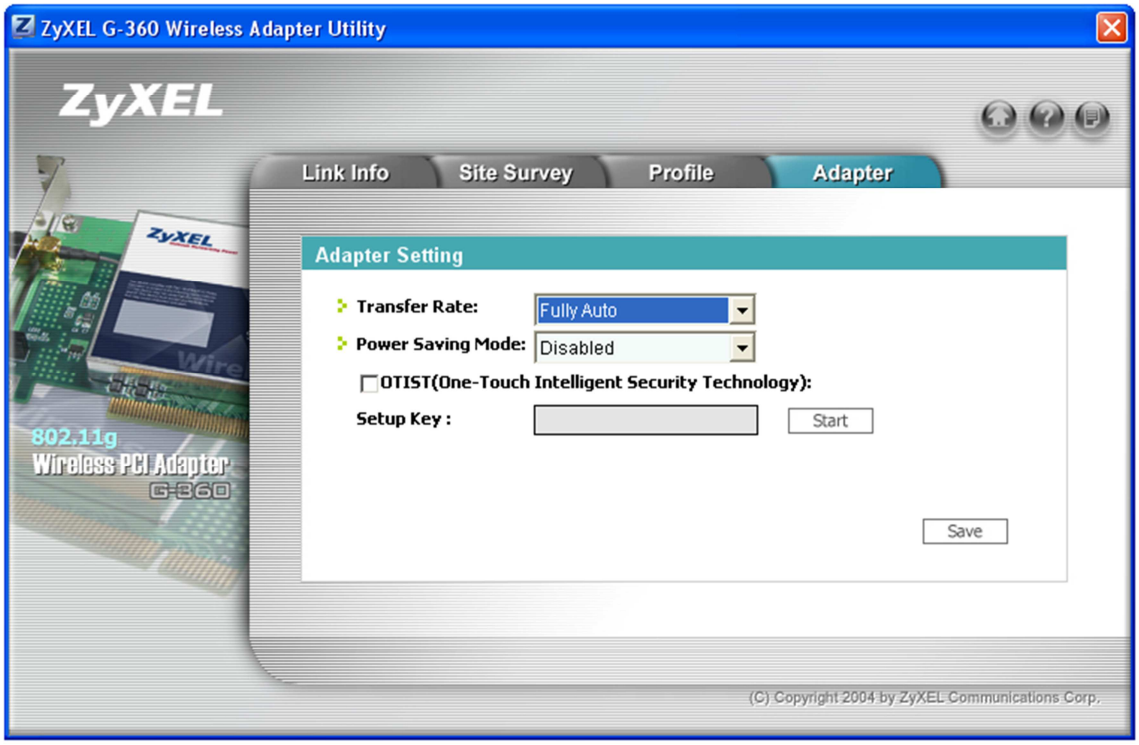
Kuva17. Zyxel Site Survey.

Profile-osioon luodaan langattoman verkon käyttäjäprofiili, jolla saadaan yhteys tukiasemaan. Ainoastaan SSID:n nimi tulee tietää (kuva18).



Kuva18. ZyXel Profile.

Adapter-osiosta pääsee muuttamaan lähetystaajuuksia sekä hyödyntämään OTIST-palvelua (One-Touch Intelligent Security Technology). OTIST on tarkoitettu ZyXelin laitteiden väliseksi salaustekniikaksi, eikä se toimi muiden valmistajien laitteiden kanssa. OTIST sallii tukiaseman SSID:n ja WEP- tai WPA-PSK -avaimen lähettämisen toisille langattoman verkon tilaajille, jotka ovat kuuluvuusalueen sisällä ja joilla on OTIST-tuki (kuva 19).

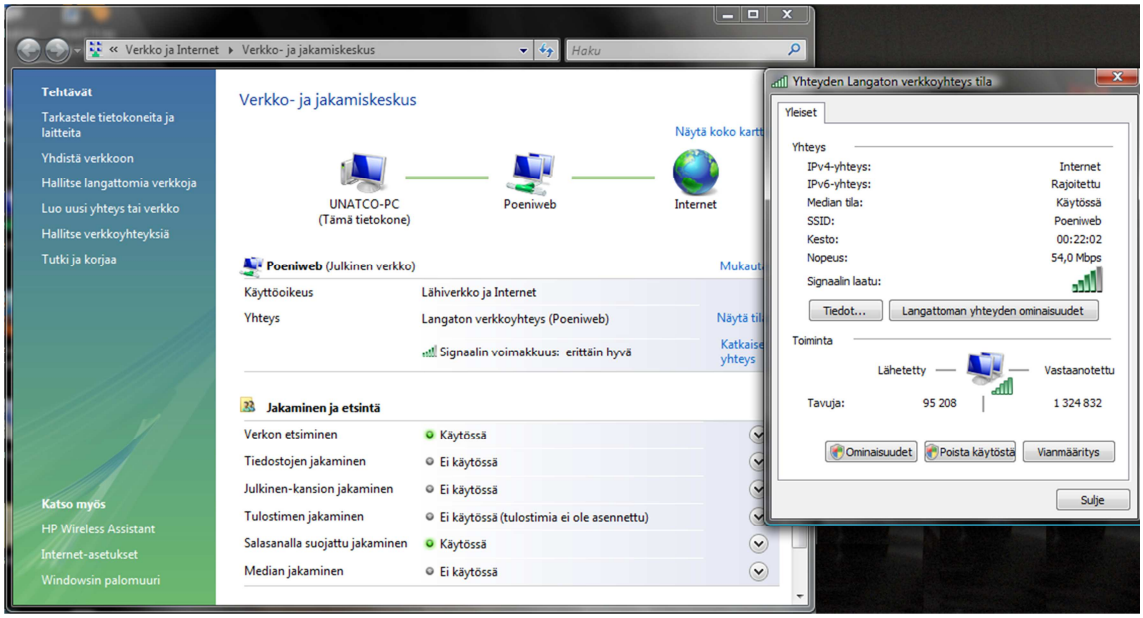


Kuva19. ZyXel Adapter.

4.4 Tilaaja3

Tilaaja3 on ensimmäinen liikkuva tilaaja verkossa, se on varustettu Windows Vistalla (kuva 20). Siinä on integroitu Atheros AR5007 WLAN-sovitin, sitä on helppo hallinnoida Windowsin omalla käyttöliittymällä (kuva 21).

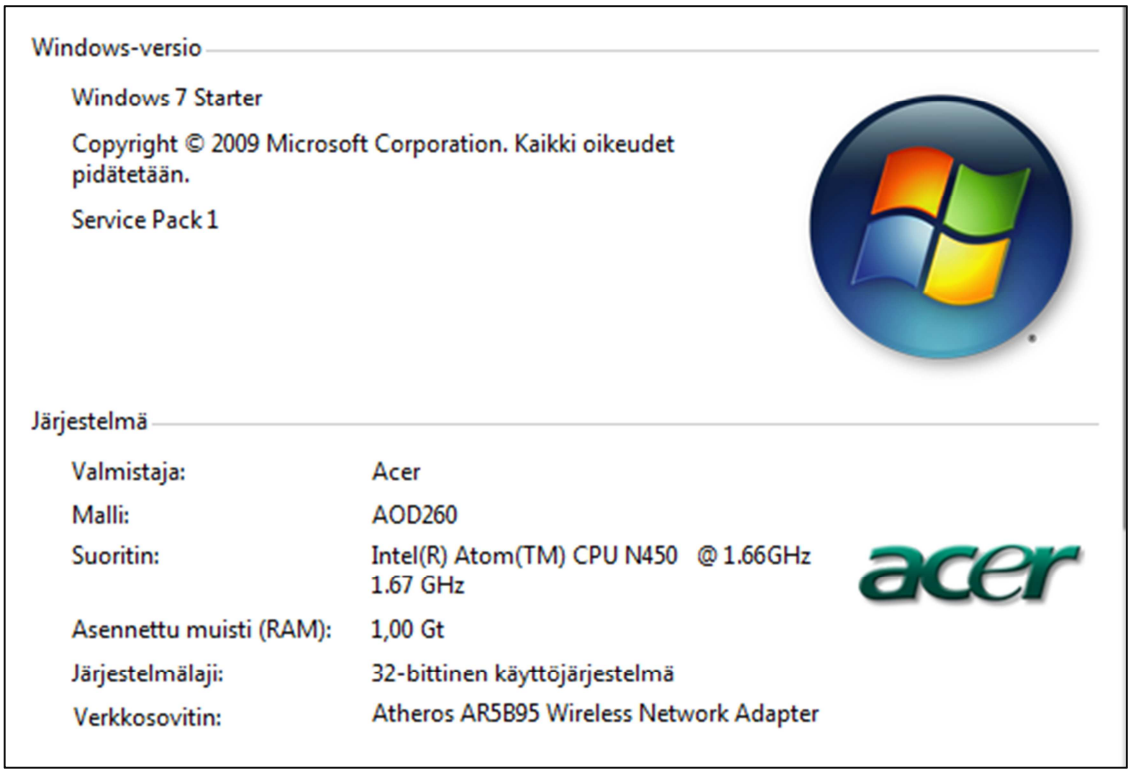
Kuva20. Tilaaja3:n tiedot.



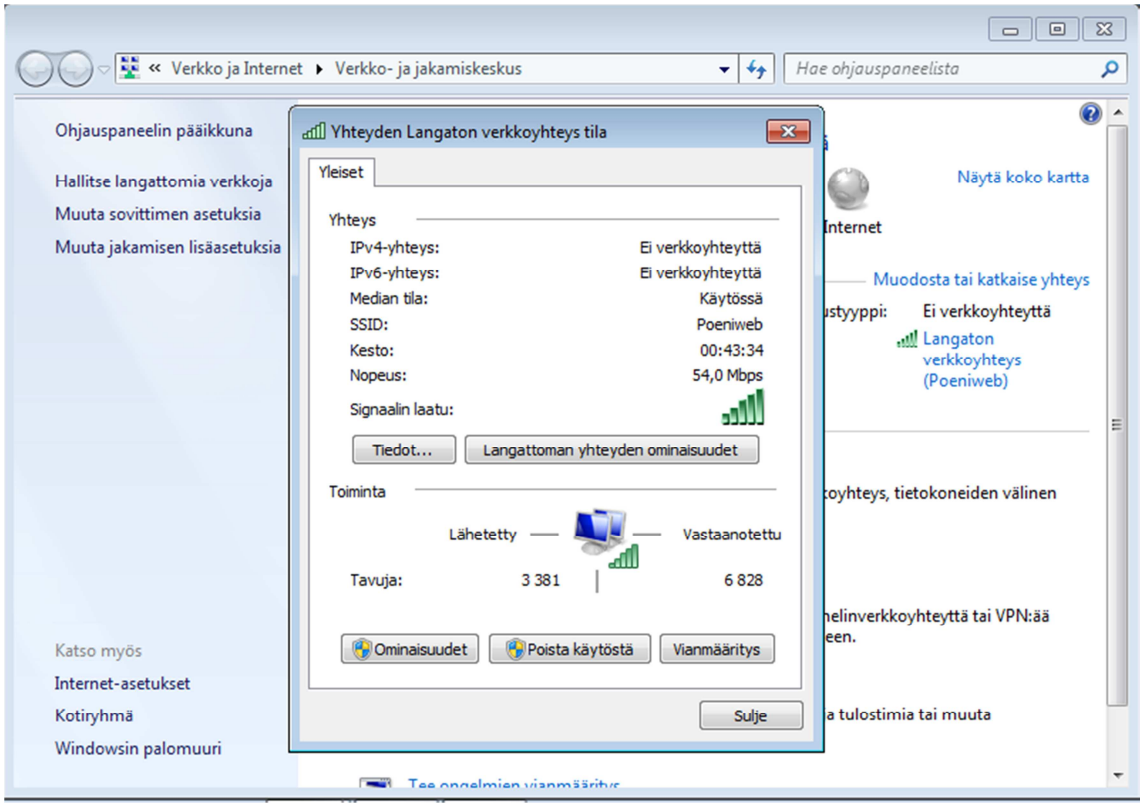
Kuva21. Tilaaja3:n langattoman verkon asetukset.

4.5 Tilaaja4

Tilaaja4 on verkon uusin tulokas, se on Acer Aspire D260 mini-laptop. Aivan kuten Tilaaja3:lla, siinä on myös Atherosin WLAN-sovitin, mutta se on hieman uudempaa mallia (kuva 22). Atheros on tässäkin integroitu, joten langattoman verkon liikennöintiä hallitaan Windowsin omalla ohjelmalla (kuva 23).



Kuva22. Tilaaja4:n tiedot.

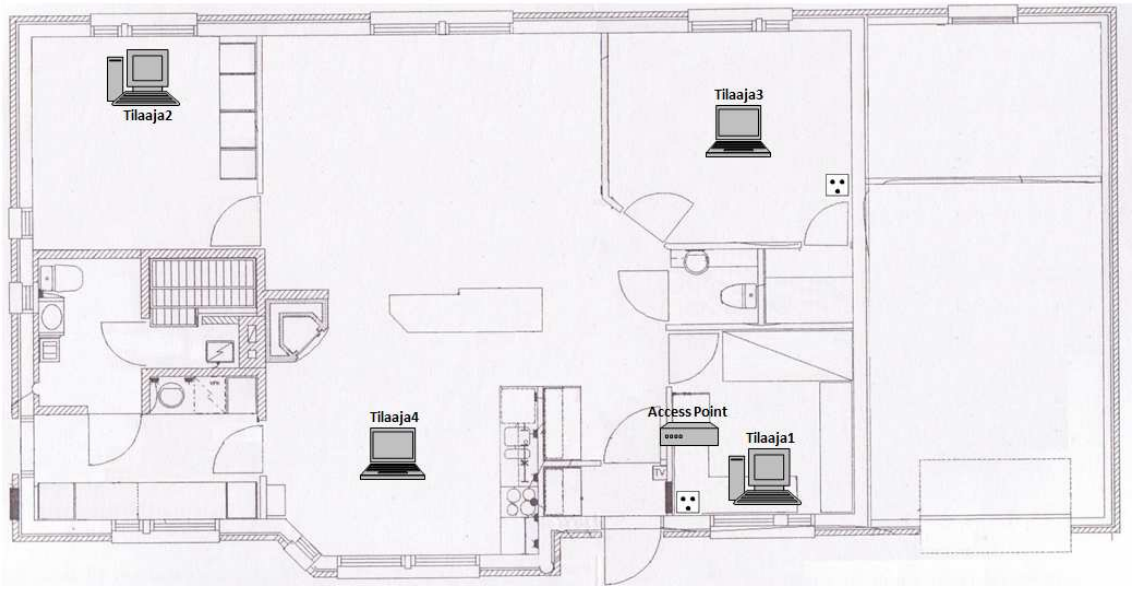


Kuva23. Tilaaja4-yhteyksien näkymä.

5 KOTIVERKON RAKENNE

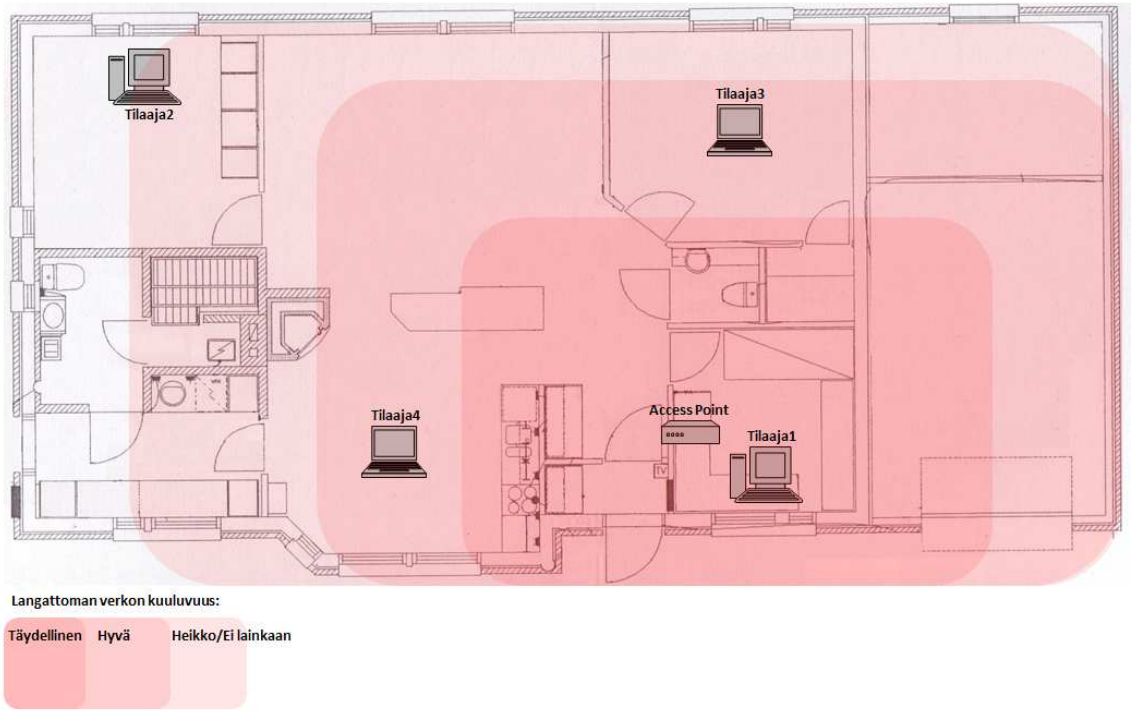
Käytössäni oleva langaton lähiverkko on nimeltään Poeniweb. Poeniweb koostuu neljästä käyttäjästä eli tilaajasta. Kaksi näistä tilaajista on kiinteitä pöytäkoneita ja toiset kaksi ovat liikkuvia tilaajia eli kannettavia tietokoneita. Puhelinpistokkeiden sijainnit talossa ovat rajoittaneet tukiaseman sijoittamista. Talosta löytyy vain kaksi puhelinpistoketta, ensimmäinen on Tilaaja1:n vieressä ja toinen löytyy läheltä Tilaaja3:a (kuva24).

Tukiasema sijoitettiin Tilaaja1:n viereen, koska se oli aikoinaan kiinni kaapelilla ja verkossa ei ollut muita tilaajia. Tukiaseman sijoittaminen Tilaaja1:n viereen on nykyäänkin viisain vaihtoehto, sillä antennin edessä on mahdollisimman vähän kuuluvuutta haittaavia esteitä. Sijoittamalla tukiasema toiseen puhelinpistokkeeseen voisi Tilaaja2:n kuuluvuus parantua jonkin verran. Tilaaja1:n yhteys kärsisi tästä huomattavasti, sillä langattoman lähiverkon signaali joutuisi kulkemaan läpi parin kaakeloidun seinän.



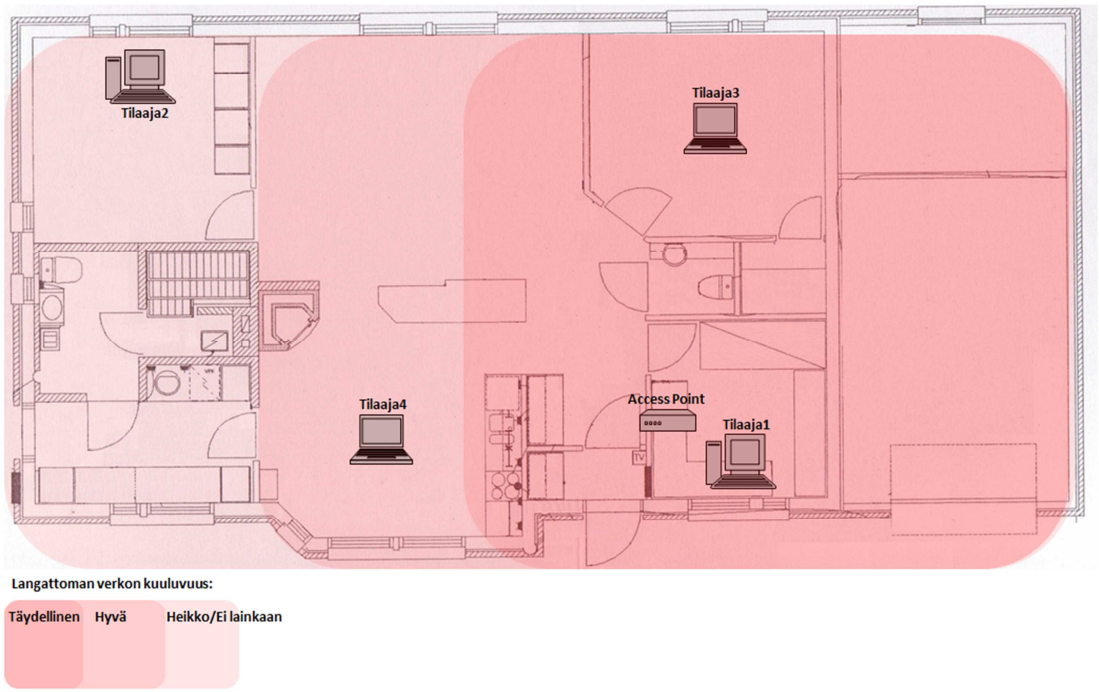
Kuva24. Laitteiden sijainti talossa.

Alusta alkaen oli ongelmia tukiaseman oman antennin kanssa. Langattoman lähiverkon signaali hädin tuskin kuului Tilaaja2:een asti. Tämä johti siihen että oli hankittava jostain vahvempi antenni. A-LINKillä itsellään oli tarjota vahva sisätiloihin tarkoitettu antenni. Kuvassa 25 on esitetty normaaliantennin kuuluvuusalue.



Kuva25. Normaaliantennin kuuluvuus.

Uuden antennin avulla saatiin nostettua langattoman lähiverkon kuuluvuutta ainakin siinä määrin, että se kuului Tilaaja2:een asti. Vahvemman antennin kanssa ongelmaksi syntyy lähiverkon liika kuuluminen. Suoritin mittauksia toisen liikkuvantilaajan kanssa. Poeniweb ei kuulu talon takapihalle, mutta tukiaseman ollessa lähempänä talon etuseinää se kuuluu huomattavasti kauemmas aukealla etupihalla. Olen havainnut langattomien lähiverkkojen listauksessa muita lähiverkkoja, jotka ovat kuuluneet heikosti minulle. Näiden täytyy olla naapuritalojen lähiverkkoja ja uskon oma verkkoni kuuluvan heikosti heidän etäisyyksilleen, varsinkin kun vielä salaan oman lähiverkkoni (kuva26).



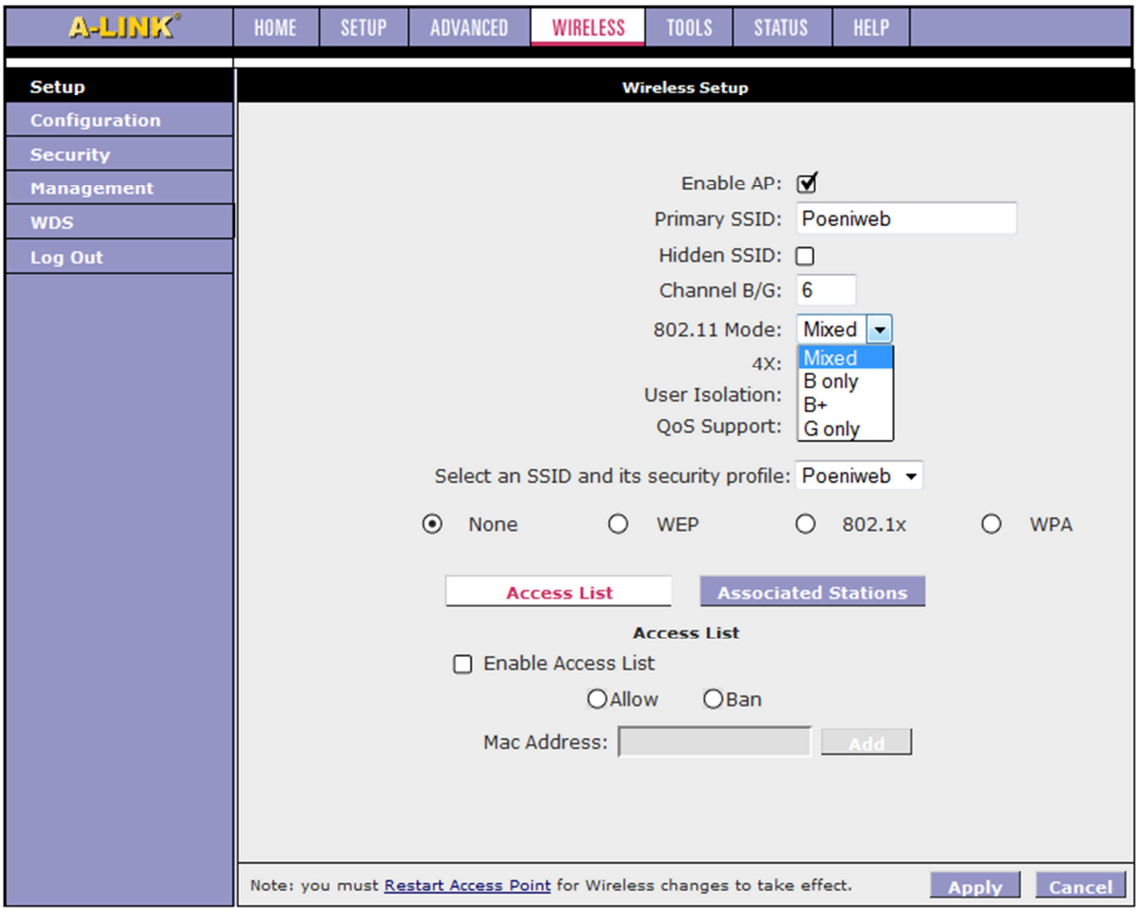
Kuva26. Kuuluvuus A-Link A6IN sisäantennilla.

6 KOTIVERKON SUOJAUS

Aiemmin työssä selvitin langattoman lähiverkon suojauksen mahdollisuudet, nyt on aika ottaa ne asteittain käyttöön. Aluksi varmistin, että verkko toimii ja kuuluu toivotusti. Aloitin ilman mitään suojauksia tai salauksia ja katsoin, että verkko kuuluu jopa Tilaaja2:lle. Lisäsin suojausmekanismeja sitä mukaa, kun verkon kuuluvuus ja toimivuus sen salli. Suurin haaste tuli olemaan sellaisen tarpeeksi turvallisen suojauksen löytyminen, joka takasi Tilaaja2:n yhteyden vakauden ja langattoman lähiverkon signaalin vahvuuden.

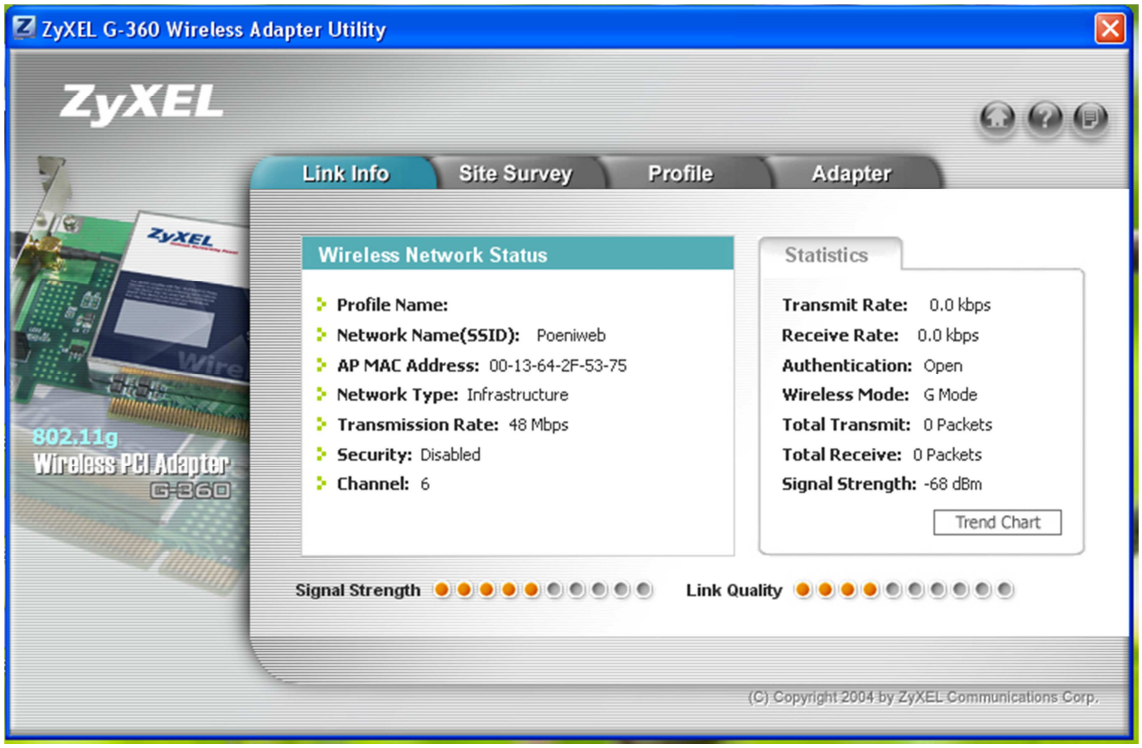
6.1 Ei suojausta

Tukiasemasta on kytketty pois salaukset, jätetty SSID näkyviin ja Access list otettu pois käytöstä. Verkko on tällä hetkellä täysin avoin, jolloin kuka tahansa sen kantamalla oleva pystyy liittymään siihen. Poistamalla SSID:n piilottamisen verkon nimi näkyy, jos skannaa langattomia lähiverkkoja alueella (kuva27).



Kuva 27. Tukiasema, verkko on täysin auki.

Tilaaja1:llä ei ole ongelmia langattoman lähiverkon kanssa, se löytyi heti ja sen signaali on 100 %. Tehokkaamman antennin avulla Tilaaja2:n langaton lähiverkko toimii vakaammin ja signaali ei ole liian heikko ylläpidettäväksi. Alkuperäisen antennin kanssa oli ongelmia kuuluvuuden suhteen, sillä signaalin kuuluvuus ei useinkaan ylittänyt40 prosenttia (kuva28).

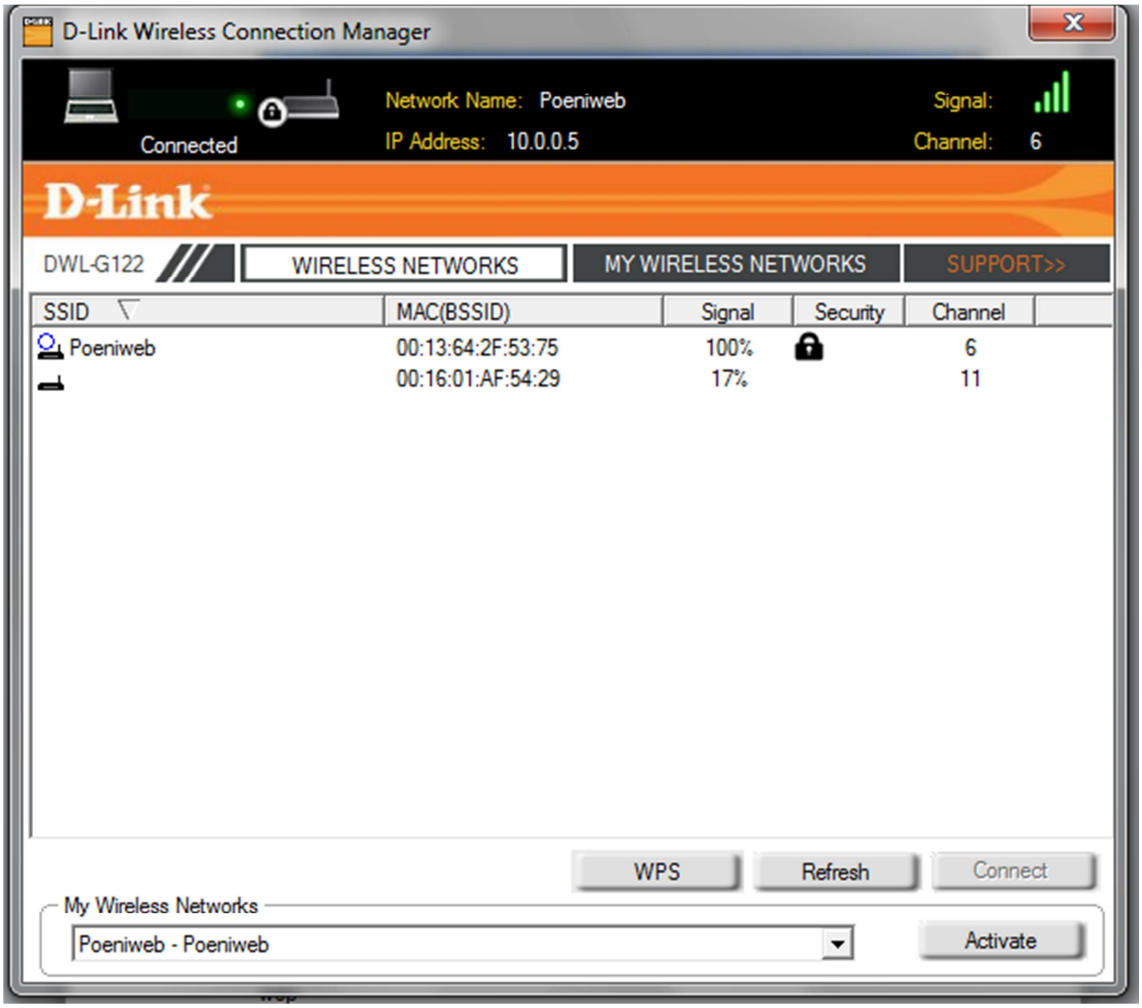


Kuva28. Tilaaja2:n yhteystoimii avoimena.

Tilaajalla3:lla ja Tilaajalla4:llä ei ollut ongelmia löytää verkkoa ja verkon kuuluvuus oli paikasta riippuen erinomainen.

6.2 SSID:n piilotus

Piilottamalla lähiverkon SSIDlähiverkonnimi ei näy alueen langattomien lähiverkkojen listauksessa. Listaus kuitenkin ilmoittaa nimettömästä lähiverkosta ja sen, että lähiverkko on suojaamaton. Hidden SSID:n pystyy murtamaan, mutta ei tavallisen käyttäjän taidoilla. Hidden SSID:n saa kuitenkin suhteellisen helposti selville, jos käytössä on oikeat työkalut (kuva29).



Kuva29. Poeniwebin rinnalla näkyy piilotettu, mutta salaamaton lähiverkko.

Lähiverkon tilaajilla ei ole ongelmaa verkon löytymisen tai toimivuuden kanssa. Ainoa ero suojaamattomaan lähiverkkoon on se, että kirjautuessa verkkoon käyttäjän tulee tietää verkon nimi.

6.3 Salaus

Hidden SSID:n kanssa saatiin kätkettyä langaton lähiverkko, mutta verkossa olevaa tietoliikennettä ei ole vielä salattu mitenkään. A-Link RoadRunner 24AP sisältää WEP-, WPA-ja WPA2-salausmenetelmät. Turvallisin salausmenetelmä olisi uusin WPA2, mutta kaikkien tilaajien laitteisto ei tue WPA2.

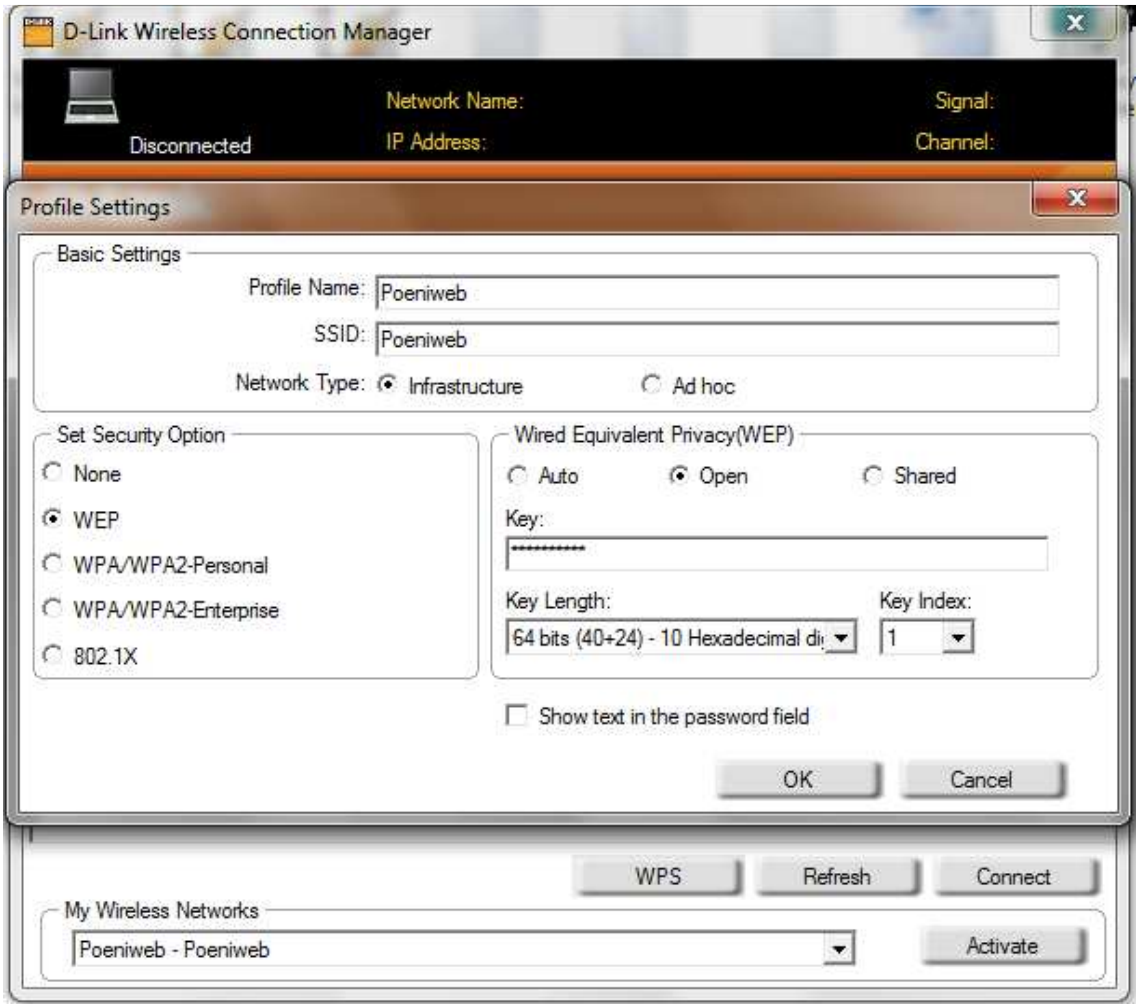
Aikaisempien kokeilujen perusteella salatusta liikenteestä saattaa tulla liian raskasta ja katkeilevaa, jotta sitä voisi käyttää tehokkaasti verkkoliikennöintiin. Nyt onkin tarkoitus koeponnistaa molemmat salausmenetelmät ja päätellä, kumpi niistä paremmin soveltuu Poeniwebin suojaukseen.

6.3.1 WEP

Tukiaseman langattoman lähiverkon turvallisuus-osiosta kytketään WEP-salaus päälle. Autentikointityypiksi on mahdollista laittaa joko Open, Shared tai Both. Valitsin Bothin, eli molemmat tyypit, koska tässä vaiheessa en halunnut tarttua hienosäätöihin. Seuraavaksi syötin salausavaimen, jolla suojataan langaton lähiverkko. Salausavaimen pituudeksi voi valita joko 64-, 125- tai 256-bittiä. Valitsin 64-bittisen salausavaimen, koska se on lyhin ja helpoin käyttää koestamisvaiheessa. Avaimen tulee olla hexadesimaali-yhteensopiva, joten valitsin helposti muistettavan 11 22 33 44 55. Lopullisessa WEP-suojauksessa kannattaa käyttää 256-bittistä salausavainta, sillä se on pisin ja vaikein murtaa. Internetissä on hyviä WEP-avaingeneraattoreita, jotka arpovat paljon turvallisempia avaimia verrattuna 11 22 33:een tai AA BB CC:hen (kuva 30).

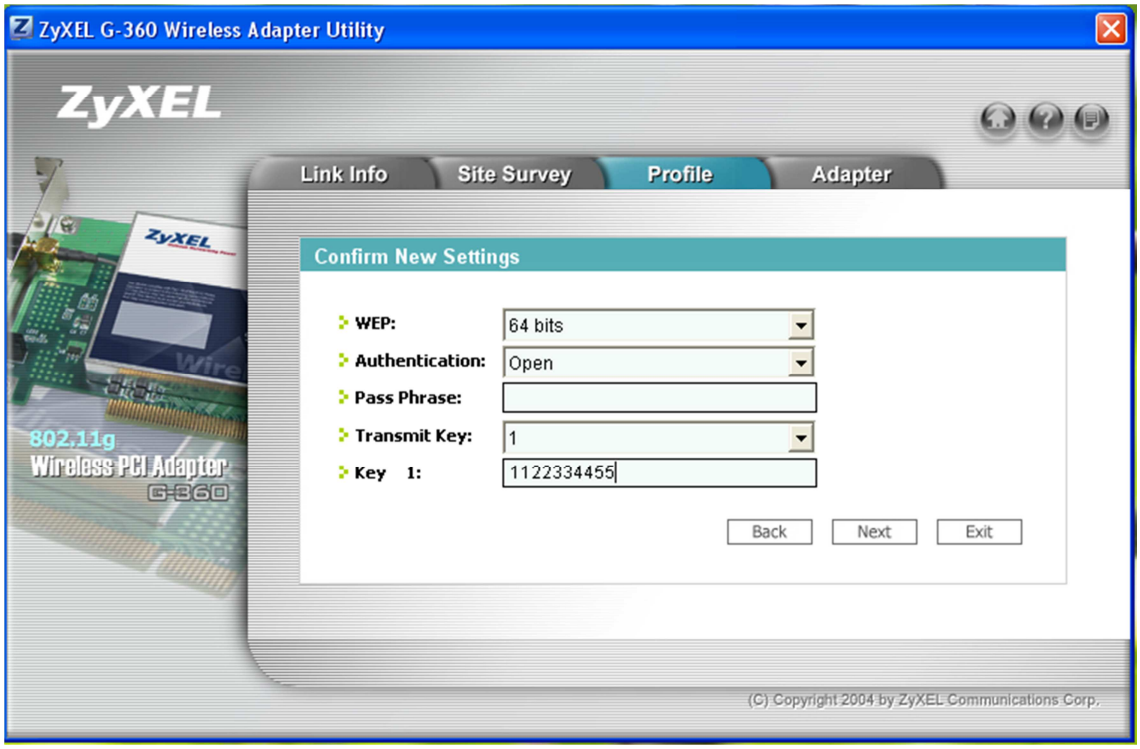
Kuva30. WEP-salaus.

Tilaaja1:n WEP-salauksen käyttöönotossa oli pieniä ongelmia. D-Link:n hallinnointiohjelmassa piti salausavain syöttää yhteen, kun taas tukiasemassa piti jokaisen parin väliin jättää välilyönti. Autentikointitavalla ei ollut väliä, koska asetin tukiaseman hyväksymään molempia tyyppejä. Tilaaja1:llä ei ollut muita ongelmia WEP-salauksen kanssa, yhteys löytyi ja se oli vakaa (kuva 31).



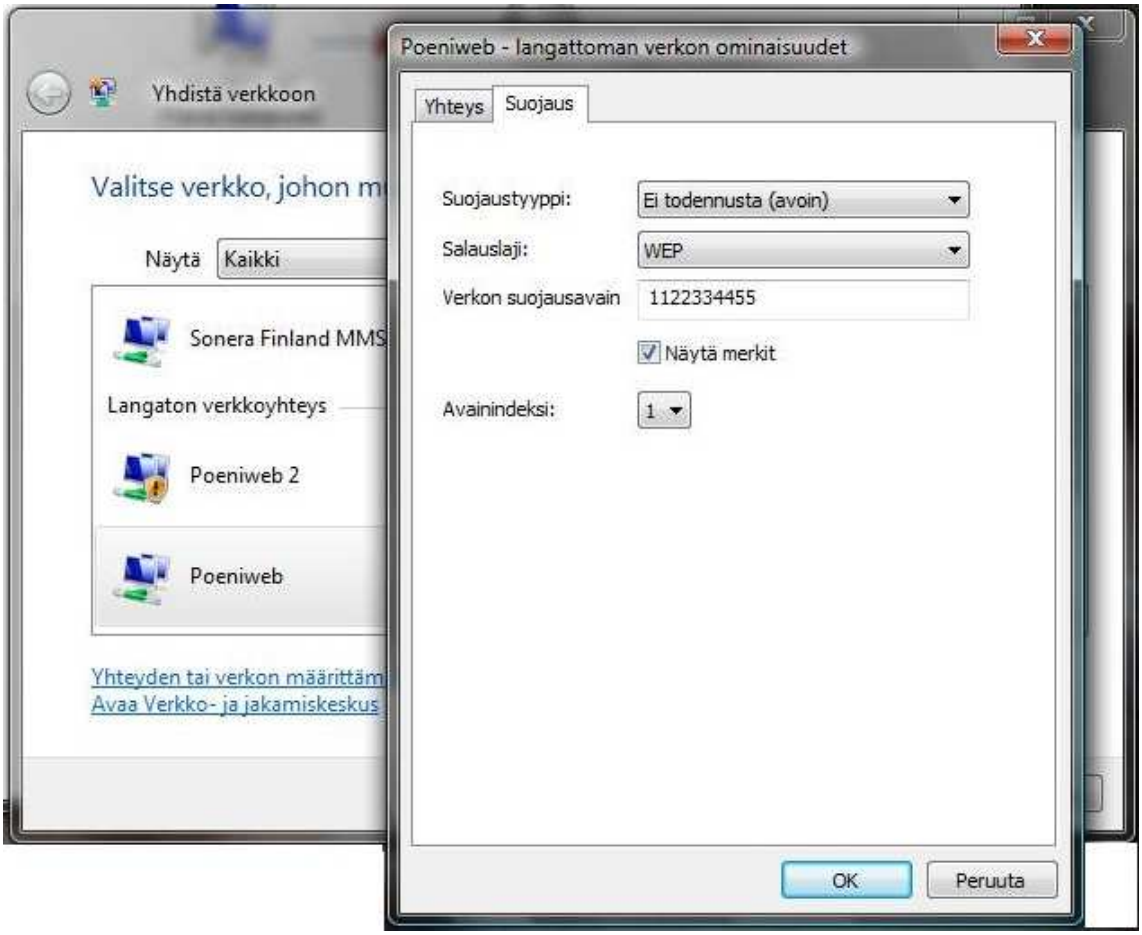
Kuva31. Tilaaja1:n WEP.

Tilaaja2:n WEP-salauksen asettaminen sujui normaalisti, salausavaimen syöttö toimi kuten Tilaaja1:llä. WEP-salattu lähiverkko kuului heikosti Tilaaja2:lle, mutta siihen saatiin yhteys. Suojattu yhteys toimi kuitenkin vakaasti, mutta hitaasti. Signaalin kuuluvuus heittelehti 25 %:n tuntumassa, joka oli tarpeeksi WEP-suojatun yhteyden ylläpitämiseksi. Yhteyden hitauden aiheutti yhteyden huono laatu, joka johtui Tilaaja2:n ja tukiaseman välisen liikenteen salauksesta (kuva 32).



Kuva32. Tilaaja2:n WEP.

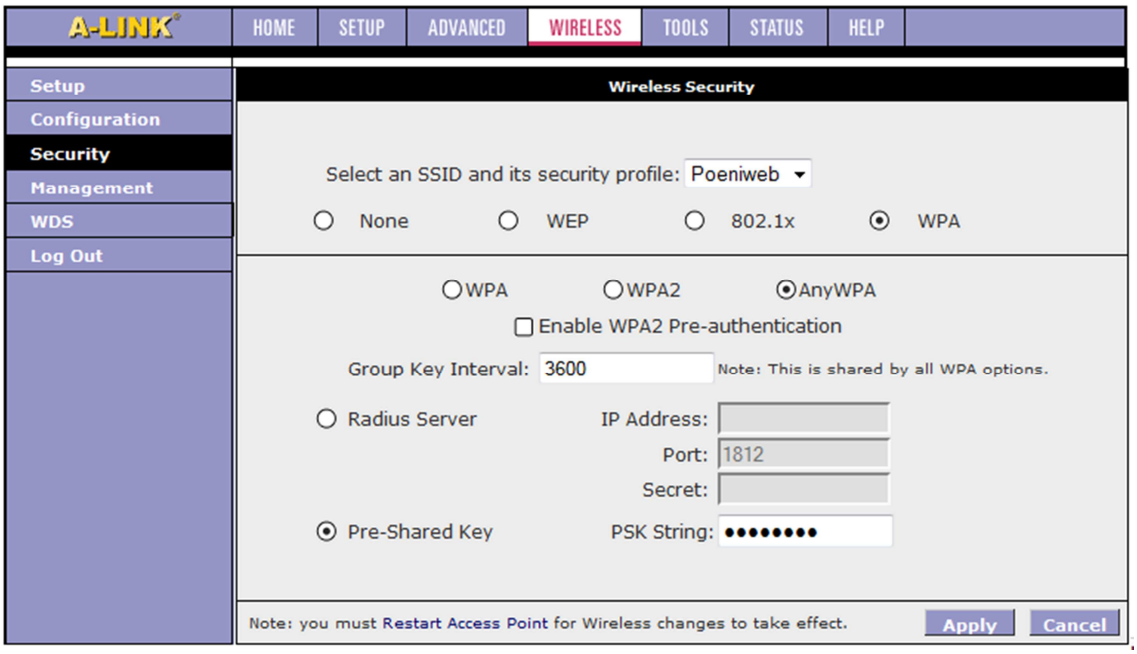
Tilaaja3:n ja Tilaaja4:n salausasetusten vaihtaminen oli helppoa Windowsin oman verkonhallinnan kautta. Autentikoinnin tai salausavaimen kanssa ei ollut ongelmia, yhteys oli taas vahva ja vakaa paikasta riippuen (kuva 33).



Kuva33. Tilaaja3:n ja Tilaaja4:n WEP.

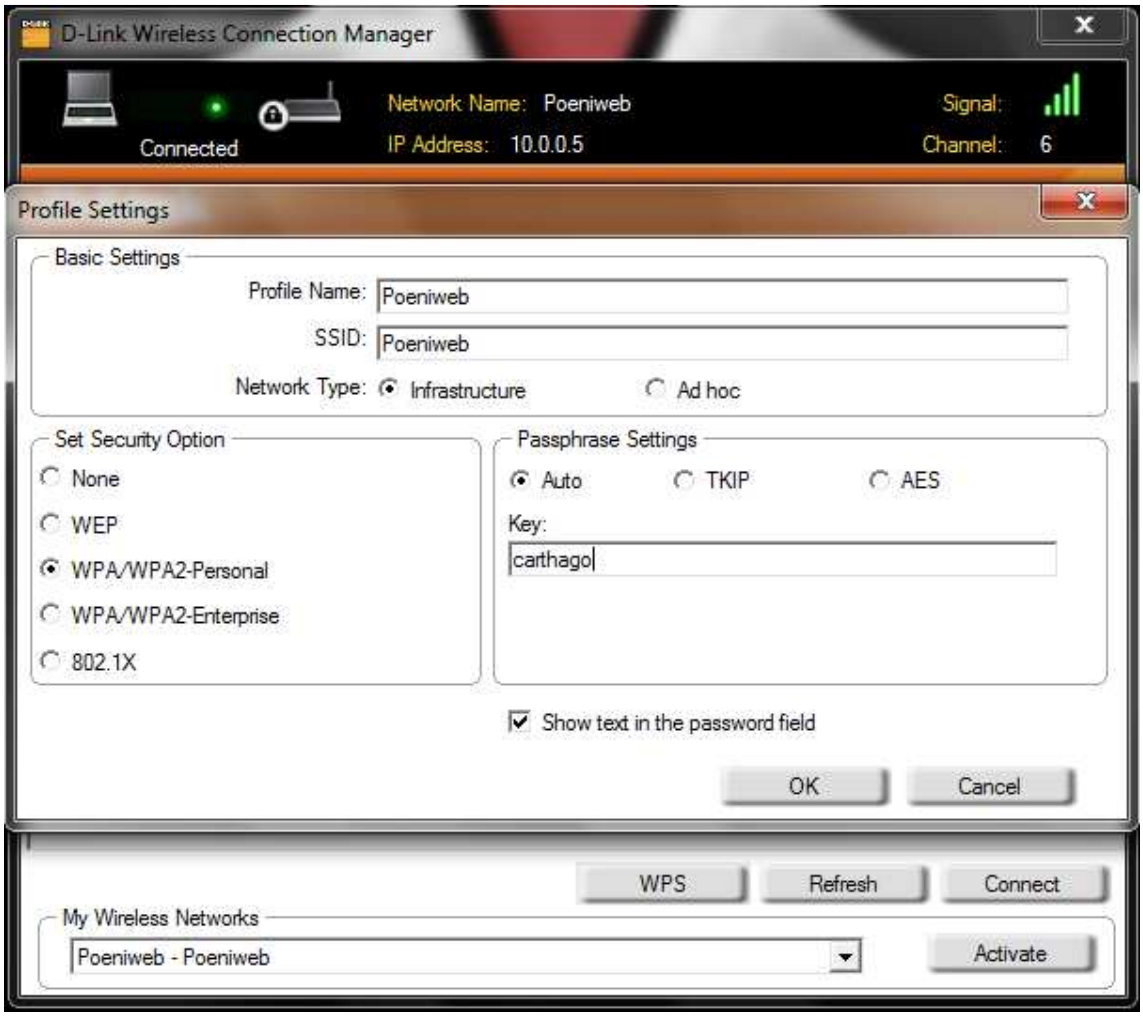
6.3.2 WPA

Tukiaseman turvallisuus-osiosta otettiin käyttöön WEPiin verrattuna uudempi ja turvallisempi WPA-salaus. Aluksi valitsin salauksen toimimaan WPA:lla ja WPA2:lla, mutta tämä aiheutti ongelmia ja kytkin käyttöön pelkän WPA-salauksen. WPA:ta on myös mahdollista käyttää Radius-palvelimen kautta, minulla on kuitenkin käytössä WPA-PSK. PSK on lyhenne sanoista Pre-Shared Key, eli etukäteen jaettu avain, joka on ”carthago” (kuva34).



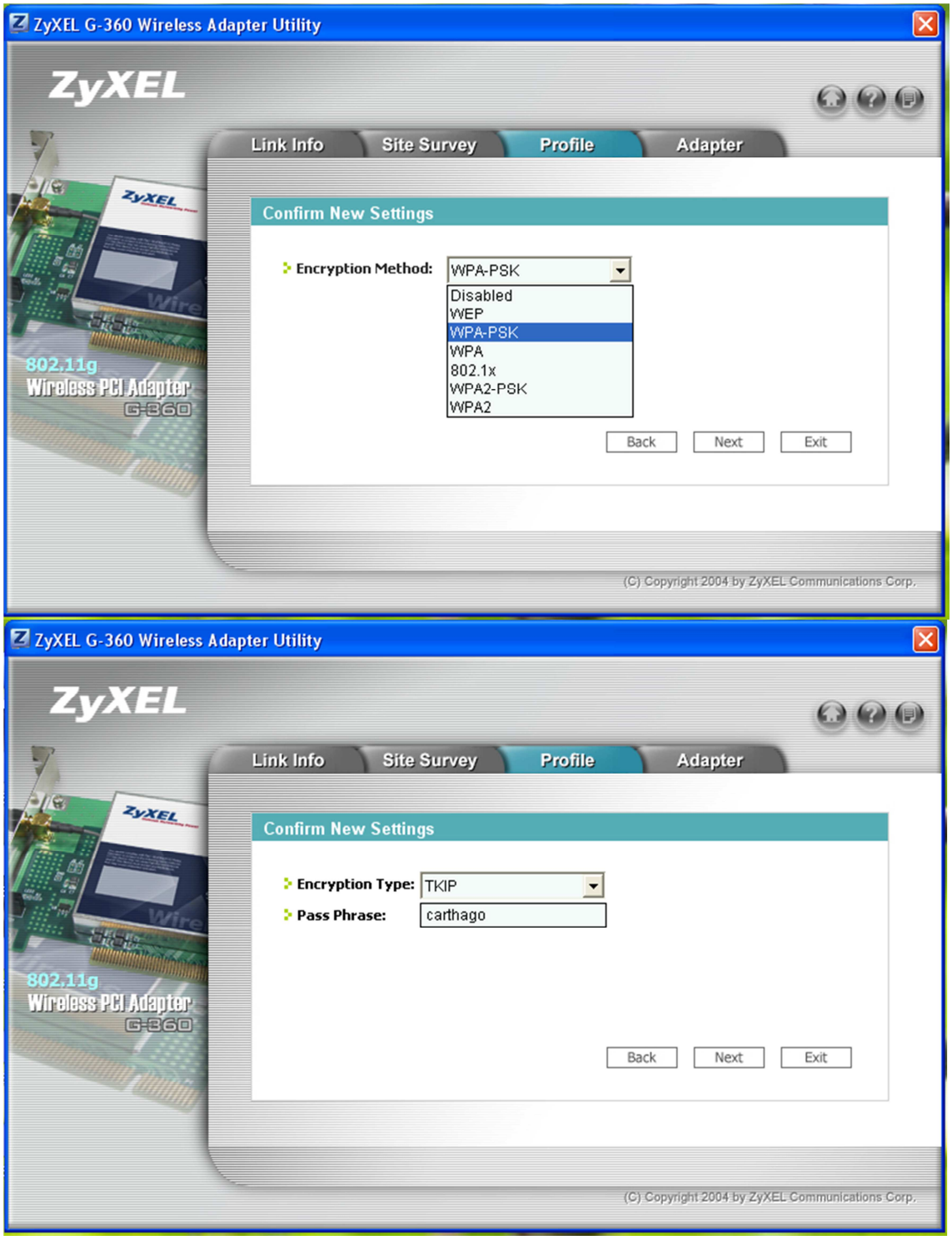
Kuva34. Tukiaseman WPA-asetukset.

Tilaaja1:n langattoman lähiverkon turvallisuusprofiilista otettiin käyttöön WPA/WPA2-Personal suojaus. Personal viittaa yksityisen henkilön ylläpitämään lähiverkkoon ja käyttää PSK-tunnusta, kun Enterprise on tarkoitettu isommille verkoille ja käyttää RADIUS-autentikointia. Tunnistuslauseeksi valittiin Auto tai TKIP ja syötetään tunnus ”carthago”. Tilaaja1 sai näillä muutoksilla yhteyden lähiverkkoon (kuva35).



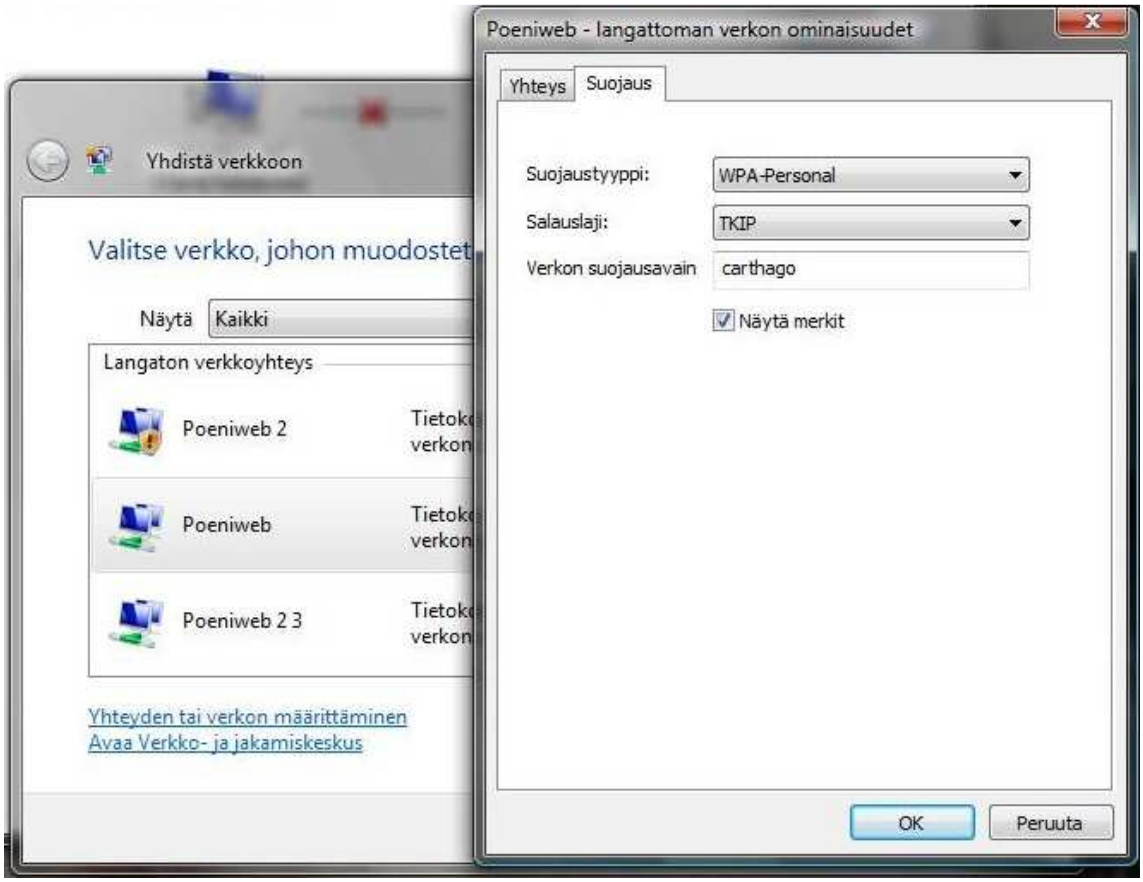
Kuva35. Tilaaja1 WPA.

Tilaaja2:n lähiverkkoprofiilista otettiin käyttöön WPA-PSK salausmetodi. Salaustyypiksi valittiin TKIP ja syötettiin tunnus ”carthago”. Yhteys ei muodostunut, mutta Poeniweb näkyi langattomien lähiverkkojen listauksessa. Tarkastaessani Poeniwebin profiilia havaitsinTilaaja2:n tulkinneen Poeniwebin WPA2-AES -salatuksi verkoksi. Muutin tukiaseman turvallisuus-osiosta Any WPA:n WPA:ksi ja Tilaaja2 tunnisti Poeniwebin WPA-PSK:ksi. Yhteydenotto ei kuitenkaan onnistunut, sillä salaus oli liian raskas ja Tilaaja2:lle ei saanut yhteyttä WPA-salauksen välityksellä (kuva36).



Kuva36. Tilaaja2 WPA.

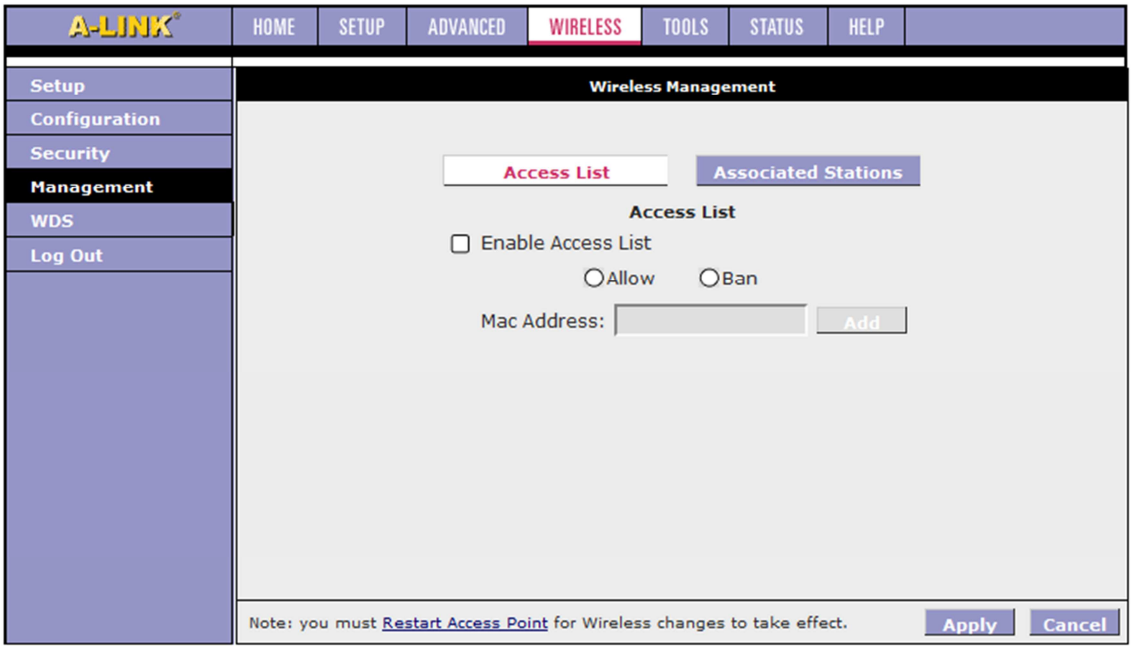
Tilaaja3:lla ja Tilaaja4:llä ei ollut ongelmia WPA-salauksen kanssa. Salaustyyppi oli sama WPA-Personal kuin muilla tilaajilla, TKIP-avaimena käytettiin sanaa ”carthago”. Lähiverkon signaali oli hieman heikompi kuin WEP-salauksella, mutta se ei vaikuttanut lähiverkon vakauteen tai nopeuteen (kuva 37).



Kuva37. Tilaaja3 ja Tilaaja4 WPA.

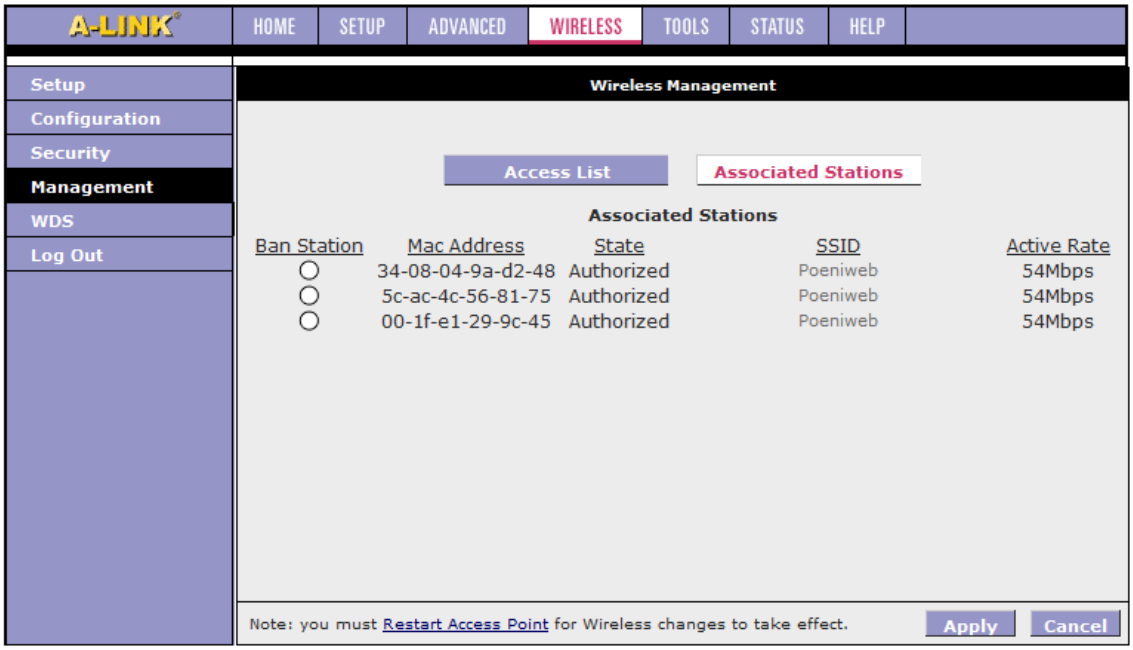
6.4 Access List

Tukiaseman hallinnointi osasta löytyy Access List eli pääsylista. Ottamalla Access Listin käyttöön langattomaan lähiverkkoon ei voi liittyä ilman, että tilaajan MAC-osoite on tällä listalla. Listalle voi lisätä osoitteet, jotka hyväksytään tai osoitteet, joilta halutaan estää pääsy lähiverkkoon. Listalla on kaikkien muiden tilaajien MAC-osoitteet paitsi Tilaaja2. Listaus oli käytössä, kun lähiverkko oli suojattu WPA-salauksella (kuva38).



Kuva38. Access Listille lisäys.

Access Lististä voi edelleen estää sillä näkyvien MAC-osoitteiden pääsyn lähiverkkoon. Tällä hetkellä kaikki kolme näkyvää osoitetta on sallittu lähiverkkoon. Listalla näkyy minkä verkkotunnuksen kautta nämä ovat lähiverkkoon liittyneet (kuva 39).



Kuva39. Lisätyt MAC-osoitteet Access Listissä.

7 TULOKSET JA JOHTOPÄÄTÖKSET

Vertailtaessa kahta salausmenetelmää WEP ja WPA WEP toimi moitteettomasti kaikilla tilaajilla, mutta se ei ole enää kovin turvallinen. WPA toimi kaikissa muissa tilaajissa paitsi Tilaaja2:ssa. Työn tavoitteen kannalta Shared WEP on ainoa mahdollinen keino saada aikaan toimiva ja turvallinen lähiverkko, mutta nykytilanteen mukaan Tilaaja2 on korvattavissa Tilaaja4:n kannettavalla tietokoneella.Tilaaja2 on jo pitkään oireillut johtuen erilaisista laite- ja ohjelmistovioista. Tilaaja4:llä ei ole niin sanottua aktiivista käyttäjää vaan se on enemmän reservikone, jos muille tapahtuu jotain yllättävää.

Ongelmia työssä aiheutti Tilaaja2:n Zyxelin WLAN-sovitin. Muiden tilaajien laitteet tai ohjelmistot eivät aiheuttaneet ongelmia. Erityisesti ongelmia oli WPA-salauksen kanssa. Tukiasema oli asetettu käyttämään molempia, sekä WPA että WPA2-avaimia. ZyXelin WLAN-sovitin ei tunnistanut asetusta, vaan yritti tarjota WPA-EAPia.WPA-EAP tarvitsee myös käyttäjätunnuksen, mutta sellaista ei ole luotu. Tukiasema laitettiin käyttämään pelkästään WPA:ta. Tilaaja2 löysi Poeniwebin, mutta signaali ei ollut tarpeeksi vahva yhteyden luomiseksi.

LÄHTEET

A6IN2011. A-LINK.Viitattu 14.11.2011

http://ftp.a-link.com/a6in/A6INFI.pdf

D-Link 2011.Viitattu 16.11.2011

http://www.dlink.com/products/?pid=334

Flyktman, R. 2010. Suuri PC-käsikirja – Windows 7. Helsinki: A Bonnier Group Company

Granlund, K. 2007. Tietoliikenne. Jyväskylä: Docendo Finland Oy.

Hakala, M; Vainio, M; Vuorinen O. 2006. Tietoturvallisuuden käsikirja.Porvoo: Docendo Finland Oy.

IEEE 802.112010. Wikipedia. Viitattu 14.11.2011

http://fi.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11i 2010. Wikipedia. Viitattu 16.11.2011

http://en.wikipedia.org/wiki/IEEE_802.11i-2004

RoadRunner 2011. A-LINK. Viitattu 14.11.2011

http://store.a-link.com/fi/RR24AP.html

WEP 2010. Wikipedia. Viitattu 15.11.2011

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

WLANWikipedia 2010a. Viitattu 14.11.2011

http://fi.wikipedia.org/wiki/WLAN

WPA2010. Wikipedia.Viitattu 15.11.2011

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Zyxel G-360 Viitattu 16.11.2011

ftp://ftp2.zyxel.com/G-360/user_guide/G-360_1.0.pdf