TAMPEREEN
AMMATTIKORKEAKOULU
LIIKETALOUS

TUTKINTOTYÖRAPORTTI

LANGATTOMAN LÄHIVERKON TOTEUTUS TAMPEREEN AMMATTIKORKEAKOULUSSA

Jyrki Pennanen

Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2005
Työn ohjaaja: Petri Heliniemi

TAMPERE 2005

Tekijä(t): Jyrki Pennanen

Koulutusohjelma(t): Tietojenkäsittelyn koulutusohjelma

Tutkintotyön nimi: Langattoman lähiverkon toteutus Tampereen ammattikorkeakoulussa

Title in English: The implementation of a wireless network in Tampere Polytechnic

Työn valmistumis-kuukausi ja -vuosi: Huhtikuu 2005

Työn ohjaaja: Petri Heliniemi **Sivumäärä:** 45

TIIVISTELMÄ

Langattomat lähiverkot eli WLANit ovat kasvattaneet suosiotaan viime vuosina, jos eivät aivan kiinteiden lähiverkkojen korvaajina, niin ainakin niiden jatkeena. Syinä tähän ovat olleet alentuneet laitekustannukset, tekniikan kehittyminen ja langattomuuden tuomat mahdollisudet. Suositus langattomissa lähiverkoissa käytettäväksi standardiksi on the Institute of Electrical and Electronics Engineersin (IEEE) kehittämä 802.11. Tätä alkuperäistä 1990-luvun alussa julkaistua standardia on paranneltu useaan otteeseen laajennuksilla, jotka ovat pyrkineet ratkaisemaan keskeisiä puutteita, kuten vaatimatonta nopeutta, yhteensopivuusongelmia, signaalin lyhyttä kantomatkaa ja tietoturvan aukkoja.

Tietoturvaongelmat langattomissa lähiverkoissa ovat puhuttaneet ihmisiä jo pitkään. Koska tieto liikkuu ilmassa kiinteän verkon kaapeleiden sijaan, sen kaappaaminen ja salakuuntelu on huomattavan helppoa. Tämän estämiseksi on kehitetty signaalin salauskeinoja, joilla langattomien laitteiden välinen liikenne saadaan muutettua selväkielisestä kryptatuksi datavirraksi. Vain oikeutettu vastaanottajalaite osaa purkaa salauksen jälleen ymmärrettävään muotoon. Tietoturvan kannalta tärkeää on myös estää ulkopuolisten pääsy langattomaan verkkoon. Tätä voidaan kontrolloida käyttäjien tunnistuksella eli autentikoinnilla. Jokin verkon laite ohjataan hyväksymään sisälle verkkoon vain ennalta määritetyt käyttäjät. Tämän tehtävän hoitaa yleensä siihen tarkoitukseen valittu palvelin.

Tämän tutkintotyön tavoitteena oli tutustua langattomiin lähiverkkoihin, niiden eri tekniikoihin ja laitteisiin, hyviin ja huonoihin puoliin sekä tietoturva-aspekteihin. Teorian pohjalta rakennettiin yhden tukiaseman ja päätelaitteen käsittävä langaton verkko Tampereen ammattikorkeakoulun tietoverkkopalvelujen suuntautumisvaihtoehdon oman WPK-lähiverkon yhteyteen. Rakennettuun verkkoon toteutettiin asiaan kuuluva tietoturva ottamalla käyttöön signaalin salaus ja autentikointi. Turvallisuusstandardina käytettiin tehokasta Wi-Fi Protected Access (WPA) -keinoa, johon sisältyi TKIP-salaus. Autentikointi toteutettiin ulkoisella WPK-verkon RADIUS-palvelimella.

Avainsanat: WLAN IEEE802.11 Autentikointi Tietoturva Langaton

Sisällysluettelo

1. Johdanto ... 4
1.1 Toimeksianto ... 4
1.2 Työn tavoitteet ... 4
1.3 Lähdeaineisto ... 4
1.4 Tampereen ammattikorkeakoulun tietoverkkopalvelujen suuntautumisvaihtoehto ... 5
2. IEEE802.11 -langattoman lähiverkkoteknologian perusteet ... 6
2.1 Määritelmät ... 6
2.2 Historia ... 6
2.3 Langaton vs. kiinteä verkko ... 6
2.4 Standardit ... 7
2.4.1 IEEE802.11a ... 7
2.4.2 IEEE802.11b ... 8
2.4.3 Muut IEEE802.11 laajennukset ... 8
2.5 Langattoman tiedonsiirron tekniikat ... 9
2.5.1 Infrapuna ... 9
2.5.2 Hajaspetritekniikka ... 9
2.6 Laitteet ... 10
2.7 Topologiat ... 11
3. Tietoturva ... 13
3.1 SSID & ESSID ... 13
3.2 Tietoturvastandardit ja salausmetodit ... 13
3.2.1 WEP ... 13
3.2.2 WPA & WPA2 ... 14
3.2.3 TKIP ... 14
3.2.4 AES ... 15
3.3 Autentikointi ... 15
3.3.1 MAC-osoite ... 15
3.3.2 IEEE802.1x & EAP ... 16
3.3.3 RADIUS ... 18
3.3.4 Kerberos ... 19
3.4 VPN ... 19
4. WLAN:in integrointi WPK-verkkoon ... 21
4.1 Lähtötilanne ... 21
4.2 WLAN:in implementointi ... 21
4.2.1 Laite- ja ohjelmistoresurssit ... 21
4.2.2 Laiteasennukset ... 22
4.2.3 Laitekonfiguroinnit ... 22
4.2.4 Toimivuuden testaus ... 40
5. Yhteenveto ... 42
Lähteet ... 43
Liitteet ... 44

1. Johdanto

Lähiverkot (Local Area Network, LAN) ovat yleistyneet viime vuosina erityisesti yritysmaailmassa. Niiden tarkoitus on helpottaa tiedostojen ja resurssien, kuten tulostuspalvelujen jakamista yhdistämällä tietokoneet ja laitteet yhteiseen linkkiin. Kannettavien tietokoneiden yleistyminen sekä kiinteän kaapeloinnin heikko skaalattavuus ja korkeat asennuskulut ovat tehneet langattomasta lähiverkkoteknologiasta (Wireless LAN, WLAN) houkuttelevan vaihtoehdon kiinteälle verkolle. Kun vielä langattoman verkon alkutaipaleen haittapuolet, kuten kalliit hankintakulut, vaatimaton kaistanleveys ja tietoturvaongelmat on saatu ratkaistua, on siitä tullut vakavasti otettava kilpailija perinteiselle kaapeloidulle verkolle.

1.1 Toimeksianto

Aloitettuani opintoihin kuuluvan työharjoittelun Tampereen ammattikorkeakoulun hallinnon harjoittelijana syksyllä 2004, antoi tietojenkäsittelyn koulutusohjelman tietoverkkopalvelujen suuntautumisvaihtoehdon vastaava lehtori Harri Hakonen minulle tehtäväksi rakentaa tietoverkkopalvelujen oman WPK-lähiverkon yhteyteen langattoman lähiverkon ja toteuttaa siihen käyttäjien tunnistaminen eli autentikointi osana tietoturvaa. Tehtävää varten minulle annettiin kaksi koulun omistamaa langattoman verkon tukiasemaa ja kaksi langatonta verkkokorttia. Tästä tuli tutkintotyöni aihe; tutustua langattomiin verkkoihin ja niiden tietoturvaominaisuuksiin sekä lopulta toteuttaa verkko käytännössä ja kuvata se.

1.2 Työn tavoitteet

Tutkintotyön tavoitteena on tutustua uuteen asiaan ja laajentaa tietämystä tietoliikenteestä tämän suhteellisen uuden osa-alueen osalta. Selvitän, mitä langattoman verkon rakentamiseen tarvitaan, miten siitä tehdään tietoturvallinen ja miksi se kasvattaa suosiotaan jatkuvasti. Lopuksi tavoitteena on suunnitella langaton verkko käyttäjien tunnistuksella tietoverkkopalvelujen WPK-verkon yhteyteen ja kuvata sen toteutus.

1.3 Lähdeaineisto

Päälähteet työssäni ovat englanninkielisiä teoksia niiden uutuuden vuoksi. Työn teoriaosa jakautuu kahteen pääosaan, WLAN-teknologian yleisesittelyyn ja siihen liittyviin tietoturva-asioihin. Ensimmäisen osan sisältö on koostettu suurimmaksi osaksi Axel Sikoran ja Nathan J. Mullerin teosten perusteella. Varsinkin Sikoran kirja on hyvin tekniikkapainotteinen ja soveltuu siksi hyvinkin syvälliseen langattomien verkkojen tutkimiseen. Mullerin teos sisältää muutaman asiavirheen, jotka koskevat lukuja ja arvoja.

Tietoturvaosuuden päälähde on Lee Barkenin teos, joka käsittelee hyvin laajasti ja käytännönläheisesti erilaisia metodeja langattomien verkkojen tiedonkulun suojaamiseksi ulkopuolisilta. Barkenin teos on uusinta painettua sanaa aiheestaan, jota on tehty, mutta koska ala kehittyy nopeasti, löytyy sieltäkin puutteita esimerkiksi aivan uusimmista standardeista. Tämän vuoksi Internetistä kannattaa usein hakea tuoreimmat ja päivitetyimmät lähteet.

Lisäksi tietoa löytyy laitteiden manuaaleista, joissa on paljon ohjeita tietoturvan parantamiseksi. WLAN-verkkoja on käsitelty paljon myös IT-alan lehdissä ja niistä saan paljon taustatietoa työhöni.

1.4 Tampereen ammattikorkeakoulun tietoverkkopalvelujen suuntautumisvaihtoehto

Tampereen ammattikorkeakoulun (TAMK) tietojenkäsittelyn koulutusohjelman tietoverkkopalvelujen suuntautumisvaihtoehto on yksi opiskelijoiden neljästä vaihtoehdosta valita erikoistumisensa. Muut ovat tietotekniikkayrittäjyys, hypermedia ja ohjelmistotuotanto. Tietoverkkopalvelut sisältää opintojaksoja muun muassa Cisco Systems:ltä (CCNA, CCNP) ja Microsoftilta (verkkopalvelut ja niiden hallinta), jotka käsittelevät pääasiassa tietoliikennettä ja verkkopalveluja.

Tätä kirjoitettaessa tietoverkkopalveluilla on käytössään Teiskontien toimipisteen Infotalon neljännessä kerroksessa sijaitseva kolme luokkahuonetta ja yhden palvelinhuoneen kattava WPK-verkoksi nimetty lähiverkko. Se on erillään TAMK:n muusta verkosta ja on ainoastaan tietoverkkopalveluiden opiskelijoiden käytössä. Verkko käsittää useita kymmeniä työasemia ja muutaman palvelimen, joita sen hetkinen työharjoittelija ylläpitää. Huoneiden työasemat on yhdistetty kytkimiin, jotka edelleen on yhdistetty pääkytkimeen, josta on yhteys reitittimen kautta ulkomaailmaan. Kyseessä on siis kiinteä kaapeloitu Ethernet-verkko.

2. IEEE802.11 -langattoman lähiverkkoteknologian perusteet

2.1 Määritelmät

Langattomat lähiverkot (Wireless Local Area Network, WLAN) ovat standardisoituja verkkoteknologioita, jotka implementoivat lähiverkkojen toimivuutta käyttämällä langatonta tiedonsiirtoa. (Sikora 2003: 1) IEEE 802.11 viittaa standardisointiorganisaation Institute of Electrical and Electronics Engineers (IEEE) kehittämään standardiperheeseen, joka määrittelee rajapinnan ja protokollan langattomalle tiedonsiirrolle. 802.11 määrittelee tiedonkululle kolme erilaista siirtotietä: taajuushyppely- ja suorasekvenssi-hajaspektritekniikat (FHSS / DSSS) sekä infrapunan (IR).

2.2 Historia

IEEE aloitti alkuperäisen 802.11-standardin kehitystyön vuonna 1990 ja seitsemän vuoden päästä se ratifioitiin. Tämän historia jäi kuitenkin lyhyeksi siinä havaittujen puutteiden vuoksi. Suurimmaksi ongelmaksi muodostui sen tiedonsiirtonopeuden jääminen yhteen ja kahteen megabittiin sekunnissa. Vuonna 1999 IEEE julkaisi 802.11-standardiin kaksi laajennusta, jotka nimettiin 802.11a ja 802.11b. Näistä jälkimmäinen yleistyi merkittävämmin, vaikka edellinen saavuttaakin teoriassa paremman tiedonsiirtonopeuden. 802.11a-standardin heikkoutena on erittäin lyhyt kantoalue ja kalliiksi muodostunut hinta. Uusimpana tuotoksena IEEE on julkaissut 802.11g-standardin, jossa on yhdistettynä a ja b laajennusten parhaimmat ominaisuudet.

2.3 Langaton vs. kiinteä verkko

Sikora (2003: 2) nostaa langattoman verkon merkittävimmäksi hyödyksi kaapeleiden puuttumisen ja siitä koituvat edut verrattuna perinteiseen kiinteään verkkoon. Mikäli kiinteä verkko on jo olemassa, päätelaitteiden vapaampi liikuteltavuus, mahdollisesti tilaa vievien kaapeleiden vähentyminen ja yhteensopimattomien liittimien ongelman poistuminen ovat seurausta siirtymisestä langattomaan verkkoon. Jos taas tarkoitus on verkottaa kokonaan uusi tila, tulee huomattavasti kalliimmaksi ja työläämmäksi asentaa kiinteä kaapelointi, kuin pystyttää langaton verkko.

Wi-Fi Alliance (Is a wired… 2004) mainitsee vertailussaan langattoman verkon eduksi myös sen skaalattavuuden ja laajennettavuuden helppouden - esimerkkinä pk-yrityksen kasvun tarve tai muutto toisiin toimitiloihin. Kasvua varten on helppo lisätä tukiasemia ja sitä kautta pidentää signaalin kantomatkaa ja muutossa taas kaikki langattoman verkon komponentit on helposti otettavissa mukaan uuteen tilaan, eikä kalliita verkkoinvestointeja tarvitse jättää

jälkeensä kuten kiinteän verkon tapauksessa.

Edelleen Sikora (2003: 2-3) nostaa esiin myös monet rajoitukset ja muut haittapuolet, joita langaton verkko asettaa verrattuna kiinteään verkkoon. Vaikka langattomien tietoliikennelaitteiden hintakehitys on jatkuvassa laskusuunnassa, jäävät ne silti kalliimmaksi vaihtoehdoksi, jos mittariksi otetaan kaistanleveys suhteessa hintaan. Nopeudeltaan langaton verkko, verrattuna vastaavaan kiinteään verkkoon, tulee Sikoran mukaan noin kymmenen kertaa kalliimmaksi laitteiden osalta. Kun mukaan lasketaan asennuskustannukset, muuttuu tilanne aivan toiseksi; jopa langattoman verkon eduksi.

Muita rajoituksia ovat kaistanleveyden pienempi määrä ja signaalin kantama. Näistä enemmän seuraavassa alaluvussa, jossa esitellään IEEE802.11-standardi ja sen laajennukset. Haittapuolina mainitaan myös langattomien tietoliikennelaitteiden tuottama elektromagneettinen säteily, joka kuitenkin on vain 5 % matkapuhelinten tuottamasta määrästä. Sikora (2003: 3) mainitsee haittapuoliksi myös langattomien laitteiden suuremman herkkyyden signaalin häiriöille ja tietoturvaongelmat. Häiriöistä enemmän langattoman tiedonsiirron tekniikat –luvussa. Tietoturva-asiat esitellään tämän työn kolmannessa luvussa.

2.4 Standardit

802.11 on IEEE:n työryhmän kehittämä spesifikaatioiden perhe langattomille lähiverkoille. Tätä kirjoitettaessa tähän perheeseen kuuluu neljä standardia ja lisäksi kaksi uutta on valmisteilla ja ne on tarkoitus julkaista lähiaikoina. Alkuperäinen IEEE802.11-standardi todettiin nopeasti julkistamisensa jälkeen puutteelliseksi ominaisuuksiltaan ja sitä onkin jatkettu kolmella eri laajennuksella, joille ominaisia piirteitä ovat muun muassa signaalin pidempi kantomatka, parantunut nopeus sekä tietoturva. Vuonna 1999 ratifioitiin kaksi 802.11 standardin laajennusta, joiden päätarkoituksena oli tarjota lisää kaistanleveyttä; syntyivät IEEE802.11a ja IEEE802.11b.

2.4.1 IEEE802.11a

Päivityksenä alkuperäiseen standardiin IEEE802.11a ei muuta MAC-kerroksen kanavallepääsymekanismeja, vaan muutokset kohdistuvat fyysiseen kerrokseen. Alkuperäisen standardin käyttämän 2.4 GHz taajuusalueen sijaan IEEE802.11a käyttää 5 GHz taajuusaluetta ja taajuushyppelytekniikan sijaan Orthogonal Frequency Division Multiplex (OFDM) -kanavanjakotekniikkaa. (Sikora 2003: 88) Tästä johtuen kaistanleveys on jopa 54 Mbps verrattuna alkuperäisen standardin yhteen ja kahteen megabittiin sekunnissa. Tämän mahdollistaa suurempi kanavamäärä ja vähemmän ruuhkainen taajuusalue.

IEEE802.11a -standardin haittapuolina ovat yhteensopivuusongelmat ja signaalin kantomatka. Se ei ole alaspäin yhteensopiva yleisemmän IEEE802.11b -standardin kanssa, joten 802.11a -laite ei voi kommunikoida 802.11b-laitteen

kanssa. Signaalin lyhyempi kantomatka puolestaan nostaa hankintakustannuksia, koska määritellylle alueelle tarvitaan siten useampi tukiasema kattamaan katveetonta verkkoa. (Barken 2004:21)

2.4.2 IEEE802.11b

Toinen alkuperäisen 802.11-standardin laajennuksista on yleistynyt huomattavasti ensimmäistä enemmän. Tämän IEEE802.11b:ksi nimetyn standardin etuina ovat parempi kantomatka ja kohtuullinen kaistanleveys. 802.11b käyttää vapaata 2.4 GHz taajuusaluetta, jota Barken (2003:17) nimittää ”roskataajuudeksi”. Tämä johtuu siitä, että kyseistä taajuutta käyttää hyvin moni eri laite ja siksi se muodostuu ruuhkaiseksi ja häiriöalttiiksi. Muun muassa mikroaaltouunit, langattomat puhelimet ja bluetooth-laitteet ovat esimerkkejä näistä. 802.11b -standardin nopeus saatiin nostettua teoreettiseen 11 Mbps, mutta tällöin jouduttiin luopumaan taajuushyppelytekniikasta ja siirtymään suorasekvenssitekniikkaan.

Kiistattomat edut 802.11b-standardissa ovat sen nopeus suhteessa hintaan ja käytön helppous. Nopeus kuitenkin kärsii, jos samassa tilassa on muita samaa taajuutta käyttäviä laitteita. Tässäkin yhteensopivuus muiden standardien kanssa on ongelmakohta. Barken kuitenkin korostaa, että vaikka 802.11a- ja 802.11b -standardit eivät voi toimia yhteen, ne eivät myöskään häiritse toisiansa. Toisin sanoen ne voivat sijaita samassa fyysisessä tilassa.

2.4.3 Muut IEEE802.11 laajennukset

IEEE:n työryhmät kehittävät jatkuvasti 802.11-standardia tavoitteenaan saada siitä entistä suorituskykyisempi, turvallisempi ja yhteensopivampi, jotta se voisi kilpailla tasaväkisesti kiinteän verkon kanssa. Vuonna 2003 ratifioitu tuotos on g-standardi, jossa a- ja b-standardien parhaat puolet on yhdistetty. Barken (2004: 22) yksinkertaistaa tätä ja kuvaa 802.11g-standardia 802.11b-standardiksi, joka vain toimii 54 Mbps nopeudella. Nopeudenlisäys saavutettiin ottamalla käyttöön a-standardin modulointitekniikka OFDM ja siirtämällä se 2.4 GHz taajuudelle. Barken huomauttaa kuitenkin, että b-standardin ongelmat (vähät kanavat ja ruuhkaisen taajuuden häiriöalttius) jäivät perintönä myös g-standardille. Ongelmista huolimatta Barken näkee suurta kasvupotentiaalia tässä uudessa standardissa, koska se on täysin yhteensopiva yleisen b-standardin kanssa, jolloin siihen kohdistetut investoinnit eivät mene hukkaan. Uusimpana laajennuksena on ratifioitu i-standardi, jolla keskitytään parantamaan tietoturvaa lisäämällä alkuperäiseen standardiin uusi signaalin salauskeino Advanced Encryption Standard eli AES.

Tällä hetkellä kehitteillä tai jo ratifioituja laajennuksia on vielä ainakin IEEE802.11d-, e-, f- ja h- laajennukset. Näistä d-standardi pyrkii ratkaisemaan yleisiä kansainvälistymisongelmia, kun taas e-standardi pyrkii parantamaan palvelun laatua (Quality of Service, QoS) sekä lisäämään standardiin multimedian tuen. F-standardi kehittää Inter-Access Point Protocol (IAPP) -

metodia, jolla pyritään parantamaan tukiasemien välistä Roaming-ominaisuutta. Roaming-ominaisuus sallii käyttäjän siirtymisen tukiasemalta toiselle yhteyden katkeamatta. H-standardin tärkeimmät uudet ominaisuudet kohdistuvat a-standardin puutteiden, kuten kanavan vaihdon ja tarkkailun sekä tehonkäytön parantamiseen. (Barken 2004: 23.)

2.5 Langattoman tiedonsiirron tekniikat

OSI-mallin alimmalla eli fyysisellä kerroksella määritellään, miten ja missä mediassa tieto liikkuu verkossa. Kiinteässä Ethernet-verkossa siirtotienä on tavallisesti Cat5-kierretty parikaapeli. Langattomissa verkoissa siirtoteitä on kolme: infrapuna (IR), suorasekvenssihajaspektritekniikka (Direct Sequence Spread Spectum, DSSS) ja taajuushyppelyhajaspektritekniikka (Frequency Hopping Spread Spectrum, FHSS) (Barken 2004: 12).

2.5.1 Infrapuna

Infrapunaa tiedonsiirtotienä käytettäessä lähettimen ja vastaanottajan välillä on oltava näköyhteys. Tämän vuoksi sen kantama jää usein hyvin lyhyeksi ja siksi varsinaisiin langattomiin verkkoihin sitä ei koskaan sovellettukaan. Barkenin (2004: 13) mukaan infrapunan yleistymistä langattomissa verkoissa vaikeutti myös se, että sitä käyttäviä merkittäviä kaupallisia tuotteita ei koskaan kehitetty. Tyypillisiä käyttökohteita sille ovatkin lyhyen kantaman ja pienen virtalähteen omaavat laitteet, kuten matkapuhelimet.

2.5.2 Hajaspetritekniikka

Hajaspektritekniikka on signaalin digitaalinen koodaustekniikka, jonka ideana on levittää signaali laajalle taajuusalueelle. Mullerin (2003: 341) mukaan sen kehitti ja patentoi säveltäjä George Antheil yhdessä näyttelijätär Hedy Lamarrin kanssa jo vuonna 1942. Tämän tekniikan etuna on sen hyvä häiriöiden sietokyky ja tietoturvallisuus; koska signaali on levitetty satunnaisesti eri taajuuksille, sen havaitseminen ja tulkitseminen on vaikeaa ja vaikuttaa lähinnä kohinalta.

DSSS

DSSS toimii siten, että se kuvaa signaalissa yhtä bittiä pitemmällä, yleensä yli kymmenen bitin pituisella, bittikuviolla, jota kutsutaan lastuksi (chip). Tämä tekniikka tekee siitä hyvin häiriösietoisen ja vaikka osa viestistä korruptoituisikin, on se usein mahdollista palauttaa. Haittapuolena tässä tekniikassa on sen suuri tehonkäyttö, koska vastaanottavassa päässä tarvitaan useita vastaanottimia.

FHSS

Taajuushyppelyhajaspektritekniikassa lähettäjä ja vastaanottaja vaihtavat ennalta sovitun järjestyksen mukaan taajuuttaan, jolla tieto kulkee. Jokaista taajuuden vaihtoa kutsutaan hypyksi (Sikora 2003: 41). Tietoturvan kannalta FHSS on hyvä valinta; jos vastaanottava laite ei tiedä oikeaa hyppelykaavaa, se ei pysty tulkitsemaan signaalia. Sikora (2003: 41) mainitsee tämän tekniikan hyväksi puoleksi myös sen, että se on edullinen ja helppo ottaa käyttöön. Lisäksi sen tehonkulutus on suhteellisen pieni.

2.6 Laitteet

Langattoman lähiverkon keskeisimmät laitteet ovat tukiasemat (Access Point, AP, Kuva 1) ja päätelaitteet. Tukiaseman tärkein tehtävä on toimia tiedon välittäjänä langattomien päätelaitteiden välillä ja niiden linkkinä kiinteään verkkoon (Muller 2003: 1). Muller huomauttaa myös, että tukiasema on tavallisimmin kytketty kiinteään verkkoon keskittimen tai kytkimen kautta CAT5-kaapelilla.

Kuva 1 Nokia A020 langattoman verkon tukiasema

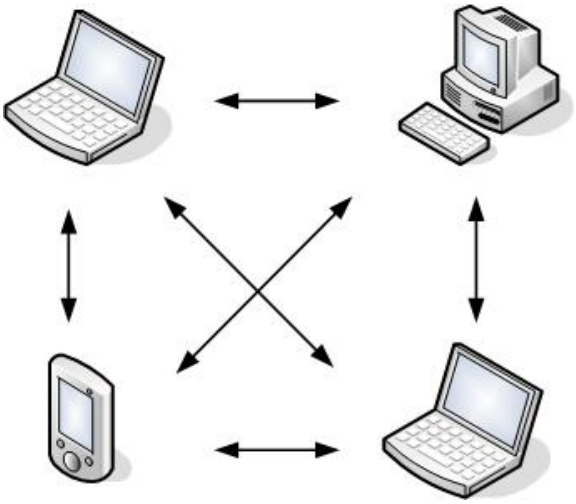
Päätelaitteena (Client) voi olla kannettavat (Laptop) tai pöytämalliset (PC) tietokoneet tai kämmentietokoneet (PDA). Viimeksi mainituissa langaton verkkoyhteys on tavallisesti yhdysrakenteisena, mutta kannettavat ja pöytämalliset tietokoneet saattavat tarvita erillisen verkkosovittimen langattoman verkkoyhteyden muodostamista varten. (Kuva 2) Näitä on markkinoilla useita erilaisia malleja erilaisilla ominaisuuksilla, tärkeimpänä sen tukema(t) standardi(t).

Kuva 2 Nokia C110 langaton PCMCIA-liitäntäinen verkkosovitin

2.7 Topologiat

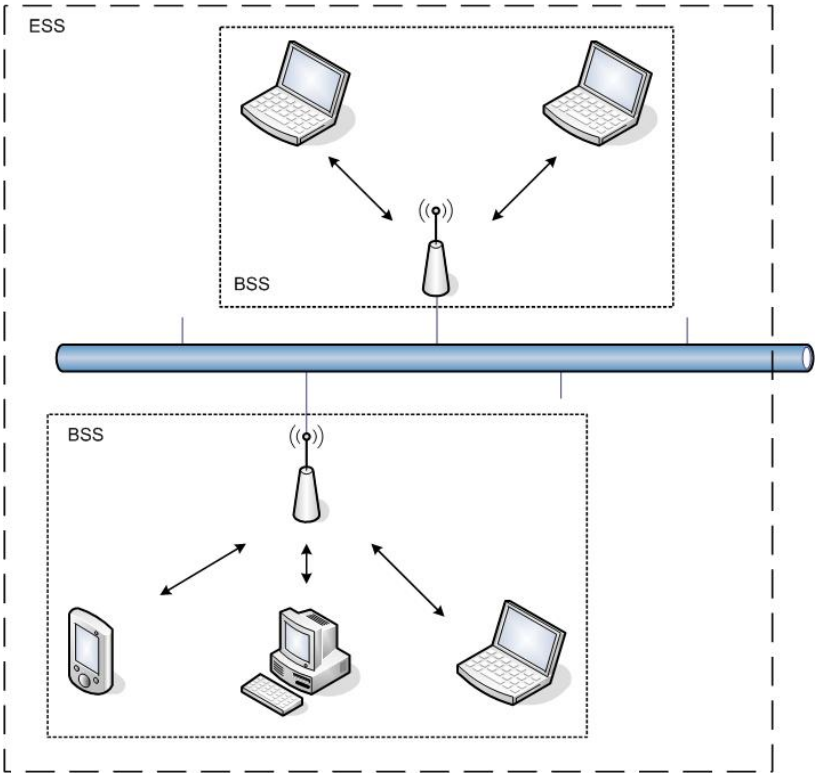
IBSS

IBSS (Independent Basic Service Set) tai tavallisemmin Ad-hoc Mode on nopeasti ja kustannustehokkaasti muodostettava yksinkertainen lähiverkko, jossa päätelaitteet kommunikoivat langattomasti keskenään ilman erillistä tukiasemaa (Kuva 3). Tällainen arkkitehtuuri soveltuu lyhyen kantaman käyttöön ja verkkoon, jossa osallistuvia päätelaitteita on rajallinen määrä. (Sikora 2003: 59.)



Kuva 3 Ad-hoc Mode

BSS/ESS (Basic Service Set/Extended Service Set) tai tavallisemmin Infrastructure Mode taas käsittää päätelaitteiden lisäksi tukiaseman, joka on kytketty olemassa olevaan kiinteään infrastruktuuriin, kuten Ethernetiin (Kuva 4). Kaikki liikenne reititetään tukiaseman kautta, eli päätelaitteiden välillä ei ilmene suoraa kommunikointia. Yksinkertaisimmillaan BSS muodostuu yhdestä tukiasemasta ja joukosta langattomia päätelaitteita tukiaseman kantaman sisällä. Kun sama verkko koostuu kahdesta tai useammasta BSS:stä, joiden tukiasemat on liitetty toisiinsa kiinteän verkon kautta, kutsutaan sitä ESS:ksi. (Sikora 2003: 60.)



Kuva 4 Infrastructure Mode

3. Tietoturva

Langattomien verkkojen huonoista puolista ja riskeistä puhuttaessa esiin nousevat tavallisesti ensimmäisenä tietoturvaongelmat. Koska tieto liikkuu ilmassa kaapelin sijasta, se on huomattavasti helpompi kaapata. Käytännössä kuka tahansa kykenee vastaanottamaan signaalia, jos vain on kantaman sisällä. Vaikka jo hajaspektri-tekniikan käyttö itsessään tekee langattoman liikenteen seuraamisen vaikeaksi, ei silti vaadita mahdottomia toimenpiteitä, joilla eitoivottu käyttäjä voi salakuunnella liikennettä. Tämän vuoksi on kehitetty eriasteisia suojauksen muotoja, joilla tietoturvaa on saatu parannettua. Tämä luku käsittelee näitä muotoja.

3.1 SSID & ESSID

Sikora (2003: 86) jakaa tietoturvallisuuden muodot karkeasti kolmeen eri tasoon: käyttäjille annettu koodi tai verkkonimi, autentikointi ja signaalin salaus eli kryptaaminen. Matalimmalla tasolla verkon suojauksessa järjestelmän pääkäyttäjä antaa verkolle nimen, jota kutsutaan laitevalmistajasta ja verkon rakenteesta riippuen lyhenteillä SSID (Service Set Identifier), ESSID (Extended Service Set Identifier) tai sitten vain yksinkertaisesti Network Name. Kyseessä on maksimissaan 32 merkin pituinen nimi, jonka tehtävä on erottaa langattomat verkot toisistaan. Kaikilla tietyn langattoman verkon laitteilla tulee olla tämä nimi tiedossaan päästäkseen sisään verkkoon.

Tietoturvan kannalta yksinomaan verkkonimen käyttö on riittämätön suojauksen keino nykyaikana. Monet valmistajat ovat lisänneet kannettaviin laitteisiinsa ominaisuuden, joka joko tunnistaa verkkonimen automaattisesti tai sallii ”mikä tahansa” (any) –verkkokonfiguraation, jolla laite pääsee sisään verkkoon. (Sikora 2003: 87.)

3.2 Tietoturvastandardit ja salausmetodit

3.2.1 WEP

Wired Equivalent Privacy eli WEP on salaus- ja tietoturvakäytäntö, joka on kuulunut IEEE802.11 -standardiperheeseen lähes alusta saakka. Kuten sen nimi vihjaa, oli se alun perin tarkoitettu tuottamaan langattoman verkon käyttäjille suunnilleen samantasoinen suoja kuin kiinteän verkon (wired) käyttäjillä on. Barken (2004: 31) luonnehtii WEP-salausta riittämättömäksi ja osoittaakin sen puutteet selviksi teoksessaan.

WEP:n tarkoitus on edistää tietoturvaa salaamalla päätelaitteen ja tukiaseman välinen liikenne käyttämällä siihen RC4-salausalgoritmiä. RC4 on laajalti käytetty salausalgoritmi, jonka tunnetuin sovellus on Internetin suojatuilla sivuilla käytetty Secure Sockets Layer (SSL). Puhuttaessa WEP:n haavoittu-

vuudesta RC4 ei olekaan ongelman ydin, vaan se, kuinka sitä on sovellettu. (Barken 2004: 35) Kaiken perustana on yksi ennalta määritetty 40- tai 128-bittinen jaettu salausavain. Tähän WEP kaatuukin; kun tämä avain löydetään, pääsee liikennettä salakuuntelemaan ongelmitta. Internetistä löytyy useita ohjelmia WEPin heikkouksien hyväksikäyttämiseen. Esimerkkeinä näistä AirSnort ja WEPCrack. Menetelmät, joilla nämä ohjelmat käyttävät hyväkseen WEPin heikkouksia, perustuvat riittävän aineiston (signaalin) kaappaamiseen ja analysointiin. Lopulta WEP-avain voidaan yksinkertaisesti laskea. (Barken 2004: 42.)

3.2.2 WPA & WPA2

WEP todettiin siis riittämättömäksi suojauskeinoksi langattomassa verkossa. Wi-Fi Alliance alkoi kehittää uutta turvallisuusstandardia, joka paikkaisi WEPissä havaitut puutteet. Syntyi Wi-Fi Protected Access eli WPA. WPA tuottaa hyvän tietosuojan käyttämällä tehokasta signaalin salausta ja käyttäjien tunnistusta. Se tukee kaikkia IEEE802.11-standardeja. Jotta WPA voidaan ottaa käyttöön langattomassa verkossa, on kaikkien verkon komponenttien tuettava sitä. Se voidaan ottaa käyttöön kahdella eri tavalla, kotikäyttöön tarkoitetulla WPA-Personalilla ja yrityskäyttöön suunnatulla WPA-Enterprisella. Molemmat moodit käyttävät 128-bittistä Temporal Key Integrity Protocol (TKIP) -salausta ja dynaamisia avaimia, jotka vaihtelevat istuntokohtaisesti. (Glossary of… 2004)

WPA-Personal käyttää ennalta määrättyä avainta (Pre-Shared Key, PSK), joka määritetään langattomaan tukiasemaan ja käyttäjien verkkokortteihin. Mikäli avaimet täsmäävät, sallitaan pääsy verkkoon ja signaalin salausprosessi käynnistyy. Erona WEPiin PSK:a käytetään vain istunnon alussa. Sen jälkeen avaimet vaihtuvat dynaamisesti päinvastoin kuin WEPissä, jossa sama salausavain on voimassa jatkuvasti. WPA-Enterprise-moodissa käytetään ulkoista käyttäjien tunnistamiseen tarkoitettua palvelinta, eikä mitään yksittäistä jaettua avainta ole. Palvelin kontrolloi pääsyä verkkoon.

WPA oli kuitenkin tarkoitettu vain paikkaamaan WEPin pahat puutteet ja pääasiana tämän ohella pidettiin sen saamista yhteensopivaksi vanhojen laitteistojen kanssa. Tämä rajoitti ideaalisen tuloksen aikaansaamista. Vanhoilla laitteilla ei ollut resursseja käyttää kehittyneempiä salausalgoritmeja ja siksi WPA jäikin vain välivaiheeksi. (Barken 2004: 66.) WPA2 on ominaisuuksiltaan hyvin edeltäjänsä kaltainen, mutta käyttää salaukseen erittäin vaikeasti murrettavaa Advanced Encryption Standard -algoritmia (AES) (Glossary of… 2004).

3.2.3 TKIP

TKIP perustuu saman RC4-salausalgoritmin käyttöön kuin WEPkin. Erona WEPiin salausavaimina käytetään kuitenkin aina 128-bittisiä avaimia ja niitä vaihdetaan jatkuvasti ja automaattisesti. Koska mahdollisia avaimia on yli 500

miljardia ja ne vaihtuvat tiheään tahtiin, on TKIP-salauksen purkaminen lähes mahdotonta. Uutena ominaisuutena TKIP tarjoaa myös Message Integrity Check -toiminnon (MIC). Sen avulla voidaan varmistua datapaketin eheydestä eli siitä, että kukaan ei ole kaapannut pakettia, muokannut sitä ja lähettänyt uudelleen. (Glossary of… 2004.)

3.2.4 AES

AES on yksi osa IEEE802.11i-standardin tietoturvaa edistävistä ominaisuuksista. Se on salauskeino, joka voidaan ottaa käyttöön 128-, 192- tai 256-bittisenä versiona. Järeään AES-salaukseen vaaditaan tehokas prosessori ja siksi yhteensopivuus vanhempien langattomien laitteiden kanssa on toistaiseksi vähäistä ja tämä osaltaan hidastaa AES-salauksen implementoinnin suuremman leviämisen. Muller (2003: 413) osoittaa esimerkillä AES:n tehokkuuden: tietokoneelta, jolla olisi tarpeeksi tehoa laskea 255 avainta sekunnissa, kestäisi 149 miljardia vuotta murtaa AES-salaus.

3.3 Autentikointi

Kun langaton laite yrittää kytkeytyä verkkoon ensimmäistä kertaa, on sen tunnistauduttava, jotta sille voidaan sallia pääsy verkkoon. Tätä tapahtumaa kutsutaan autentikoinniksi. IEEE802.11 -standardi määrittelee kaksi erilaista autentikointityyppiä; avoin autentikointi ja jaetun avaimen autentikointi.

Avoin autentikointi on vain nimellisesti autentikointia, jossa tietoturva on hyvin puutteellista. Avoimessa autentikoinnissa autentikoija, esimerkiksi tukiasema, lähettää selväkielisen haastetekstin autentikointia pyytäneelle laitteelle, joka palauttaa sen yksinkertaisella algoritmilla koodattuna takaisin autentikoijalle. Jos koodaus on oikein, niin pääsy sallitaan. (Sikora 2003: 78.)

Jaetun avaimen autentikoinnin käyttö on huomattavasti turvallisempaa. Siinä kommunikaatio laitteiden välillä on aina joko WEP-, TKIP- tai AES-salattua verkosta riippuen. Pääsy verkkoon hyväksytään, jos molemmilla langattoman verkon laitteilla on sama salainen avain. Nämä avaimet voivat olla kiinteitä, laitteisiin ennalta määritettyjä tai sitten kolmas osapuoli voi jakaa niitä automaattisesti ja dynaamisesti.

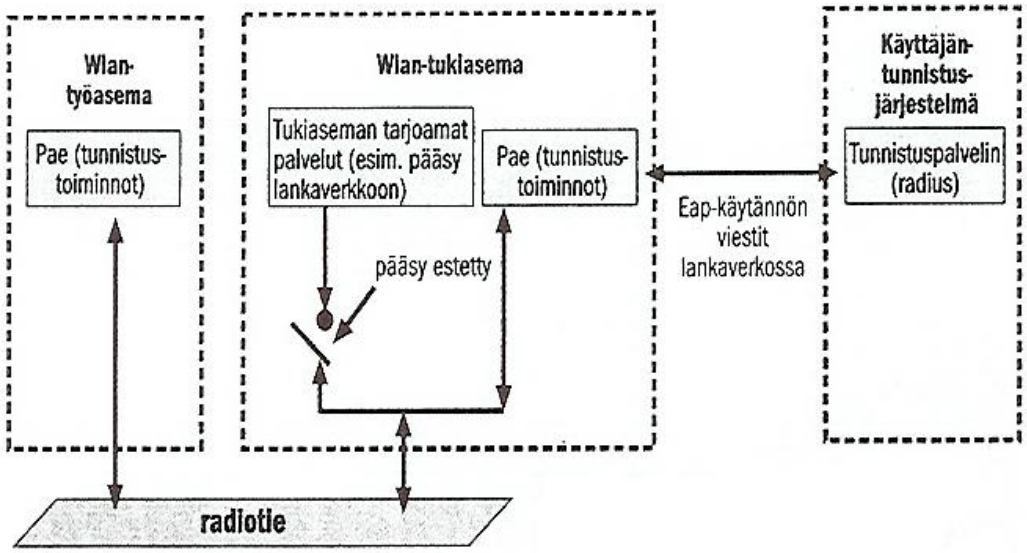
3.3.1 MAC-osoite

Yksinkertaisin taso tietoturvan luomisessa käyttäjän tunnistamisella on Media Access Control Addressin eli MAC-osoitteen käyttö. Jokaiselle tietoliikennelaitteelle annetaan tehtaassa valmistusvaiheessa uniikki numeroista ja kirjaimista koostuva tunnus, jota kutsutaan MAC-osoitteeksi. Ajatuksena tässä on se, että tukiasemaan luodaan lista niiden laitteiden verkkosovittimien MAC-osotteista, joille pääsy verkkoon sallitaan. Jos osoite on sallittujen luettelossa, pääsy sallitaan, muussa tapauksessa evätään.

Tietoturvan kannalta tässä tekniikassa on suuri epäkohta. MAC-osoitteet lähetetään selväkielisenä tekstinä jopa WEP-salatuissa paketeissa, joten verkkoon pyrkivän hyökkääjän on helppo kaapata sallittu MAC-osoite. MAC-osoitteiden muuttamiseen löytyy useita ohjelmia, kuten Spoof MAC. Tällä tavalla hyökkääjä voi huijata tukiasemia luulemaan omaa päätelaitettaan sallituksi ja pääsee siten verkkoon. Toinen MAC-osoitteiden suodatuksen huono puoli on sen työläs ylläpito suuremmassa ympäristössä. Aina kun verkkoympäristöön lisätään uusi langaton laite, jolle pääsy tulee sallia, sen MAC-osoite pitää kirjata jokaisen tukiaseman tietoihin erikseen. Barken (2004: 7) sanookin tämän olevan aivan liian työläs ja turvaton metodi suojata verkkoa, jossa langattomia päätelaitteita on enemmän kuin kourallinen.

3.3.2 IEEE802.1x & EAP

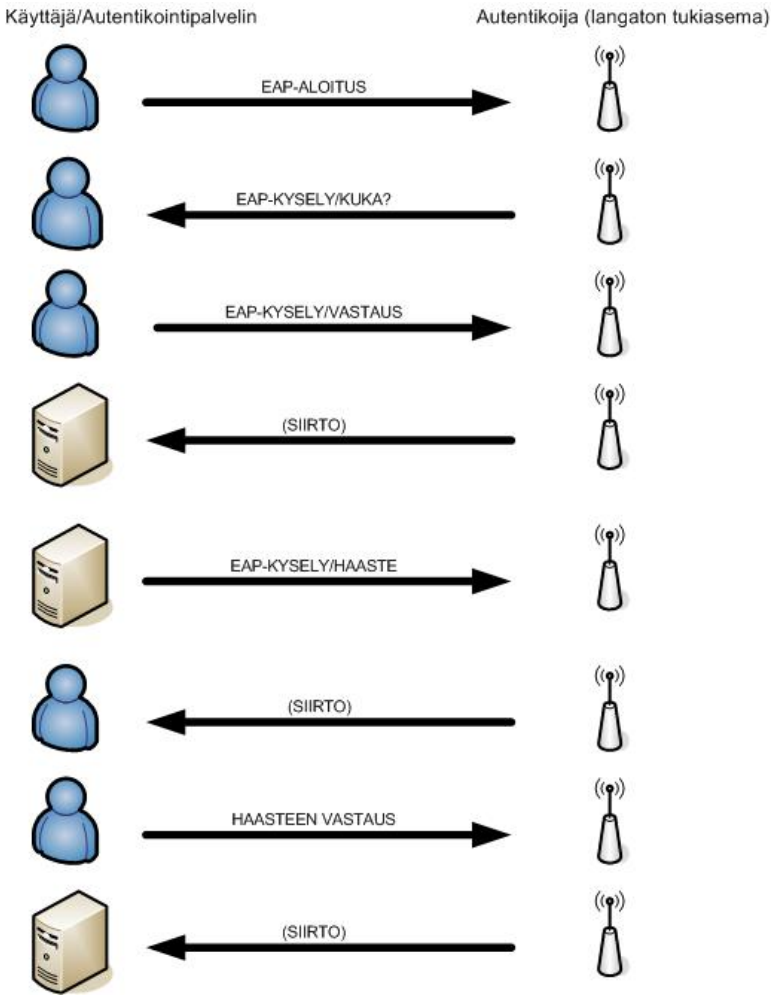
Vuonna 2001 IEEE julkaisi uuden kehittyneen tietoturvastandardin IEEE802.1x., jolla määritetään yleinen käyttäjätunnistusmalli lähiverkoille. Alun perin standardi kehitettiin yleiseksi lähiverkoissa käytettäväksi autentikoinnin toteuttajaksi. Se kuitenkin soveltuu hyvin myös langattomiin verkkoihin. Alla oleva kuva 5 näyttää sen sovitettuna langattomaan ympäristöön, jossa käytetään ulkoista autentikointipalvelinta.



Kuva 5 IEEE802.1x langattomassa lähiverkossa. Portti tukiaseman palveluihin aukeaa vasta, kun tunnistuspalvelu on hyväksynyt työaseman (Hämäläinen 2004: 66).

Barken (2004: 70) kuvaa 802.1x-standardia protokollaksi, joka yksinkertaistettuna vain käyttää Extensible authentication Protocol:a (EAP) ”kielenään” tukiaseman ja työaseman välisessä kommunikaatiossa. Barken huomauttaa myös, että 802.1x-standardia käyttävään verkkoon kuuluu aina kolme osapuolta: käyttäjä, joka pyytää pääsyä verkkoon, autentikoija (yleensä tukiasema), joka kontrolloi liikennettä ja autentikointipalvelin, joka hoitaa käyttäjän

tunnistuksen. Näiden välinen autentikointitapahtuma on kuvattuna alla (Kuva 6).



Kuva 6 Autentikointitapahtuma

EAP-autentikointimetodit

EAP kehitettiin alkujaan Point-to-Point Protocol:n (PPP) laajennukseksi. Ideana oli saada keskitetty ja yleistetty standardi useille eri autentikointimetodeille. Tällä tavalla käyttäjiä pystyttäisiin tunnistamaan erilaisten tunnisteiden, kuten salasanojen, sertifikaattien ja biotunnisteiden avulla. Barken (2004: 74) nostaa esiin muutaman tunnetuimmista ja yleisimmistä EAP-metodeista.

MD5 on matalimman tason EAP-tunnistuskeino. Se on helppo ottaa käyttöön, mutta on altis monenlaisille hyökkäyksille, kuten yksinkertaisille sanakirjahyökkäyksille. Toinen puute on se, että se ei käytä kaksisuuntaista autentikointia. Tämä tarkoittaa sitä, että tukiasema autentikoi asiakkaan (verkkoon pääsyä pyytävän käyttäjän), mutta ei päinvastoin. Barken (2004: 75) toteaa, että tämä ei riitä, vaan riittävän tietoturvan aikaansaamiseksi tulee käyttää kaksisuuntaista autentikointia. Kolmas vakava MD5:n puute on sen tuen puut-

tuminen salausavainten dynaamiseen uusimiseen. Barken vielä lisää, että MD5:a ei tule koskaan käyttää tuotantoympäristössä edellä esitettyjen puutteiden vuoksi.

Transport Layer Security (TLS) on kaikkein tietoturvallisin, mutta myös vaikein käyttöönottaa EAP-metodeista. Se käyttää kaksisuuntaista autentikointia ja dynaamista avainten vaihtoa. TLS muodostaa salatun tunnelin autentikointipalvelimen ja asiakkaan väliin, mutta vaatii sen muodostaakseen molemmilta osapuolilta digitaaliset sertifikaatit. Barken (2004: 76) toteaakin, että TLS on hyvin turvallinen, mutta sen käyttöönotto on huomattavan monimutkaista. Barkenin mielestä helpompia ja lähes yhtä turvallisia keinoja voidaan käyttää TLS:n asemasta ja viittaa TTLS- ja PEAP-metodeihin.

TTLS eli Tunneled Transport Layer Security on siis kevyempi versio TLS:sta. Se tukee kaksisuuntaista autentikointia ja dynaamista avaintenvaihtoa. Erona TLS:n on se, että TTLS ei vaadi sertifikaattia asiakkaalta, ainoastaan palvelimelta. Asiakas voi tällöin tunnistautua käyttämällä esimerkiksi salasanaa.

Protected EAP (PEAP) on hyvin samanlainen kuin TTLS. Se tukee niin ikään kaksisuuntaista autentikointia ja avainten dynaamista vaihtoa. Aluksi tukiasema autentikoi palvelimen sen sertifikaatilla, jonka jälkeen voidaan valita toinen EAP-metodi asiakkaan autentikointiin. Tämä tapahtuukin jo turvallisessa PEAP-tunnelissa, jolloin voidaan käyttää vähemmän suojattua keinoa, kuten Microsoftin Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2).

Lopuksi Barken (2004: 78) summaa, että suunniteltaessa langattoman verkon autentikointia, tulee ottaa huomioon, mikä EAP-metodi sopii siihen parhaiten. Toiset ovat turvallisempia, mutta myös yleensä hankalampia toteuttaa ja vaativat ylläpitäjältään enemmän. Toiset taas helpompia asentaa, ylläpitää ja käyttää, mutta eivät tuo ääritapauksissa täydellistä suojaa hyökkääjiä vastaan.

3.3.3 RADIUS

Remote Access Dial-In User Service eli RADIUS on alun perin modeemikäyttäjien tunnistamiseen kehitetty autentikointimenetelmä, joka on yleistynyt nykyisin myös monenlaisiin langattomiin ja kiinteisiin verkkoihin sovellettuna (Hämäläinen 2004: 67). Se perustuu käyttäjien sisäänkirjautumisnimen ja salasanan yhdistelmään, jonka perusteella pääsy verkkoon hyväksytään tai hylätään. RADIUS ei tee mitään muutoksia, kuten salausta, liikenteeseen.

Autentikointitapahtuman kulku yksinkertaistettuna menee siten, että aluksi verkkoon haluava käyttäjä syöttää käyttäjätunnuksensa ja salasanansa työasemaansa, josta ne kulkeutuvat RADIUS-palvelimelle. Palvelimen tehtävä on tarkistaa, että käyttäjällä on tili ja että salasana täsmää ennalta määritetyn kanssa. Silloin pääsy verkkoon sallitaan. (Wi-Fi security at work… 2004.)

RADIUS-palvelin voidaan konfiguroida tuottamaan eritasoisia pääsynrajoit-

teita. Esimerkiksi yhdelle käyttäjälle voidaan sallia pääsy vain Internetiin ja toiselle sekä Internetiin että sähköpostiin ja vaikka verkon palvelimiin. Kaikille käyttäjille yhteinen rajoite voisi olla vaikka pääsyn kieltäminen yöaikana verkkoon.

RADIUS-ohjelmisto on saatavilla sekä kaupallisina, että avoimen lähdekoodin ilmaisena versiona. Jälkimmäisestä esimerkkinä Free RADIUS Server Project, jonka saa ladattua osoitteesta www.freeradius.org. Kaupallisista esimerkkinä Windows-pohjaisen verkon palvelinten Windows Server 2000 ja 2003 RADIUS-sovellus Internet Authentication Service (IAS) (Barken 2004: 122).

3.3.4 Kerberos

Kerberos on Massachusetts Institute of Technologyn (MIT) kehittämä verkon autentikointiprotokolla kiinteille tai langattomille verkoille. Se mahdollistaa palvelimen ja käyttäjän välisessä kommunikaatiossa tunnistautumisen toisilleen samalla, kun se estää ulkopuolisten salakuuntelun. Kerberos perustuu sala-avainten jakamiseen palvelimen ja asiakkaan välillä. Siitä on saatavilla useiden kaupallisten versioiden lisäksi ilmainen Internetistä ladattava sovellus. Kerberos lisää tietoturvaa käyttämällä salauskeinona Data Encryption Standardia (DES), joka tukee eheyden tarkistusta datapaketeissa kaappausten ja muutoksien estämiseksi. Se muistuttaa TKIP -salausta, mutta käyttää siihen vain 64 bittiä. Uusin, tammikuussa 2005 julkaistu, Kerberoksen versio Kerberos 5 Release 1.4 käyttää salaukseen vahvempaa AES:a. (Kerberos: The Network… 2005.)

Kerberoksen toimintaperiaate on, että se jakaa digitaalisia muutaman sadan tavun pituisia ”pääsylippuja”, joita päätelaitteet voivat käyttää tunnistautumiseen verkossa sekä salaisia kryptograafisia avaimia, joilla salataan ja puretaan liikenne (Wi-Fi security at work… 2004).

3.4 VPN

VPN, eli Virtual Private Network on etäkäyttäjille suunnattu tietoturvan muoto, joka yhdistää tunneloinnin, signaalin salauksen, autentikoinnin sekä kulunvalvonnan ja -rajoittamisen tekniikat. Sitä käytetään yhdistämään kaksi tai useampia lähiverkkoja keskenään tai yksittäisen tietoliikennelaitteen, kuten etätyöntekijän työasema, organisaation verkkoon. VPN:a voidaan käyttää kuljettamaan tietoa Internetissä tai missä tahansa suojaamattomassa verkossa, joka käyttää TCP/IP-protokollaa tiedonvälittämiseen (VPN Overview… 2004).

VPN toimii siten, että kaikki liikenne lähettäjän ja vastaanottajan välillä tunneloidaan jonkin liikenteen salaavan protokollan sisään. Yleisesti käytössä olevia VPN-protokollia ovat IPSec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point to Point Tunneling Protocol) (Tietoturva: tietoturvallisuuden… 2001).

Barken (2004: 101) summaa, että VPN:t ovat suuresti lisänneet käyttäjien mahdollisuuksia kytkeytyä yritysten verkkoihin etäkäyttäjänä. Hän myös mainitsee yhden sovellusesimerkin VPN:n käytöstä langattomissa verkoissa. Siinä langattoman verkon käyttäjät pakotetaan autentikoimaan VPN:n kautta. Tämä tapahtuu siten, että koko langaton verkko sijoitetaan kiinteän verkon palomuurin ulkopuolelle ja sallitaan määrityksissä ainoastaan VPN-liikenteen pääsy läpi.

4. WLAN:in integrointi WPK-verkkoon

Tampereen ammattikorkeakoulun tietoverkkopalvelujen suuntautumisvaihtoehdon opiskelijoilla on käytössään koulun muusta tietoliikenneverkosta erillään oleva WPK-verkoksi nimetty lähiverkko. Tämä käsittää kolme luokkatilaa ja yhden Kehitys- ja tutkimuslaboratorioksi nimetyn huoneen, jossa sijaitsevat WKP-verkon palvelimet ja osa tietoverkkopalvelujen opetuskäyttöön tarkoitetuista laitteista ja materiaaleista. Tällä hetkellä huone toimii myös työharjoittelijan työpisteenä.

Toimeksiantona saatu tehtävä oli luoda toimiva ja tietoturvallinen langaton lähiverkko osaksi kiinteää WPK-verkkoa ja sen tueksi. Riittävä tietoturva saavutettiin ottamalla käyttöön signaalin salaus ja käyttäjän tunnistus eli autentikointi, johon käytetään ulkoista RADIUS-palvenlinta. Tässä luvussa esitellään langattoman lähiverkon käyttöönoton vaiheet WPK-verkon yhteyteen askel askeleelta.

4.1 Lähtötilanne

WPK-verkon huoneissa on kiinteä kaapelointi, missä työasemat on yhdistetty kytkimiin ja ne edelleen yhteen pääkytkimeen. Verkon fyysinen topologia kuvaa sitä, kuinka verkon laitteet on liitetty toisiinsa. Tässä tapauksessa se on laajennettu tähti. Looginen topologia sen sijaan on Ethernet 10BASE-T-verkkojen mukaisesti väylä ja sillä kuvataan tiedon siirtymistä lähiverkossa.

Palvelimien ohjelmistoalustana on Microsoftin Windows Server 2003, tarvittavat palvelut jo valmiiksi asennettuina. Työasemien käyttöjärjestelmänä on Windows XP. Tietoverkkopalveluilla on kaksi langatonta tukiasemaa (Nokia A020) ja kaksi langatonta PCMCIA-väylään asennettavaa verkkokorttia (Nokia C110), mutta ne eivät ole aktiivisessa käytössä.

4.2 WLAN:in implementointi

4.2.1 Laite- ja ohjelmistoresurssit

Microsoftin uusimpien Windows-versioiden ollessa käytössä sekä palvelimissa että työasemissa, yhteensopivuusongelmat ovat erittäin epätodennäköisiä. Pääosa tietoliikennelaitteiden valmistajista tukee suoraan uusia Windowsin versioita ja taas toisaalta Windowsit sisältävät kattavan tuen uusille laitteille.

Aloitettaessa langattoman verkon pystytystä, ongelmaksi ei muodostunut ohjelmistopuoli, vaan jo vanhaksi käynyt laitteisto. Nokian valmistamat tukiasemat ja verkkokortit eivät tukeneet mitään alkuperäisen IEEE802.11-standardin laajennuksista. Laitteistolle ei ollut tarjolla enää tuotetukea ja ohjekirjatkin olivat vajavaiset. Tietoturvan ylläpitoon oli tarjolla vain yksinkertainen

WEP-salaus ja autentikoinninkin soveltaminen tuntui lähes mahdottomalta. Kun vielä signaalin kantomatka ja kaistanleveys jäivät vaatimattomaksi, oli syytä harkita uusien laitteiden hankintaa. Tarvittiin laitteita, joilla olisi mahdollista toteuttaa nykyaikainen ja ominaisuuksiltaan monipuolinen sekä tietoturvallinen langaton verkko.

Päädyttiin hankkimaan uusi tukiasema ja langaton verkkosovitin. Merkiksi valittiin laadustaan tunnettu ZyXEL; tukiasemaksi Prestige 334W ja verkkosovittimeksi USB-väylään liitettävä ZyAIR G-220 lähinnä asiantuntevan myyjän suosituksesta. USB-väyläistä sovitinratkaisua tuki tässä tapauksessa sen yleisyys sekä kannettavissa että pöytämallisissa tietokoneissa. Molemmat uusista verkkotuotteista tukevat uusimpia standardeja ja mahdollistavat suhteellisen helpon käyttöönoton ja laajennettavuuden. Tärkeänä ominaisuutena niissä on myös se, että ne mahdollistavat kattavimpien tietoturvaominaisuuksien käyttöönoton.

4.2.2 Laiteasennukset

Tukiaseman käyttöönotto alkoi kytkemällä laitteen takapaneelissa sijaitsevan WAN 10/100-portin ja kiinteän lähiverkon kytkimen portin välille tavallinen Ethernet-kaapeli. Alkuasennusta varten kytkettiin toinen Ethernet-kaapeli tukiaseman yhden LAN 10/100-portin ja työaseman verkkokortin välille. Tämä yhteys voidaan haluttaessa purkaa tukiaseman konfiguroinnin ollessa valmis. Lopuksi virtakaapeli kytkettiin paikalleen, jolloin laite käynnistyi ja aloitti järjestelmätestauksen. PWR-valon palaessa yhtäjaksoisesti vihreänä on laite valmis konfiguroitavaksi.

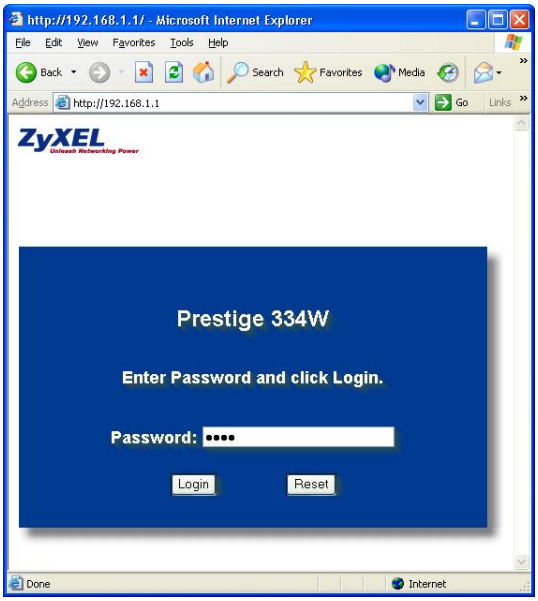
Verkkosovittimen asennus alkoi CD:llä toimitettavien ajureiden asentamisella ennen itse laitteen kytkemistä tietokoneeseen. Ajureiden lisäksi langattomaan päätelaitteeseen tulee asentaa ohjelmisto (wireless client supplicant), jonka tehtävänä on toimia käyttöjärjestelmän ja verkkosovittimen välillä kertoen, kuinka WPA:ta tulee käyttää. Tämän kirjoitushetkellä yleisimmät tällaiset ohjelmistot olivat Funk Softwaren Odyssey client ja Meetinghouse Data Communicationin AEGIS client. Windows XP -käyttöjärjestelmään on saatavilla WPA-päivitys, joka voi korvata tarvittaessa tällaisen ohjelmiston. Näistä kaksi viimeksi mainittua ovat ilmaisia ohjelmia ja ensimmäinen tulee ostaa erikseen. ZyXELin tuotteet kuitenkin sisälsivät lisenssin Odyssey client -ohjelmistoon, joten se valittiin käyttöön monipuolisempien ominaisuuksiensa, kuten useampien autentikointiprotokollien tuen vuoksi. Ohjelmistojen asennus sujui oletusarvoilla hyvin yksinkertaisesti ja nopeasti.

4.2.3 Laitekonfiguroinnit

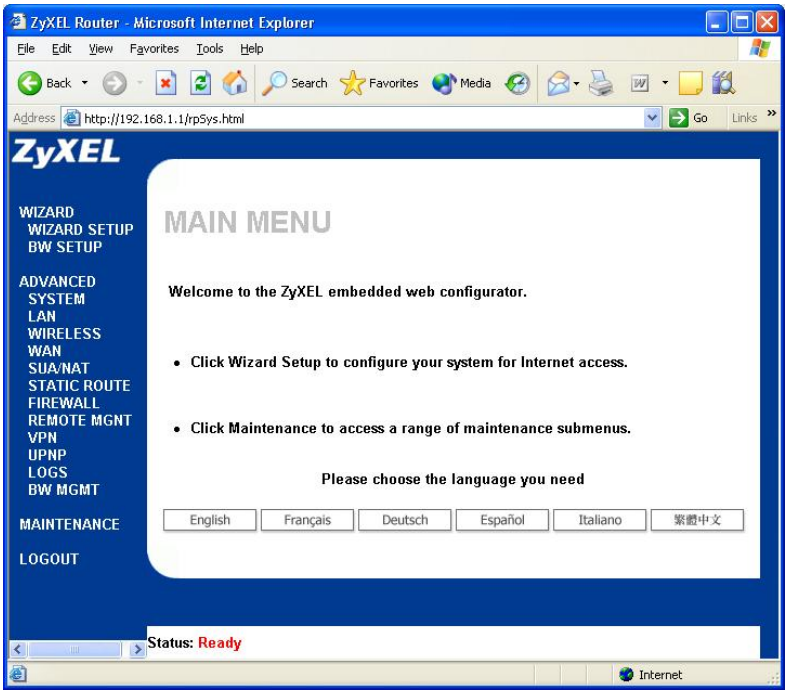
ZyXEL Prestige 334W

Ensimmäinen tarvittava konfigurointi langattoman verkon pystyttämisessä on tukiaseman asetusten muuttaminen sopiviksi. ZyXELissä näitä asetuksia pää-

see muuttamaan tukiasemaan kiinteästi (tai myöhemmin langattomasti) kytketyn työaseman selaimella. Osoiteriville kirjoitetaan oletusarvoinen LAN-portin IP-osoite 192.168.1.1, jolloin yhteys muodostuu. ZyXEL kysyy aluksi salasanaa (Kuva 7), jonka hyväksymisen jälkeen avautuu pääikkuna (Kuva 8).



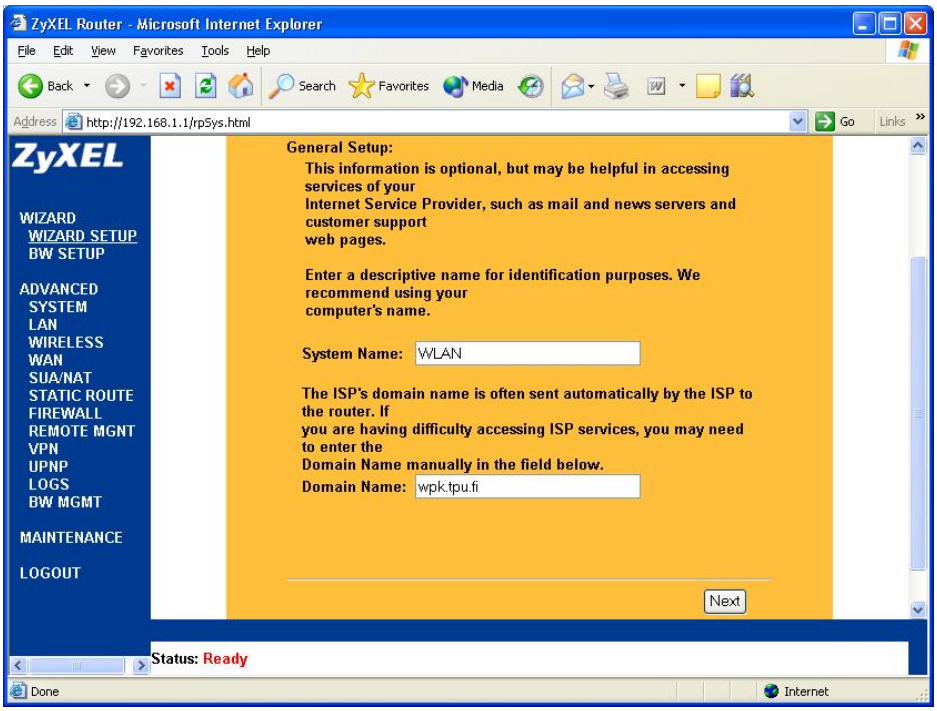
Kuva 7 Tukiaseman konfigurointiin tarvittava salasana



Kuva 8 Pääikkuna

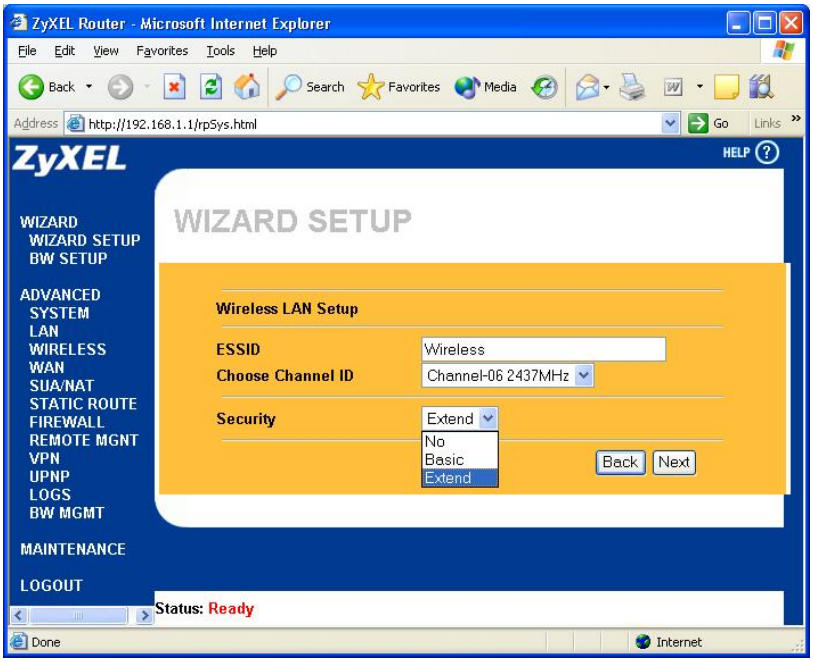
Vasemmalla olevasta kehyksestä valitaan käyttäjäystävällinen alkuasetusten muokkaus eli Wizard Setup. Ilmaantuvaan ruutuun kirjoitetaan kuvaava nimi (System Name) järjestelmälle, tässä tapauksessa vaikkapa WLAN. Lisäksi,

liityttäessä jo ennalta olevaan toimialueeseen (domain), kirjoitetaan sen nimi Domain Name -kohtaan. Next-painikkeella pääsee seuraavaan asetusikkunaan (Kuva 9).



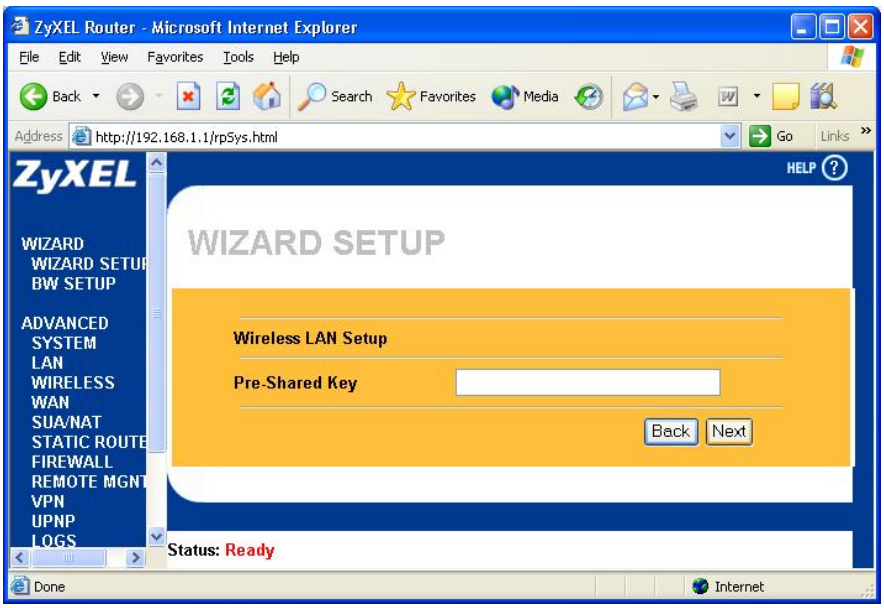
Kuva 9 Järjestelmän nimi ja toimialue

Seuraavassa ikkunassa asetetaan langattomalle yhteydelle verkkonimi, käytettävä kanava ja suojauksen taso. Verkkonimen voi jättää oletusarvoiseksi (Wireless) kuten myös kanavan. Eri kanavia (Channel) tarvitaan ainoastaan, jos samoissa tiloissa on useampi erillinen langaton verkko. Suojauksen taso asetetaan kolmesta vaihtoehdosta *no*, *basic* ja *extend* korkeimpaan, eli *extend*. Tämä valinta ottaa käyttöön WPA-suojauksen vahvalla salauksella. Next-painikkeella pääsee seuraavaan asetusikkunaan ja Back palauttaa edelliseen, mikäli muutoksia tarvitsee tehdä (Kuva 10).



Kuva 10 Suojauksen taso

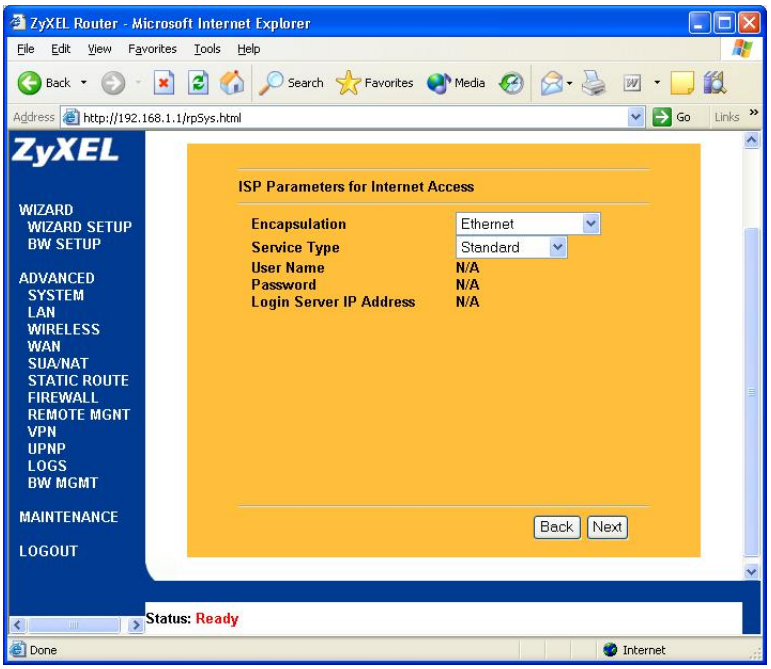
Seuraavassa ikkunassa ZyXEL kysyy ennalta määrättyä jaettua salausavainta (pre-shared key, PSK). Tämän kohdan voi jättää huomiotta, jos autentikointi tullaan järjestämään ulkoisen palvelimen avulla ja tällöin tätä yhtä salausavainta ei käytetä lainkaan. Next-painikkeella pääsee seuraavaan asetusikkunaan (Kuva 11).



Kuva 11 PSK

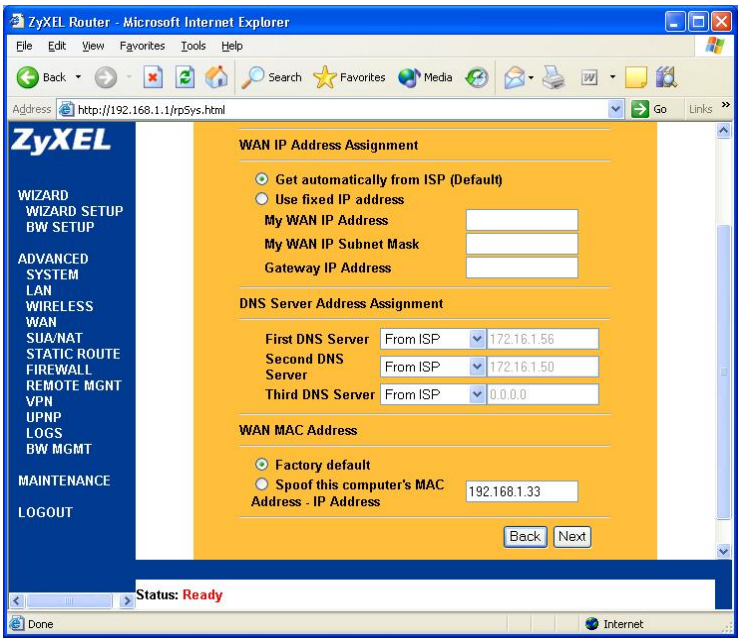
Seuraavaksi määritetään Internet-palveluntarjoajan (ISP) parametrit Internet-yhteyttä varten. Tässä tapauksessa palveluntarjoaja on WPK-lähiverkko ja sen palvelimet. Oletusasetukset kapseloinnille ja palvelun tyypille voidaan jättää

ennalleen. Next-painikkeella pääsee jälleen eteenpäin (Kuva 12).



Kuva 12 Palveluntarjoajan parametrit

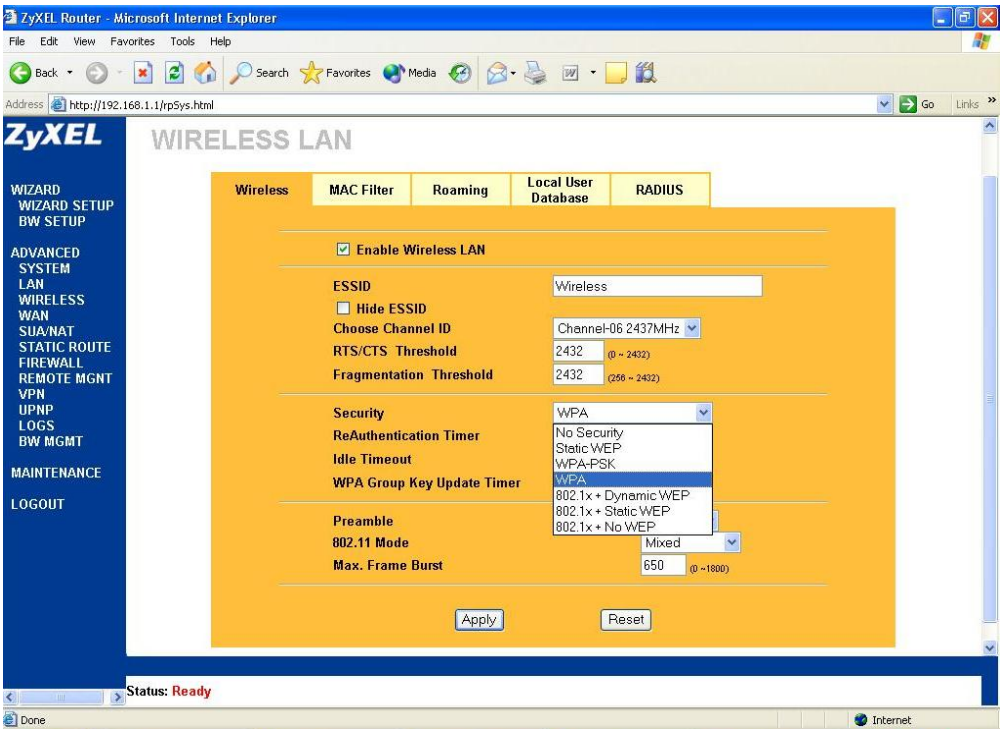
Niin ikään seuraavassakin ikkunassa oletusasetukset voidaan jättää ennalleen. WPK-verkossa on käytössä dynaaminen IP-osoitteiden jakaminen (DHCP) ja nimipalvelu (DNS), joita ZyXEL Prestige voi hyödyntää. Oletusasetuksilla tällä sivulla ZyXEL hakee tiedot automaattisesti näistä palveluista. Tiedot voi halutessaan syöttää käsin, jos IP-osoitteet ja aliverkon peitteet ovat tiedossa. Next-painike vie konfigurointiprosessissa eteenpäin (Kuva 13).



Kuva 13 IP-osoitetiedot

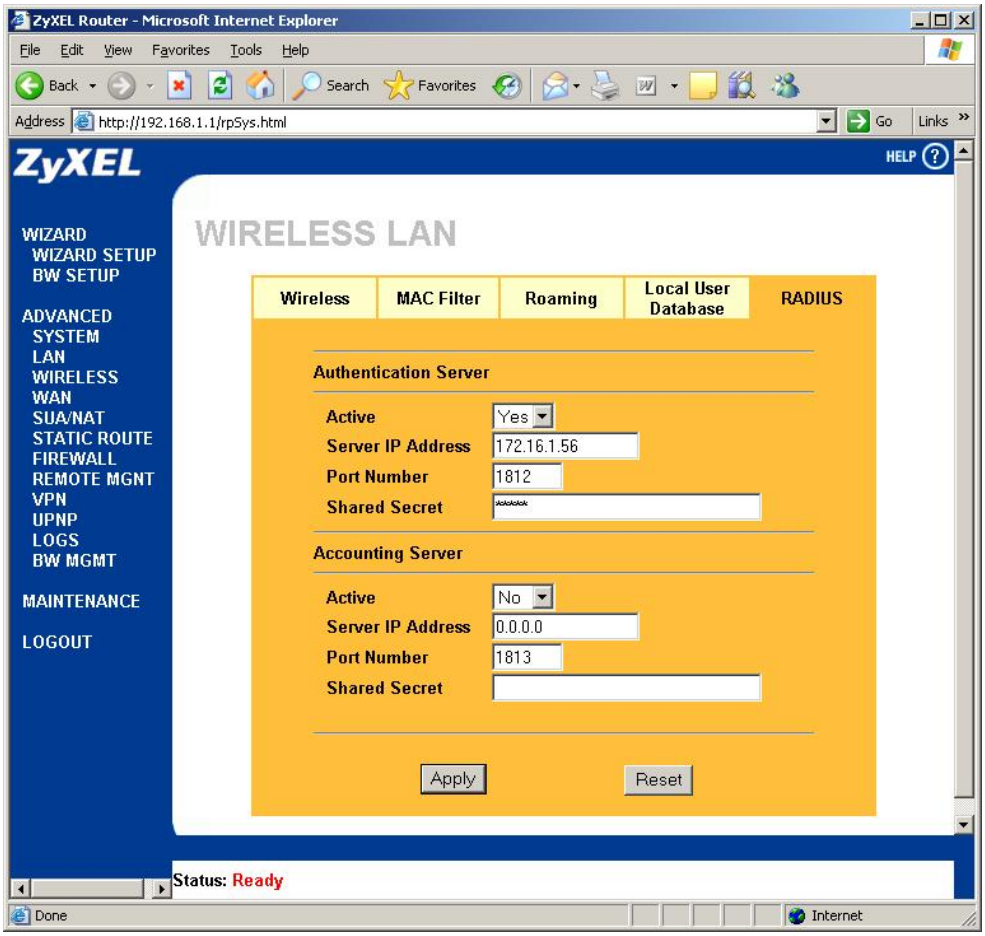
Seuraavassa ikkunassa hyväksytään tehdyt muutokset painamalla Finish, jolloin ZyXEL Prestige tallettaa tiedot muistiinsa. Alkuasetukset on näin tehty, mutta vielä kaikki ei ole valmista.

Seuraavaksi vasemmasta kehyksestä valitaan Wireless-kohta. Avautuvaan asetusikkunaan tehdään muutos Security-kohtaan, jossa valitaan WPA, mikäli se ei ole jo valittuna. Jos käyttäjä kirjoitti alkuasetuksissa jotain ennalta määrättyyn salausavaimeen (Kuva 9), niin Security-kohdassa on valittuna WPA-PSK. Muut kohdat voidaan jättää oletusarvoihinsa. Mahdolliset tehdyt muutokset hyväksytään Apply-painiketta painamalla (Kuva 14).



Kuva 14 Suojauksen tason tarkemmat määritykset

Saman ikkunan RADIUS-välilehdellä määritellään ulkoisen palvelimen IP-osoite, jonne RADIUS-palvelu on asennettu. Tässä työssä RADIUS-palvelinta käytetään autentikoinnin toteuttajana. Authentication Server -kohdassa valitaan autentikointi aktiiviseksi valitsemalla Y*es* ja Server IP Address -kohtaan asetetaan RADIUS-palvelimen IP-osoite 172.16.1.56. Porttinumero voidaan jättää oletusarvoonsa 1812. Shared Secret -kohtaan keksitään salasana, joka asetetaan myös RADIUS-palvelimelle. Tehdyt muutokset hyväksytään ja tallennetaan Apply-painiketta painamalla. Näin tukiaseman tarvittavat konfiguroinnit on tehty (Kuva 15).

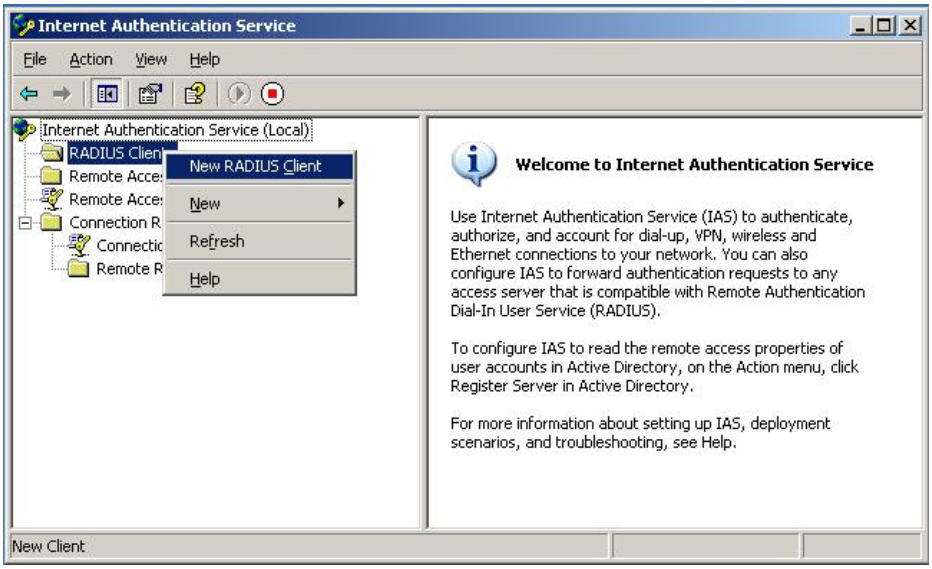


Kuva 15 Autentikointipalvelimen tiedot

Windows 2003 Server

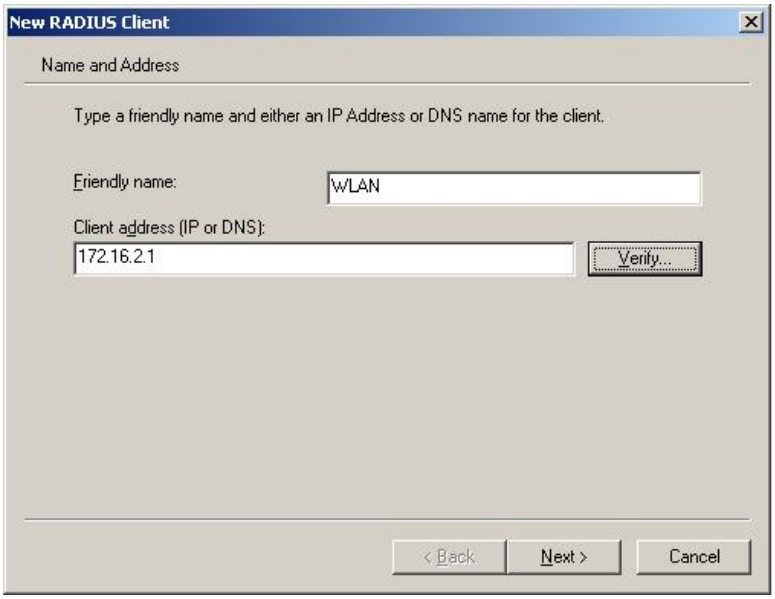
Windows 2003 Serverin palvelu, jota tarvitaan käyttäjän tunnistukseen, on Internet Authentication Service (IAS). Sitä ennen konfiguroitiin kuitenkin ZyXEL Prestigelle muuttumaton IP-osoite WAN-porttiin. DHCP-palveluun määritettiin IP-osoite 172.16.2.1, joka varattiin Prestigen MAC-osoitteelle. Toisin sanoen aina kun Prestige on yhteydessä WPK-verkkoon, antaa DHCP-palvelin tämän ennalta määritetyn IP-osoitteen sille. Tämä on välttämätön toimenpide autentikoinnin soveltamisen kannalta, koska RADIUS-palvelimelle täytyy kertoa tukiaseman IP-osoite.

IAS-moduuli avataan Käynnistä-valikosta. Ensimmäisestä ikkunasta RADIUS Clients -kohta korostetaan ja painetaan hiiren kakkospainikkeella sekä valitaan New RADIUS Client (Kuva 16).



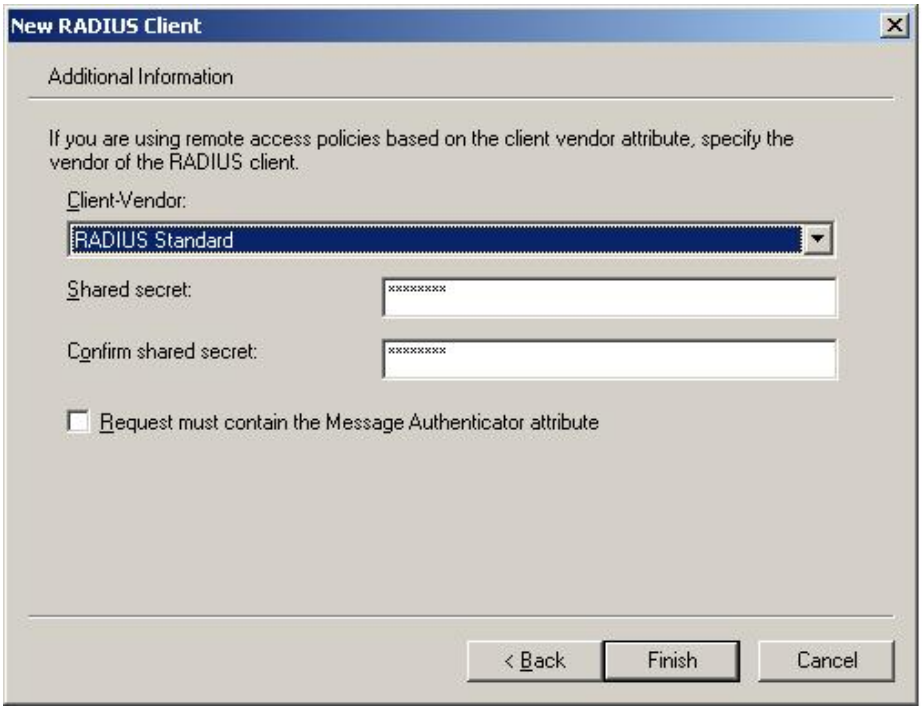
Kuva 16 IAS-pääikkuna

Seuraavassa ikkunassa valitaan aluksi kuvaava nimi RADIUS-asiakkaalle Friendly name -kohtaan. Valitaan nimeksi WLAN. Osoitekenttään tulee edellisessä kappaleessa määritetty pysyvä IP-osoite 172.16.2.1. Next-painikkeella pääsee seuraavaan ikkunaan (Kuva 17).



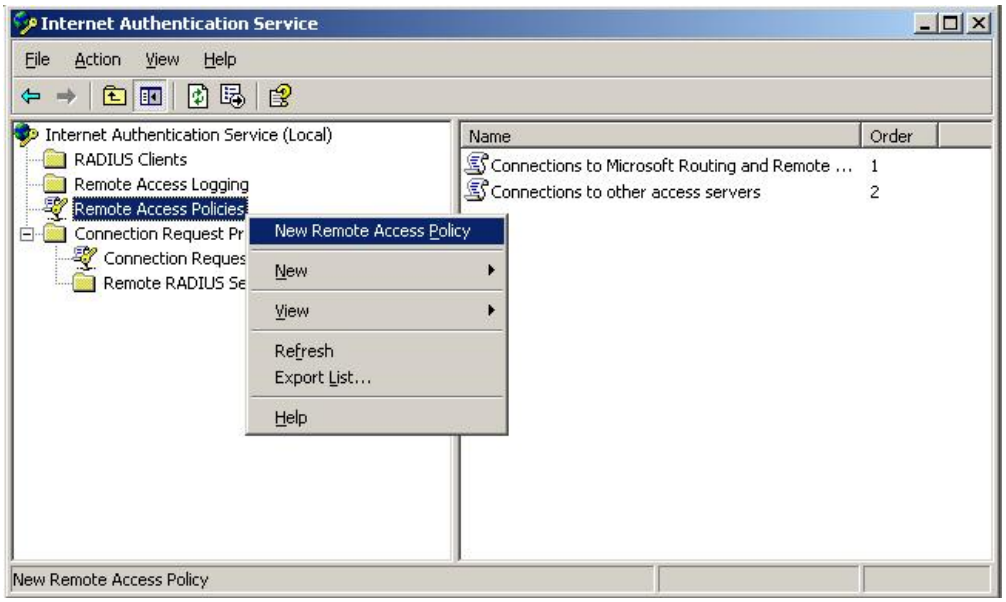
Kuva 17 RADIUS-asiakkaan nimi ja IP-osoite

Seuraavassa ikkunassa kirjoitetaan kahdesti Prestigeen aiemmin määritetty Shared Secret -salasana. Oletusarvo RADIUS-palvelun muodolle voidaan pitää voimassa. Finish-painike lopettaa toiminnon ja tallettaa konfiguroinnin (Kuva 18).



Kuva 18 RADIUS-palvelun muoto ja salasana

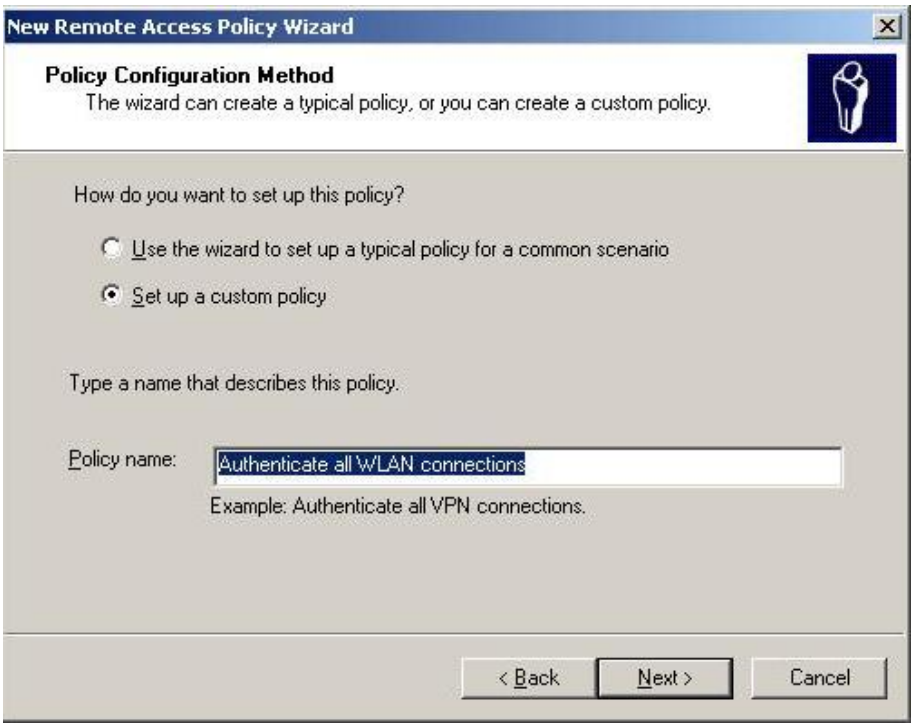
Seuraavaksi tulee asettaa pääsykäytäntö etäkäytölle. Hiiren kakkospainikkeella painetaan kohdassa Remote Access Policies ja valitaan New Remote Access Policy (Kuva 19).



Kuva 19 Uusi pääsykäytäntö etäkäytölle

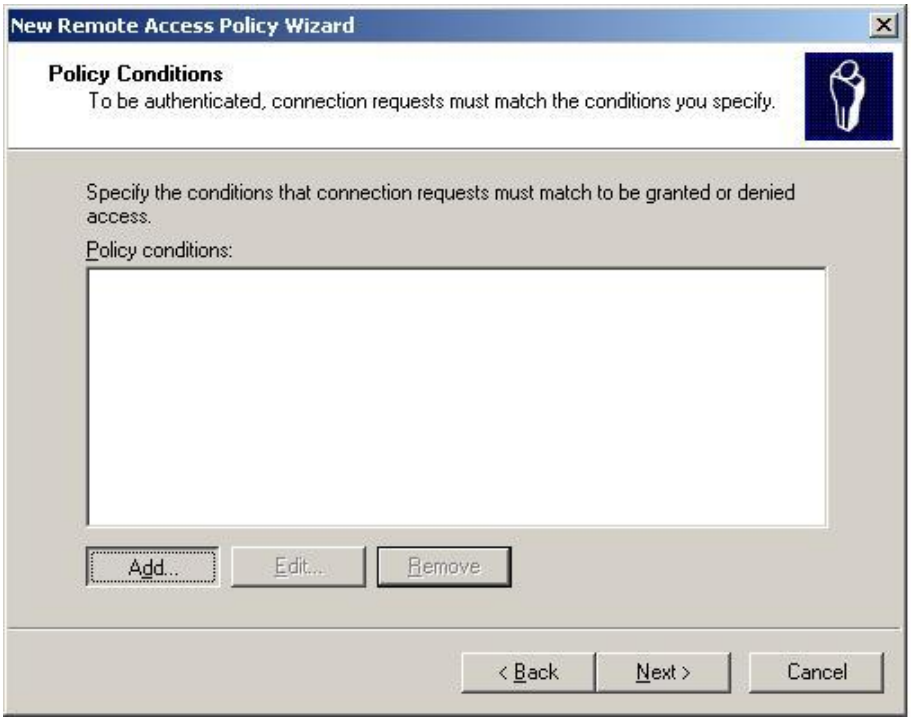
Näyttöön aukeaa jälleen Wizard, jolla asetukset saadaan helposti konfiguroitua. Ensimmäisessä ikkunassa valitaan itse muokattava käytäntö (Custom Policy) ja nimetään se kuvaavasti ja hyvin tunnistettavaksi. Tässä tapauksessa *Authenticate all WLAN connections*. Next-painikkeella päästään seuraavaan

ikkunaan (Kuva 20).

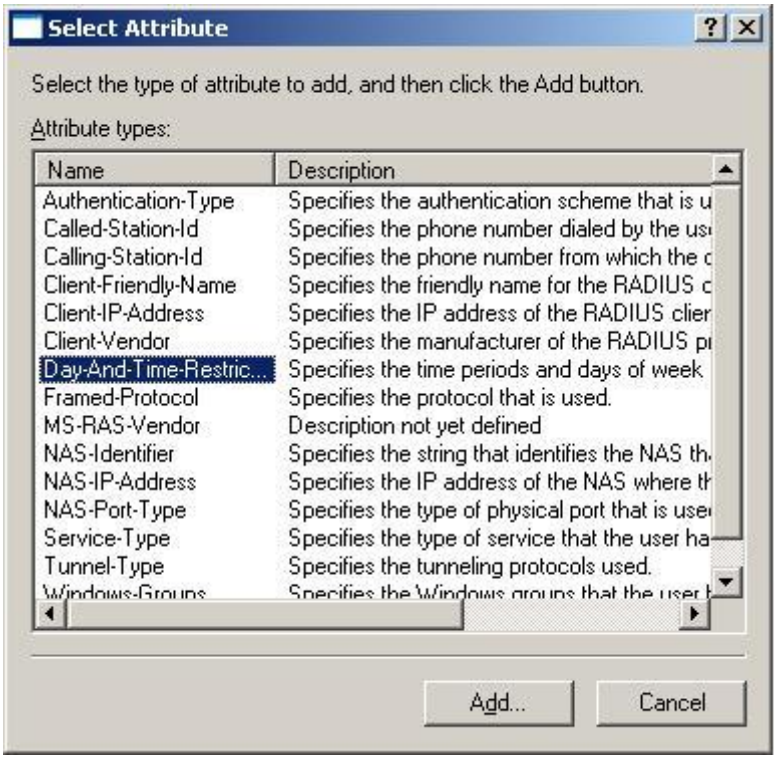


Kuva 20 Uuden käytännön nimi

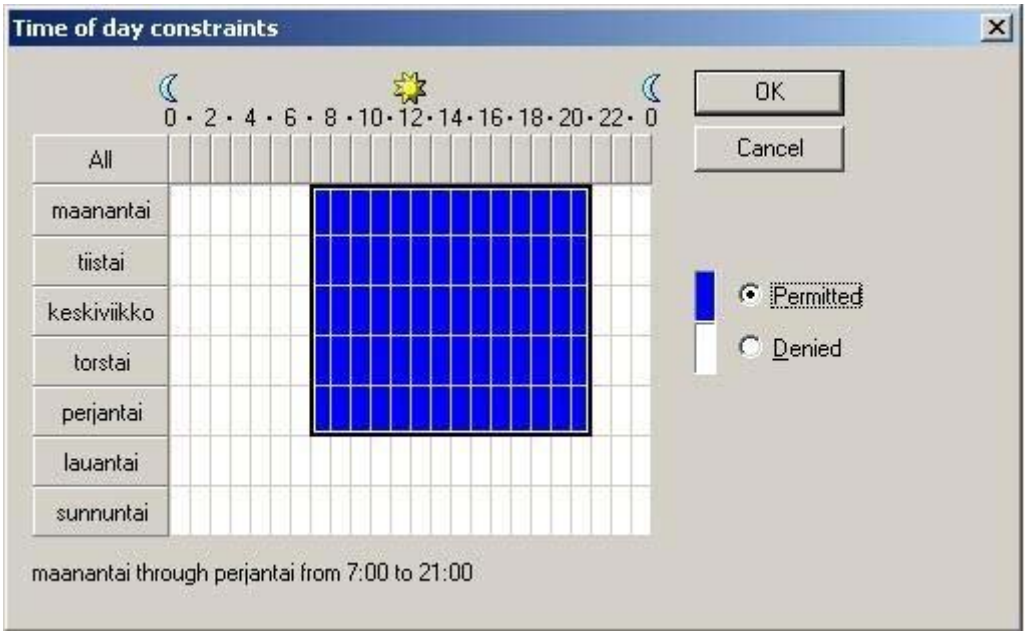
Tässä ikkunassa määritellään säännöt ja ehdot, joilla yhteys sallitaan tai kielletään. Add-painiketta painamalla tulevat näkyviin ne erilaiset ominaisuudet, joilla pääsyä voidaan rajoittaa. Esimerkkinä tässä työssä on valittu aikarajoitukset tietyille viikonpäiville ja kellonajoille. Seuraavaksi tulee sallia (Grant) yhteys, mikäli edellä määritetyt ehdot täyttyvät. Next-painikkeella päästään jälleen eteenpäin eri näytöillä (Kuvat 21-24).



Kuva 21 Uuden säännön lisäys



Kuva 22 Rajoitteiden lista

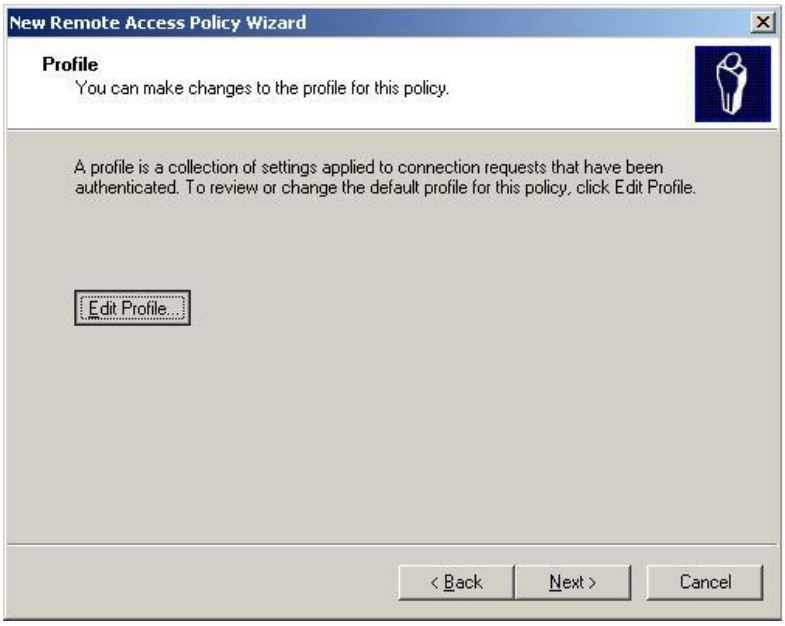


Kuva 23 Viikonpäivä- ja kellonaikarajoitteet

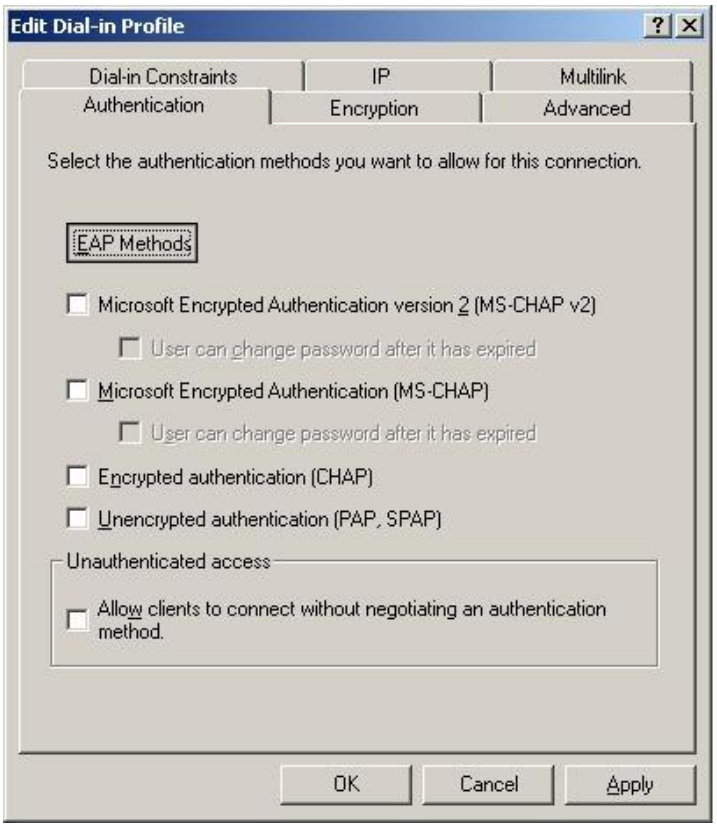
Kuva 24 Etäkäytön salliminen määritellyillä ehdoilla

Seuraava tehtävä on määrittää autentikointimetodi Edit Profile -kohdassa. Authentication-välilehdellä painetaan EAP Methods -painiketta, jolloin avautuu lista mahdollisista metodeista. Valitaan listasta Protected EAP (PEAP) ja painetaan OK. Mikäli muissa autentikointimetodikohdissa on rasti, tulee ne

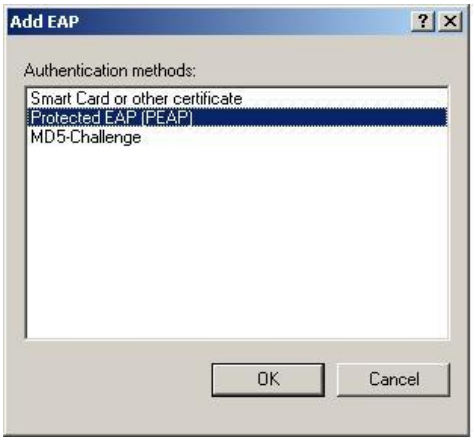
poistaa, jotta käytössä olisi ainoastaan PEAP. Hyväksytään valinnat OK-painikkeella ja Profiili-kohdassa Next-painikkeella sekä painetaan lopuksi Finish-painiketta. Näin RADIUS-palvelin on konfiguroitu autentikoimaan langattomat verkkoyhteyspyynnöt (Kuvat 25-27).



Kuva 25 Profiilin muokkaus



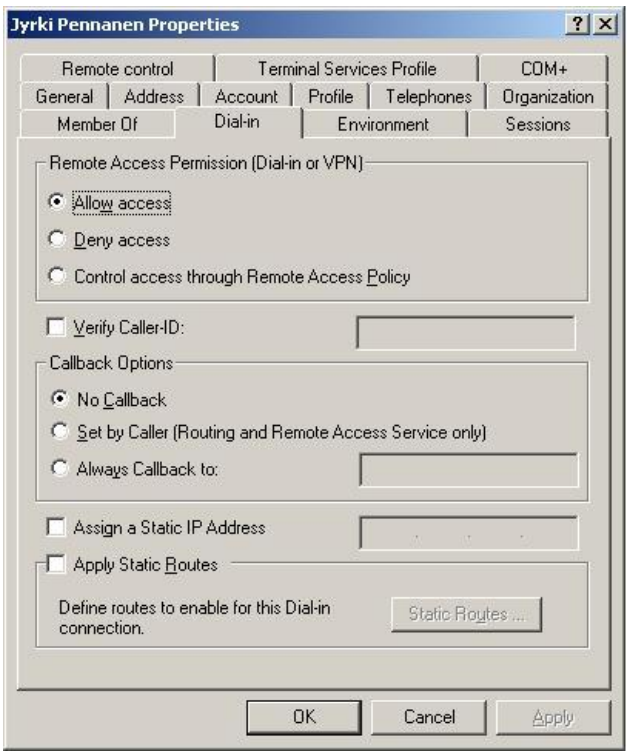
Kuva 26 Autentikointimetodit



Kuva 27 Autentikointimetodin valinta

Langaton päätelaite

Viimeisenä langattoman verkon komponenttina tehdään päätelaitteen konfigurointi, jolla se määritetään ottamaan vastaan tietyllä tavalla salattu signaali sekä autentikointi. Ennen sitä kuitenkin varmistetaan, että käyttäjä, jolla on oikeus liittyä WPK-verkkoon, voi tehdä sen myös langattomasti. Tähän tarvitaan palvelimelta Aktiivihakemistopalveluja ja siellä käyttäjäkohtaista profiilin muokkausta. Valitaan haluttu käyttäjä ja sen ominaisuudet. Dial-in-välilehdellä Remote Access Permission -kohtaan tulee valita Allow access. OK-painikkeella hyväksytään muutokset (Kuva 28).



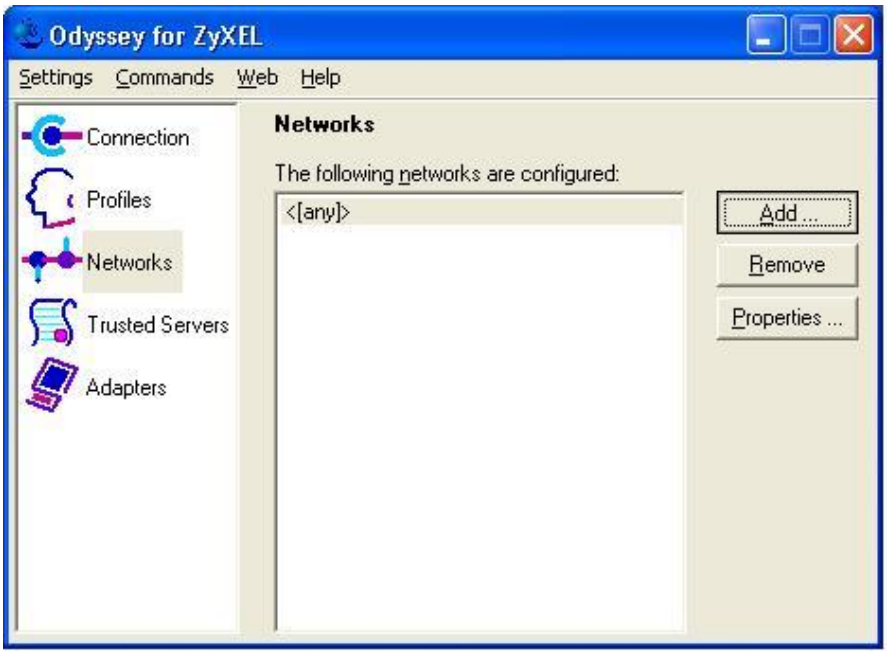
Kuva 28 Käyttäjän profiilin muokkaus

Langattoman päätelaitteen eli tässä tapauksessa työaseman konfigurointiin riittää Odyssey clientin asetusten tekeminen. Alkutilanteessa ei voi tehdä vielä mitään, koska verkkosovitinta (adapter) ei ole valittu (Kuva 29). Valinta tapahtuu Adapters-kohdasta ja sieltä Add-painiketta painamalla. Mikäli sovittimen ajurit on asennettu onnistuneesti ja laite on kytketty koneeseen, pitäisi sen olla avautuvalla listalla. Valitaan oikea sovitin ja hyväksytään OK-painikkeella (Kuva 30).

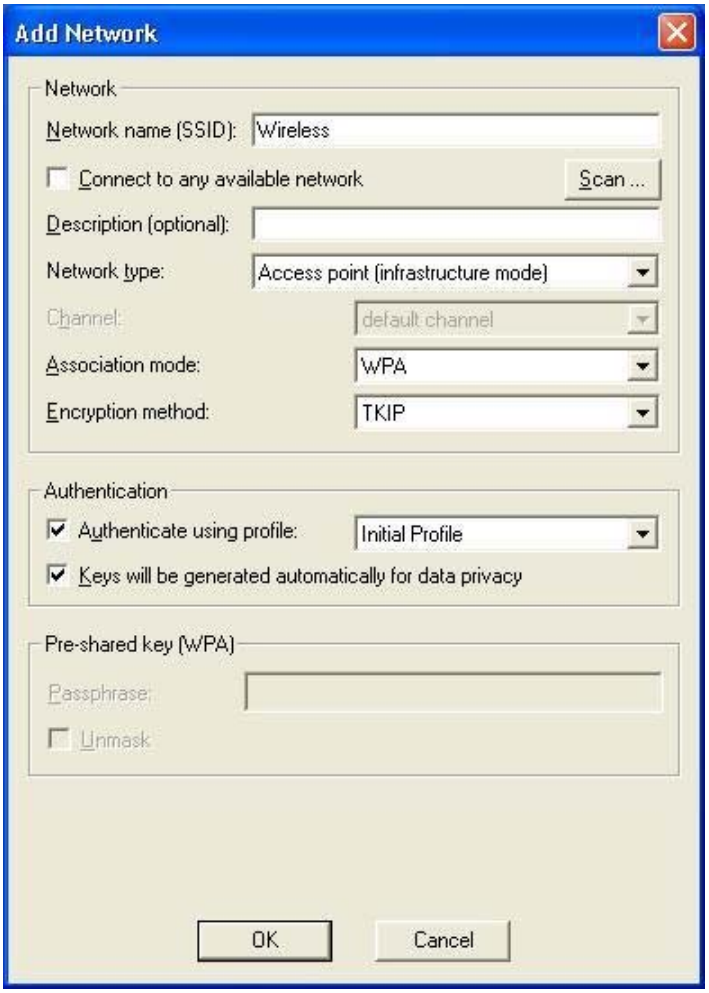
Kuva 29 Odyssey client –lähtötilanne

Kuva 30 Verkkosovittimen valinta

Seuraavaksi tehdään verkon asetukset kohdassa Networks, jossa painetaan Add-painiketta (Kuva 31). Avautuvaan ikkunaan kirjoitetaan ensiksi verkon nimi kohtaan Network name, mikäli ohjelma ei ole sitä jo löytänyt valmiiksi. Association Mode -kohtaan valitaan WPA ja sen alapuolella salausmetodiksi TKIP. Authenticate Using Profile -kohtaan laitetaan rasti ja oletusarvo Initial Profile voidaan jättää ennalleen. OK-painikkeella hyväksytään tehdyt valinnat (Kuva 32).



Kuva 31 Uuden verkon lisäys



Kuva 32 Verkon asetukset

Viimeinen vaihe Odyssey clientin ja samalla koko tämän langattoman verkon konfiguroinnissa on profiilin luominen verkkoon haluavalle käyttäjälle. Profiles-kohdassa halutaan konfiguroida alkuperäistä profiilia (Initial profile). Painetaan Properties-painiketta, jolloin avautuu ominaisuuksien User Info -välilehti. Login name -kohtaan kirjoitetaan käyttäjänimi, jolla verkkoon liitytään. Verkkoon pääsyyn vaaditaan ennalta määritetty salasana ja siksi merkitään rasti kohtaan Permit login using password. Lisäksi valitaan kohta Prompt for password, jotta ohjelma kysyy erikseen salasanaa aina kun sitä tarvitaan (Kuva 33). Authentication-välilehdeltä poistetaan ensin oletuksena oleva EAP/TTLS -autentikointiprotokolla Remove-painikkeella ja sen jälkeen lisätään Add-painikkeella avautuvalta listalta EAP/PEAP. Tehdyt muutokset hyväksytään OK-painikkeella (Kuva 34).

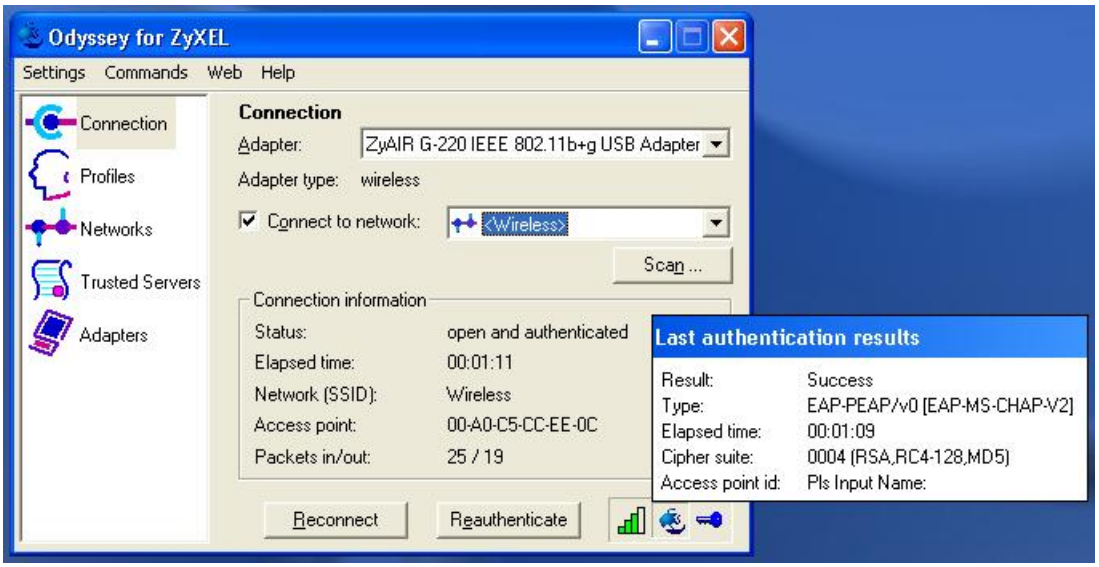
Kuva 33 Profiilin asetukset

Kuva 34 Autentikointiprotokollan valinta

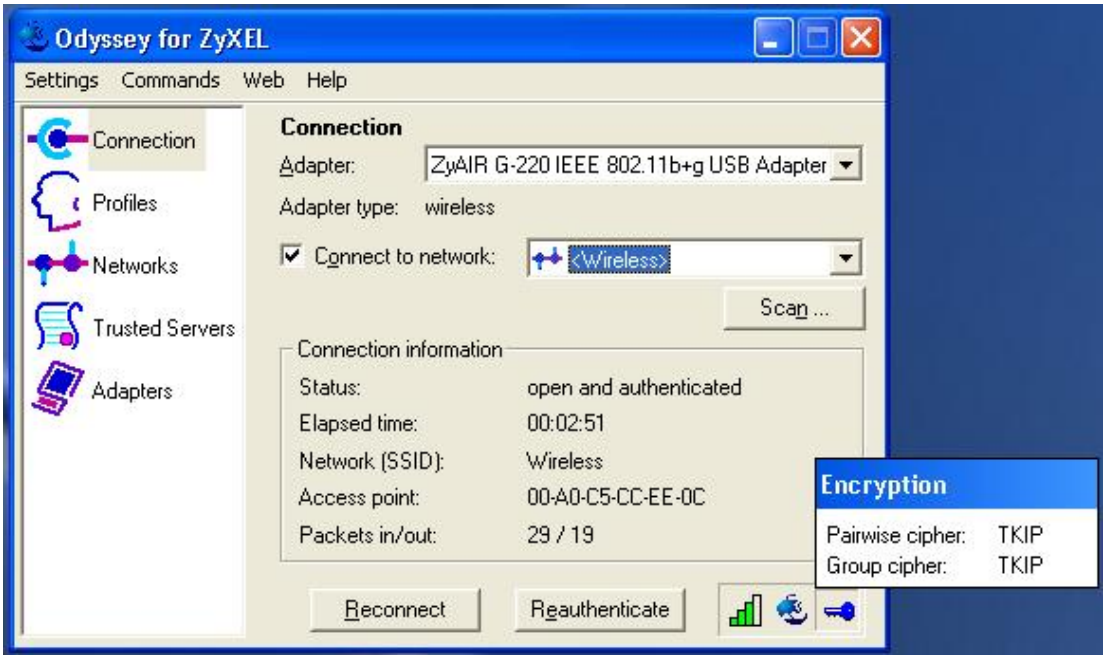
4.2.4 Toimivuuden testaus

Kun kaikki on valmista ja verkkoon koetetaan ottaa yhteys, Odyssey client -ohjelmisto tekee salasanakyselyn. Ikkunassa näkyy tarvittavat tiedot, kuten sisäänkirjautumisnimi ja verkon, johon liitytään, nimi (Kuva 35). Salasanan hyväksymisen jälkeen voidaan tulokset tarkistaa Odyssey clientin Connection-kohdassa. Oikeassa alakulmassa olevilla painikkeilla voidaan tarkistaa sen hetkisen yhteyden signaalin vahvuus, autentikoinnin tiedot ja salauksen tiedot (Kuvat 36 ja 37).

Kuva 35 Salasana verkkoon pääsemiseksi



Kuva 36 Autentikoinnin tulos



Kuva 37 Salauksen tilanne

5. Yhteenveto

WLAN-tekniikan tarkoitus on tarjota lähiverkko langattomasti, ilman kiinteää kaapelointia. Tiedonsiirto tapahtuu tällöin ilmassa perinteisen kaapelin sijaan. Langattomuus tuo mukanaan paljon mahdollisuuksia, kuten laitteiden vapaan liikuteltavuuden sekä verkon pystyttämisen nopeuden, helppouden ja edullisuuden. WLAN-verkko on mainio ratkaisu sellaisiin tilanteisiin, joissa kiinteän kaapeloinnin toteuttaminen on erittäin hankalaa tai jopa mahdotonta. Esimerkkeinä voidaan pitää kahden rakennuksen välille rakennettavaa yhteyttä tai vaikkapa toimistoa, jossa on runsaasti kannettavia tietokoneita.

Suositus langattoman verkon implementoinnille on standardiperhe IEEE802.11. Se on laajimmalle levinnyt WLAN-standardeista. Alkuperäinen versio esiteltiin jo vuonna 1990 ja sitä on sen jälkeen paranneltu useilla laajennuksilla. Työryhmät pyrkivät edelleenkin parantamaan standardin ominaisuuksia ja kehitteillä onkin useita, lähinnä tietoturvan parantamiseen keskittyviä laajennuksia.

Tietoturva (tai pikemminkin sen riittämättömyys) on ollut langattomien verkkojen yleistymisen esteenä tähän mennessä. Koska tiedonsiirto tapahtuu ilmassa, se on helposti kenen tahansa kaapattavissa, jolla tarvittavat laitteet siihen on. Kotikäyttäjälle kyseessä ei ehkä ole tärkein seikka, mutta ammattikäytössä riittävä tietoturva on monesti ehdoton edellytys teollisuusvakoilun estämiseksi. Uusimmat IEEE802.11-standardin laajennukset ovat pyrkineet ratkaisemaan näitä ongelmia, siinä hyvin jo onnistuen. Signaalia voidaan salata erilaisilla keinoilla ja verkkoon pääsyä voidaan kontrolloida käyttäjien tunnistuksella eli autentikoinnilla.

Vielä vajaa vuosi sitten WLAN-verkkojen leviämistä esti lähinnä kaistanleveyden riittämättömyys, laitteiden hintavuus ja toimimattomuus. Nyt nämä ongelmat alkavat olla jo historiaa ja tulevaisuus näyttääkin WLAN:n osalta valoisalta.

Tutkintotyön tavoite oli tutustua langattomiin lähiverkkoihin, niiden tekniikoihin, standardeihin ja positiivisiin sekä haittapuoliin. Työn tärkein osuus kuitenkin muodostui toimeksiantoni kautta, jolla oli tarkoitus rakentaa langaton lähiverkko koulun tiloihin ja liittää se tietoverkkopalvelujen WPK-verkon yhteyteen. Lisäksi oli toteutettava käyttäjien tunnistus jollakin autentikointimenetelmällä, jotta ulkopuoliset eivät pääsisi käsiksi WPK-verkkoon.

Alkuvaikeuksien jälkeen onnistuin verkon pystyttämisessä ja autentikoinnin toteuttamisessa. Autentikoinnin toteutin käyttämällä yleisesti siihen tarkoitukseen käytettyä RADIUS-palvelinta. Aikataulussa pysyminen oli tavoite alusta saakka, mutta se ei onnistunut lähinnä käytännön ongelmista, kuten uusista laitehankinnoista, johtuen. Työ oli kuitenkin mielekästä ja mielenkiintoista ja uskon lopputuloksesta olevan vielä hyötyä minulle työmarkkinoilla.

Lähteet

Barken, Lee 2004. How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN. New Jersey: Prentice Hall

Glossary of terms 2004. [online] [viitattu 23.3.2005]. www.wi-fi.org/OpenSection/glossary.asp?TID=2

Hämäläinen, Pertti 2004. 802.1x-tukiasemat. Tietokone 10 (6), 66–67

Is a Wired, Wireless or Wireless/Wired Network Best For You? 2004. [online] [viitattu 23.3.2005]. www.wi-fi.org/OpenSection/wireless_vs_wired.asp?TID=2

Kerberos: The Network Authentication Protocol 2005. [online] [viitattu 23.3.2005]. web.mit.edu/kerberos/

Muller, Nathan J. 2003. Wireless A to Z. New York: The McGraw-Hill Companies, Inc

Sikora, Axel 2003. Wireless personal and local area networks. Chichester: John Wiley & Sons Ltd

Tietoturva: tietoturvallisuuden perusteet 2001. [online] [viitattu 31.3.2005]. www.ficora.fi/suomi/tietoturva/vpn.htm

VPN Overview 2004. [online] [viitattu 30.3.2005]. ftp.zyxel.com/P334W/document/P334W_v3-60_UsersGuide.pdf

Wi-Fi Security at Work and on the Road 2004. [online] [viitattu 23.3.2005]. www.wi-fi.org/
OpenSection/secure.asp?TID=2

Liitteet

Liite 1: Lyhenteet

AES	Advanced Encryption Standard. Uusi vaikeasti murrettava salauskeino.
AP	Access Point. Tukiasema.
bps, Mbps	(Mega)bits per second. (Mega)bittiä sekunnissa. Mittayksikkö kaistanleveydestä puhuttaessa.
DHCP	Dynamic Host Configuration Protocol. Palvelu, jolla dynaamisesti jaetaan IP-osoitteita verkon työasemille.
DNS	Domain Name Service. Nimipalvelu, joka kääntää alfanumeeriset toimialuenimet vastaaviksi IP-osoitteiksi ja päinvastoin.
EAP	Extencible Authentication Protocol. Erilaisia käyttäjätunnistusmenetelmiä tukeva PPP-käytännön laajennus.
EAP-TLS	EAP Transport Layer Security. Microsoftin kehittämä varmennepohjainen käyttäjätunnistusmenetelmä.
EAP-TTLS	EAP Tunneled TLS. Funk Softwaren ja Certicomin ehdottama käyttäjätunnistusmenetelmä.
ESSID	Extended Service Set Identifier. Langattomalle verkolle asetettava nimi.
IEEE	Institute of Electrical and Electronics Engineers. Standardisointiorganisaatio.
IP	Internet Protocol. Internetin pääasiallinen tiedonsiirtoprotokolla.
LAN	Local Area Network. Lähiverkko.
MAC	Media Access Control. Jokaiselle tietoliikennelaitteelle valmistusvaiheessa annettava uniikki kahdestatoista heksadesimaalisesta numerosarjasta koostuva osoite.
MIC	Message Integrity Check. Datapaketin eheyden varmistamiseksi kehitetty menetelmä, jotta pakettia ei voitaisi muuttaa ja lähettää uudelleen.
PAE	Port Access Entity. IEEE802.1x:n käyttämä tunnistustoiminnon toteutus.
PCMCIA	Personal Computer Memory Card International Association. Tavallisesti kannettavissa tietokoneissa esiintyvä lisälaitteiden liitäntä.
PDA	Personal Digital Assistant. Käsitietokone.

PEAP	Protected EAP. Ciscon, Microsoftin ja RSA Securityn ehdottama menettely, jossa tunnistusviestit siirretään TLS-tunnelissa, eikä työasemissa tarvita var menteita.
PPP	Point-to-Point Protocol. Protokolla, jota yleisesti käytetään muodostamaan suora yhteys verkkolaitteiden välillä. Sen ensisijainen käyttökohde on ollut puhelinverkko ja modeemiyhteydet.
PSK	Pre-Shared Key. WPA-tietoturvastandardin käyttämä keino, jossa manuaalisesti syöttämällä salasana tai avain käynnistetään WPA-suojaus.
RADIUS	Remote Access Dial-In User Service. Alun perin modeemikäyttäjien tunnistamiseen kehitetty autentikointimenetelmä.
RC4	Salaus-algoritmi, jota käyttää muun muassa WEP- ja TKIP-salauskeinot.
SSID	Service Set Identifier. Langattomalle verkolle asetettava nimi.
SSL	Secured Sockets Layer. Internetissä usein käytetty protokolla salaamaan yhteyttä.
TKIP	Temporal Key Integrity Protocol. WPA-tietoturvastandardin käyttämä salauskeino.
VPN	Virtual Private Network. Etäkäyttäjille suunniteltu suojattu yhteys yrityksen sisäiseen verkkoon Internetin yli.
WEP	Wired Equivalent Privacy. WLAN:n alkuperäinen salaus- ja tietoturvakäytäntö.
WLAN	Wireless Local Area Network. Langaton lähiverkko.
WPA	Wireless Protected Access. Wi-Fi Alliancen määrittelemä tietoturvastandardi.