TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Arttu Minkkinen

VIERAILIJAVERKON RAKENTAMINEN

Työn ohjaaja Jorma Peltoniemi
Työn teettäjä Tampereen ammattikorkeakoulun tietokonekeskus
valvojana Kari Timonen

Tampere 2005

TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka
Tietoliikennetekniikka
Minkkinen, Arttu Vierailijaverkon rakentaminen
Tutkintotyö 44 sivua + 10 liitesivua
Työn ohjaaja Jorma Peltoniemi
Työn teettäjä Tampereen ammattikorkeakoulun tietokonekeskus
valvoja Kari Timonen
Huhtikuu 2005
Hakusanat vierailijaverkko, 802.1x, autentikointi, WLAN

TIIVISTELMÄ

Verkkoyhteyden tarve päivittäisessä elämässä on lisääntynyt huomattavasti viime vuosien aikana ja tarve kasvaa edelleen. Verkkoyhteydeltä vaaditaan luotettavuutta ja turvallisuutta, jotta yksityisyys nykyajan verkkoliikenteessä pystyttäisiin takaamaan.

Vierailijaverkon tehtävänä on tarjota verkkoyhteyksiä langallisesti ja langattomasti rajatulle käyttäjäryhmälle. Tässä työssä on pyritty löytämään mahdollisimman hyvä, ennen kaikkea oppilaitosympäristöön sopiva vierailijaverkko Tampereen ammattikorkeakoulun opiskelijoiden ja henkilökunnan käyttöön.

Työn teoriaosuudessa on käsitelty vierailijaverkoihin liittyviä standardeja ja menetelmiä. Ensin selvitetään langattoman lähiverkon standardeja, sen etuja ja haittoja sekä muita siihen liittyviä ominaisuuksia. Seuraavaksi kerrotaan erilaisista tietoturvaan liittyvistä standardeista ja salausmenetelmistä. Lopuksi työssä kerrotaan Tampereen ammattikorkeakoulun tietokonekeskuksen toimeksiantona suoritetusta käytännön toteutuksesta, jossa suunniteltiin ja rakennettiin vierailijaverkko ammattikorkeakoulun käyttöön.

TAMPERE POLYTECHNIC
Computer Systems Engineering
Telecommunications Engineering
Minkkinen, Arttu Building a guest network
Engineering Thesis 44 pages, 10 appendices
Thesis Supervisor Jorma Peltoniemi
Commissioning Company Computer center of the Tampere Polytechnic
Supervisor: Kari Timonen
April 2005
Keywords guest network, 802.1x, authentication, WLAN

ABSTRACT

Need for network connection in every day living has increased considerably during the last years and still increases. Demands on network connection are reliability and security, in order to be able to ensure the privacy in today's network traffic.

Guest network task is to provide network connections wired and wireless to a limited user group. In this engineering thesis has been tried to find as good guest network solution as possible for educational institution environment of Tampere Polytechnic.

In thesis theory has been handled standards and methods dealing with guest networks. After introducing the guest network are WLAN standards, its pros and cons and other features explained. In The following different data security standards and encryption methods are presented. Final section consists of the practical implementation for Tampere Polytechnic Computer center, where guest network was implemented and built for educational use.

ALKUSANAT

Olen tehnyt tutkintotyönäni vierailijaverkkoa Tampereen ammattikorkeakoulun tietokonekeskukselle. Työni on ollut haastavaa ja sen aikana olen oppinut paljon uusia asioita tehtävän aihepiiristä. Haluan kiittää koko tietokonekeskuksen henkilökuntaa, erityisesti Janne Hapuojaa, joka on auttanut minua muun muassa kaikissa lähiverkkoon liittyvissä ongelmissa. Kiitos kuuluu myös Riku Itäpurolle, jolta sain asennusapua RADIUS-palvelimen pystyttämisessä.

TTY:n tutkijaa Sami Keski-Kasaria haluan kiittää työn eri vaiheissa saamastani neuvonnasta. Kiitän Jussi Kivistä, joka työskenteli samojen asioiden parissa kesällä 2004, omien kokemustensa jakamisesta. Lopuksi haluan kiittää tutkintotyöni valvojaa Kari Timosta ja ohjaajaa Jorma Peltoniemeä.

Tampere 21.huhtikuuta 2005

Arttu Minkkinen

SISÄLLYSLUETTELO

LYHENNELUETTELO

AES – Advanced Encryption Standard

EAP – Extensible Authentication Protocol

EAPOL – EAP over LANs

EAP-TLS – EAP with Transport Layer Security

EAP-TTLS – EAP with Tunnelled TLS

ETSI – The European Telecommunications Standards Institute

CCMP – Counter mode with Cipher-Block Chaining-Message Authentication Code Protocol

CHAP – Challenge Handshake Authentication Protocol

DHCP – Dynamic Host Control Protocol

IAS – Internet Authentication Service

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

LEAP – Cisco's Lightweight EAP

MS-CHAP v2 – Microsoft Challenge-Handshake Authentication Protocol version 2

OFDM – orthogonal frequency division multiplexing

PEAP – Protected EAP

PKI – public key infrastructure

PPP – Point-to-Point Protocol

RADIUS – Remote Access Dial-in User Service

RFC – Request For Comments

RSN – Robust Security Network

SSID – Service Set Identifier

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

WEP – Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WPA – Wireless Protected Access

WRAP – Wireless Robust Authenticated Protocol

1 JOHDANTO

Vierailijaverkon avulla verkkoyhteyttä voidaan tarjota käyttäjälle langallisesti tavallisessa lähiverkossa tai langattomasti radioteitse. Verkko voidaan rajata käyttäjätietokannan sisältämiin tunnuksiin tai se voi olla kaikille avoin. Vierailijaverkkoja käytetään yleisesti julkisissa rakennuksissa, kuten lentokentillä, hotelleissa ja oppilaitoksissa.

Internet-yhteyden tarve on lisääntynyt huomattavasti viime vuosina ja vierailijaverkkojen rakentaminen julkisiin paikkoihin on näin ollen myös lisääntynyt. Päivittäisten asioiden hoitamisessa yhä useammin tarvitaan sähköpostia ja muita Internetyhteyttä käyttäviä palveluja. Vierailijaverkolla luodaan ihmisille mahdollisuus liittää oma kannettava tietokoneensa esimerkiksi työpaikan tai koulun Internetyhteyteen. Vierailijaverkko toimii yleensä erillään muusta verkosta. Tällöin on useasti jokin järjestelmä, jonka avulla sisäverkon palveluita päästään käyttämään.

Langattoman verkon tuoma liikkumisen vapaus tuo mukanaan myös ongelmia. Tiedonsiirto täytyy pystyä salaamaan hyvin, jotta päästään turvallisen langattoman tiedonsiirron edellyttämälle tasolle. Työssäni selvitetään, miten tarvittava tietoturva saadaan aikaiseksi.

Opinnäytetyössäni käsitellään useita standardeja, jotka liittyvät langattomaan lähiverkkoon ja vierailijaverkkoon. Lisäksi kerrotaan myös tietoturvaa parantamaan luoduista standardeista, kuten IEEE 802.1x:stä sekä erilaisista EAP- variaatioista.

Opinnäytetyöni teorian lisäksi työssä käsitellään langattoman vierailijaverkon käytännön toteutusta Tampereen ammattikorkeakoulussa 2004–2005.

2 VIERAILIJAVERKKO

Vierailijaverkolla tarkoitetaan verkkoa, jonka kautta saa pääsyn Internetiin ja tarvittaviin palveluihin. Suomessa maksullisia vierailijaverkkoja on tällä hetkellä käytössä ainakin DNA Finlandilla ja TeliaSoneralla. Näitä verkkoja yritykset kutsuvat Hotspot-nimellä. Palvelu perustuu lentokentillä, hotelleissa, rautatieasemilla, areenoilla ym. julkisissa paikoissa oleviin WLAN-tukiasemiin. Asiakas pystyy hyödyntämään tietoliikenneyhteyksiä em. paikoissa hankkimalla käyttöönsä joko palveluliittymän tai ostamalla itse käyttöaikaan perustuvan ns. raaputuskortin, josta ilmenevät kertakäyttöinen käyttäjänimi ja salasana. Palvelun käytön edellytyksenä on, että asiakkaan koneeseen on asennettu langaton verkkokortti. Liittymän hinta muodostuu avausmaksun ja kuukausimaksun lisäksi liittymätyypin mukaan joko minuuttilaskutuksesta tai käyttömäärästä megabitteinä. /20/

Vierailijaverkkoja voidaan rakentaa myös esimerkiksi oppilaitoksiin, joissa verkon käytöstä ei peritä maksua. Verkon käyttöoikeudet rajataan yleisesti oppilaitoksessa työskenteleviin ja opiskeleviin henkilöihin, joilla on jo käyttöoikeudet oppilaitoksen muuhun verkkoon. Vierailijaverkko voidaan toteuttaa langallisena tai langattomana. Molemmilla vaihtoehdoilla on omat hyvät ja huonot puolensa.

Langallisen version etu on hyvä tietoturva. Langallisessa vierailijaverkossa ei tarvitse välttämättä käyttää vahvinta mahdollista suojausta, koska siinä vaaditaan kuitenkin pääsy rakennukseen ja vierailijaverkossa olevan ATK-rasian luo. Huonona puolena taas on sidottu paikka, jolloin liityntäpisteen luota ei voida liikkua kovin kauas.

Langattoman version hyvänä puolena taas on liikkumisen vapaus, jolloin vierailijaverkkoon voidaan liittyä mistä vain verkon kantaman rajoissa. Langattomuus tuo myös tietoturvan tärkeämmäksi osaksi luotettavaa tiedonsiirtoa kuin langallisessa verkossa. Langatonta verkkoa ei voida tarkkaan rajata kattamaan esimerkiksi vain pelkkiä sisätiloja, jolloin langattomaan verkkoon on myös mahdollista päästä rakennusten ulkopuolelta. Jotta verkon laiton käyttö saadaan estettyä, voidaan käyttää vahvoja salausmenetelmiä ja autentikointia. Näistä kerron enemmän luvussa neljä.

3 WLAN

WLAN-verkolla tarkoitetaan langatonta lähiverkkoa, jossa yhteys tukiasemaan tai toiseen langattomaan laitteeseen muodostetaan radiotaajuuksia käyttäen. Langattomia lähiverkkoja käytetään yleisesti paikoissa, joihin langallista verkkoa on vaikea tai mahdoton rakentaa.

IEEE (Insititute of Electrical and Electronic Engineering) perusti projektin langattomien lähiverkkojen standardoimiseksi, koska aiemmin esitellyt kaupalliset toteutukset olivat hyvin häiriöille alttiita ja kuluttajille liian kalliita. Nykyisin suurin osa langattomista lähiverkoista onkin toteutettu juuri IEEE:n 802.11–standardeja käyttäen. /8/

802.11 on Yhdysvalloissa kehitetty standardi ja sen kilpaileva eurooppalainen standardi on HIPERLAN. HIPERLAN on ETSI-organisaation (The European Telecommunications Standards Institute) aikaansaannos ja siitä kerrotaan lisää myöhemmin tässä luvussa. Tässä työssä käsitellään pääasiassa 802.11-standardeja, koska HIPERLAN ei ole saavuttanut samanlaista suosiota kuin IEEE:n toteutus ja näin ollen laitetuki on paljon suppeampi HIPERLANissa. /8/

3.1 WLAN-verkon etuja

Langattomalla verkolla on paljon ominaisuuksia, joita langallinen verkko ei pysty koskaan tarjoamaan. Liikkuvuus tulee tärkeäksi asiaksi, kun puhutaan nimenomaan langattomista verkoista. Langallisessa verkossa joudutaan olemaan kaapelilla kytkettynä verkkorasiassa, jolloin etäisyys rajoittuu kaapelin pituuteen. Langattomassa verkossa etäisyys ei ole ongelma niin kauan, kun signaalin laatu pysyy edes kohtuullisena. Nykyaikaiset verkot kykenevät vähentämään nopeutta ja lisäämään lähetystehoa saadakseen kuuluvuuden mahdollisimman kauas. Lisäksi uusissa tukiasemissa tuetaan palvelua nimeltä roaming, josta kerrotaan lisää myöhemmin tässä luvussa.

Langattoman lähiverkon yksi merkittävimmistä eduista on varmasti sen nopea pystyttäminen toimintaan, jota tarvitaan lähinnä väliaikaisissa ratkaisuissa, kuten messuilla ja erilaisissa tapahtumissa sekä paikoissa, joihin johtoja ei voida erinäisistä syistä vetää, esimerkkinä historialliset kohteet.

Pidemmät etäisyydet ja esimerkiksi vesistöjen ylitykset ovat halvempia toteuttaa langattomasti, mikäli ei välttämättä tarvita 100–1000 megabitin nopeuksia. Suuntaantenneja käytettäessä voidaan helposti päästä kymmenien kilometrien yhteysetäisyyksiin.

3.2 WLAN-verkon haittoja

Monien etujen lisäksi langattomuus tuo mukanaan myös ongelmia. Yksi asia on ajureiden puutteellisuus, jolloin kaikkia käytettäviä ominaisuuksia ei pystytä käyttämään. Laitteet yritetään saada mahdollisimman nopeasti markkinoille ja yleensä kunnolla toimivat ajurit tahtovat monilla valmistajilla jäädä tekemättä. Uusien ominaisuuksien mukanaan tuomat ongelmat lisäävät myös ylläpitäjien työtä.

Jaettu taajuusalue, jota langattomat verkot käyttävät, on myös ongelma. Samalla taajuudella toimivat laitteet häiritsevät toisiaan. Langattomien lähiverkkojen kanssa samalla taajuusalueella toimivat muun muassa mikroaaltouuni ja erilaiset Bluetoothia käyttävät laitteet. Osa langattomien lähiverkkojen standardeista käyttää korkeampaa taajuutta, jolla ei ole niin paljon häiritseviä laitteita. Korkeampi taajuus taas lyhentää verkon kantamaa, jolloin tukiasemia tarvitaan enemmän saman alueen kattamiseksi kuin alemmalla taajuudella toimivien tukiasemien kanssa.

3.3 Langattoman verkon standardit

802.11 on IEEE:n standardoima tuoteperhe langattomille lähiverkoille. Tuoteperheeseen kuuluu tällä hetkellä neljä langattomaan tiedonsiirtoon liittyvää standardia.

Lisäksi käytössä on tiedonsiirron laadun parantamiseen sekä muihin tärkeisiin ominaisuuksiin, kuten tietoturvaan liittyviä standardeja.

ETSI on julkaisut kaksi HIPERLAN-standardia HIPERLAN/1:n ja HIPERLAN/2:n, joiden lisäksi sillä on laajennuksia uudempaan HIPERLAN-standardiin.

3.3.1 802.11

Vuonna 1997 valmistui IEEE:n ensimmäisen langattoman lähiverkon standardi 802.11. Standardi tukee maksimissaan 2 Mb:n siirtonopeutta. 802.11 käyttää ISM-taajuutta (Industrial Scientific Medicine), joka toimii 2.4 - 2.4835 GHz:n taajuusalueella. Standardissa määriteltiin kolme fyysisen tason menetelmää: suorasekvenssi (DSSS), taajuushyppely (FHSS) ja infrapuna. Lisäksi standardissa määriteltiin verkkotyypit ad-hoc ja infrastruktuuri. /15/

Hitaan siirtonopeutensa vuoksi 802.11 ei yleistynyt verkkomarkkinoilla, niinpä alkuperäisiä 802.11-tuotteita ei ole valmistettu enää vähään aikaan. /15/

3.3.2 802.11a

IEEE:n parannus 802.11-standardiin vuonna 1999 toi mukaan kaksi uutta standardia, 802.11a:n sekä 802.11b:n. 802.11a tukee maksimissaan 54 Mb:n siirtonopeutta, jolla todellisuudessa päästään 30–40 Mb:n siirtonopeuteen. 802.11a käyttää Euroopassa taajuuksia 5,15 - 5,35 ja 5,470 - 5,725 GHz. Tälle taajuusalueelle tarkoitetuille 802.11a-laitteille on asetettu tehorajoituksia useissa Euroopan maissa ja joissakin maissa käyttö on kielletty kokonaan, mikä osaltaan on myös hidastuttanut standardin yleistymistä. /15/

802.11a onkin suunnattu lähinnä yrityskäyttöön jo pelkästään korkeahkon hinnan takia. 802.11a perustuu OFDM-kanavanjakotekniikkaan, joka sallii suuremman maksimisiirtonopeuden muihin standardeihin nähden sekä enemmän yhtäaikaisia

käyttäjiä. Lisäksi 5 GHz:n taajuusalueella ei ole yhtä paljon häiriölähteitä kuin alemmalla 2,4 GHz:n ISM-taajuusalueella. Tosin myös langattoman verkon kantavuus on lyhyempi kuin alemmalla taajuusalueella. /12/

Eräät laitevalmistajat ovat tehneet tukiasemia, jotka tukevat sekä 802.11b- että 802.11a-standardeja. Tukiasema sisältää kaksi erillistä radiota, toisen 802.11a:n langattomalle verkolle ja toisen 802.11b:n langattomalle verkolle. Verkot toimivat rinnakkain eri taajuusalueilla. /15/

3.3.3 802.11b

802.11b tukee 11 Mb:n siirtonopeutta ja se käyttää samaa ISM-taajuuskaistaa kuin alkuperäinen 802.11-standardi.

ISM-taajuuskaista on vapaasti käytettävissä ja kyseisille taajuuksille saa kuka tahansa rakentaa laitteen. Yleisimpiä tätä taajuusaluetta käyttäviä laitteita ovat kuitenkin mikroaaltouunit, langattomat puhelimet ja Bluetooth-laitteet. Nämä laitteet saattavat häiritä toisiaan, jos niiden etäisyys toisistaan ei ole riittävän pitkä.

Kuten muutkin 802.11-standardit, 802.11b:kin käyttää Ethernet-protokollaa ja CSMA/CA:ta kanavan jakoon. Lisäksi 802.11b:ssä käytetään CCK-modulaatiota. /15/

3.3.4 802.11h

802.11h on uusi kehitysversio 802.11a:lle langattomaan lähiverkkoperheeseen. 802.11h:lla on tarkoitus ratkaista 802.11a:n käytössä havaittuja yhteensopivuusongelmia, erityisesti sotilas- ja sairaalalaitteiden kanssa. Lisäksi Euroopassa on tarkat vaatimukset 5 GHz:n taajuusalueella toimivien laitteiden kanssa.

Säännöt 802.11h:ta varten ITU:n esittäminä. 802.11h:ssa tuli kaksi uudistusta minimoimaan epäsovitusta. Ensimmäinen uudistus on dynaaminen kanavan valinta, DFS, joka havaitsee ja muuttaa kanavaa automaattisesti, jos toinen laite toimii samalla kanavalla toisen kanssa. Toinen uudistus on lähetystehon säätö, TPC, joka säätää lähetystehoa automaattisesti siten, että kauimmainen käyttäjä pysyy vielä kuuluvuusalueella. /19/

3.3.5 802.11d

802.11d liittyy h-standardiin kiinteästi. Standardi antaa laitteille mahdollisuuden neuvotella käytettävät taajuuskaistat sopiviksi jokaiselle maalle erikseen. Se tarkoittaisi sitä, että WLAN-kortti osaisi automaattisesti virittäytyä kunkin maan tarjoamille taajuuksille. WLAN-kortti osaisi lukea tiedot suoraan siltä tukiasemalta, johon se ottaa yhteyden. /15/

3.3.6 802.11g

Vuonna 2003 julkaistiin tällä hetkellä viimeisin WLAN-standardi, 802.11g. 802.11g:ssä yhdistyvät 802.11b:n pidempi kantomatka ja 802.11a:n siirtonopeus. 802.11g:n tiedonsiirtonopeus on 54 Mb ja se käyttää ISM-taajuuskaistaa, jonka avulla langattoman verkon kantavuutta saadaan pidennettyä. 802.11g on yhteensopiva 802.11b:n kanssa, joten 802.11g-tukiaseman kanssa toimivat 802.11b:n langattomat verkkokortit ja vastaavasti 802.11b-tukiaseman kanssa toimivat 802.11g:n langattomat verkkokortit.

802.11g perustuu myös OFDM-modulaatioon, jossa käytetään useita kantoaaltoja, joihin moduloitava signaali jaetaan. Tällä mahdollistetaan suurempi siirtonopeus muihin standardeihin nähden.

3.3.7 802.11e

802.11e lisää palveluntason (QoS) sekä multimediatuen olemassa oleviin 802.11b- ja 802.11a-standardeihin. Näitä tarvitaan langattomissa verkoissa, joissa siirretään viivekriittistä tietoa, kuten ääntä, esimerkiksi VOIPilla ja kuvaa. /18/

3.3.8 802.11f

802.11f parantaa e-version tavoin laitteiden ominaisuuksia. F-version tarkoituksena on parantaa eri valmistajien laitteiden välistä yhteensopivuutta. /17/

3.3.9 802.11n

802.11n on noin kymmenen kertaa nykyistä langatonta standardia nopeampi. 802.11n yltäisi parhaimmillaan 540 megabitin sekuntinopeuteen. /10/

Ongelmia aiheuttaa Wi-fi Alliance, joka on ilmoittanut, ettei se sertifioi laitteita, jotka käyttävät 802.11n-teknologiaa ennen kuin IEEE on hyväksynyt standardin. /6/

Standardin odotetaan valmistuvan vuonna 2006, mutta ennen sitä luultavasti nähdään standardia tukevia laitteita. Ensimmäisen version on tarkoitus olla valmis kesällä 2005. /10/

Käytettävistä ratkaisuista yritykset ovat esitelleet ehdotelmia ja ne ovat sopineet yhteen aikaisempien tekniikoiden kanssa. 802.11n-pohjaisissa tukiasemissa nähdään monitie-etenemistä hyödyntävää antennitekniikkaa. Niissä on vähintään kaksi lähetysantennia ja kaksi vastaanottavaa antennia kaistanleveyden lisäämiseksi ja ne käyttävät 20 MHz:n kanavaa. /10/

Ehdotelmat sisältävät myös mahdollisuudet lisätä antennien määrä neljään ja käyt-

tää 40 MHz:n kanavaa. Tämä vaihtoehto mahdollistaa viidensadan megabitin sekuntinopeudet. /10/

3.3.10 HIPERLAN

HIPERLAN (High Performance Radio Local Area Networks) on ETSI:n standardoima langaton lähiverkkostandardi. HIPERLANilla on kaksi valmista standardia ja muutama lisämääritelmä olemassa oleviin standardeihin.

3.3.10.1 HIPERLAN/1

ETSI aloitti WLAN-standardinsa kehittämisen vuonna 1991. Ensimmäinen HIPERLAN-standardi julkaistiin vuonna 1998. Standardin käyttämä radiotaajuus on 5 GHz ja maksimi yhteysnopeus on 23,5 Mbps. HIPERLAN/1 käyttämät viisi kanavaa sijoittuu taajuusalueelle 5,15–5,30 Ghz. /2/

3.3.10.2 HIPERLAN/2

ETSI julkaisi HIPERLAN/2-standardin vuonna 2000. HIPERLAN/2 tarjoaa edeltäjäänsä verrattuna uusia ominaisuuksia, kuten verkon entistä paremman tietoturvan, nopeammat verkkoyhteydet ja aikakriittisyyden. HIPERLAN/2 käyttää 5 GHz:n taajuutta kuten aikaisempi versiokin, mutta maksiminopeus on lisätty 54 Mbps:iin. /3/

Peruspalveluina HIPERLAN/2:ssa on datan, äänen ja videon siirto. Standardi määritellään tiedonsiirto-aikakriittiseksi niin, että suurempaa nopeutta tarvitsevat yhteydet saavat käyttöönsä enemmän kaistaa. Tämä on hyödyllinen ominaisuus siirrettäessä reaaliaikaista videota ja puhetta. /3/

HIPERACCESS on suunniteltu pitkän kantaman point-to-multipoint-ratkaisuksi. HIPERACCESS-nopeus on tyypillisesti 25 Mbit/s:ssa. HIPERACCESSia on suunniteltu käytettäväksi UMTS-, ATM- ja IP-pohjaisten verkkojen jatkeena. Taajuusalueeksi HIPERACCESSille kaavaillaan 40,5-43,5 GHz:ä. /3/

HIPERLINK on suunniteltu lyhyen kantaman nopeaksi protokollaksi. Siinä käytetään HIPERLANia ja HIPERACCESSia. Mahdollinen 155 Mbit/s:n maksiminopeus voidaan saavuttaa vielä 150m:n päästä tukiasemasta. HIPERLINKin käyttämä taajuuskaista on 17GHz. /3/

3.4 Roaming

Langattoman lähiverkon yhtenä etuna pidetään liikkuvuutta. Jos käytössä on ainoastaan yksi tukiasema, ongelmaa ei tule, kun pysytään verkon kantaman sisäpuolella. Usean tukiaseman tapauksessa tarvitaan ominaisuutta, jolla onnistutaan siirtämään yhteys tukiasemalta toiselle yhteyden katkeamatta. Tätä ominaisuutta kutsutaan nimellä roaming.

Kuuluvuuden heiketessä tukiasemaan tarpeeksi alkaa clientin langaton verkkokortti etsiä muita paremmin kuuluvia tukiasemia. Mikäli paremmin kuuluva tukiasema löydetään, lähetetään yhteydenmuodostuspyyntö uudelle tukiasemalle. Jos pyyntö hyväksytään, siirretään liikenne kulkemaan voimakkaammin kuuluvan tukiaseman kautta. Tästä muutoksesta ilmoitetaan kiinteälle verkolle, joka purkaa vanhan yhteyden aiempaan tukiasemaan. /15/

Roaming-ominaisuutta käytettäessä tarvitaan langallista verkkoa, koska tukiasemien väliset yhteydet on toteutettu kiinteän verkon välityksellä. WLAN-standardeissa määritellään joitakin roamingia koskevia sääntöjä, jotka langallisen verkon tulee toteuttaa. /15/

3.5 WLAN-verkon topologiat

WLAN-verkko voidaan rakentaa joko tukiasemalla tai ilman sitä. Jos käytössä ei ole tukiasemaa, on kyseessä Ad-Hoc-verkko. Jos taas tukiasema on liitetty osaksi verkkoa, käytössä on infrastruktuuriverkko.

3.5.1 IBSS-verkko

Verkon laitteiden koostuessa ainoastaan langattomilla verkkokorteilla varustetuista tietokoneista puhutaan Ad-Hoc-verkosta eli tilapäisverkosta. Verkosta käytetään myös nimitystä IBSS (Independent Basic Service Set). Verkkoa käytettäessä ei tarvita lainkaan tukiasemaa. Tästä on kuitenkin omat haittapuolensa, sillä ilman tukiasemaa tietokoneiden välinen kantama ei ole kovinkaan suuri, koska kaikkien verkossa olevien tietokoneiden pitää olla yhteydessä toisiinsa. /12/

Ad-Hoc on hyödyllinen ratkaisu pienissä tiloissa, koska verkko tietokoneiden välillä saadaan rakennettua nopeasti ja vaivattomasti. Ad-Hoc-verkkoja käytetäänkin yleisimmin erilaisissa neuvottelu- ja kokoustilanteissa, joissa kaikki verkon käyttäjät ovat samassa tilassa. /12/

Kuva 1. Ad-Hoc/IBSS-verkko. /12/

3.5.2 Infrastruktuuriverkko, BSS

Infrastruktuuriverkossa on ainakin yksi tukiasema langattomien tietokoneiden lisäksi. Yhden tukiaseman tapauksessa käytetään nimitystä BSS (Basic Service Set). BSS-verkot ovat yleisiä kodeissa ja pienissä toimistotiloissa. Tässä verkossa on käytössä ainoastaan yksi tukiasema, jonka kautta tietokoneet ovat yhteydessä lähiverkkoon. Tukiaseman avulla kantama saadaan pidennettyä jopa kaksinkertaiseksi verrattuna IBSS-verkkoon. /12/

Kuva 2. Infrastruktuuriverkko, BSS /12/

3.5.3 Infrastruktuuriverkko, ESS

BSS-verkko muuttuu ESS-verkoksi (Extended Service Set), kun aliverkon muodostaa useampi kuin yksi BSS-verkko. Se tarkoittaa sitä, että tukiasemia on kaksi tai useampia. Yleensä tukiasema on yhteydessä langalliseen verkkoon, mutta on myös mahdollista yhdistää tukiasemat langattomasti toisiinsa, jolloin kuormitetaan enemmän tukiasemia, joista on yhteys langalliseen verkkoon. Tämä toteutus toimii hyvin, kun käyttäjämäärät ovat pienet, mutta käyttäjien määrän kasvaessa suureksi solmukohdat ruuhkautuvat ja aiheuttavat mahdollisesti nopeuden alenemista. Tosin tällainen tilanne on varsin harvinainen, koska hidastumiseen tarvitaan monen käyttäjän maksiminopeuden hyödyntäminen yhtaikaa. /12/

Kuva 3. Infrastruktuuriverkko, ESS /12/

4 VIERAILIJAVERKON TIETOTURVA

Tietoturva on nykyään tärkeä asia aina, kun uusia verkkoratkaisuja suunnitellaan. Verkoista pitää saada mahdollisimman turvallisia aiheuttamatta liikaa lisäongelmia, kuten siirtonopeuden hidastumista ja verkon monimutkaistumista. Langallisessa käytössä vierailijaverkon tapauksessa tämä ei ole niin suuri ongelma. Siinä tarvitaan kuitenkin aina fyysinen yhteys verkkoon, eli kaapeli pitää päästä kytkemään verkkorasiaan. Lisäksi yhteyttä ei pysty ilman fyysistä verkkoyhteyttä kukaan kuuntelemaan. Käyttäjän tunnistuksen tapahtuessa samalla tavalla kuin langattomassakin verkossa, voidaan langallista vierailijaverkkoa pitää turvallisena vaihtoehtona ilman mitään epäilyksiä.

Langattomat verkot ovat yleistyneet parin viimeisen vuoden aikana runsaasti. Laitteiden käyttöönotto on tehty todella helpoksi, mikä heikentää langattoman verkon tietoturvaa. Perusasetuksilla tukiasemissa ei ole yleensä mitään salausta ja näin ollen kuka tahansa pääsee verkkoon käsiksi ilman minkäänlaisia salasanoja. Jotta langattoman verkon luvaton käyttö pystytään estämään, pitää tukiasemat aina konfiguroida asianmukaisella käyttökohteen vaatimalla tavalla.

Langattomassa vierailijaverkossa käytettyihin tietoturvaominaisuuksiin on tullut monia parannuksia. Näistä mainittakoon tässä WPA, 802.1x ja 802.11i. 802.1x:ää

tosin käytetään myös langallisessakin verkossa, eikä se ole siis pelkästään langattoman verkon standardi. Uusilla menetelmillä langattomasta verkosta saadaan oikein toteutettuna ja käytettynä hyvin turvallinen verkko.

4.1 Verkon salaaminen

Ensimmäinen askel entistä turvallisempaan langattomaan verkkoon on ottaa tukiasemien SSID:n mainostus pois päältä. Tämä vähentää heti ei-toivottuja yhteysyrityksiä, kun kannettava tietokone tai kämmentietokone ei havaitse verkkoa automaattisesti. Myös verkon tunnukseksi kannattaa valita tarpeeksi pitkä sana, jotta sitä ei helposti voi arvata. SSID ei ole siis mikään salausmenetelmä, vaan sen avulla voidaan erotella langattomat verkot toisistaan. Verkko voidaan tosin löytää käyttämällä erillisiä skanneri-ohjelmia.

4.2 WEP (Wired Equivalent Privacy)

Langattoman verkon salaamisen lisäksi täytyy lähetettävä informaatio kryptata. Yksi tavoista on käyttää WEP-salausta. WEP käyttää tiedon salaamiseen RC4-algoritmia.

WEPissä salaisen avaimen koko on perinteisessä versiossa 40 bittiä ja laajennetussa versiossa 104 bittiä. Salainen avain yhdistetään 24-bittiseen alustusavaimeen, jolloin tulokseksi saadaan 64- tai 128-bittinen avain. Tämä alustusavaimen liittäminen salaiseen avaimeen tehdään jokaisen salattavan paketin yhteydessä, jotta jokaiselle paketille saataisiin samasta salaisesta avaimesta huolimatta erilainen RC4-avain. /13/

WEP-salauksen julkaisemisen jälkeen oletettiin, että langaton verkko saadaan kyseistä salausta käyttämällä yhtä turvalliseksi kuin langallinenkin verkko. Myöhemmin salauksesta on löytynyt kuitenkin suuria puutteita, jotka mahdollistavat verkon käytön salauksesta huolimatta.

Yksi WEP-protokollan haavoittuvuuksista liittyy alustusavaimeen. Yleensä salaista WEP-avainta harvoin vaihdetaan, minkä takia alustusavain varmistaa sen, että koko RC4-avain olisi jokaisella lähetyskerralla erilainen. Salausavaimen erilaisuus on tärkeää, sillä samoilla salausavaimilla salattujen kahden paketin purkaminen on mahdollista, jos liikenteestä pystytään eristämään salattuja sanomia niin, että tiedetään myös niiden selväkielinen merkitys. Alustusavaimen kierrätyksessä on kuitenkin heikkouksia, sillä WEP-määrittelyssä on vain suositus alustusavaimen vaihtamisesta jokaiselle paketille. Toisaalta alustusavaimen pituuden ollessa vain 24 bittiä, se mahdollistaa uniikkien salausavaimien riittämisen ainoastaan noin puoleksi päiväksi, minkä jälkeen samat avaimet alkavat toistua. /13/

Nykyään WEP-salaus ei ole enää riittävä, eikä sitä voi enää ensisijaisesti suositella käytettäväksi langattomissa verkoissa. Ainoastaan riittävän usein tehdyllä salausavaimen vaihdolla verkosta saadaan hieman turvallisempi, mutta se lisää taas ylläpidon tehtäviä.

4.3 WPA (Wireless Protected Access)

WPA kehitettiin paikkaamaan WEPin vakavia tietoturva-aukkoja odoteltaessa vielä vahvempaa suojausmenetelmää, 802.11i:tä. WPA on yhteensopiva myös vanhempien laitteiden kanssa pelkällä ajureiden päivityksellä.

WPA:sta on tarjolla kaksi eri versiota: yritysversio, joka perustuu autentikointipalvelimeen sekä koteihin ja pienyrityksiin tarkoitettu jaettuun salasanaan perustuva salausmenetelmä, WPA-PSK. Autentikointipalvelinta käytettäessä mitään salausavaimia ei syötetä tukiasemaan tai verkkokortille, koska jokaiselle istunnolle annetaan oma salausavain. WPA:ssa käytetään 128-bittistä TKIP-salausta (Temporal Key Integrity Protocol), joka salaa liikenteen RC4-algoritmilla. WEP-salauksessa havaitut heikkoudet on korjattu WPA:han. Lisäksi dynaaminen avainten hallinta tuo turvallisuutta, koska kiinteitä salausavaimia ei ole. /15/

Kodeissa ja pienyrityksissä autentikointipalvelimeen investointi ei välttämättä ole kannattavaa. WPA-salausta voidaan kuitenkin käyttää. WPA-PSK (Pre-Shared

Key) perustuu nimensä mukaan jaettuun salasanaan. Muilta osin WPA-PSK on yritysversion veroinen. /15/

4.4 802.11i

802.11i on IEEE:n uusi tietoturvastandardi, joka tunnetaan myös nimellä WPA2.

802.11i mahdollistaa uuden AES-tietoturvaprotokollan käytön langattomissa 802.11-verkoissa. 802.11i-standardin mukaisia langattomia verkkoja kutsutaan RSN-verkoiksi.

Standardissa käytetään 802.1x:n mukaista todentamista ja avainten hallintaa, lisäksi on myös mahdollista käyttää koteihin ja pienyrityksiin tarkoitettua 802.11i-PSK:ta, joka perustuu WPA-PSK:n tavoin jaettuun avaimeen. Lisäksi standardissa on parannetut tiedonsalausmenetelmät. Salaukseen voidaan käyttää kolmea eri menetelmää: TKIP:tä, WRAP:tä ja CCMP:tä. RSN-verkoissa kaksisuuntainen todentaminen ja yksilöllisten avainten käyttö on mahdollista myös Ad-Hoc-tilassa, kun aiemmin kaksisuuntainen todentaminen oli saatavilla vain infrastruktuuritilassa oleviin verkkoihin. /1/

TKIP:llä saadaan vaihtoehdoista heikoin salaus käyttöön, mutta sen avulla säilytetään yhteensopivuus vanhempien laitteiden kanssa. Tämä kuitenkin edellyttää, että laitteet on päivitetty.

WRAP ja CCMP käyttävät salaukseen kehittyneempää 128-bittistä AES-algoritmia. AES-algoritmin käyttäminen vaatii muutoksia laitteiston toteutukseen eikä sitä voida pelkällä ohjelmistopäivityksellä ottaa käyttöön. TKIP sisältää 128-bittisen WEP-salauksen, pakettikohtaisten avainten käytön ja MIC-tarkistussumman. WPA:n yhteydessä toteutettu TKIP on vastaava kuin IEEE 802.11i -standardiin tuleva. 802.11i:n kanssa käytettäväksi soveltuvat kaikki EAP-protokollat, joissa on toteutettuna dynaaminen avainten hallinta. /1/

4.5 AES

AESin Rijndael-algoritmi valittiin seuraavan sukupolven salausalgoritmiksi korvaamaan nykyisiä heikompia salauksia. Algoritmia vastaan kehitetään jatkuvasti uusia hyökkäyksiä, ja etenkin algebrallisten hyökkäysten toimivuuden mahdollisuuksia tutkitaan tarkasti. Yhtään todistetusti toimivaa hyökkäystä ei ole vielä tähän päivään mennessä ilmoitettu, joten voidaan olettaa, että AES-algoritmin myötä langattomissa lähiverkoissa päästään entistä lähemmäksi langallisen verkon tietoturvatasoa. /1/

AES eroaa toiminnaltaan täysin RC4-algoritmista. AES on symmetrinen lohkosalausalgoritmi, joka pystyy käyttämään eripituisia avaimia. Avainvaihtoehtoina ovat 128-, 192- ja 256-bittinen. IEEE 802.11i-standardin yhteydessä käytetään 128-bittistä salausta. RC4-algoritmiin verrattuna AESin vaatima laskentateho ja siitä aiheutuva otsikkokuorma on suurempi. Suuremmasta laskentateho vaatimuksesta johtuen AESin käyttö vaatii laitteistolta rautakiihdytystä. Siten sen käyttöönotto vaatii laitteiden uusimista, eikä näin ollen pelkkä softan vaihto riitä. /1/

4.6 Autentikointi

Autentikoinnilla tarkoitetaan tunnistusta ja langattoman lähiverkon tapauksessa nimenomaan käyttäjän tunnistamista. Autentikointia tarvitaan langattomissa lähiverkoissa, jotta käyttäjät voidaan tunnistaa ennen verkkoon pääsyä. Alkuperäinen langattomien lähiverkkojen määrittely toi mukanaan autentikointi-protokollan WEP. Kuten edellisistä kappaleista on saatu lukea, on WEP osoittautunut melko heikoksi, ja myös salasanojen jakaminen on muodostunut ongelmaksi. Monissa paikoissa WEPiä käytettiin ja käytetään edelleen jaetulla avaimella, eli kaikilla käyttäjillä on sama salasana, jolloin se ei ole enää niin salainen. IEEE on määritellyt 802.1x-protokollan 802-lähiverkoissa käytettäväksi. 802.1x:n suurin etu on siinä käytettävä EAP-protokolla, joka tukee RADIUSta. RADIUS-palvelimen avulla WLAN-palvelussa ei tarvitse käyttää erillisiä käyttäjätunnuksia, joten hallinta helpottuu niiden osalta. 802.1x:ää voidaan käyttää myös langallisten lähiverkkojen kanssa, jolloin niidenkin autentikointi voidaan suorittaa samalla protokollalla.

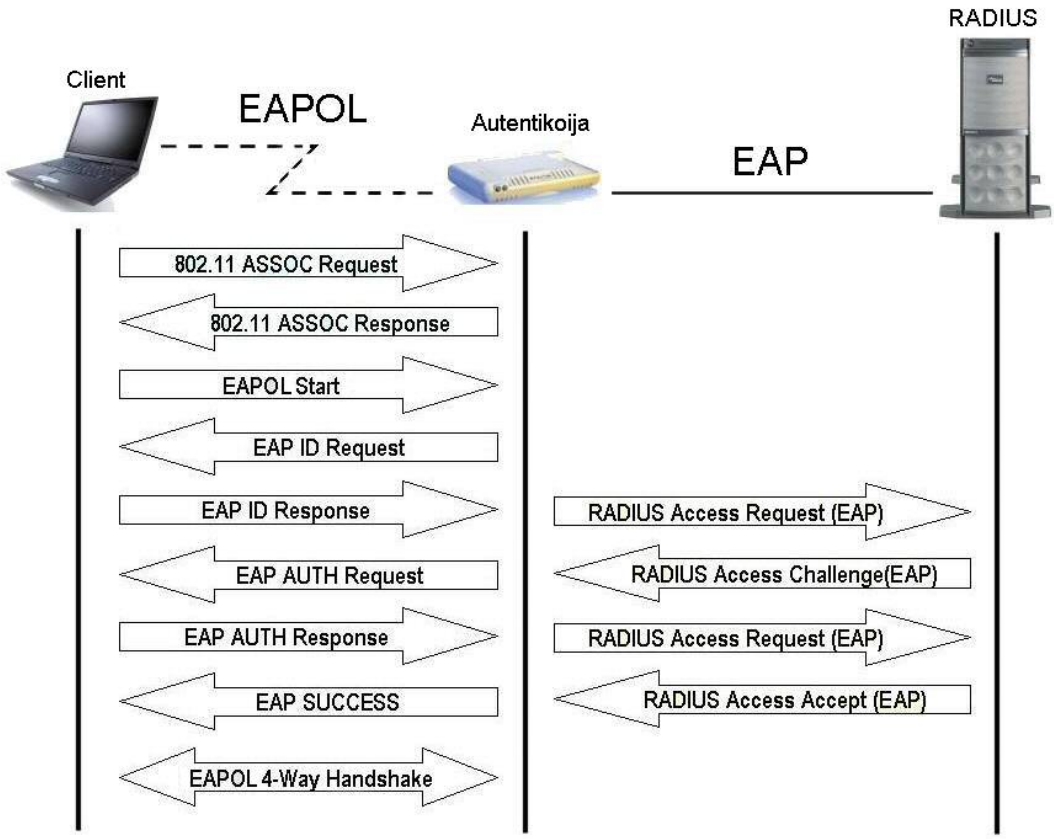
802.1x:n määrittelystä WLAN-laitteissa on paljon valmistajakohtaisia ratkaisuja, jotka eivät ole aina keskenään yhteensopivia. /7/

4.7 802.1x

Ihmiset tarvitsevat nykyään useammin verkkoyhteyksiä kuin ennen. Enää ei haluta olla sidoksissa tiettyyn paikkaan verkkoon pääsemiseksi, vaan verkko halutaan myös sinne, minne ikinä liikutaankin. Tätä muutosta osaltaan ovat vauhdittaneet monen valmistajan julkaisemat PDA-laitteet ja kännykät, jotka sisältävät langattoman verkkoyhteyden.

Autentikointia tarvitaan lähiverkoissa, jotta käyttäjäkunta voidaan jollain tavoin rajata. Langattomissa verkoissa autentikoinnin tärkeys lisääntyy entisestään, koska verkon käyttöoikeutta ei voida niin selkeästi rajata. 802.1x-standardi mahdollistaa eri lähiverkkotekniikoilla käyttäjän porttikohtaisen autentikoinnin. Tämä malli toimii suoraan nykyisissä Ethernet-lähiverkoissa, mutta myös muunlaisissa lähiverkkoratkaisuissa. Esimerkiksi langattomissa lähiverkoissa tukiasema muodostaa jokaista käyttäjää kohden virtuaaliportin, jonka avulla käyttäjän liikennöinti voidaan joko sallia tai estää. /7/

Porttipohjaista autentikointia käytettäessä asiakaslaitteet on kytketty verkon aktiivilaitteeseen, joka ei päästä liikennettä käyttäjälle, ennen kuin käyttäjä on tunnistautunut. Tällainen aktiivilaite voi olla kytkin, silta tai langattoman verkon tukiasema. Koska nämä verkkolaitteet ovat IP-kerroksen alapuolella, eli ne eivät ohjaa liikennettä IP-osoitteen perusteella, täytyy autentikoituminen tehdä alemman tason protokollalla. Nykyisin yleisimmin käytössä oleva protokolla on Ethernet. Vasta onnistuneen autentikoinnin jälkeen laite voi saada esimerkiksi DHCP:llä IP-osoitteen. 802.1x käyttää seuraavassa kappaleessa esiteltävää EAP-protokollaa autentikointiprotokollanaan ja oikeastaan se vain määrittelee keinot, joilla EAP saadaan kuljetettua lähiverkkoprotokollien päällä. Tämä paketointitekniikka on nimeltään EAPOL, joka on lyhenne englanninkielisistä sanoista EAP over LAN. /7/



Kuva 4. 802.1x autentikoinnin kulku

Kuvasta 4 nähdään 802.1x-pohjaisen autentikoinnin kulku. Todentaminen aloitetaan clientin liittymisellä avointa todentamista käyttäen tukiasemaan. Autentikoija, joka tässä tapauksessa on tukiasema, asettaa kontrolloidun 802.1x-portin estotilaan. 802.1x-todennuksen toiminta alkaa joko clientin lähettämällä EAPOL-Start-paketilla tai suoraan autentikoijan lähettämällä EAP-Request-paketilla, jossa pyydetään clientin tunnistetietoja. Client vastaa pyyntöön lähettämällä tunnistetietonsa autentikoijalle. Autentikoija välittää tunnistetiedot RADIUS:lle turvallisesti. RADIUS vastaa tunnistetietoihin lähettämällä haastepaketin clientille. Paketin rakenne riippuu käytettävästä EAP-menetelmästä ja haastepaketteja voidaan lähettää useampiakin. Client lähettää vastauksen haastepakettiin ja palvelin suorittaa todentamisen. Onnistuneen todentamisen seurauksena palvelin lähettää autentikoijalle EAP-Success-paketin menestyksekkään todentamisen merkiksi. Epäonnistuneen todentamisen seurauksena lähetetään EAP-Failure-paketti. /1/

Onnistuneen todentamisen jälkeen autentikoija lähettää clientille EAPOL-Key-viestin, jota käytetään salausavaimien välittämiseen salattuna päätelaitteelle. Sa-

laamisessa on käytössä avaimet sekä kohdelähetystä että levityslähetystä varten. Kohdelähetysavaimia käytetään päätelaitteen ja tukiaseman väliseen viestintään ja levityslähetysavaimia kaikille välittyvään liikenteeseen. Ensimmäinen kohdelähetysavain luodaan todentamisprosessin aikana sekä clientilla että RADIUS:lla, ja palvelin toimittaa avaimen todentamisen onnistuttua autentikoijalle. Tätä avainta käyttämällä salataan ensimmäiset EAPOL-Key-paketit ja päivitetään clientin salausavaimet. /1/

4.8 EAP (Extensible Authentication Protocol)

EAP on IETF:n kehittämä standardi (RFC 2284). Tässä RFC:ssä protokollaa ei ole käsitelty kuin PPP-yhteyksillä. EAP on erilaisia käyttäjäntunnistusmenetelmiä tukeva PPP-käytännön laajennus. Tietojen vaihto tukiaseman ja tunnistuspalvelimen välillä tapahtuu käyttäen lähiverkolle sovitettua EAP-käytäntöä. EAP:n laajennettavuudella tarkoitetaan sitä, että tunnistuskäytäntöä voidaan vaihtaa tavoitellun turvatason mukaan. Näistä eri vaihtoehdoista kerron seuraavaksi. /4, 16/

4.8.1 EAP-MD5

EAP-MD5 antaa heikoimman mahdollisen turvatason. EAP-MD5 käyttää MD5-hajautusalgoritmia todentamiseen. EAP-MD5:n kanssa tunnistetaan ainoastaan käyttäjä, ei tunnistusinfrastruktuuria, jolloin dynaamisten avainten vaihtaminen ei ole mahdollista. Myöskään päätelaite ei voi varmistua tukiaseman oikeellisuudesta kaksisuuntaisen todentamisen puuttuessa. EAP-MD5 ei paranna merkittävästi turvallisuutta perusratkaisuihin verrattuna, eikä sitä näin ollen voida missään olosuhteissa suositella käytettäväksi langattomien lähiverkkojen suojauksessa. /1, 4/

4.8.2 EAP-TLS

EAP-TLS käyttää TLS-protokollaa ja PKI-tunnisteita käyttäjäntunnistukseen. EAP-TLS on alun perin Microsoftin kehittämä pelkästään varmenteisiin perustuva menetelmä. Tunnistus tapahtuu kahteen suuntaan. Sekä käyttäjän työasema että tunnistuspalvelin todennetaan. EAP-TLS vaatii varmennepalvelimen. EAP-TLS:n huonona puolena voidaan pitää sitä, että suoranaisesti käyttäjää ei tunnisteta. Siinä ainoastaan tarkastetaan oikeanlaisen varmenteen löytyminen käyttäjän työasemasta. /4/

4.8.3 EAP-TTLS

EAP-TTLS on kevyempi versio, jossa ensin perustetaan tietoturvallinen TLS-tunneli tunnistuspalvelimeen. Käyttäjän tunnistaminen tapahtuu toisessa vaiheessa kyseistä tunnelia käyttäen. Tunnistamisessa voidaan käyttää mitä tahansa palvelimen tukemista vaihtoehdoista. EAP-TTLS:n kehittivät alun perin Funk Software ja Certicom. Vuonna 2002 marraskuussa EAP-TTLS luovutettiin IETF:lle standardoitavaksi, mutta vielä sitä ei ole viralliseksi standardiksi hyväksytty. Windowsista ei suoraan löydy tukea EAP-TTLS:lle. Muiden valmistajien toteutuksia löytyy kuitenkin myös Windowsille ja monille muille työasemakäyttöjärjestelmille. /1, 4/

4.8.4 PEAP

PEAP on Ciscon, Microsoftin ja RSA Securityn kehittämä kilpailija EAP-TTLS:lle. Siinä perustetaan tietoturvallinen TLS-tunneli tunnistuspalvelimeen ja käyttäjä tunnistetaan kyseistä tunnelia käyttäen. Tunnistamisessa voidaan käyttää esimerkiksi Windows käyttäjätunnus ja salasanapohjaista tunnistusta, missä tunnistaudutaan aktiivihakemiston käyttäjätietokantaa vastaan. Yksi käytetyimmistä menetelmistä on MS-CHAP v2, joka vastaa edellä kuvattua tapaa. PEAP-tukea löytyy Windowsille Microsoftin toteutuksina ja muiden valmistajien tekeminä, tosin esimerkiksi Ciscon toteutus eroaa hieman Microsoftin vastaavasta. PEAP luovutettiin

IETF:lle maaliskuussa 2003, mutta myöskään PEAPia ei ole vielä hyväksytty viralliseksi standardiksi. /4/

4.8.5 LEAP

LEAP on Ciscon kehittämä ja standardoima EAP-menetelmä. LEAP perustuu jaetun salasanan menetelmään. LEAP ei ole erityisen vahva käyttäjäntunnistusmenetelmä, vaan se on murrettavissa sanakirjahyökkäyksellä. Heikkouksista huolimatta LEAP on laajimmalle levinnyt valmistajakohtainen standardi. Ciscolla on kolmasosa yrityskäyttöön suunnatuista tukiasemamarkkinoista. /4/

4.9 MS-CHAP v2

MS-CHAP v2 tarjoaa kaksipuolisen tunnistuksen, vahvempien salausavainten luomisen alkutiedoille ja erilaiset salausavaimet lähetetylle ja vastaanotetulle datalle. Salasanan vaihdon yhteydessä mahdollisten riskien minimointi on toteutettu ottamalla pois tuki vanhemmille MS-CHAP-metodeille salasanan vaihtoon. /11/

MS-CHAP v2 on kaksipuolinen tunnistusprotokolla, joka tarkoittaa että molemmat (client ja palvelin) todistavat tietävänsä käyttäjän salasanan. Ensin palvelin pyytää todistusta clientilta lähettämällä sille haasteen. Sitten sama toiminta tehdään toisin päin ja client lähettää haasteen palvelimelle. Jos palvelin ei pysty todistamaan, että sillä on tieto käyttäjän salasanasta vastaamalla clientin haasteeseen oikein, client katkaisee yhteyden. Ilman kaksipuolista tunnistusta client ei voi havaita, jos yhteys luodaan väärennettyyn palvelimeen. /11/

4.10 RADIUS (Remote Access Dial-in User Service)

Alun perin Livingstone-yhtiössä kehitetystä RADIUS-protokollasta tuli IETF:n RFC, kun yhtiö julkaisi protokollamäärittelyn. Muillakin valmistajilla oli myös ke-

hitteillä omia protokollia, joista ei kuitenkaan Livingstonen RADIUS-protokollan julkaisun jälkeen tullut yhtä käytettyjä. /7, 9/

Ensi vaiheessa RADIUS-protokollaa käytettiin sisäänsoittopalvelussa tapahtuvaan autentikointiin, kuten modeemi-, ISDN- ja xDSL-yhteyksissä, näissä palveluissa RADIUS-protokollaa käytetään vieläkin laajalti. Nykyisin RADIUS:ta käytetään myös erilaisissa verkoissa käyttäjien tunnistukseen ja tilastointiin. Näitä ovat muun muassa erilaiset langattomat verkkoratkaisut, kuten esimerkiksi langattomat vierailijaverkot. Tällaisissa verkoissa RADIUS hoitaa kyselyt käytettyyn käyttäjäkantaan ja hyväksyy tai hylkää käyttäjän pääsyn verkkoon. RADIUS-palvelimia voi olla useita, eikä niiden tarvitse välttämättä sijaita samassa organisaatiossa, autentikoitumispyynnöt ohjataan vain osoitetun organisaation RADIUS-palvelimelle. Tällä menettelyllä käyttäjät voivat olla vaikka eri maissa. /7, 9/

4.10.1 Radiator

Radiator on kaupallinen RADIUS. Valmistaja on Australialainen yritys Open System Consultants, joka aloitti toimintansa 1991. Radiator tukee noin 60:tä eri autentikointimetodia. Radiator tukee esimerkiksi monia EAP-metodeja, kuten TLS, TTLS, PEAP, MD5, MSCHAPV2, LEAP ja monia muita. /14/

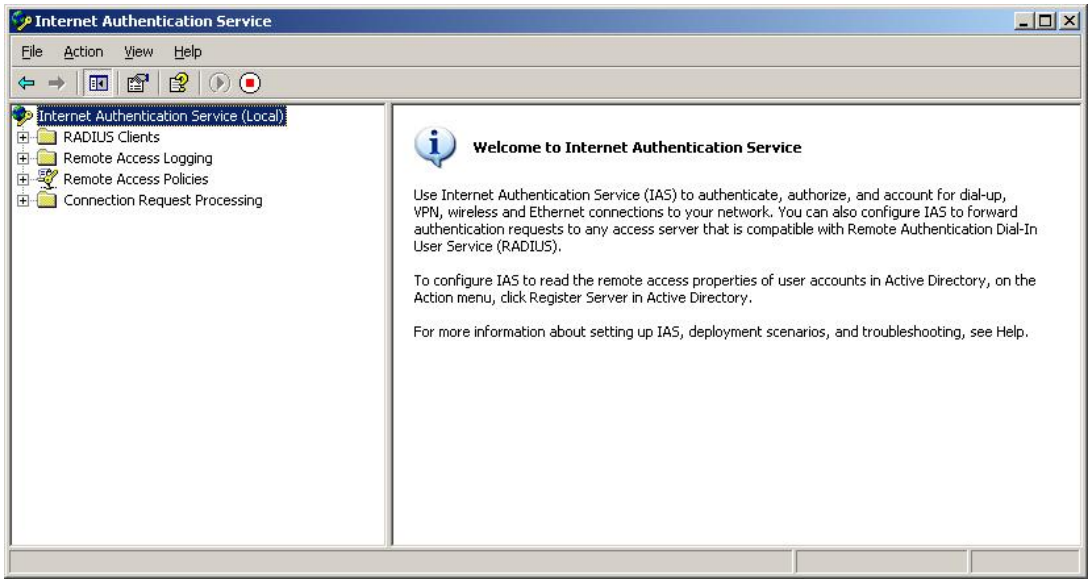
Radiator voi toimia monissa eri laitteistoissa, kuten useimmissa Unix- ja Linux-pohjaisissa laitteissa, Windows NT-, Windows 95-, Windows 98-, 2000-, XP-, Windows Server 2003- ja MacOS X-alustoilla. Radiator on kirjoitettu kokonaan Perl-ohjelmointikielellä ja on siksi hyvin skaalautuva. Uusien autentikointitapojen lisäys Radiatoriin on standardoitu, joten sen voi helposti integroida olemassa oleviin järjestelmiin ja ohjelmistoihin. /14/

4.10.2 IAS (Internet Authentication Service)

IAS on Microsoftin toteutus RADIUS-palvelimesta. IAS tulee sekä Windows 2000 Serverin, että Windows 2003 Serverin mukana.

IAS tukee muutamia eri autentikointiprotokollia, jotka ovat turvallisimmasta heikoimpaan metodiin PEAP-EAP-TLS, EAP-TLS, PEAP-EAP-MS-CHAPv2, MS-CHAP v2, MS-CHAP, EAP-MD5, CHAP ja PAP. PAP ei ole suositeltavien listalla sen heikon turvatason takia, joten sitä ei kannata käyttää, jos järjestelmät eivät sitä vaadi. /5/

IAS:ssa on graafinen käyttöliittymä, jonka ulkoasu näkyy kuvasta 5. IAS on kohtuullisen yksinkertainen käyttää ja konfiguroida, eikä se vaadi kovin pitkää opettelua. Ominaisuuksiensa puolesta se ei kuitenkaan pärjää esimerkiksi Radiatorille.



Kuva 5. IAS-käyttöliittymä

5 VIERAILIJAVERKKO TAMPEREEN AMMATTIKORKEAKOULUSSA

Langaton lähiverkko ja siihen tuleva vierailijaverkko tuli ajankohtaiseksi Tampereen ammattikorkeakoulussa keväällä 2004. Vierailijaverkkoa rakentaminen aloitettiin syksyllä 2004. Aikaisemmin kesällä tutkin, millä periaatteilla verkko kannattaa TAMK:n tapauksessa toteuttaa. EAP-käytännöistä käytettäväksi valittiin PEAP, joka on hyvä oppilaitosympäristössä siinä mielessä, ettei varmenteita tarvitse jakaa asiakaslaitteille. RADIUS-palvelimeksi valittiin aluksi IAS, mutta TTY:n vierailun jälkeen heidän suosituksestaan päätettiin vaihtaa RADIUS-palvelimeksi Radiator. Radiatorin suurin etu on sen ominaisuudet, joiden avulla siitä saadaan juuri halutun kaltainen lähes jokaisen tarpeisiin. Langaton yhteys tullaan suojaamaan WPA:lla. Autentikointi suoritetaan 802.1x-protokollan mukaan.

Vierailijaverkkoja on rakennettu viime vuosina useisiin yliopistoihin ja ammattikorkeakouluihin Suomessa. Myös esimerkiksi Yhdysvalloissa useimmat kampukset ovat rakentaneet langattomia lähiverkkoja opetuskäyttöön.

5.1 Vierailijaverkon hyödyt

Aiemmin on tullut esille monia hyötyjä niin langattomasta verkosta kuin vierailijaverkosta. Vierailijaverkon rakentaminen on ajankohtaista, ja herättää varmasti kiinnostusta. Langattomilla yhteyksillä varustetut kannettavat PDA-laitteet ja kännykät lisääntyvät lähiaikoina runsaasti, koska

Langattoman vierailijaverkon edut liittyvät nimenomaan liikkuvuuteen, kun verkkoon voi liittyä mistä vain verkon kantaman rajoissa. Käyttäjien rajaaminen oppilaitoksessa työskenteleviin ja opiskeleviin henkilöihin voidaan toteuttaa jo olemassa olevan käyttäjäkannan avulla.

Langattoman verkon tietoturva saadaan nostettua uudelle tasolle käyttämällä uusia vahvempia salausmenetelmiä. Käyttämällä laadukkaita laitteita, jotka tukevat myös uusimpia ominaisuuksia, säästytään laitteistopäivityksiltä pitkään.

Vierailijaverkon käyttö edellyttää, että opiskelijoilla on omat vaadittavat laitteet verkon käyttöä varten. Tämä tarkoittaa käytännössä sitä, että tarvitaan kannettava tietokone ja langaton verkkokortti.

5.2 Vierailijaverkon suunnittelu

Ennen varsinaista verkon toteutusta täytyy monta asiaa ottaa huomioon. Tukiasemien paikat täytyy valita oikein, jotta kuuluvuus saadaan mahdollisimman hyväksi. Myös käyttäjille pitää tehdä selväksi, mitä varten verkko on rakennettu ja miten sitä käytetään.

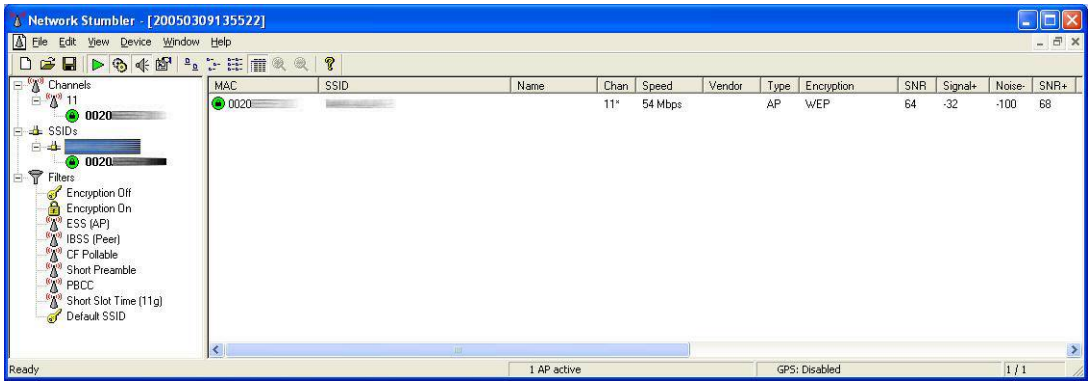
Suunnittelun lähtökohtana oli saada verkon kantaman sisään paikat, joissa oletetaan olevan eniten käyttäjiä. Näitä ovat muun muassa auditoriot, aulat, infokahvila ja ruokalan edusta. Koko rakennusta on turha lähteä kerralla kattamaan, koska ensin täytyy saada käyttökokemuksia vierailijaverkosta. Tämän jälkeen sitä voidaan tarpeiden mukaan laajentaa. Myös kerralla koko rakennukseen ostettavien tukiasemien hinta nousisi liian suureksi.

Suunnittelussa pitää ottaa huomioon ympäristön vaikutukset paikoissa, joihin tukiasemia ollaan laittamassa. Seinien rakennusmateriaalit vaikuttavat paljon siihen, miten radioaallot sen läpäisevät. Muovi ja lasipinnat eivät vaimenna signaalia merkittävästi, kun taas paksut tiili- tai betoniseinät ja metallirakenteet saattavat joissain tapauksessa heikentää kuuluvuutta niin, että tyydyttävää yhteyden laatua ei saada. Käytännössä tukiaseman lähettimestä riippuen signaali läpäisee yhden suurenmankin seinän, katon tai lattian, tosin siinä heiketen, mutta yleensä yhteys tukiasemaan saadaan vielä hyvin. Myös isommat koneet ja konehuoneet tuottavat paljon häiriöitä ja sähkömagneettista säteilyä, eikä niiden välittömään läheisyyteen ole järkevää tukiasemaa sijoittaa. Samalla taajuusalueella toimivat laitteet saattavat myös häiritä tukiaseman toimintaa. Mikroaaltouunit ja Bluetooth-laitteet saattavat aiheuttaa häi-

riöitä langattomaan verkkoon. Tukiasemia ei saisi laittaa myöskään liian lähekkäin, jotta ne eivät häiritsisi toisiaan.

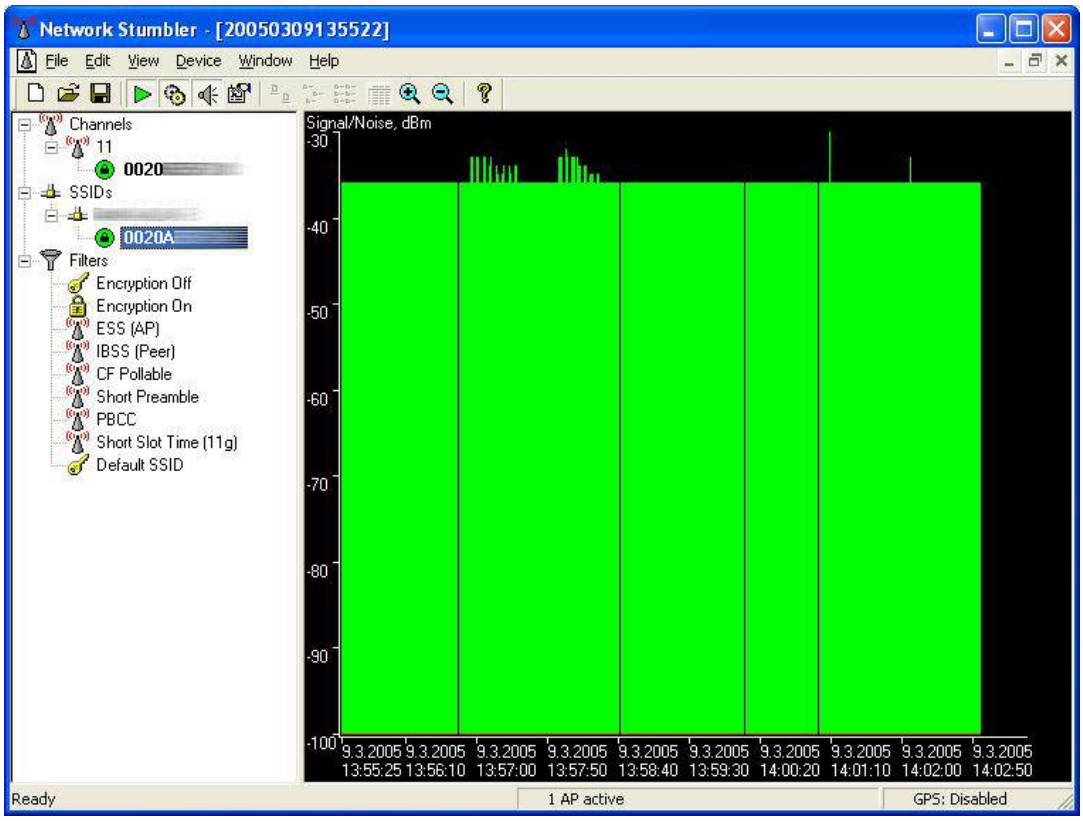
5.3 Kuuluvuusmittaukset

Kuuluvuusmittauksia suoritettiin ennen tukiasemien asennusta, jotta tukiasemille löydettäisiin mahdollisimman hyvä kuuluvuus. Asennuksien jälkeen suoritettiin uusi kuuluvuusmittaus, jolloin saatiin tarkka kuva kuuluvuusalueista. Kuuluvuusmittaukset suoritettiin kannettavan tietokoneen avulla, johon oli asennettu Netstumbler-ohjelma. Lisäksi käytettiin Windowsin omaa kuuluvuusmittaria, joka on kuitenkin vain suuntaa antava. Netstumbler on hyvin yksinkertainen ohjelma, joka näyttää kerralla kaikki kuuluvat tukiasemat. Kuvista 6 ja 7 näemme Netstumblerin käyttöliittymän ja piirrettävän signaali/kohina-suhteen käyrän.



Kuva 6. Netstumler-ohjelmanäkymä SSID kohdasta.

Netstumbler näyttää vaihtoehtoisia tietoja langattomasta verkosta, riippuen siitä, miten verkko on suojattu ja lähetetäänkö SSID:ä broadcast-lähetyksenä vai ei. Netstumbler ei näytä SSID:ä, jos Broadcast-lähetys on otettu pois, paitsi mikäli kuunneltava langaton verkko on asennettu samaan laitteeseen kuunneltavan laitteen kanssa. Netstumbler ei myöskään pysty kertomaan, onko verkon salaus esimerkiksi WPA, vaan se näyttää aina WEP, jos salaus on käytössä. Tämä voidaan todeta myös kuvasta 6, jossa salauksena käytettiin WPA:ta, mutta silti encryption-kohdassa lukee WEP.



Kuva 7. Netstumbler-ohjelmanäkymä signaali/kohina-suhde mittauksesta.

Netstumbler:sta saa näkyviin myös signaali/kohina-suhde mittauksen, jonka näkymä on yllä olevan kuvan kaltainen. Kuvan mittaus on suoritettu tukiaseman lähistöllä, joten kuuluvuus on lähes maksimissaan.

5.4 Laitteiden valinta

Joitakin aktiivilaitteita vaihdettiin samalla, ja niissä on tarkoitus ottaa käyttöön langallinen vierailijaverkko. Uudet kytkimet ovat HP:n Procurve 28xx- ja 26xx-sarjaa. Kaikki uudet hankitut kytkimet tukevat 802.1x:ä. Langallinen versio vierailijaverkosta toimii kuten langatonkin ja siinä tullaan käyttämään samanlaisia salauksia.

Tukiasemia vertailtiin lähinnä ominaisuuksien mukaan. Tietokonelehdissä julkaistuja vertailuja käytimme apuna valitessamme sopivia tukiasemia. Tietokonelehdessä 05/2004 oli vertailussa 802.1x-tukiasemat, joiden joukosta löytyy myös tietokonekeskuksen valitsema tukiasema. Tukiasemaksi valittiin Proxim AP-4000, jonka hyvien ominaisuuksien pohjalta ratkaisu tehtiin. Proxim AP-4000 sisältää ra-

diot sekä 802.11a-standardille, että 802.11b/g-standardeille. Tukiasema mahdollistaa 16 eri SSID:n käytön, eli siihen voidaan laittaa 16 erillistä verkkoa. AP-4000 tukee myös uusinta 802.11i-standardia ja mahdollistaa siten AES-algoritmin käytön salauksessa.

Syksyllä 2004 Proxim julkaisi uuden tukiasemamallin. Mallimerkinnäksi tuli AP-700, joita hankittiin myös vierailijaverkkokäyttöön. AP-700 ominaisuudet ovat isoveljeä vastaavat ja ainoaksi eroksi muodostuu kahden yhtäaikaisen radion käyttö. AP-700 sisältää molemmat radiot sekä 802.11a:lle että 802.11b/g:lle, näitä ei voida kuitenkaan AP4000 tavoin pitää yhtä aikaa päällä. 802.11a-standardille ei ole pakollista tarvetta, koska esimerkiksi lähes kaikki kannettavien integroidut langattomat verkkokortit tukevat ainoastaan 802.11g-standardia. Ulkoisesti AP-700 on isoveljensä näköinen.

Kuva 8. Proxim AP-700/AP-4000 tukiasema

Kannettaviin, jotka eivät sisällä integroitua langatonta verkkokorttia, joudutaan hankkimaan ulkoinen lisäkortti PCMCIA-paikkaan (Personal Computer Memory Card International Association), tai USB-liitäntään. Uusien kannettavien integroidut verkkokortit on todettu toimiviksi vierailijaverkkokäytössä, tosin hieman vanhempiin kannettaviin tarvitaan langattoman verkkokortin ajuripäivitys, jotta mahdollinen WPA-tuki saadaan käyttöön. Ilman WPA-tukea vierailijaverkon käyttö on mahdotonta. Alla esitetyissä kuvissa on langattomat mallit PCMCIA- ja USB-verkkokorteista.

Kuva 9. Proxim Orinoco 11a/b/g ComboCard Gold

Kuva 10. Langaton verkkokortti USB-väylään

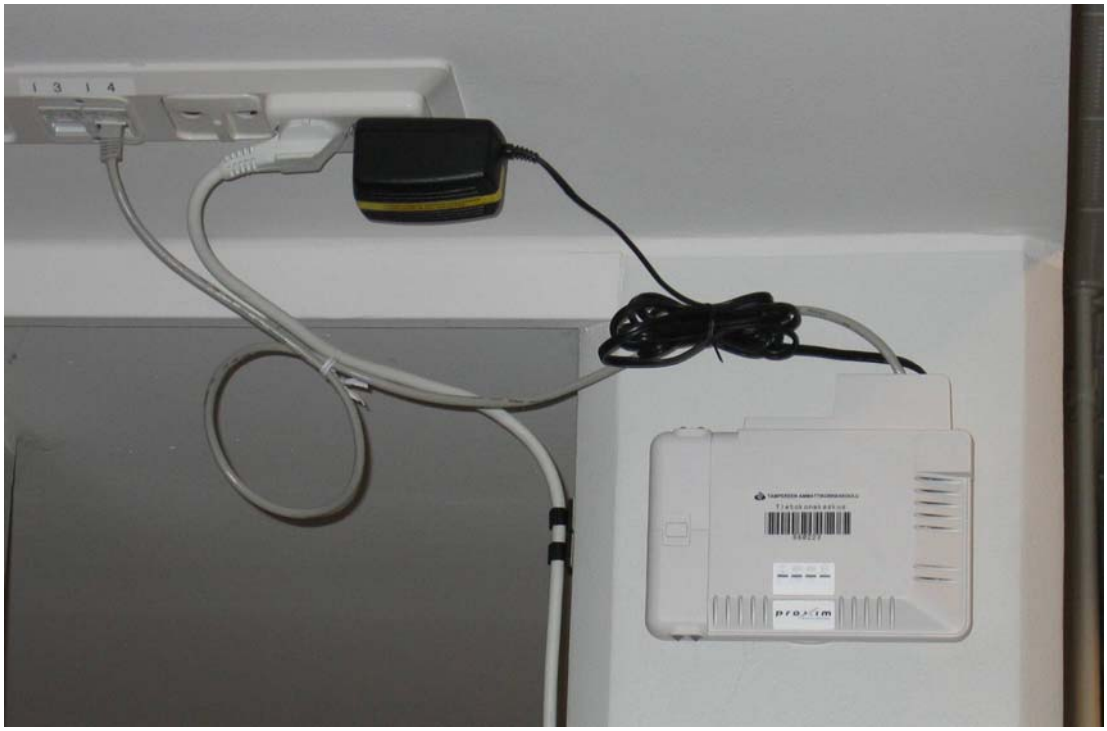
5.5 Tukiasemien asennus

Tukiasemien paikat valittiin pitkälti kuuluvuusmittausten perusteella. Paikat yritettiin valita niin, että tukiasemalla saadaan mahdollisimman hyvä peitto ja näin kuuluvuus moneen tilaan. Tämä on tärkeää, jotta kustannukset saataisiin mahdollisimman alhaisiksi. Tukiasemille yritettiin löytää hyvät paikat ATK- ja sähkörasioiden läheisyydestä, jotta uusien rasioiden asennuksilta säästyttiin. Tämä onnistui yllättävän hyvin rakennusten saneerauksien ansiosta, sillä myös johdotukset on uusittu ja rasioita lisätty myös katonrajaan.

Seuraavista kuvista nähdään kahden tukiaseman asennukset. Ensimmäinen tukiasemista on sijoitettu käytävälle katonrajaan. Tukiasemalla katetaan muutama luok-

ka ja yksi auditorio. Toinen tukiasemista on sijoitettu pylvääseen, jonka ympärillä on paljon vapaata tilaa. Kuuluvuus saadaan tällaisen asennuksen johdosta maksimoitua. Pelkästään tällä tukiasemalla saadaan katettua juhlasali, yksi auditorio, kahvila ja osa aulasta.

Kuva 11. Tukiaseman käytäväasennus (tukiasema oikealla)



Kuva 12. Tukiaseman pylväsasennus

5.6 Vierailijaverkon tietoturva

Tietoturvaan on yritetty panostaa mahdollisimman paljon vierailijaverkon suunnittelussa ja se olikin yksi lähtökohdista, kun verkkoa lähdettiin toteuttamaan. Langattoman verkkoyhteyden tulee olla hyvin suojattu, jotta käyttäjät voivat luottaa täysin yksityisyyden säilymiseen. Langattoman verkon salauksena vierailijaverkossa käytetään WPA:ta. Salauksen avulla estetään mahdolliset tietomurtoyritykset. Autentikointi verkossa toteutetaan 802.1x-pohjaisesti PEAP-käytännön avulla. Tällä varmistetaan, etteivät koulun ulkopuoliset henkilöt pääse käyttämään verkkoa.

5.7 Vierailijaverkon käyttäminen

Vierailijaverkon käyttäminen vaatii käyttäjältä kannettavan tietokoneen, sekä verkkokortin. Suurimmassa osassa kannettavissa tietokoneissa on sisäänrakennettu verkkokortti, jota voidaan käyttää langallisessa vierailijaverkossa. Langaton verkkokortti tarvitaan, jos halutaan käyttää langatonta versiota vierailijaverkosta. Käyttöjärjestelmäksi suositellaan Windows XP:tä varsinkin langattoman verkon käyttäjille. Lisäksi tarvitaan myös voimassa olevat tunnukset koulun verkkoon.

Liitteenä olevan asennusohjeen avulla jokaisen käyttäjän tulisi pystyä itse asentamaan vierailijaverkon käyttöön.

5.8 Vierailijaverkon kehityskohteita

Langattoman verkon kuuluvuusalueen laajentaminen on ensimmäisiä kehityskohteita. Tällä hetkellä vierailijaverkon tukiasemia on seitsemän. Tällä määrällä päästään jo hyvin alkuun, ja tukiasemia tullaan lisäämään tarpeen vaatiessa paikkoihin, missä tarvetta vierailijaverkolle ilmenee.

FUNET Roaming on myös yksi suurella todennäköisyydellä tulevaisuudessa mukaan tulevista ominaisuuksista. Tällä tarkoitetaan, että opiskelijat ja henkilökunta

voivat omilla tunnuksilla päästä käyttämään muiden korkeakoulujen ja yliopistojen vierailijaverkkoja edellyttäen, että toisella koululla on myös FUNET Roaming-sopimus. Kirjautumisen yhteydessä tarkastetaan, mihin oppilaitokseen henkilö kuuluu, ja tämän avulla autentikoitumispyyntö osataan ohjata oikean koulun RADIUS-palvelimelle.

Vierailijaverkossa voidaan tulevaisuudessa mahdollisesti sallia myös muunlaisia autentikoitumistapoja kuin PEAP. Tällä parannetaan muiden käyttöjärjestelmien yhteensopivuutta. Lähtökohtana tälle muutokselle on, ettei tietoturvantaso saa laskea nykyisestä PEAP-käytännöstä. Ennen suurempia lisäyksiä täytyy verkosta kuitenkin saada käyttökokemuksia, jonka jälkeen mahdolliset parannukset on helpompi toteuttaa.

5.9 Projektin yhteenveto

Langattomat lähiverkot ovat nostaneet suosiotaan merkittävästi viimeaikoina. Vierailijaverkon rakentaminen Tampereen ammattikorkeakouluun oli tästä syystä mielestäni kannattava projekti. Verkon avulla opiskelijat ja henkilökunta voivat käyttää omia tietokoneitaan hyväksi opiskelussa ja opetuksessa.

Vierailijaverkosta hyötyvät niin opiskelijat, opettajat kuin vierailevat luennoitsijatkin. Vierailijaverkon avulla pystytään tarjoamaan verkkoyhteyttä suoraan henkilön langattoman päätelaitteen kautta. Päätelaite voi olla kannettava tietokone, PDA-laite, matkapuhelin tai mikä tahansa samaa tekniikkaa tukeva laite, jossa on tuki käytetyille protokollille.

Langattoman verkon tietoturvan paranemisen takia voidaan verkon salauksen vahvuuteen luottaa. Ensimmäinen suojaus, mikä langattomalle verkolle kannattaa tehdä, on ottaa SSID:in broadcast-lähetys pois päältä, jotta verkkoa ei mainosteta ulospäin. Vierailijaverkossa käyttöön tuleva WPA-salaus ei ole vahvin mahdollinen, mutta tämäkin salaus on täysin riittävä. Syy siihen, miksi uusinta 802.11i-salausta ei otettu vielä käyttöön, on, etteivät laitevalmistajat ole julkaisseet riittävästi uusia ajureita laitteisiinsa. Tästä syystä on vielä tässä vaiheessa turha lähteä

etsimään toimivia kortteja, sillä muutamien kuukausien kuluttua tullaan varmasti näkemään uusia ajureita monelta laitevalmistajalta. Tampereen ammattikorkeakouluun hankitut tukiasemat tukevat uusinta 802.11i-salausta. Tämä salaus tullaan ottamaan käyttöön WPA:n rinnalla jossain vaiheessa, jolloin halukkaat 802.11i:tä tukevan verkkokortin omistajat pääsevät testaamaan niitä.

Kotihakemistojaan käyttäjät voivat käyttää normaalisti Citrixin avulla. Citrix mahdollistaa esimerkiksi tiedostojen kopioinnin omasta kotihakemistosta kannettavalle. Sillä voi myös käyttää sovelluksia kuten selaimia, jolloin mahdollistetaan ainoastaan koulun sisäverkossa toimivien palvelujen käyttäminen. Myös Open Office:n käyttäminen onnistuu Citrixin avulla.

LÄHTEET

1 Ahvenainen, Marko, Langattomien Lähiverkkojen Turvallisuus. [Sähköinen dokumentti]. Diplomityö. Teknillinen korkeakoulu, Sähkö- ja Tietoliikennetekniikan osasto. Helsinki 2003. 80 s.
http://keskus.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf

2 ETSI HIPERLAN/1 Standard. [www-sivu].
http://portal.etsi.org/bran/kta/Hiperlan/hiperlan1.asp

3 ETSI HIPERLAN/2 Standard. [www-sivu].
http://portal.etsi.org/bran/kta/Hiperlan/hiperlan2.asp

4 Hämäläinen, Pertti, Langaton verkko turvalliseksi. Tietokone-lehti 05/2004, s. 64-71.

5 Internet Autentication Service for Windows 2000. White Paper. [Sähköinen dokumentti]. http://download.microsoft.com/download/b/6/4/b64bcb2e-867c-4458-aee8-589d750e68a8/IAS.doc

6 Karvonen, Tuomas, Wi-fi Alliance ei hyväksy ennenaikaisia 802.11n laitteita. Digitoday. [www-sivu]
http://www.digitoday.fi/showPage.php?page_id=12&news_id=36038

7 Keski-Kasari, Sami, Verkkopalveluiden autentikointi yhteisen käyttäjätietokannan avulla. [Sähköinen dokumentti]. Diplomityö. Tampereen teknillinen korkeakoulu, Tietotekniikan osasto. Tampere 2002. 54 s.
http://www.wirlab.net/pdf/di_tyo_samikk.pdf

8 Langattomien lähiverkkojen tietoturva. [www-sivu]
http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/wlan/Wlan.html

9 Luoma-aho, Vesa, Ruuska, Tomi, Saarinen, Toni, Simola, Mikko, RADIUS. [Sähköinen dokumentti]. Raportti. Lappeenrannan Teknillinen Yliopisto, Tietotekniikan osasto. www.it.lut.fi/kurssit/03-04/010628000/Seminars/Radius.pdf

10 Mannila, Marko, Texas ehdottaa uutta, nopeata Wi-fi standardia. ITviikko. [www-sivu]. http://www.itviikko.fi/uutiset/uutinen.asp?UutisID=62623

11 Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2). [www-sivu]
http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/auth_mschapv2.asp

12 Muropaketti: WLAN. [www-sivu].
http://www.soneraplaza.fi/tietokoneet/artikkeli/0,2998,h-9093_a-142588,00.html

13 Niemi, Juha, WLAN-turvallisuus. [Sähköinen dokumentti]. Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä – seminaari. Helsingin yliopisto, Tietojenkäsittelytieteen laitos. Helsinki 2003.
http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf

14 Radiator RADIUS Server, Installation and reference manual for Radiator version 3.12. [Sähköinen dokumentti]. http://www.open.com.au/radiator/ref.pdf

15 Ranta-Eskola, Joni, Wlanin rakentaminen. [Sähköinen dokumentti]. Opinnäytetyö. Vaasan ammattikorkeakoulu, Liiketalous ja matkailu. Vaasa 2003. 62 s. http://www.wlan.puv.fi/wlan_lopputyo.pdf

16 RFC 2284: PPP Extensible Authentication Protocol (EAP). [Sähköinen dokumentti]. The Internet Society (1998). 15 s. http://www.ietf.org/rfc/rfc2284.txt

17 Wikipedia: 802.11. [www-sivu]. http://fi.wikipedia.org/wiki/IEEE_802.11

18 Wireless Glossary: 802.11e. [www-sivu].
http://www.devx.com/wireless/Door/11409

19 Wireless Glossary: 802.11h. [www-sivu].
http://www.devx.com/wireless/Door/11412

20 Wireless house: DNA WLAN & SONERA HOMERUN. [www-sivu].
http://www.wirelesshouse.fi/tuotteet-homerun.shtml

LIITE

LIITE 1: VIERAILIJAVERKON KÄYTTÖOHJE

Tuetut käyttöjärjestelmät:

- Microsoft Windows XP SP1 tai SP2
- w2k SP4 + windows update päivitykset

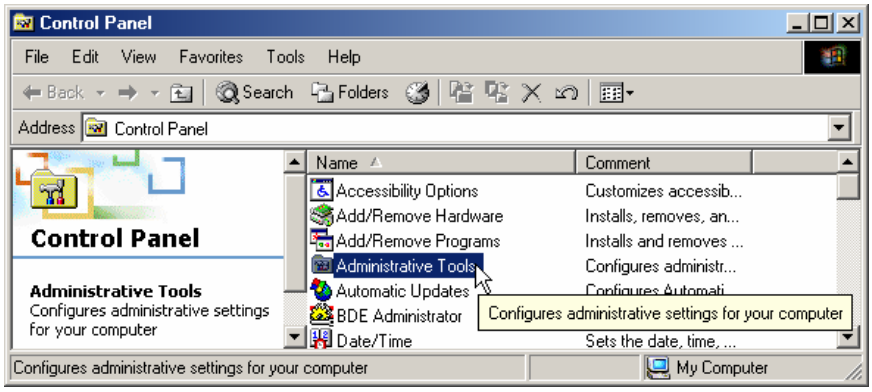
OSA I:

Asennusohje vierailijaverkon kytkemisestä päälle tavalliseen LAN verkkokorttiin:

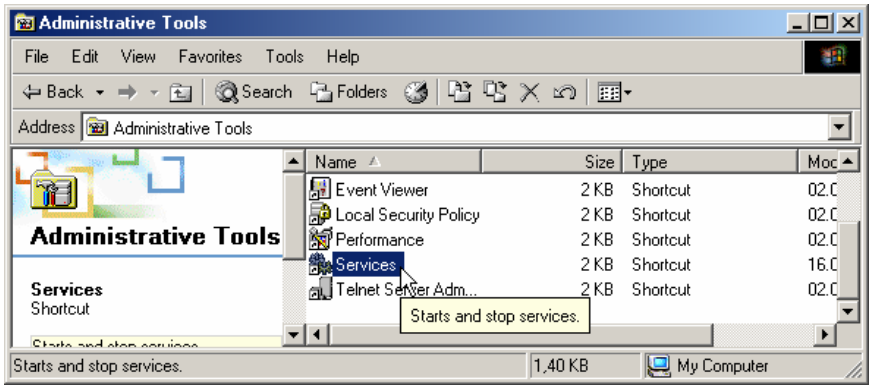
Toimii sekä Windows 2000 ja XP:n kanssa.

<u>Vaihe1:</u> Käynnistä *wireless configuration service*

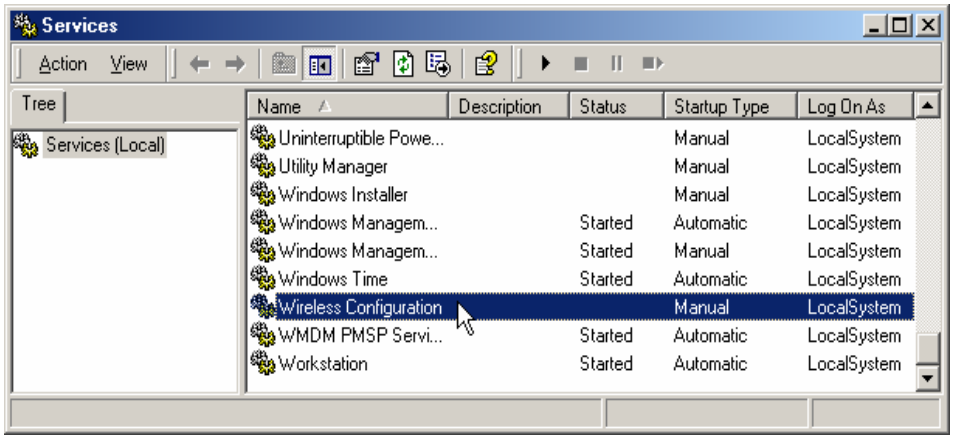
Avaa Käynnistä-valikko - Settings - Control Panel - Administrative Tools



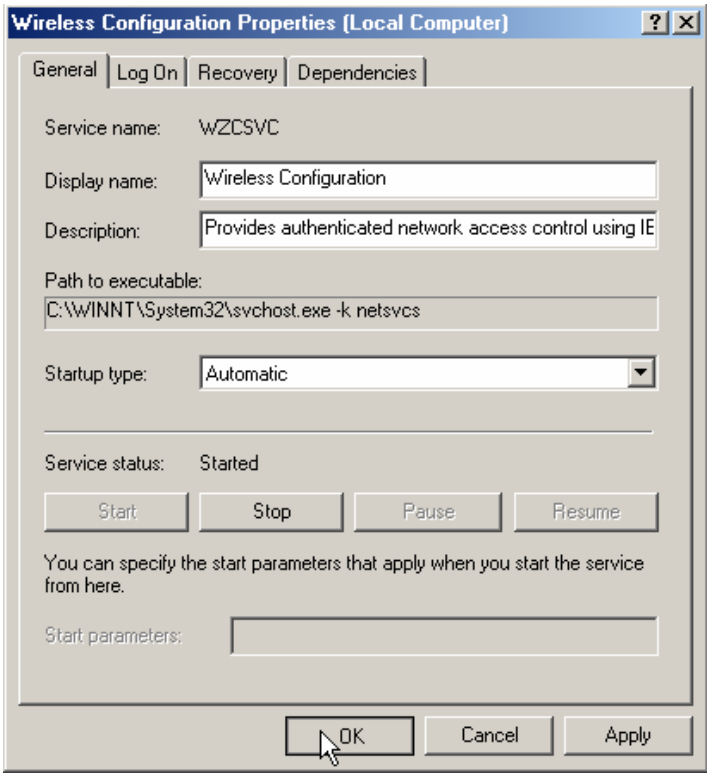
<u>Vaihe 2:</u>
Avaa Services



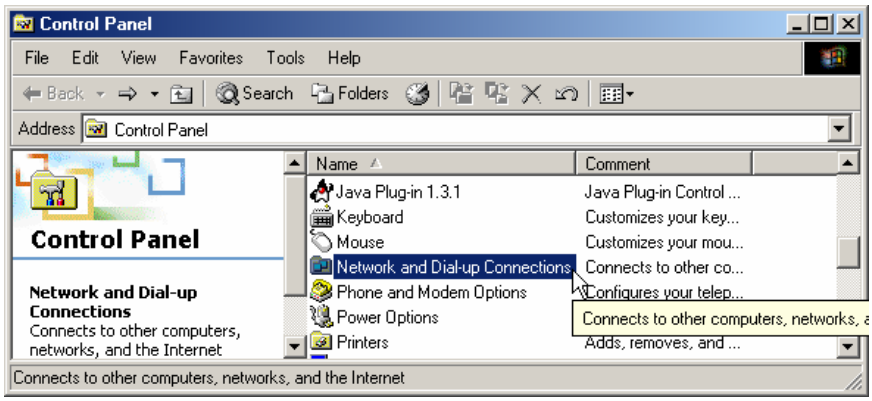
<u>Vaihe 3:</u>
Tuplaklikkaa hiiren vasenta nappia Wireless Configuration kohdalla.



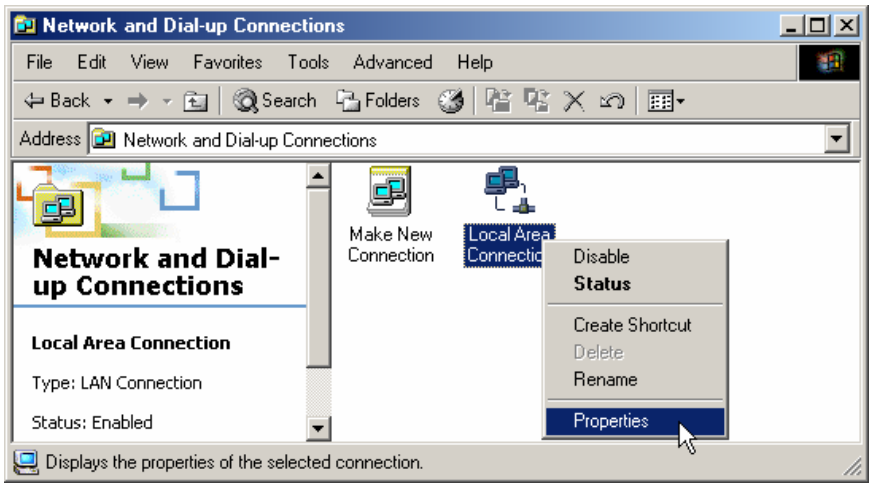
<u>Vaihe 4:</u>
Paina Start, jos palvelu ei ole automaattisesti käynnistynyt. Vaihda Startup type automaattiseksi, niin palvelu käynnistyy automaattisesti joka käynnistyksessä.



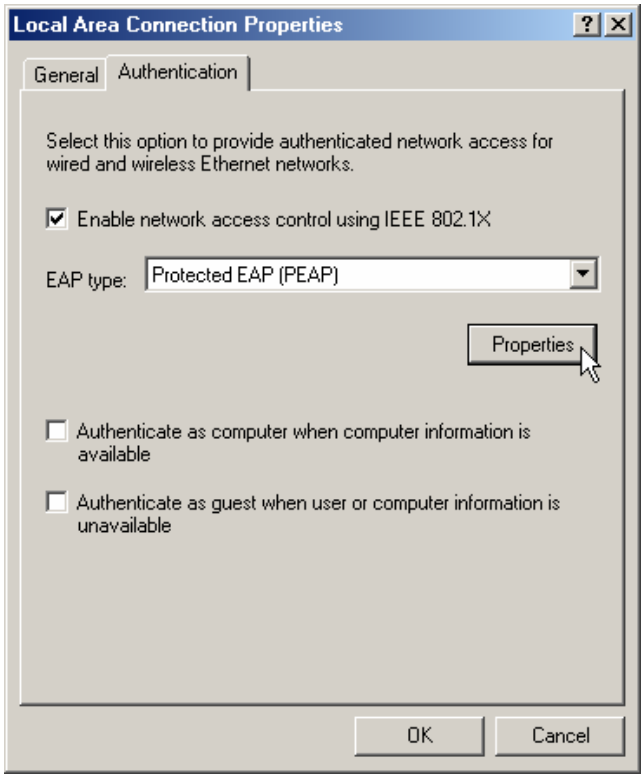
<u>Vaihe 5:</u>
Avaa Control Panel - Network and Dial-up Connections.

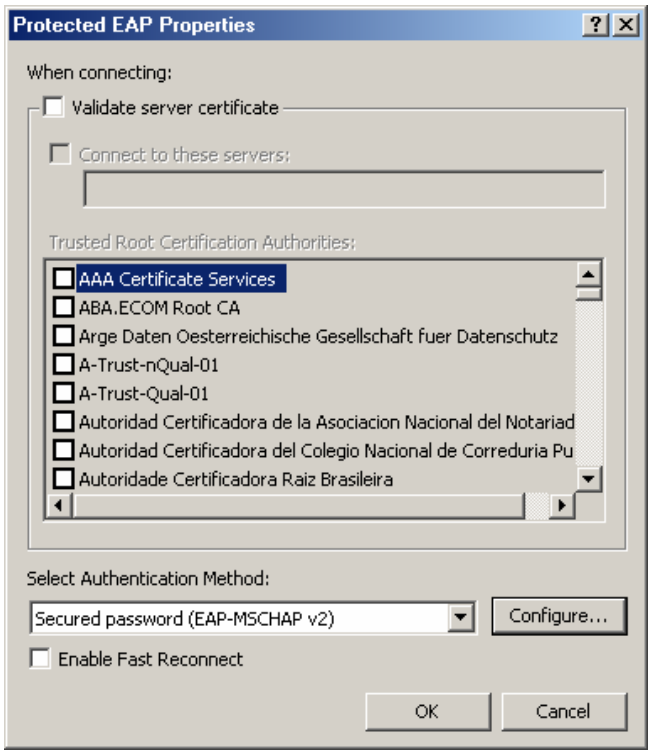


Vaihe 6:
Paina hiiren oikeaa nappia Local Area Connection kohdalla ja valitse Properties.



Vaihe 7:
Valitse Authentication-välilehti ja laita asetukset kuvan mukaisesti. Tämän jälkeen paina Properties nappia. (Authentication-välilehti puuttuu jos vaiheita 1-4 ei ole suoritettu Windows 2000 kanssa)





Vaihe 8:
Ota ruksi pois Validate server certificate kohdasta, jonka jälkeen paina Configure…

Vaihe 9:
Ota ruksi pois Automatically use my Windows logon name and password (and domain if any). Sulje kaikki ikkunat ok:lla.

Vaihe 10:
Ruudulle pitäisi ilmestyä seuraavan näköinen ikkuna. Kirjoita annetuille kohdille käyttäjätunnuksesi ja salasanasi, domain kohta jätetään tyhjäksi.

Kuittaa ikkuna OK:lla ja hetken kuluttua yhteyden pitäisi toimia.

OSA 2:

Tässä ohjeessa opastetaan käyttämään vain Windowsin omaa langatonta yhteysohjelmaa, voit käyttää myös langattoman verkkokortin valmistajan omia yhteysohjelmia.

Suosittelemme käyttöjärjestelmäksi Windows XP:tä, jossa on paremmat langattoman verkon ominaisuudet kuin Windows 2000:ssa. Ohje on tehty Windows XP:lle.

Laitteistovaatimukset:

Langaton verkkokortti 802.11b, 802.11g tai 802.11a

Kaikkien WPA:ta tukevien langattomien korttien pitäisi toimia alla olevan määrittelyn mukaisesti. On kuitenkin mahdotonta testata kaikkia langattomia kortteja, joten olemme testanneet vain muutamia kortteja:

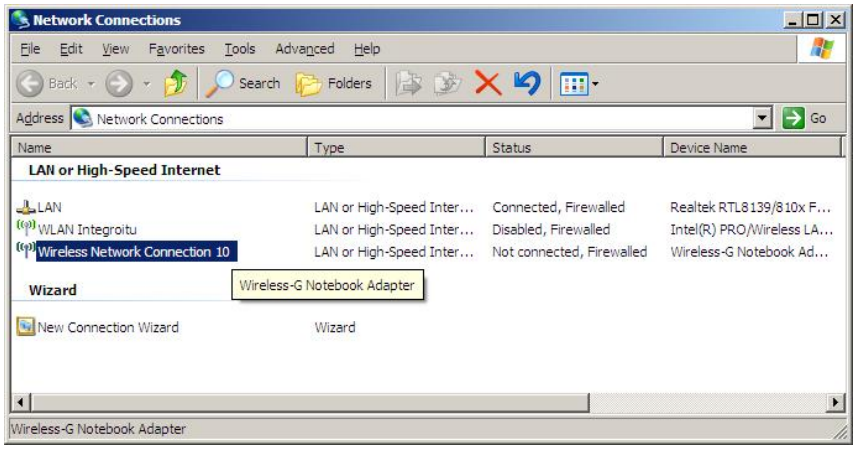
- Proxim ORiNOCO 11a/b/g ComboCard Gold
- Linksys WPC54G
- Intel PRO/Wireless LAN 2100 3B Mini PCI Adapter

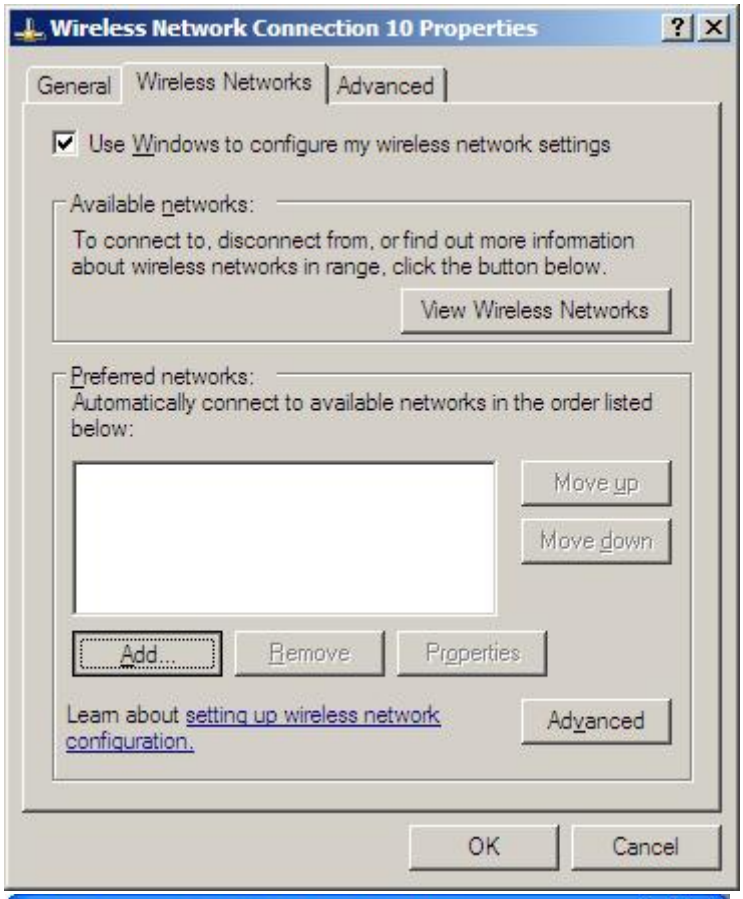
Asenna langattoman verkkokortin ajurit. Seuraa verkkokortin mukana tulleita ohjeita.

Tarkista onko *wireless configuration service* päällä, OSA 1 vaiheet 1-4. Tämän palvelun pitäisi olla oletuksena päällä Windows XP:ssä.

<u>Vaihe 1:</u>
Avaa Käynnistä-valikko – Settings - Network Connections

Valitse verkkosovitin, joka viittaa langattomaan verkkokorttiin. Paina sen päällä hiiren oikeaa nappia ja valitse *Properties.*

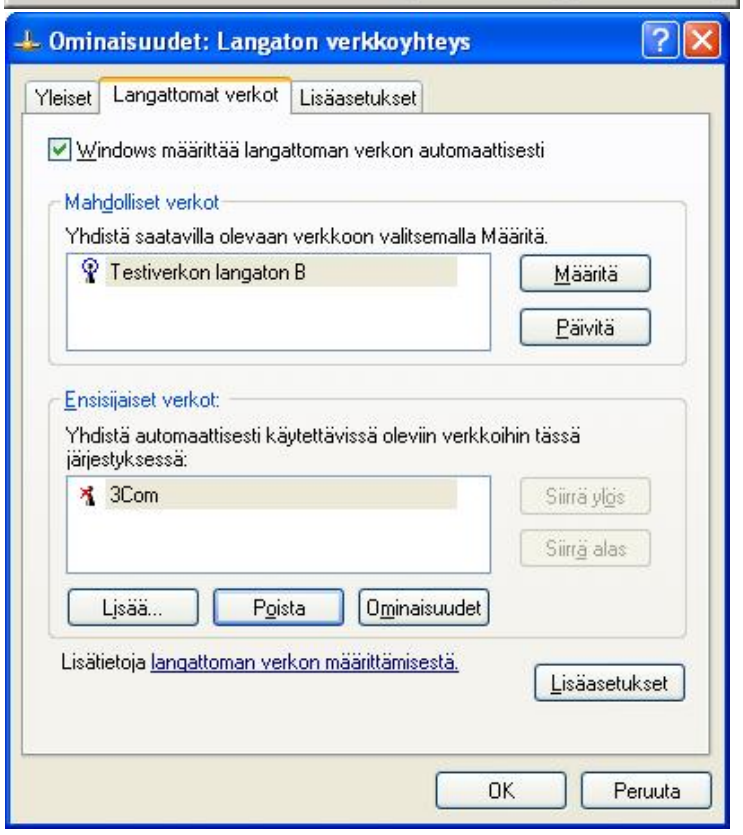




<u>Vaihe 2:</u>
Valitse *Wireless Networks* tai *Langattomat verkot* välilehti. Laita ruksi kohtaan *Use Windows to configure my wireless network settings* tai *Windows määrittää langattoman verkon automaattisesti.* ja paina *Add…* tai *Lisää…*-nappia lisätäksesi SSID:in.

Näkymä on voi olla erilainen riippuen Windows XP versiosta.

Ylempi kuva on englanninkielisestä Windows XP Pro SP2:sta ja alempi kuva suomenkielisestä Windows XP Home Editionista.

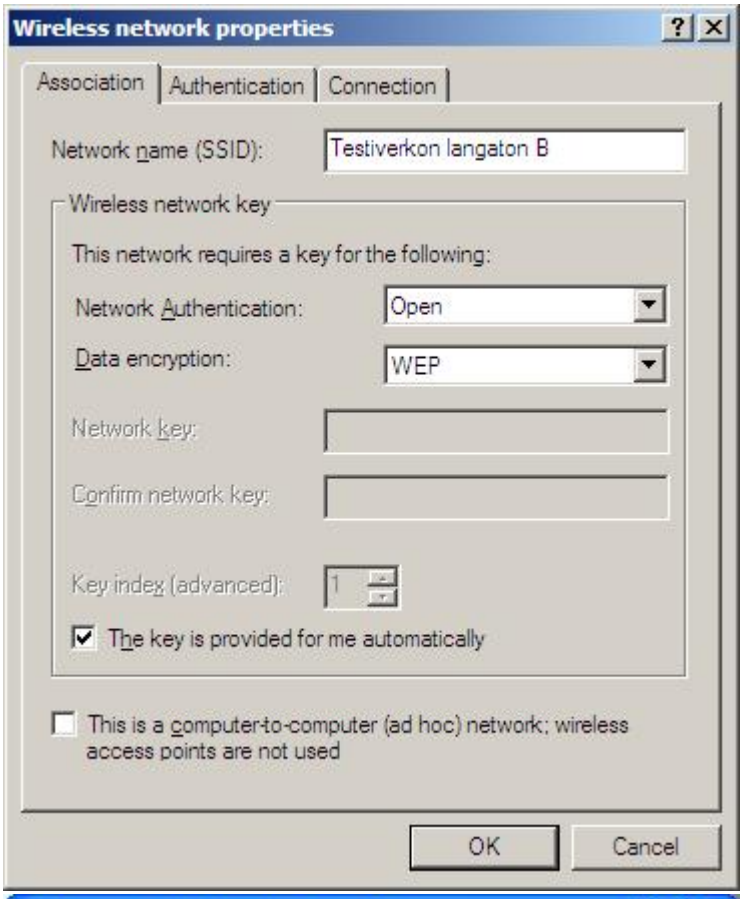


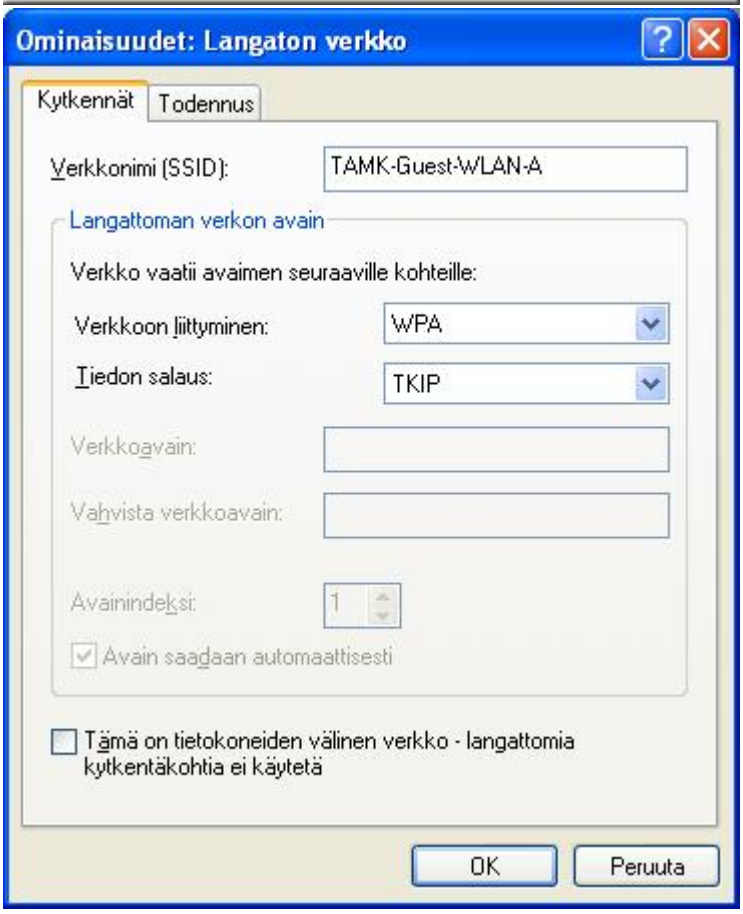
<u>Vaihe 3:</u>
Valitse Association tai *Kytkennät* välilehti. Kirjoita SSID kohtaan TAMK-WLAN-B tai muu vierailijaverkon tunnus (nimi saattaa muuttua).

Korttisi täytyy olla 802.11b tai 802.11g standardin mukainen. 802.11a-standardin mukaiset kortit toimivat rajoitetusti vain tietyissä paikoissa.

Network Authentication / Verkkoon Liittyminen kohtaan tulee WPA.

Data encryption / Tiedon salaus kohtaan tulee TKIP.



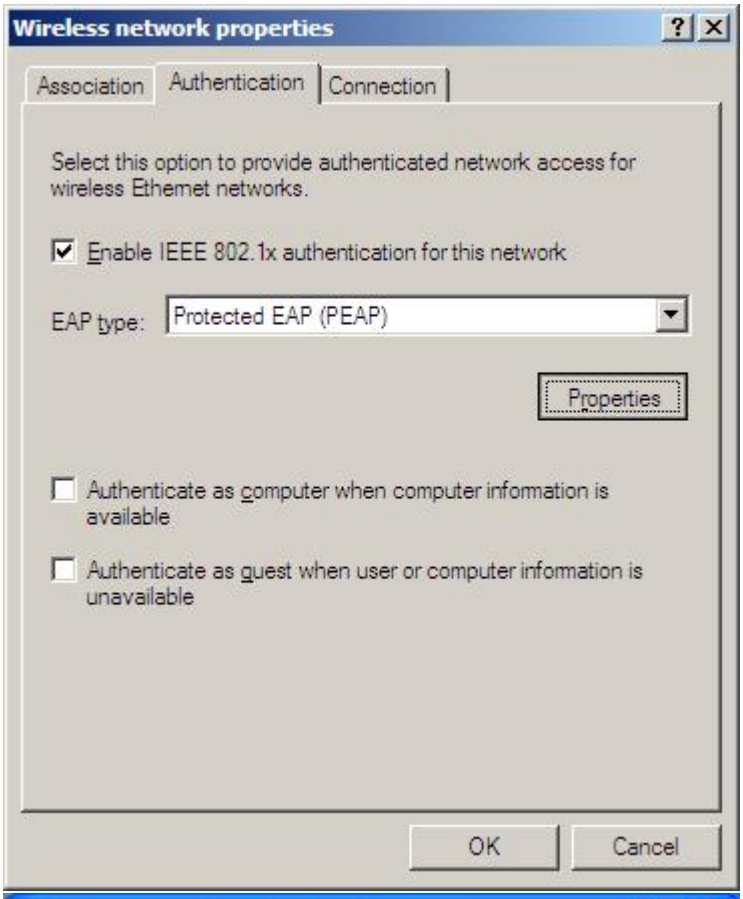


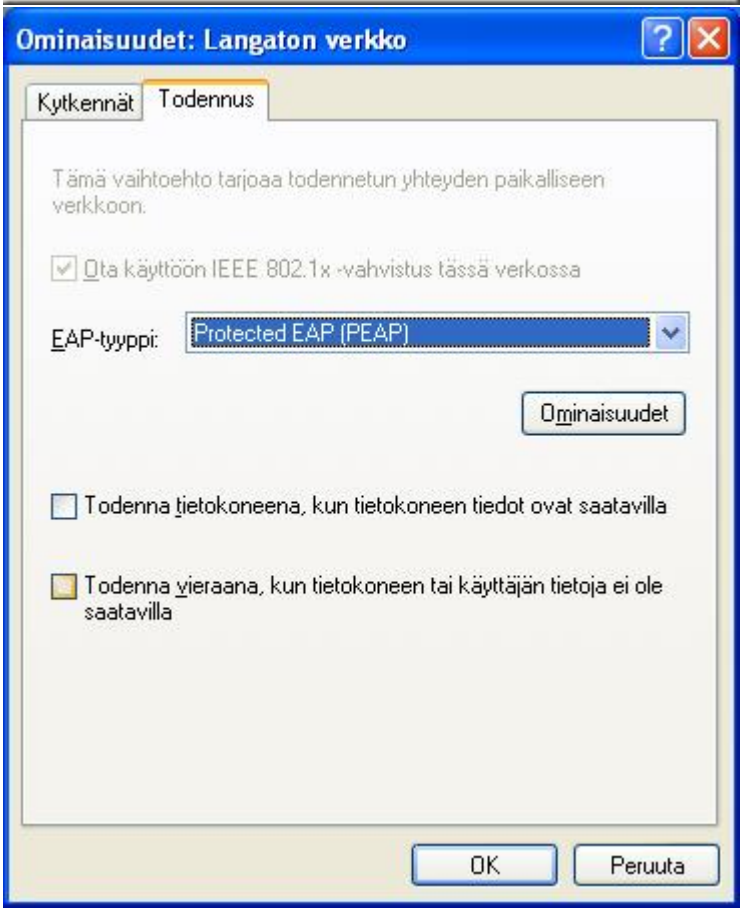
<u>Vaihe 4:</u>
Valitse *Authentication* tai *Todennus* välilehti.

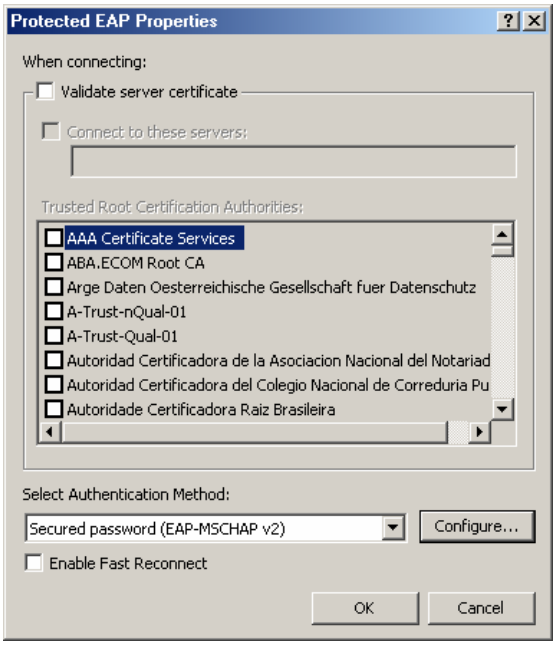
Laita ruksi kohtaan *Enable IEEE 802.1x authentication for this network.*

Ota mahdolliset ruksit pois kahdesta alemmasta kohdasta.

Valitse EAP-tyypiksi *Protected EAP (PEAP)* ja paina *Properties*- tai *Ominaisuudet*-nappia.



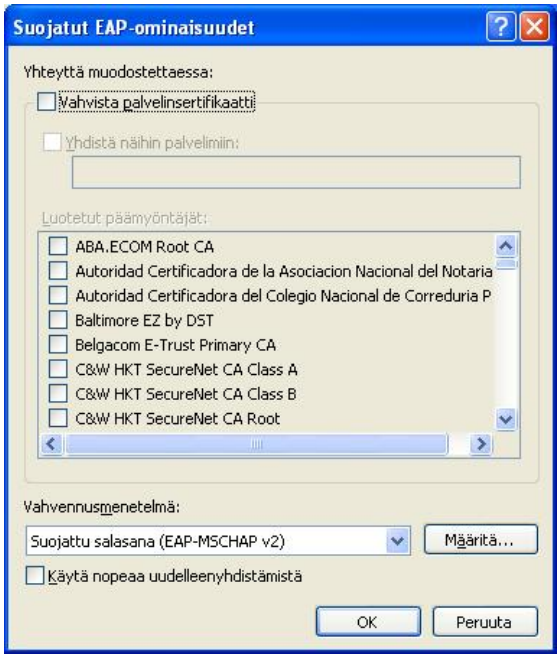




<u>Vaihe 8:</u>
Ota ruksi pois *Validate server certificate* tai *Vahvista palvelinsertifikaatti* kohdasta.

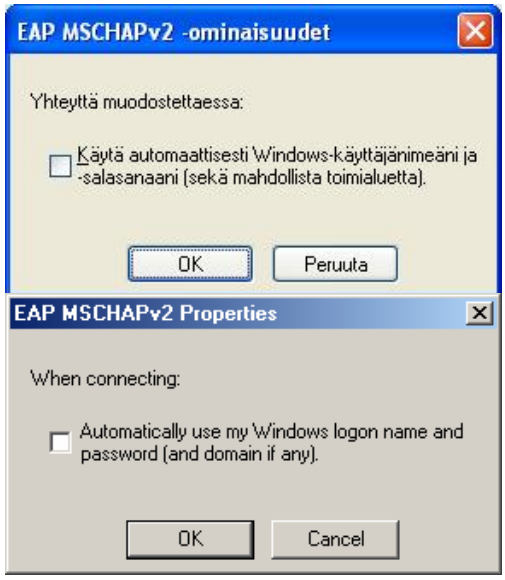
Varmista että *Authentication Method / Vahvennusmenetelmä* on *Secured password (EAP-MSCHAP v2) / Suojattu salasana (EAP-MSCHAP v2).*

Tämän jälkeen paina *Configure…/ Määritä…*

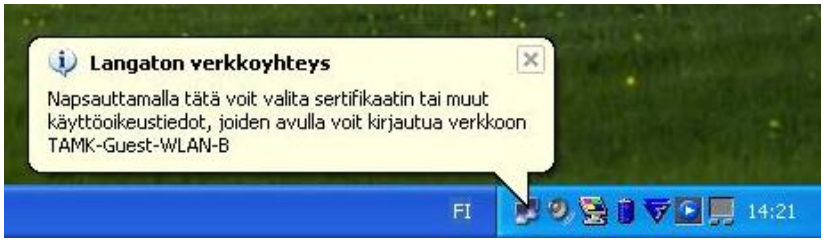


<u>Vaihe 9:</u>
Ota ruksi pois kohdasta *Automatically use my Windows logon name and password (and domain if any)* tai *Käytä automaattisesti Windows-käyttäjänimeäni ja salasanaani (sekä mahdollista toimialuetta).*

Tämän jälkeen sulje kaikki ikkunat ok:lla.



Vaihe 10:
Kuitattuasi kaikki ikkunat OK-painikkeella, pitäisi oikeaan alareunaan tulla puhekupla. Sitä painamalla saat kirjautumisikkunan näkyviin.



Vaihe 11:
Kirjoita käyttäjänimen ja salasanan kohdalle koulun tunnuksesi, joilla normaalistikin kirjaudut verkkoon.

Jätä Logon domain / Kirjautumistoimialue kohta tyhjäksi.

Kuittaa ikkuna OK:lla ja hetken kuluttua yhteyden pitäisi toimia.