TAMPEREEN
AMMATTIKORKEAKOULU

OPINNÄYTETYÖRAPORTTI

Langattoman lähiverkon toteutus

Tuire Vähä-Touru

Tietojenkäsittelyn koulutusohjelma
Huhtikuu 2007
Työn ohjaaja: Harri Hakonen

TAMPERE 2007

TAMPEREEN
AMMATTIKORKEAKOULU

Tekijä(t) Tuire Vähä-Touru

Koulutusohjelma(t) Tietojenkäsittely

Tutkintotyön nimi Langattoman lähiverkon toteutus

Työn valmistumis-kuukausi ja -vuosi Huhtikuu 2007

Työn ohjaaja Harri Hakonen **Sivumäärä:** 50

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee langattoman lähiverkon toteuttamista yrityksessä. Työ on tehty toimeksiannosta tamperelaiselle Anilinker Oy:lle, jossa päätettiin loppukesästä 2006 rakentaa langaton lähiverkkosegmentti kiinteän Ethernet-lähiverkon lisäksi. Langattomalla verkolla haluttiin mobilisoida kannettavien tietokoneiden käyttäjien verkkokäyttöä. Aiemmin käyttäjän liikkumavara oli rajattu lyhyen verkkokaapelin pituuteen, käytännössä korkeintaan pariin metriin.

Opinnäytetyön teoriaosuus on jaettu kahteen lukuun. Luvussa 2 tarkastellaan langattomien IEEE 802.11 -standardin mukaisten lähiverkkojen perusteoriaa. Perusteoriaan kuuluu muun muassa langattoman siirtotien, standardien sekä langattoman verkon laitteiden esittelyä. Lisäksi ensimmäinen osa käsittelee langattoman verkon suunnittelun periaatteita, jotka eroavat hieman perinteisen kaapeliverkon suunnittelun periaatteista erilaisen siirtotien vuoksi. Luvussa 3 tarkastellaan langattoman verkon tietoturvaa ja salausmenetelmiä. Tietoturva mielletään edelleen langattomuuden heikoksi kohdaksi, vaikka uudet salausmenetelmät ovatkin jo paljon kehittyneempiä verrattuna alkuperäisiin menetelmiin.

Opinnäytetyön käytännön osuus esittelee toimeksiantajalle toteutetun langattoman lähiverkon ratkaisuja. Langaton verkkosegmentti toteutettiin perinteisen tukiasemaratkaisun sijaan kytkimellä. Se sijoitettiin tietoturvasyistä erilleen kiinteästä lähiverkosta, palomuurin ulkopuolelle. Langattomia lähiverkkoja toteutettiin käytännössä kaksi, toinen henkilökunnan ja toinen vierailijoiden käyttöön. Molemmat verkot salattiin WPA-TKIP-menetelmällä ja henkilökunnalle tarjottiin pääsy kiinteän lähiverkon resursseihin Virtual Private Network -tunnelia pitkin.

Opinnäytetyön tarkoituksena on toimia teoriapakettina kenelle tahansa lukijalle ja samalla toteutetun langattoman verkon dokumentointina. Työ sisältää myös toteutuksen aikana syntyneitä kehitysideoita ja asioita, joita verkon ylläpitäjien olisi hyvä pohtia kehittäessään verkkoa. Tämä työ on tekijälleen korvaamaton dokumentti toteutetun verkon ylläpidon ja jatkon kehitystoimenpiteiden kannalta.

Avainsanat Langattomat lähiverkot WLAN IEEE 802.11 Tietoturva

TAMPERE
POLYTECHNIC

Author(s)	Tuire Vähä-Touru
Degree Programme(s)	Business Information Systems
Title	WLAN realization
Month and year	April 2007
Supervisor	Harri Hakonen

Pages: 50

ABSTRACT

This thesis discusses WLAN (Wireless Local Area Network) realization in a company. This subject was assigned by Anilinker Oy in Tampere. Decision of building a WLAN to Anilinker Oy was made in late summer 2006. Network usage of laptop users needed to be mobilized. Laptop users' space was earlier limited to the network cables length, to couple of meters at the most.

The theory of this thesis is divided into two chapters. Chapter 2 discusses basics of IEEE 802.11- standard based WLANs. The basics present wireless transmission path, standards and wireless network equipment for instance. In addition also wireless network planning principals are presented. They differ from cable based network planning because of the different transmission path. Data protection and encryption methods are discussed in chapter 3. Data protection in wireless networks is still perceived weak though new encryption methods are more safe and sophisticated than the earlier ones.

The practical part of this thesis presents solutions of the realized wireless local area network. This realization is built by using a wireless switch instead of traditional access points. The wireless network is separated from the local area network and is placed outside of the local area networks firewall, because that secures companys cable based LAN (Local Area Network). Actually two wireless local area networks are implemented in the wireless network segment, the other for staff usage and the other for guests. Both networks are encrypted with WPA-TKIP-method. The staff has ability to connect to the local area network resources via a Virtual Private Network- tunnel.

The meaning of this thesis is to act as theory package for readers and documentation of this wireless network. This thesis includes also ideas and good points for developing this WLAN. These ideas and points should be considered among companys network administrators. This thesis is irreplaceable document for its creator, because it contains material needed for administrating the built wireless local area network in future.

Keywords Wireless local area networks WLAN IEEE 802.11 Data protection

Sisällysluettelo

WLAN-verkkoihin liittyvää käsitteistöä

AES (Advanced Encryption Standard) on toistaiseksi murtamaton 128-bittinen salausalgoritmi.

Alustusvektori Tarkoittaa bittijonoa salausavaimen alussa.

Autentikointi (Authentication) tarkoittaa osapuolen identiteetin todentamista luotettavaksi tai luvalliseksi tahoksi esimerkiksi salasanan avulla.

Bluetooth on tiedonsiirtotekniikka, joka on tarkoitettu lyhyille etäisyyksille. Tarkoituksena on ollut lähinnä yhdistää esimerkiksi matkapuhelin muihin oheislaitteisiin langattomasti (esim. hands-free).

BSS (Basic Service Set), jota kutsutaan myös peruspalveluryhmäksi. Tämä termi kuvaa yhden WLAN (Wireless Local Ara Network) tukiaseman kattamaa aluetta

CCMP (Counter Mode With Cipher Block Chaining Message Protocol) on salausmenetelmä, joka käyttää salaukseen kehittyneempää 128-bittistä AES (Advanced Encryption Standard)- algoritmia. Menetelmää käytetään 802.11i/ WPA2 (Wireless Fidelity/ Wi-Fi Protected Access)- salauksessa.

DHCP (Dynamic Host Configuration Protocol) on protokolla, joka jakaa IP (Internet Protocol)- osoitteita lähiverkkoon kytkeytyville laitteille.

DSSS (Direct Sequence Spread Spectrum) tarkoittaa suorasekvenssitekniikkaa.

EAP (Extensible Authentication Protocol) on käytännössä todennusprotokollan runko, jolla neuvotellaan käytettävä todennusmekanismi.

ESP (Encapsulating Security Payload*)* on salausprotokolla, jolla salataan pakettivirtoja IPSec (Internet Protocol Security) VPN (Virtual Private Network) - tunneloinnissa.

ESS (Extended Service Set) kutsutaan myös laajennetuksi palveluryhmäksi. ESS sisältää useamman WLAN-tukiaseman eli peruspalveluryhmän (Kts. BSS).

Ethernet on laajasti vakiintunut kiinteä lähiverkkotekniikka.

FHSS (Frequency Hopping Spread Spectrum) tarkoittaa taajuushyppelytekniikkaa.

GHz	(gigahertsi, 1 000 000 000 hertsiä) taajuuden yksikkö (Kts. Taajuus).
IEEE	(Institute of Electrical and Electronics Engineers) on järjestö, jonka työryhmät kehittävät ja julkaisevat tietoliikenneverkkoihin liittyviä standardeja.
IKE	(Internet Key Exchange) on avaintenvaihtoprotokolla, jota käytetään IPSec-protokollan kanssa VPN-toteutuksissa.
IPSec	(Internet Protocol Security) joukko tietoliikenneprotokollia, jotka jakavat luottamuksellisuuden, eheyden varmistuksen ja avainten hallinnan eri protokollille (mm. ESP ja IKE).
ISM siirtotaajuus	(Industrial, Scientific and Medical) on maailmanlaajuinen radiotaajuuskaista, jonka käyttöön ei tarvita erillistä lupaa.
LAN	(Local Area Network) on pienen alueen, kuten yrityksen toimipisteen, tietoverkko.
Mbit/s	(megabittiä sekunnissa) on tiedonsiirtonopeus, sekunnissa siirretyn tiedon määrä bitteinä. Megabitti = 1 000 000 bittiä sekunnissa.
Peittoalue	tarkoittaa alaa, jolla WLAN-verkkoa pystytään hyödyntämään kohtuullisella tiedonsiirtonopeudella
RF-signaali	on sähkömagneettinen aalto, joka etenee kahden antennin välissä.
RSN	(Robust Security Network) on IEEE 802.11i -standardin mukainen WLAN.
Salausavain	on merkkijono, jota käytetään tiedon salaamiseen, salauksen purkamiseen tai alkuperän todentamiseen.
SSID	(Service Set Identifier) on verkon uniikki nimi.
Standardi	on jonkin organisaation (esim. IEEE) laatima määritelmä asioiden suositeltavasta toteuttamistavasta.
Taajuus	Taajuuden yksikkö on hertsi (Hz), joka kertoo tapahtuman toistojen määrän sekunnissa.
Thin Access Point	on ominaisuuksiltaan karsittu tukiasema. Thin Access Point -tukiasemia käytetään yleensä WLAN-kytkimiä sisältävissä WLAN-toteutuksissa.

Tiedonsiirtonopeus	kuvaa tiedon siirtymisen nopeutta tietyn ajan sisällä. Yksikkö on yleensä bittiä sekunnissa (bit/s). (Kts. myös Mbit/s.)
TKIP	(Temporal Key Integrity Protocol) on salausmenetelmä, joka käyttää 10 000 paketin välein vaihtuvia pidempiä salausavaimia. TKIP kehitettiin paikkaamaan WEP (Wired Equivalent Policy) -salauksen puutteita.
WEP	(Wired Equivalent Policy) on IEEE 802.11 -standardiin kuuluva liikenteen salausmenetelmä.
WPA	(Wireless Fidelity/ Wi-Fi Protected Access) salausmenetelmä, joka kehitettiin paikkaamaan WEP: n heikkouksia.
WPA2	(Wireless Fidelity/ Wi-Fi Protected Access 2) on kehittyneempi salausmenetelmä, joka perustuu 802.11i-tietoturvastandardiin.
VPN	(Virtual Private Network) termillä tarkoitetaan yleensä suojattua, tunneloitua yhteyttä etäpäätteeltä esimerkiksi internetin yli yrityksen lähiverkkoon.

1 Johdanto

1.1 Yleistä

> *Tukipisteiden määrä kasvaa rivakasti: Langaton lähiverkko 60 prosentilla yrityksistä*
>
> *Jo 60 prosentissa suomalaisista yrityksistä on käytössä langaton lähiverkko. Pohjoismaisista kotitalouksista WLAN on käytössä 7,9 prosentilla. Hotspotien eli wlan-tukipisteiden määrä kasvaa puolestaan kiivaasti.*
>
> *Yritysten WLAN-käyttöä selvitti Market-Visio. Tutkimukseen vastasi 167 yli 20 henkilöä työllistävää yritystä ja julkishallinnon organisaatiota. Vastanneista 62 prosenttia kertoi, että verkon hyödyntäminen yleistyy vuoden 2006 aikana, selviää tutkimustietoja keränneen Ficom ry:n tiedotteesta.* (Reiss 2006.)

Myös Anilinker Oy liittyy näihin langattoman lähiverkon omistaviin yrityksiin tämän opinnäytetyöprosessin aikana. Langattoman verkon edut palvelevat hyvin liikkuvaa käyttäjää, joka hyödyntää yrityksen verkkopalveluita kannettavan tietokoneensa kautta. Langattoman verkon hankintaan päädyttiin Anilinker Oy:llä loppukesästä 2006 ja päädyin tekemään opinnäytetyöni tästä aiheesta.

1.2 Opinnäytetyöni taustat

Opinnäytetyöni perustuu Anilinker Oy:lle toteutettavaan lähiverkon päivitysprojektiin, jossa rakennetaan langaton lähiverkko. Langatonta verkkosegmenttiä ei aiemmin ole ollut yrityksellä käytössä. Aihealue on uusi sekä minulle että muille yrityksen verkkotukihenkilöille. Haastetta verkon suunnitteluun ja toteutukseen tuo langattomien verkkojen vieläkin hieman kyseenalainen tietoturva. Koska langattomassa verkossa tullaan käyttämään yrityksen sisäisiä sovelluksia, intranetiä ja muita liiketoiminnalle kriittisiä sovelluksia, on verkosta saatava riittävän turvallinen ja salattu. Näiden lähtökohtien saattelemana olen tutustunut opinnäytetyötä tehdessäni WLAN (Wireless Local Area Network) -verkkoihin yleisesti sekä olen selvittänyt mitä ratkaisuvaihtoehtoja nykytekniikka tarjoaa tietoturvallisen WLAN-verkon toteuttamiseen.

Langattoman verkon avulla on tarkoitus helpottaa esimerkiksi yrityksen myyjien sekä vierailijoiden liittymistä lähiverkkoon. Myyjät ovat yrityksessä eniten liikkuvaa väkeä. Heillä on käytössään vain kannettava tietokone, jonka he joutuvat aina kytkemään kiinteään verkkokaapeliin, joka rajaa liikkumavaraa.

Opinnäytetyön tavoitteena on saada rakennettua langaton lähiverkko, joka on mahdollisimman tietoturvallinen. Tavoitteeni on myös tutustua itselleni uuteen asiaan ja soveltaa lähdemateriaalien teoriatietoa toteutuksessa. Pyrin saavuttamaan sellaisen osaamistason, että pystyn osallistumaan langattoman verkon ylläpitotehtäviin jatkossa. Pidän tärkeänä, että työn jälkeen minulla on ymmärrys langattomien verkkojen toiminnasta ja projektissa tehdyistä ratkaisuista. Mielestäni asioiden ymmärtäminen on avain hyvään ammattitaitoon.

Työssäni en ole lähtenyt tarkemmin esittelemään itse WKAN-verkon tiedonsiirtotekniikkaa, sillä Teemu Wilkman samalta vuosikurssilta on esitellyt sitä kattavasti omassa työssään ”Tietoturvallinen WLAN-CASE: ICM Finland Oy”. Suosittelenkin tiedonsiirtotekniikasta tarkemmin kiinnostunutta lukijaa käymään läpi Wilkmanin opinnäytetyön luvun 3. *Tiedonsiirtotekniikka.*

1.3 Toimeksiantaja

Toimeksiantajana opinnäytetyölleni toimi tamperelainen IT (Information technology) -alan yritys, Anilinker Oy. Työskentelen Anilinker Oy:llä päätoimisesti asiakaspalveluasiantuntijana, käytännössä yrityksen teknisessä tuessa eli helpdeskissä.

Anilinker Oy:n liiketoimintaan kuuluu yritysten välisten liiketoiminta-prosessien sähköistäminen erilaisilla palveluilla. Anilinker Oy kuvaa itseään sähköisiin ratkaisuihin keskittyneeksi palveluntarjoajaksi ja kansainväliseksi operaattoriksi. Anilinker Oy:n tarjoamien palveluiden asiakas- ja käyttäjäverkostoon kuuluu noin 1300 yritystä 25 eri maasta. Verkostoon kuuluvat yritykset ovat suurimmaksi osaksi teollisuuden alalla toimivia yrityksiä. Anilinker Oy:n toiminta on käynnistynyt jo vuonna 1992. Nykyisellä nimellä yritys on toiminut vuosituhannen alusta lähtien.

Henkilökuntaan kuuluu noin 30 henkilöä. Kiinteä tietokone (Personal Computer, PC) on tällä hetkellä 17 henkilöllä ja kannettavia on käytössä noin 14 kappaletta, tosin kaikki eivät ole samaan aikaan toimitiloissa. Suurin osa kannettavista tietokoneista on käytössä myyjillä, jotka eivät työskentele säännöllisesti toimistossa. Pienellä osalla henkilökunnasta on kannettava käytössään kiinteän PC:n lisäksi, jotta voivat esimerkiksi pitää palaveritiloissa omaa konetta mukana. Karkeasti arvioituna kannettavia koneita on toimitilassa yhtä aikaa käytössä 5-10 kappaletta. Tosin poikkeustilanteissa tämä luku voi nousta muutamalla, mikäli toimitiloissa vierailee kannettavan koneen omistavia vieraita.

Tällä hetkellä yrityksen ainoa toimipiste sijaitsee Tampereen Sarankulmassa, johon myös tutkintotyössä käsitelty langaton lähiverkko rakennetaan. Langaton lähiverkko rakennetaan helpottamaan kannettavien tietokoneiden verkkokäyttöä toimistolla.

1.4 Johdatus lähiverkkoihin

Lähiverkolla (*LAN, Local Area Network*) tarkoitetaan yleisesti pienen alueen, kuten yrityksen yhden toimipisteen, tietoverkkoa. Lähiverkkoon kuuluu työasemia, palvelimia sekä muita verkkolaitteita kuten tulostimia, jotka sijaitsevat fyysisesti lähellä toisiaan. Anilinker Oy:n lähiverkko tarjoaa tärkeitä palveluita käyttäjilleen. Lähiverkon kautta esimerkiksi teknisen tuen käyttäjät pääsevät käyttämään sanomaliikenteen hallintakonsolia, tärkeiden palvelimien ja hakemistojen valvontakonsolia sekä useampaa eri intranetia, joista jokainen palvelee tiettyä tarkoitusta. Windowsin päivitykset jaetaan koneille automaattisesti WSUS (Windows Server Update Services) -palvelimelta lähiverkon koneille. Lähiverkko tarjoaa käyttäjille myös omat ”perinteiset” hakemistokansiot, joihin käyttäjä pääsee käsiksi miltä tahansa lähiverkkoon liittyneeltä päätteeltä. Anilinker Oy:n lähiverkon käyttäjätietokantana palvelee Active Directory -hakemistopalvelu, joka kokoaa selkeästi yhteen kaikki verkon resurssit. Lähiverkkoon tarjotaan pääsy rajatuille käyttäjille myös ulkoverkoista VPN (Virtual Private Network) -tunnelin välityksellä. VPN-käyttäjät autentikoidaan ennen lähiverkkoon pääsyä palomuurin omaa käyttäjätietokantaa vasten.

Lähiverkot ovat tulleet jäädäkseen yritysmaailmaan. Ilman lähiverkkoa yrityksen erilaisten verkkopalveluiden tarjoaminen olisi huomattavasti hankalampaa toteuttaa. Mikäli verkkoa ei ole, tietokoneet toimivat yksittäisinä yksikköinä, joita on käsiteltävä ja päivitettävä konekohtaisesti. Lähiverkko palvelee hyvin tarkoitusta yhdistää toisiaan lähellä olevat verkkolaitteet.

Nykyään yleisimpänä perinteisen kiinteän lähiverkon tekniikkana pidetään Ethernetiä. Ethernetin juuret ulottuvat 1970-luvulle asti. Ensimmäinen mikrotietokoneilla toteutettu Ethernet-verkko tunnetaan nimellä *ALTO ALOHA* ja se toimi ensimmäisen kerran jo vuonna 1973 2,94 Mbit/s siirtonopeudella (Jaakohuhta 2000: 12). Vuonna 1995 nopeus saatiin nostettua jo 100 Mbit/s (*FastEthernet*) ja kolmen vuoden päästä, vuonna 1998, saavutettiin 1 Gbit/s:n siirtonopeus (Wikipedia… Ethernet 2006).

Perinteisen kiinteän lähiverkkoratkaisun rinnalle on yrittänyt kiriä langaton lähiverkko, WLAN (Wireless Local Area Network). Se helpottaa esimerkiksi kannettavien laitteiden lähiverkkoon liittymistä. Kannettavaa laitetta on tällöin helpompi käyttää optimaalisemmasta paikasta ja sen voi siirtää helposti paikasta toiseen kuuluvuusalueen sisällä. Heinosen, Hovatan & Hummelinin (2005: 7) mukaan yleisimpänä lähiverkkotekniikkana tulee lähivuosinakin vielä pysymään kiinteästi kaapeloitu 100 Mbit/s tai Gigabit Ethernet.

2 Langaton lähiverkko (WLAN)

2.1 Yleistä

Erona perinteiseen lähiverkkoon WLAN-verkko käyttää siirtotienä langatonta radiotietä. Muuten langaton verkko voi sisältää samoja verkkolaitteita kuin perinteinen lähiverkko. Tietoturvaa pidetään heikompana, koska radioteitse kulkevaan dataan on epärehellisen tahon helpompi päästä käsiksi. Tästä syystä WLAN-verkkojen yleistyminen yritysmaailmassa on ollut viime vuosina hidasta. Nykyisten standardien parannetut tietoturvaominaisuudet ovat kuitenkin edistäneet käyttöönottoa myös yrityksissä (Hovatta ym. 2005: 7).

Langattomien lähiverkkojen historia alkaa jo 1980-luvulta, jolloin Motorola esitteli ensimmäisen WLAN-tuotteensa, *Altairin*. Ensimmäiset tuotteet sitoivat käyttäjät yhteen laitetoimittajaan, sillä ratkaisut toimivat vain tietyn valmistajan laitteiden kesken. Eri valmistajien laitteet eivät siis toimineet keskenään. Standardikehitys aloitettiin IEEE:n (Institute of Electrical and Electronics Engineers) toimesta vuonna 1990, jonka tuloksena nykyisinkin käytössä oleva standardiperhe 802.11 julkaistiin vuonna 1997. Siirtonopeudet olivat aluksi 1 ja 2 Mbit/s, kun nykyisin on saavutettu jopa 54 Mbit/s teoreettinen siirtonopeus. (Puska 2005: 15)

WLAN-verkkojen toteutukseen liittyy myös haasteita. Tietoturvaa pidetään yhtenä haasteellisimmista toteutettavista seikoista. Mielestäni tietoturva voidaan tänä päivänä saada kuitenkin riittävän turvalliselle tasolle uhkista huolimatta, sillä salaukseen käytettävät menetelmät ovat kehittyneet viime vuosina. Suorituskyky on heikompi verrattuna langalliseen toteutukseen, koska siihen vaikuttavat myös radiosignaalien ulkoiset häiriöt, kuten kalusteet, ihmiset ja sääolosuhteet. Puskan (2005: 99) mukaan todellinen siirtonopeus olisi WLAN-verkoissa 60–70 % ilmoitetusta bittinopeudesta. Hovatan ym. (2005: 12) mukaan esimerkiksi teoreettinen 54 Mbit/s nopeus tarkoittaisi käytännössä vain 22 Mbit/s siirtonopeutta. Tällöin todellinen siirtonopeus olisi vain noin 40 % teoreettisesta. Erilaisista asiantuntijoiden näkemyksistä päätellen voisi todeta, että täyttä varmuutta todellisesta siirtonopeudesta ei ole. Todellinen siirtonopeus riippuu luullakseni paljon ympäristöstä, johon verkko rakennetaan. Voisiko tästä siis päätellä, että mitä vähemmän esteitä ja häiriöitä, sitä lähempänä todellinen siirtonopeus on teoreettista? WLAN-verkkojen suunnittelu on vaikeampaa, sillä erilaisia häiriötekijöitä on vaikea huomioida aina etukäteen. (Puska 2005: 21–22.)

2.2 Langaton siirtotie

WLAN-verkossa tieto kulkee langattomasti radioteitse. Tieto siirretään valosignaaleina tai yleisimmin RF (Radio Frequency) -signaaleina. Koska valosignaaleja käytetään tavallisten WLAN-verkkojen sijaan enemmän esimerkiksi rakennusten välisissä WLAN-linkeissä (Geier 1 2005: 76), en perehdy niihin opinnäytetyössäni tarkemmin.

RF-signaali on sähkömagneettinen aalto, joka etenee kahden antennin välissä. Toinen antennin pää sijaitsee lähettävässä ja toinen vastaanottavassa laitteessa. RF-signaali koostuu amplitudista, taajuudesta ja vaiheesta. *Amplitudi* kertoo signaalin voimakkuuden, joka heikkenee etäisyyden kasvaessa. Geier vertaa amplitudin voimaa "*ponnistukseen, joka henkilön on tehtävä ajaakseen polkupyörällä tietyn matkan*". Mitä enemmän voimaa, amplitudia, sitä pidemmälle pääsee. *Taajuus*, Hz (hertsi) kertoo, montako kertaa signaali värähtelee sekunnissa. Esimerkiksi taajuudella 2,4 GHz signaali värähtelee siis 2400 000 000 kertaa sekunnissa. Kolmas elementti on *vaihe*. Se kertoo signaalin poikkeaman viitepisteestä. Polkupyörä esimerkkiä soveltaen vaihe kertoo, missä kohtaa pyörämatkaa ollaan menossa. (Geier 1 2005: 70-72.)

RF-signaaleiden heikkouksia ovat mm. herkkyys ulkoisille häiriöille ja tietoturvan heikko laatu. Ulkoisia häiriöitä ovat esimerkiksi interferenssi ja heijastuminen. *Interferenssissä* on kaksi samantyyppistä signaalia läsnä vastaanottavassa päässä yhtä aikaa. Tämä tilanne haittaa viestintää lähettäjän ja vastaanottajan välillä ja suorituskyky heikkenee. Geier vertaa tilannetta siihen, kun yksi henkilö yrittää kuunnella kahden ihmisen puhetta samaan aikaan. RF-signaalin osat kulkevat eri "polkuja" lähteestä kohteeseen, esimerkiksi kannettavasta tukiasemaan. Osa signaalista kulkee suoraan kohteeseen ja toinen osa voi esimerkiksi kimmota pöydästä kattoon ja katosta tukiasemaan. Tätä kutsutaan *heijastumiseksi* ja se aiheuttaa käytännössä viivettä RF-signaalin kulkuun pidemmän kulkumatkan vuoksi. (Geier 1 2005: 73-74.)

2.3 Keskeiset käyttösovellutukset

WLAN-teknologiaa voidaan hyödyntää erilaisissa käyttökohteissa. Käyttökohteita ovat esimerkiksi *yrityksen lähiverkko*, *WLAN-toimialasovellukset* sekä *julkiset WLAN-palvelualueet* eli ns. hotspotit (Hovatta ym. 2005: 9-10).

Yrityksen lähiverkko

Tätä pidetään ehkä yleisimpänä langattoman teknologian käyttökohteena. Yrityksessä langattomuus mahdollistaa mm. kannettavien tietokoneiden vapaan sijoittelun ja liikkuvuuden kuuluvuusalueen sisällä. Yritykseen langaton verkko rakennetaan yleensä kattamaan vain ne tilat, joissa sitä on tarpeen käyttää. Yrityksen WLAN-verkko koostuu yleensä esimerkiksi seuraavista osista:

- Tukiasemat
- WLAN-kytkin
- Liitäntä yrityksen lähiverkkoon (langalliseen)
- Palomuuri
- Liityntä Internetiin

Yritysten WLAN-verkkojen kohdalla on syytä muistaa tietoturvauhat. Verkko on lähes poikkeuksetta salattava ja siinä on oltava vahva tunnistautumismenetelmä, etteivät ulkopuoliset käyttäjät pääse käsiksi verkossa liikkuvaan dataan.(Hovatta ym. 2005: 9-10.)

WLAN-toimialasovellukset

Henkilöhakujärjestelmiä sekä langattomia puhelimia on hyödynnetty eri toimialoilla esimerkiksi erilaisissa tavoitettavuussovelluksissa. Näiden avulla voidaan paikantaa ihmisiä sekä tavaroita. Terveydenhuoltosektorilla voidaan haluta paikantaa henkilökuntaa tai potilaita, turvallisuussektorilla taas esimerkiksi vanginvartijoita hätätilanteen sattuessa. WLAN tarjoaa paremmat paikallistamismahdollisuudet sisätiloissa, kun taas aiemmin käytetty GPS (Global Positioning System) -paikannus toimii vain ulkotiloissa. (Hovatta ym. 2005: 10.)

Julkiset WLAN-palvelualueet (hotspot)

Julkisiin WLAN-verkkoihin eli ”hotspoteihin” voi törmätä esimerkiksi hotelleissa, lentokentillä tai jopa kahviloissa. Näillä alueilla langattomuutta tukevilla verkkolaitteilla voi saada yhteyden internetiin (Hovatta ym. 2005: 10).

Näitä julkisia palvelualueita voi etsiä internet-sivustolta www.wi-fihotspot-list.com mm. kadunnimen, kaupungin ja maan perusteella. Näin voi esimerkiksi tarkistaa Tampereen julkiset palvelualueet (Puska 2005: 19). Epäilen tosin sivuston ajantasaisuutta, sillä sen mukaan Tampereen alueella olisi tällä hetkellä (20.10.2006) vain kaksi hotspotia osoitteissa:

Sonera IN, Hatanpaan Valtatie 18–20, Tampere, 33101, Finland
Sonera IN, Pyharanta 4, Tampere, 33101, Finland

2.4 Keskeiset standardit

Standardien tavoite on saada eri valmistajien laitteet toimimaan yhdessä. WLAN-verkot perustuvat yleensä IEEE 802.11 standardiperheeseen. Tämä standardiperhe on julkaistu 1997 ja siitä on muodostunut ns. perusstandardi langattomissa lähiverkoissa (Hovatta ym. 2005: 11). Esittelen seuraavaksi mitä standardeja 802.11-perhe pitää sisällään.

Tämä standardiperhe perustuu alkuperäiseen 802.11-standardiin, joka tarjosi vain 1 ja 2 Mbit/s siirtonopeuden. Alkuperäinen standardi määrittelee kolme tiedonsiirtomenetelmää (Frequency Hopping Spread Spectrum eli FHSS, Direct Sequence Spread Spectrum eli DSSS ja infrapunatekniikat) sekä kaksi verkkotopologiaa (Ad-hoc ja infrastruktuuriverkko), jotka on esitelty aliluvussa 2.5 *Langattoman verkon topologioista*. *IEEE 802.11b* toi parannuksena alkuperäisen 802.11-standardin nopeuksiin (1 ja 2 Mbit/s) nähden paremmat teoreettiset siirtonopeudet 5,5 Mbit/s ja 11 Mbit/s. 802.11b-standardi on ominaisuuksillaan edistänyt WLAN-markkinoiden nopeaa kasvua. Se käyttää alkuperäisen standardin tavoin ISM (Industrial, Scientific and Medical) -siirtotaajuutta 2,4 Ghz ja on yhteensopiva 802.11g-standardin kanssa, koska ne molemmat käyttävät samaa tiedonsiirtomenetelmää. Vuonna 1999 802.11b-standardin lisäksi julkaistiin myös *IEEE 802.11a.* Tämä standardi tarjoaa jopa teoreettisen 54 Mbit/s nopeuden, joka on huomattavasti korkeampi kuin edeltävissä standardeissa. 802.11a käyttää ISM-siirtotaajuutenaan harvinaisempaa 5 Ghz:ä, joka tarjoaa parempaa suorituskykyä useampien häiriöttömien kanaviensa ansiosta. Taajuus on häiriöttömämpi verrattuna ruuhkaiseen 2,4 Ghz:n taajuuteen. Peittoalue ei yllä 2,4 Ghz:n taajuuden laajuuteen, mutta käyttämänsä taajuuden ansiosta 802.11a tukee raskaampien sovelluksien käyttöä WLAN-verkossa. (Hovatta ym. 2005: 11; IEEE-SA 2005.)

802.11b-standardin kanssa yhteensopiva *IEEE 802.11g* on myös saavuttanut julkisuutta edellä mainittujen lisäksi. Myös 802.11g yltää teoreettiseen 54 Mbit/s tiedonsiirtonopeuteen, mutta käyttää ruuhkaisempaa 2,4 Ghz:n taajuutta. Vaikka 802.11g toimii yhdessä 802.11b standardin mukaisten laitteiden kanssa, ei 802.11g saavuta maksiminopeuttaan, jos samassa verkossa on käytössä molempien standardien mukaisia laitteita. (Hovatta ym. 2005: 12; IEEE-SA 2005.)

Kutsun 802.11-, 802.11b-, 802.11a- ja 802.11g-standardeja niin sanotuiksi perusstandardeiksi, koska ne määrittelevät esimerkiksi käytettävän taajuuden ja siirtonopeuden. Seuraavaksi esittelen standardeja, jotka tarjoavat lisäominaisuuksia WLAN-verkkoihin.

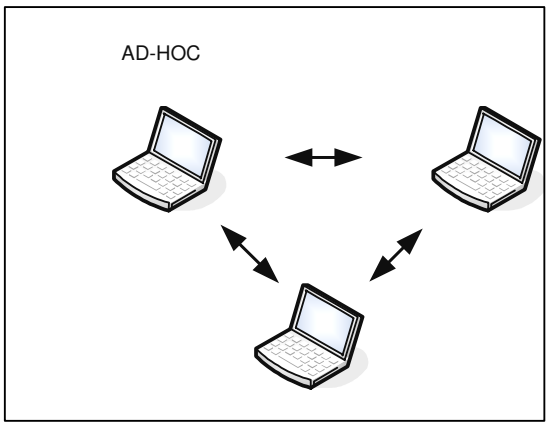
IEEE 802.11h on a-standardista kehittyneempi versio, jonka mukaiset laitteet pystyvät säätelemään lähetystehoaan ja valitsemaan käytettävän kaistan dynaamisesti (Hovatta ym. 2005: 11-12). Näillä ominaisuuksilla on pyritty paikkaamaan a-standardin puutteita. 802.11h käyttää 5 Ghz:n taajuutta Euroopan alueella (IEEE-SA 2006).

IEEE 802.11n -standardin tavoite on tarjota 4-5-kertaiset nopeudet verrattuna a- ja g-standardeihin. Teoreettinen nopeus olisi siis jo 250 Mbit/s luokkaa ja käytännössä nopeudet olisivat kiinteän 100 Mbit/s Ethernetin tasolla. (Hovatta ym. 2005: 12.)

IEEE 802.11i on uudenaikainen tietoturvastandardi, joka sisältää paremmat salausmenetelmät TKIP (Temporal Key Integrity Protocol) ja CCMP (Counter Mode With Cipher Block Chaining Message Protocol). 802.11i tarjoaa myös paremman salausalgoritmin, AES (Advanced Encryption Standard) -protokollan, jota pidetään erittäin vahvana salausmekanismina. Tätä standardia käytetään pääasiassa 802.1x-käyttäjäntunnistusta hyödyntävissä järjestelmissä. 802.11i edellyttää verkossa käytettävän standardia tukevia tukiasemia ja verkkokortteja, mikä saattaa aiheuttaa hankintakustannuksia standardin käyttöönotossa. (Hovatta ym. 2005: 12; Puska 2005: 83–85.)

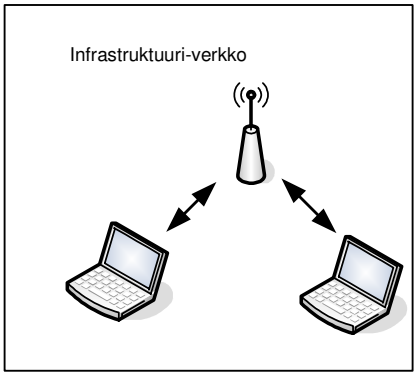
2.5 Langattoman verkon topologioista

Perusstandardi 802.11 esittelee siis kaksi WLAN-topologiaa, Ad-Hoc- sekä infrastruktuuriverkon. Ad-Hoc-verkko koostuu yleensä kannettavista työasemista, jotka kommunikoivat suoraan keskenään ilman tukiasemaa. Tällaista verkkotyyppiä voidaan käyttää lähinnä pienessä ryhmässä lyhyen kantaman sisällä. Kuvassa 2.1. on esitetty Ad-Hoc-verkon rakenne yksinkertaisimmillaan.



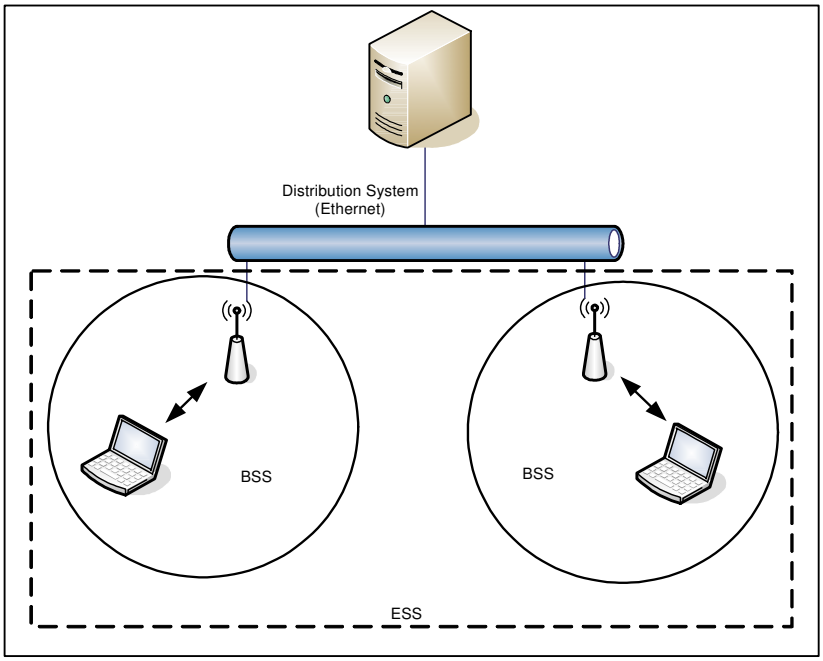
Kuva 2.1 Ad-Hoc-verkko

Infrastruktuuriverkko koostuu työasemien lisäksi vähintään yhdestä tukiasemasta, jolla liitytään langalliseen verkkoon.(Hovatta ym. 2005: 11.) Kuvassa 2.2. on esitetty infrastruktuuriverkon rakennetta yksinkertaisimmillaan.



Kuva 2.2 Infrastruktuuri-verkko

Yhden tukiaseman kattamaa aluetta, solua, kutsutaan *peruspalveluryhmäksi* (Basic Service Set, BSS). Kun näitä peruspalveluryhmiä on verkossa useita, tarvitaan jakelujärjestelmä (Distribution System), joka on yleensä kiinteä Ethernet-lähiverkko. Kun WLAN sisältää useamman peruspalveluryhmän, sitä kutsutaan *laajennetuksi palveluryhmäksi* (Extended Service Set, ESS).(Puska 2005: 132-133.) Kun peruspalveluryhmiä on samassa verkossa useampia, tulee niiden välille järjestää etäisyyttä, etteivät ne häiritse toistensa liikennöintiä. Tätä seikkaa ratkotaan kanavasuunnittelulla, johon palaan hieman tarkemmin tämän luvun aliluvussa 2.6 *WLAN-verkon suunnittelu*. Kuva 2.3. esittää laajennetun palveluryhmän rakennetta.



Kuva 2.3 Laajennettu palveluryhmä (Extended Service Set, ESS)

2.6 Langattoman verkon laitteet

Langaton radioverkko toteutetaan käytännössä *tukiaseman* (access point) avulla. Tukiasema siltaa liikennettä päätelaitteen ja langallisen verkon välillä sekä huolehtii muun muassa liikenteen salaamisesta ja käyttäjien autentikoinnista. Niin sanottujen perinteisten tukiasemien lisäksi on olemassa Thin Access Pointeja, joita käytetään yleensä WLAN-kytkimien kanssa. Thin Access Point on tukiasema, josta on karsittu ominaisuuksia ja toimintoja, jolloin tällainen asema toimii käytännössä pelkkänä radiolähettimenä. (Hovatta ym. 2005: 13-15.)

WLAN-kytkimelle voidaan keskittää tukiasemien toimintoja, jolloin voidaan hankkia ”kevyempiä” ja täten halvempia Thin Access Point -tukiasemia. Kytkimelle keskitettyjen toimintojen avulla esimerkiksi ohjelmistopäivityksiä saadaan jaettua usealle tukiasemalle kerralla eikä uutta tukiasemaa tarvitse erikseen konfiguroida, kun se voi hakea valmiit asetukset kytkimeltä. WLAN-kytkimen käyttö on edullisinta verkoissa, joissa on useita tukiasemia. (Hovatta ym. 2005: 15-16.)

Langattomasta verkosta löytyy myös *päätelaitesovittimia*, jotka sijaitsevat käytännössä esimerkiksi kannettavassa tietokoneessa. Vanhempiin koneisiin voi joutua hankkimaan tällaisen sovittimen erikseen, mutta uudet kannettavat sisältävät useimmiten jo sisäänrakennetun WLAN-verkkosovittimen vakiona (Hovatta ym. 2005: 17).

Antennit kuuluvat yleensä vakiona useimpiin WLAN-laitteisiin. Ympärisäteilevillä vakioantenneilla saadaan yleensä riittävä peittoalue. Peittoaluetta voi kuitenkin joskus olla tarpeen suunnata ja kohdistaa tietylle alueelle. Tällöin vakioantennit korvataan suuntaavilla antennityypeillä kuten esimerkiksi paneeliantennilla, joka asennetaan seinään. Suuntaavia antenneja käytettäessä tulee huomioida erityisesti lähetystehojen pysyminen säädöksien rajoissa. Vakioantenneilla näitä rajoja ei yleensä pysty ylittämään vahingossa. (Hovatta ym. 2005: 16.)

2.7 WLAN-verkon suunnittelu

On olemassa käytäntöjä, joita suositellaan noudatettavaksi WLAN-verkkoa suunnitellessa. Suunnitelma on tietysti aina yksilöllinen riippuen käyttötarkoituksesta ja ympäristöstä. On kuitenkin olemassa muutamia yleisiä seikkoja, jotka on hyvä ottaa huomioon WLAN-verkon suunnittelussa.

2.7.1 Vaatimusmäärittely ja verkkosuunnitelma

WLAN-verkon suunnittelussa voitaneen soveltaa perinteisten lähiverkkojen suunnitteluperiaatteita. Kuten verkkoprojektit yleensä, myös WLAN-verkon suunnittelu aloitetaan vaatimusmäärittelyllä. Vaatimusmäärittelyssä tulee ottaa huomioon loppukäyttäjien määrä, sijainti sekä käytetyt sovellukset (Hovatta ym. 2005: 19). Langatonta lähiverkkoa suunnitellessa tulee huomioida erityisesti tietoturvan tarve. On hyvä tietää kuinka kriittistä tietoa WLAN-verkon kautta tulee siirtymään. Yritysten WLAN-verkon kautta käytetään useimmiten kiinteän lähiverkon sisäisiä sovelluksia ja tästä syystä tietoturvataso on tarpeen olla korkea.

Vaatimusmäärittelyyn pohjaten tehdään verkkosuunnitelma. Verkkosuunnitelma sisältää esimerkiksi verkko- ja sähköpistokepisteiden selvityksen, tukiasemien sijoittelu- sekä konfigurointisuunnitelman ja käytettävät kanavat. Suunnitelmaan sisältyy myös selvitys siitä, miten WLAN-verkko ja kiinteä lähiverkko tullaan yhdistämään. Verkkosuunnitelman yhteydessä tulee kartoittaa myös radiotien häiriölähteet, kuten seinämateriaalit ja suuret metalliset esineet, mikroaaltouunit sekä mahdolliset langattomat sisäpuhelimet, kaiuttimet ja kuulokkeet.(Hovatta ym. 2005: 19.) Nykyään lienee myös tarpeen selvittää muut samalla alueella toimivat WLAN-toteutukset, sillä samalla 2,4 GHz:n taajuudella ja päällekkäisillä kanavilla toimivat verkot häiritsevät toistensa liikennöintiä. Langaton Bluetooth-järjestelmä voi aiheuttaa myös häiriöitä langattomaan lähiverkkoon, sillä se toimii samalla 2,4 GHz:n taajuudella ja käyttää osittain samoja kanavia kuin WLAN- verkko. Bluetoothilla voidaan yhdistää esimerkiksi matkapuhelin langattomasti erilaisiin oheislaitteisiin, kuten tulostimeen tai hands-free-laitteeseen.

2.7.2 Katselmus ja tukiasemien sijoittelu

Jotta häiriölähteet sekä riittävä peittoalue saadaan varmistettua, on paikan päällä hyvä suorittaa katselmus (Site Survey). Katselmuksessa saadaan selville langattoman verkon peittoalue, suorituskyky sekä häiriölähteet. Sen avulla voidaan selvittää myös laiteasennusten yksityiskohdat ja sitä varten olisi hyvä rakentaa ne olosuhteet laitteiston sekä ympäristön osalta, jotka tulevat olemaan myös lopullisessa verkossa. Eli rakennetaan testiverkko, joka vastaa lopullista verkkototeutusta. Peittoalueen mittaaminen aloitetaan sijoittamalla tukiasema toivotulle alueelle. Tämän jälkeen kävellään kannettavan laitteen kanssa ja haetaan alue, jossa bittinopeus pysyy vielä vaaditulla tasolla. Saatujen mittaustulosten perusteella voidaan määrittää lopulliset asennuspaikat kuuluvuusalueineen ja ne voidaan merkitä pohjapiirustukseen. (Puska 2005: 220-222.)

2.7.3 Kanavasuunnittelu

WLAN-verkkoa suunnitellessa on suoritettava kanavasuunnittelua varsinkin silloin, kun verkkoon aiotaan asettaa useampi tukiasema. 2,4 GHz:n siirtotaajuudella toimivien verkkojen kanavien taajuudet menevät hieman päällekkäin. Esimerkiksi 802.11b-standardilla toteutetussa verkossa on Euroopan alueella käytettävissä 13 kanavaa, jotka on jaettava useamman tukiaseman kesken (Geier 2005 2B). Yhden tukiaseman verkossa kanavavalinta ei ole niin olennainen, sillä se voi periaatteessa käyttää mitä tahansa kanavaa 13:sta. Isommissa, esimerkiksi kolmen tukiaseman verkoissa, on tukiasemille valittava omat kanavat, jotka ovat riittävän ”kaukana” toistensa taajuusalueilta. Euroopassa kolmen tukiaseman verkossa tulisi tukiasemille jakaa esimerkiksi kanavat 1, 7 ja 13 (Seppänen). Kanavien päällekkäisyys tulee huomioida useampi kerroksissa rakennuksissa myös eri kerrosten välillä, sillä WLAN-verkko ”kuuluu” myös ylä- sekä alapuolelle (Geier 2005 2B).

Mikäli kanavasuunnittelu 2,4 GHz:n siirtotaajuuden verkossa osoittautuu mahdottomaksi, on aiheellista harkita verkon toteuttamista 5 GHz:n siirtotaajuutta käyttävällä 802.11a-standardilla. Tällä siirtotaajuudella on käytettävissä kahdeksan kanavaa (Euroopassa), joiden taajuudet eivät mene päällekkäin (Seppänen). Suorituskyky on myös parempi, koska 5 GHz:n siirtotaajuudella on vähemmän häiriöitä ja ruuhkaa. 802.11a-standardin mukaisessa verkossa on tosin lyhyempi kantama, jonka vuoksi isompaa verkkoa rakentaessa tukiasemia joudutaan hankkimaan useampia. Yhteensopivuuden puute 802.11b- ja 802.11g-standardien mukaisten laitteiden kanssa voi myös aiheuttaa ongelmia. Sekä tukiasemien, että päätteiden verkkokorttien on tuettava a-standardia, jotta yhteys toimii. (Geier 2005 2A.)

2.7.4 VLAN (Virtual LAN) osana WLAN-verkkoa

Nykyään WLAN-verkkoon on mahdollista implementoida useampia loogisia verkkoja eli virtuaalisia lähiverkkoja (VLAN, Virtual Local Area Network). Virtuaaliset lähiverkot voidaan toteuttaa käyttämällä useaa SSID (Service Set identifier) -tunnistetta. SSID on verkon uniikki nimi, joka erottaa eri WLAN-verkot toisistaan. Yksi fyysinen tukiasema voidaan siis jakaa useaan loogiseen tukiasemaan. Samaan verkkoon voidaan toteuttaa esimerkiksi yksityinen verkko ja vierasverkko, joihin asetetaan esimerkiksi eri tietoturvapolitiikat, palvelut ja oikeudet. (Geier 2005 2C.)

Usean SSID:n ja VLAN-toteutusten käyttäminen edellyttää ominaisuutta tukevien verkkolaitteiden hankkimista. Perinteiset tukiasemat tukevat yleensä vain yhtä SSID:tä (Geier 2005 2C).

3 WLAN ja tietoturva

3.1 Uhat

Tietoturvauhat WLAN-verkoissa voidaan jakaa *aktiivisiin* ja *passiivisiin* uhkiin. Aktiivisia uhkia ovat *palvelunestohyökkäykset* ja *välistävetohyökkäykset*. Palvelunestohyökkäyksissä hakkeri tulvittaa verkkoa esimerkiksi suurella määrällä turhia palvelu- tai liityntäpyyntöjä, jotka voivat kaataa koko verkon. Välistävetohyökkäyksissä, jotka tunnetaan myös nimellä *man-in-the-middle,* hakkeri voi asettaa langattomien päätteiden ja tukiasemien "väliin" oman laitteensa, niin sanotun rosvotukiaseman. ARP (Address Resolution Protocol) -protokollan avulla hakkeri voi huijata lähettävää ja vastaanottavaa päätä esittämällä luotettavan laitteen IP (Internet Protocol) -osoitetta omanaan. Näin hakkeri saa ohjattua liikennettä itselleen. Tällainen rosvotukiasema voi tulla verkkoon myös luvallisen ja vilpittömän käyttäjän toimesta. Tästä syystä verkon tukiasemia on tarkkailtava koko ajan. Käyttäjän ja tukiaseman välillä tulisi myös käyttää kahdensuuntaista todennusta, jossa sekä käyttäjä että tukiasema tunnistautuvat toisilleen. Aktiivisia uhkia voidaan torjua myös rajoittamalla palvelupyyntöjen määrää ja käyttämällä SARP (Secure Address Resolution Protocol) -protokollaa hyödyntäviä laitteita verkossa. SARP:n käyttöönotto tosin edellyttää erikoisohjelmistojen asentamista kaikille laitteille. (Geier 1 2005: 173-176; Puska 2005: 69.)

Passiivisiin uhkiin kuuluvat liikenteen *salakuuntelu* ja *analysointi*. Salakuuntelemalla hakkeri voi kerätä tietoa, jonka avulla tunkeutua verkkoon. Salakuuntelu onnistuu antennien avulla ja sitä on vaikea estää tai havaita. Analysoimalla liikennettä hakkeri voi saada selville luottamuksellistakin tietoa. Hakkerin työtä helpottamaan on olemassa valmiita ohjelmia, joiden avulla hakkeri voi saada pahimmillaan selville jopa salausavaimet.(Puska 2005: 69.)

3.2 Salaus langattomissa lähiverkoissa

Esittelen seuraavaksi neljä WLAN-verkoissa käytettävää menetelmää, jolla verkkoa voidaan salata. Näistä WEP (Wired Equivalent Policy) edustaa heikoimpana tunnettua menetelmää. Yrityskäyttöön WEP-salausta ei suositella käyttämään. Yrityskäyttöön soveltuvat paremmin WPA (Wireless Fidelity/ Wi-Fi Protected Access) sekä kehittynein WPA2. WLAN-verkoissa voidaan myös hyödyntää salaukseen VPN-tunnelointia esimerkiksi silloin, kun se rakennetaan erilleen kiinteästä lähiverkosta.

3.2.1 WEP (Wired Equivalent Policy)

WEP-salaus on IEEE 802.11 -standardiin kuuluva liikenteen salausmenetelmä, joka on laajasti tuettu (Hovatta ym. 2005: 28). Oikeastaan kukaan ei tunnu suosittelevan tänä päivänä WEP-salauksen käyttöä varsinkaan langattomissa yritysverkoissa. Tämä johtunee siitä, että WEP sisältää paljon heikkouksia, joiden vuoksi se on helppo murtaa.

WEP-salauksessa tukiasemiin ja päätelaitteisiin määritetään staattinen salausavain, joka on sama kaikissa laitteissa. Kaikki data salataan siis samalla avaimella. Samana pysyvän avaimen voi selvittää kuuntelemalla liikennettä. WEP:n salausavain on yleensä 128 bittiseksi merkitty avain, joka koostuu 24 bitin alustusvektorista ja 104 bitin avaimesta (Hovatta ym. 2005: 28). Tätä avainta käytetään lähettävässä päässä datan salaukseen ja vastaanottavassa päässä avaimen avulla puretaan salattu datapaketti ja tarkistetaan koskemattomuus. Datapaketin lyhyen ja salaamattoman alustusvektorin voi arvata melko suurella varmuudella, koska tarkalleen ottaen 2^{24}=16,7*10^6 paketin jälkeen samaa alustusvektoria joudutaan käyttämään uudelleen (Sikora 2003: 154).

3.2.2 WPA (Wireless Fidelity/ Wi-Fi Protected Access)

WPA kehitettiin korjaamaan WEP:n puutteita ja mukaan on saatu myös tuki käyttäjien autentikoinnille (Hovatta ym. 2005: 29). WPA käyttää salaukseen 10 000 paketin välein vaihtuvia pidempiä salausavaimia. Tämä menetelmä tunnetaan nimellä TKIP (Temporal Key Integrity Protocol). WPA-salausmenetelmässä käyttäjien autentikointi voidaan toteuttaa IEEE 802.1x -protokollan avulla. 802.1x autentikoi erillisen tunnistuspalvelimen käyttäjätietokantaa, kuten esimerkiksi Radiusta tai Active Directoryä, vasten.

WPA tarjoaa TKIP-tekniikan ja 802.1x-tuen johdosta dynaamisen avaimensalauksen ja kaksisuuntaisen todennuksen (Geier 1 2005: 184). WPA:n huonona puolena todettakoon sen toiminta palvelunestohyökkäyksissä. Jos hakkeri tai tietämätön, luvallinen käyttäjä lähettää vähintään kaksi datapakettia sekunnissa väärää WPA-kryptausavainta käyttäen, sulkee tukiasema pääsyn kaikilta verkon käyttäjiltä yhden minuutin ajaksi. Tällä tavalla WPA-järjestelmä estää luvattomia käyttäjiä pääsemästä verkkoon.(Geier 2005 2D.) Tämä on tosin ikävä ominaisuus, jos hyökkäyksiä tapahtuu verkossa usein. Luvallistenkin käyttäjien verkkokäyttö häiriintyy aina minuutiksi kerrallaan.

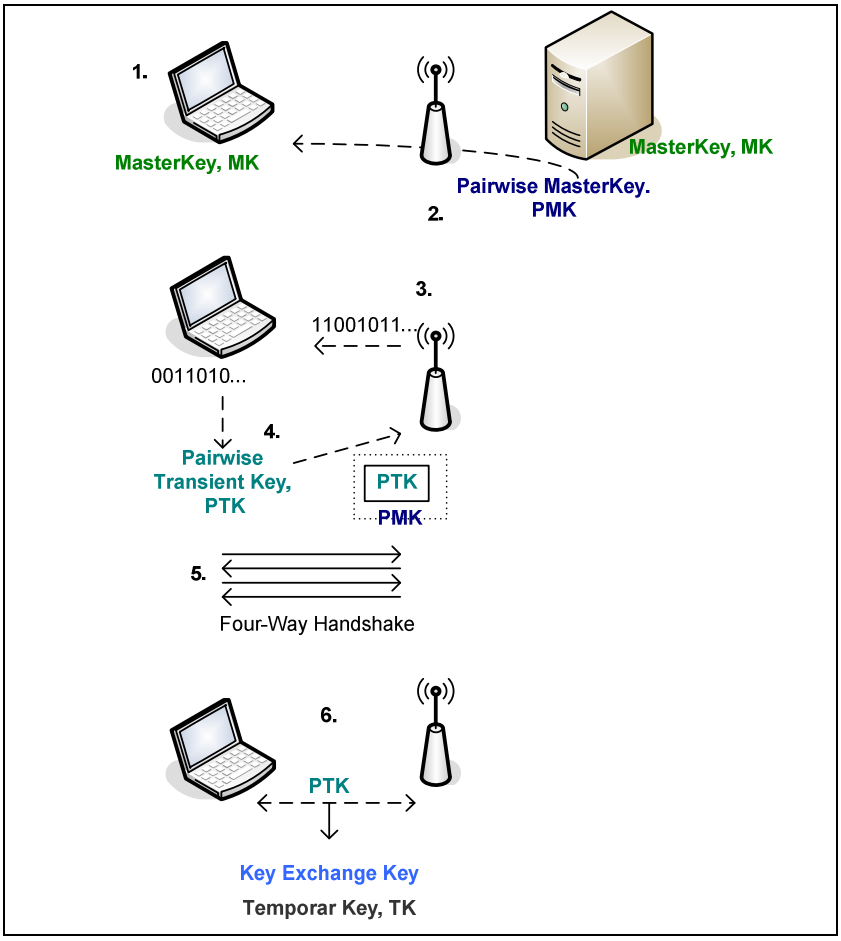
3.2.3 WPA2 (IEEE 802.11i / Robust Security Network)

WPA2 on viimeisin ja lienee myös ollut odotetuin menetelmä WLAN- verkkojen salaukseen. WPA2:ta pidetään turvallisimpana, kehittyneimpänä sekä suositeltavimpana salausmenetelmänä toimitilakiinteistöihin. WPA2 perustuu aiemmin esiteltyyn IEEE 802.11i -standardiin. Salaukseen voidaan käyttää TKIP:n

sijaan AES-salausta, jota pidetään erittäin tehokkaana algoritmina. AES tosin vaatii enemmän suoritustehoa laitteilta ja vanhaa laitekantaa on vaikeampi päivittää tukemaan WPA2:ta.(Hovatta ym. 2005: 30.)

IEEE 802.11i -standardia käyttäviä WLAN-verkkoja kutsutaan myös nimellä RSN-verkko, joka lyhennetään sanoista Robust Security Network. Kyseistä standardia käytetään pääasiassa yhdessä 802.1x-järjestelmän kanssa. Parempien salausmenetelmien lisäksi 802.11i sisältää avainpareihin perustuvan avainhallinnan, jossa pääte ja tukiasema salaavat liikenteen pareittaisella lähetysavaimella, joka vaihtuu määräajoin. Se sisältää myös esitunnistuksen (Pre-Authentication), jonka ansiosta langatonta päätettä voidaan siirtää eri yhteyspisteiden välillä ilman uudelleen tunnistautumisen aiheuttamia katkoksia. Esitunnistuksessa tunnistuspalvelin lähettää hyväksytyn käyttäjän tiedot kaikille verkon yhteyspisteille. (Puska 2005: 83-85.)

Käydään seuraavaksi kuvan 3.1. avulla läpi tarkemmin miten 802.11i avaintenhallinta toimii.



Kuva 3.1 802.11i avaintenhallinta

1. Työasemiin ja tunnistuspalvelimeen on määritelty valmiiksi yleisavain (Master Key, MK), jonka avulla prosessin muut avaimet luodaan.

2. Työasema ja tunnistuspalvelin generoivat yleisavaimestaan (MK) parittaisen yleisavaimen (Pairwise Master Key, PMK), jonka tunnistuspalvelin toimittaa yhteyspisteelle.

3. Työaseman ja tunnistuspalvelimen välinen yhteyspiste lähettää seuraavaksi työasemalle bittijonon, josta työasema generoi oman bittijononsa kanssa parittaisen tilapäisavaimen (Pairwise Transient Key, PTK).

4. Työasema lähettää yhteyspisteelle generoimansa parittaisen tilapäisavaimen (PTK), joka on salattu parittaisella yleisavaimella (PMK).

5. Viestinvaihto kuitataan nelinkertaisella kättelyllä (Four-Way Handshake) työaseman ja yhteyspisteen välillä.

6. Parittaisesta tilapäisavaimesta (PTK) lasketaan vielä avaintenvaihdon vahvistusavain ja salausavain (Key Exchange Key) sekä tilapäisavain (Temporar Key, TK), jota käytetään itse datan salaukseen työaseman ja yhteyspisteen välillä. (Puska 2005: 84-85.)

3.2.4 VPN (Virtual private Network)

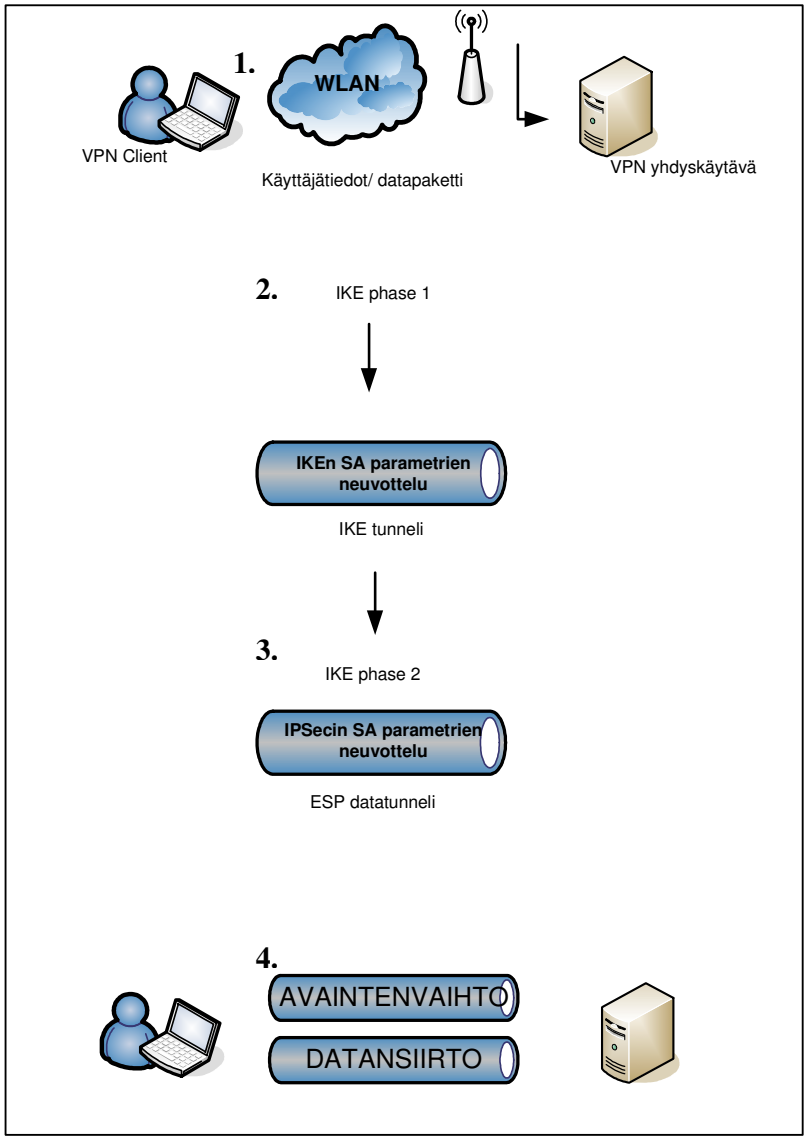
VPN on yleinen nimitys toteutuksille salata IP-liikenne turvattoman verkon yli. WLAN-verkon VPN-ratkaisussa WLAN edustaa turvatonta verkkoa, jonka yli liikenne tunneloidaan.

Puska pitää verkkokerroksen IPSec (Internet Protocol Security) -protokollalla toteutettua VPN-ratkaisua parhaana vaihtoehtona WLAN-verkolle. IPSec on joukko tietoliikenneprotokollia, jotka jakavat luottamuksellisuuden, eheyden varmistuksen ja avainten hallinnan eri protokollille. ESP (Encapsulating Security Payload) -protokolla takaa luottamuksellisuutta valitun salausalgoritmin avulla. ESP osallistuu myös eheyden varmistukseen. AH (Authenticating Headers) -protokolla hoitaa tunnistuksen esimerkiksi HMAC (The Keyed-Hash Message Authentication Code) -, MD5 (Message-Digest algorithm 5) - tai SHA (Secure Hash Algorithm) -algoritmin avulla. Avainten hallinta voidaan hoitaa joko käsin tai automaattisesti IKE (Internet Key Exchange) -protokollan avulla. (Puska 2005: 85-86.)

Salattu yhteys muodostetaan työaseman VPN-ohjelmiston (client) ja VPN-yhdyskäytävän välille. Salatussa yhteydessä muodostuu kaksi eri tunnelia. Ensin muodostuu tunneli, jota käytetään avainten vaihtoon (IKE-tunneli). Tämän jälkeen datansiirtoa varten muodostuu datatunneli (ESP-tunneli). ESP- eli datatunnelissa datapaketti kehystetään uudella IP-otsikolla sekä ESP- ja/tai AH-otsikoilla. VPN-yhdyskäytävä tarkistaa käyttäjän antamat tunnukset tunnistuspalvelimen käyttäjätietokannasta. Osapuolet, työasema ja VPN-yhdyskäytävä, var-

mistavat aina toistensa autenttisuuden, jonka jälkeen ne muodostavat turvaliitoksen (SA, Security Assosiationin). Turvaliitoksen parametrit neuvotellaan yhteyden muodostuksen alussa. (Puska 2005: 87.)

Kuvassa 3.2. käydään läpi mitä IPSec-protokollalla toteutetussa VPN-yhteyden muodostuksessa tapahtuu.



Kuva 3.2 VPN-yhteysprosessi

1. Käyttäjä avaa työasemallaan VPN-asiakasohjelman (client), joka joko pyytää käyttäjän tunnisteet tai lähettää automaattisesti paketin etäkohteeseen, jolloin VPN-ohjelmisto tunnistaa liikenteen salattavaksi.

2. Seuraavaksi tapahtuu IKE-vaihe yksi (IKE phase 1). Tässä tunnistetaan etäpää, jonka kanssa neuvotellaan turvaliitoksen parametrit. Ensimmäisen

IKE-vaiheen jälkeen muodostuu turvallinen kanava, jossa neuvotellaan IP-Sec-turvaliitoksen parametrit.

3. IKE-vaiheessa kaksi (IKE phase 2) neuvotellaan IPSec-turvaliitoksen parametrit. Tämän seurauksena muodostuu ESP-tunneli, jota pitkin data siirretään.

4. Datan siirtymistä tapahtuu IPSec-turvaliitosta eli ESP-tunnelia pitkin.

IKE- ja IPSec-turvaliitokset katkaistaan joko manuaalisesti tai automaattisesti, kun datansiirtoa ei ole tapahtunut tietyllä aikavälillä. (Puska 2005: 89.)

3.3 802.1x käyttäjäntunnistus (Port Based Authentication)

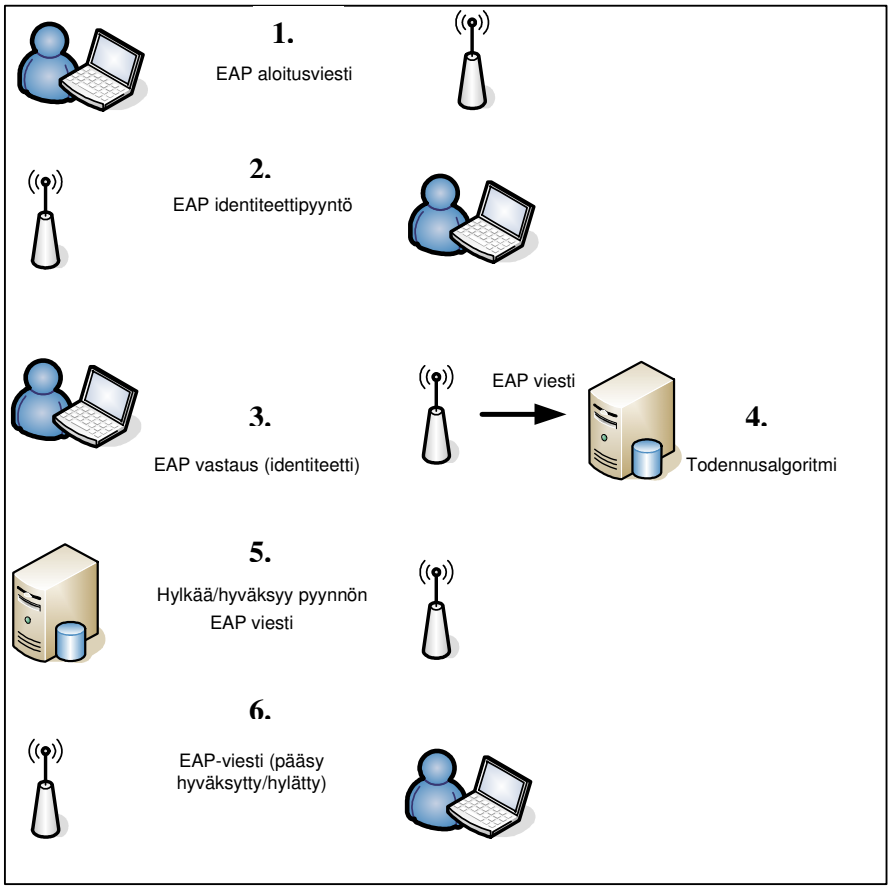
802.1x porttikohtaisen autentikoinnin tarkoitus on estää luvattoman langattoman päätelaitteen kommunikointi lähiverkkoon tukiaseman tai kytkimen portin kautta.

802.1x käyttää EAP (Extensible Authentication Protocol) -protokollaa kuljetusalustana tunnistustoteutuksille (Puska 2005: 25). EAP:a voisi kuvata todennusprotokollan rungoksi, jota käytettäessä on valittava EAP-todennustyyppi, jota tukeva sovellus asennetaan todennuspalvelimelle ja asiakaslaitteelle. Erilaisia EAP-todennustyyppejä ovat esimerkiksi EAP-TLS (EAP Transport Layer Security) ja EAP-TTLS (EAP Tunneled Transport Layer Security) (Geier 1 2005: 190).

EAP-järjestelmä sisältää päätelaitteen ohjelman (Supplicant), tunnistajan (Authenticator) ja todennuspalvelimen, joka sisältää käyttäjätietokannan. Langattomissa verkoissa Supplicant ja Authenticator käyttävät viestintäänsä EAPOW (EAP over WLAN) -protokollaa. Authenticator ja todennuspalvelin voivat keskustella esimerkiksi Radius-protokollan avulla (Puska 2005: 76).

802.1x-liikenne käynnistyy, kun todentamaton langaton laite, esimerkiksi kannettava tietokone, yrittää muodostaa yhteyden langattomaan tukiasemaan. Tukiasema vastaa avaamalla portin, joka sallii ainoastaan EAP-paketit asiakkaalta todennuspalvelimelle. Todennuspalvelin, esimerkiksi Radius-palvelin, sijaitsee käytännössä tukiaseman ”langallisella” puolella. Kunnes laite on todennettu, tukiasema estää muun liikenteen, esimerkiksi http (Hypertext Transfer Protocol) -, DHCP (Dynamic Host Configuration Protocol) - ja POP3 (Post Office Protocol version 3) -liikenteen, kulkemisen kauttansa. Mikäli todennus onnistuu, portti avataan muullekin liikenteelle todennuspalvelimen sallimien oikeuksien mukaisesti (Geier 1 2005: 188-189).

Käydään kuvan 3.3. avulla läpi mitä vaiheita 802.1x-prosessiin sisältyy:



Kuva 3.3 802.1x-prosessin kuvaus

1. Asiakaslaite lähettää EAP-aloitusviestin langattomalle tukiasemalle. Asiakas kysyy käytännössä tukiasemalta lupaa liikennöintiin.

2. Tukiasema vastaa EAP-viestillä, joka sisältää pyynnön asiakkaan identiteetistä.

3. Asiakas vastaa EAP-paketilla, joka sisältää identiteetin. Tiedot välitetään määritellylle todennuspalvelimelle.

4. Todennuspalvelin käyttää määriteltyä todennusalgoritmia identiteetin tunnistamiseen.

5. Todennuspalvelin joko hyväksyy tai hylkää pyynnön ja lähettää tästä tiedon EAP-viestillä tukiasemalle. Jos todennuspalvelin hyväksyy asiakkaan, tukiasema muuttaa asiakkaan portin valtuutettuun tilaan.

6. Tukiasema ilmoittaa EAP-viestillä asiakaslaitteelle, onko tälle myönnetty pääsy vai ei. (Geier 2005.)

3.4 Tietoturvakäytäntöjä

Tietoturvatekniikoiden ja standardien lisäksi on olemassa ns. arkisia käytäntöjä, joita noudattamalla voidaan suojata langatonta lähiverkkoa erilaisilta uhkatekijöiltä. On tärkeää huomioida myös nämä seikat WLAN-verkkoa suunnitellessa ja toteutettaessa:

- **Fyysisesti suojatut tukiasemat** estävät ulkopuolisten pääsyn itse laitteelle. Tehokas tapa on sijoittaa tukiasemat näkymättömiin kattolevyjen yläpuolelle.

- **Tukiasemien konfiguraatioiden tarkkailulla** saadaan selville, mikäli jonkin tukiaseman asetukset muuttuvat tai noudattavat tietoturvapolitiikan vastaisia konfiguraatioita.

- **Tukiaseman SSID-mainosten lähetysten estämisen** ansiosta käyttäjien on vaikeampi saada tietoonsa tukiaseman verkkojen SSID-tunnuksia ja assosioitua verkkoon niiden avulla.

- **Radioaaltojen rajoittaminen** voidaan toteuttaa käyttämällä suunnattuja antenneja. Tällöin radioaaltoja saadaan ohjattua enemmän halutuille alueille.

- **Vahvojen salasanojen käyttäminen tukiasemissa** on ehdottoman tärkeää. Oletussalasanojen sijaan tulee käyttää vaikeasti arvattavia ja usein vaihdettavia salasanoja.

- **Tehokas salausmenetelmä** on elinehto turvalliselle WLAN-verkolle. WEP-salauksen sijaan on tänä päivänä syytä käyttää parempia salausmenetelmiä, kuten WPA:ta tai WPA2:ta, joka käyttää tehokasta AES-salausta. Tehokas salausmenetelmä estää ulkopuolisten murtautumista verkkoon.

- **Laiteohjelmistojen säännöllinen päivittäminen** on tärkeää, sillä laitevalmistajien päivitykset tuovat parannuksia ja korjauksia mm. tietoturvaan. Laitteita hankittaessa on selvitettävä, miten helppoa laitteisiin on saada päivityksiä.

- **Sijoittamalla langattomat käyttäjät palomuurin ulkopuolelle** verkkoon saadaan lisää turvaa, sillä käyttäjät pääsevät lähiverkkoon käsiksi vain VPN-yhteyden avulla. VPN on turvallisena pidetty menetelmä, jossa käyttäjä autentikoidaan ja vasta sitten annetaan pääsy määrättyihin sovelluksiin.

- **Henkilökohtaisten palomuurien käyttäminen** on erityisen tärkeää käytettäessä WLAN-verkkoa julkisissa tiloissa. Jos hakkeri pääsee tukiaseman kautta verkkoon, pystyy hän pääsemään myös siinä oleviin käyttäjälaitteisiin ja jaettuihin resursseihin, jos niitä ei ole mitenkään suojattu.

- **Toteutusten valvonnalla** voidaan varmistaa, että verkon käyttäjät käyttävät verkkoa oikein ja esim. eivät asentele omia tukiasemia organisaatiossa. On myös syytä valvoa verkon käyttäjien ”liikkeitä”, jotta voidaan paikallistaa mahdolliset ylimääräiset vierailijat. (Geier 1 2005: 195-199.)

4 WLAN-projekti Anilinker Oy:ssä

4.1 Projektin taustaa

Anilinker Oy:n toimitiloissa käytetään paljon kannettavia tietokoneita. Tähän asti kannettavan käyttäjät ovat olleet sidottuja tiettyyn työpisteeseen, lähelle fyysistä lähiverkkoliitäntää. Lähiverkkoon kytketyn koneen liikkumavara on ollut riippuvainen verkkokaapelin pituudesta, käytännössä se on siis rajoittunut korkeintaan pariin metriin. Tästä syystä tuli aiheelliseksi rakentaa langaton lähiverkko kiinteän Ethernet-lähiverkon rinnalle. WLAN-verkon rakennusprojekti liittyy lähiverkon uudelleenrakentamisprojektiin, jossa uusitaan myös kiinteän verkon laitteita. Kiinteän verkon vanhat työryhmäkytkimet korvataan modulaarisella reitittävällä kytkimellä ja verkko segmentoidaan uudelleen.

WLAN-hankkeen suunnittelun yhteydessä syntyi myös idea langattomasta vierasverkosta. Yrityksen toimitiloissa vierailee melko paljon ulkopuolisia vieraita, joilla on usein tarve liittää kannettavansa Internetiin. Tämän tarpeen pohjalta toteutettiin myös oma WLAN-verkko vierailijoita varten. Tämä oli huomioitava myös laitteiden hankinnassa, sillä normaalit tukiasemat tukevat useimmiten vain yhtä SSID:tä.

Toimeksiannossa toivottiin, että tutustuisin myös langattomien lähiverkkojen olemassa oleviin tietoturvaratkaisuihin. Verkkoa tullaan käyttämään yrityksen toimitiloissa, joten tietoturvan taso on saatava riittävän korkealle. Näistä lähtökohdista lähdin syksyllä 2006 tutustumaan WLAN-verkkojen maailmaan.

4.2 Projektin aloitus

Projektin aloitusvaiheessa syys- ja lokakuussa 2006 tehtiin tarjouspyyntöjä modulaarisista kytkimistä eri laitetoimittajille. Samoissa tarjouspyynnöissä pyydettiin tarjousta myös heidän suosittelemistaan WLAN-tukiasemista. Saaduissa tarjouksissa tarjottiin useimmiten Hewlett Packardin (HP) tukiasemia ProCurve Access Point 530 ja ProCurve Networking Wireless Access Point 420. Yksi laitetoimittajista tarjosi poikkeuksellisesti WLAN-kytkintä Symbol WS2000 kahden AP300 Wireless Access Portin kanssa. Kyseinen laitemerkki ei ollut ennestään tuttu, mutta kytkin sisälsi paljon ominaisuuksia, jotka olivat mielestämme hyödyllisiä rakennettavan verkon kannalta. Yksi ominaisuuksista oli mm. tuki useammalle WLAN-verkolle ja SSID:lle. Sama laitetoimittaja tarjosi myös sopivinta modulaarista kytkintä, joten heiltä tilattiin sekä verkko- että WLAN-kytkin marraskuun 2006 alussa.

4.3 WLAN-kytkin ja tukiasemat

Kytkin Symbol WS2000

Symbol kuvaa laitettaan tehokkaaksi ”all-in-one”-ratkaisuksi, joka pitää WLAN-verkon hallintakustannukset alhaalla. WS2000 kytkimessä on runsaasti integroituja toimintoja, kuten reititin, palomuuri sekä tuki Power Over Ethernet -ominaisuudelle.(Symbol 1 2006.) Näiden ominaisuuksien ansiosta WLAN-verkko voidaan eristää kiinteästä lähiverkosta. Tätä mahdollisuutta hyödynsimmekin WLAN-verkkosegmenttiä suunnitellessamme.

WS2000-kytkimessä on paljon hyödyllisiä ominaisuuksia, kuten esimerkiksi:

- Integroitu AAA (Authentication, Authorization, Accounting) -palvelin
- Tuki “hotspot”-verkoille
- Rosvotukiasemien paljastustoiminto
- Quality of Service - liikenteen priorisointi

Symbol WS2000 kytkimen ominaisuuksiin ja spesifikaatioihin voi tutustua tarkemmin osoitteessa: www.symbol.com/ws2000. Lisäominaisuudet saadaan otettua tarvittaessa helposti käyttöön. WS2000 tukee myös uusinta tietoturvatekniikkaa 802.11i/WPA2:ta. (Symbol 1 2006.)

Tukiasemat Symbol AP300 Wireless Access Port

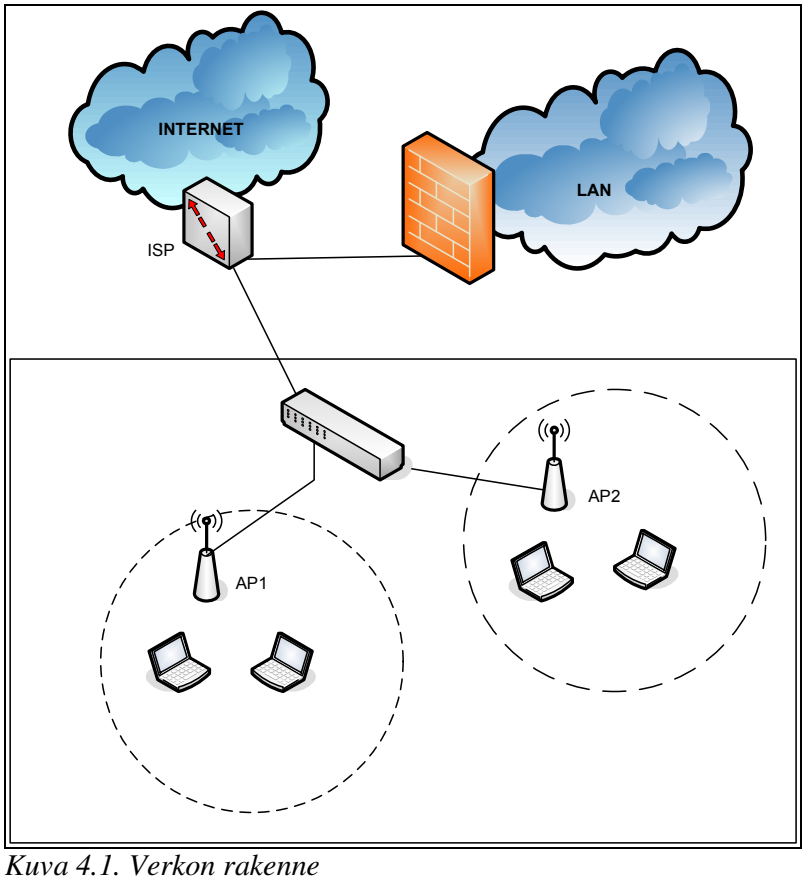
Tukiasemat toimivat tässä verkossa ns. Thin Access Point -rooleissa eli asetukset ja konfiguraatiot on tehty keskitetysti kytkimelle, joka jakaa tiedot tukiasemilleen. Tämä säästää verkon tukihenkilön työtä, sillä asetuksia ei tarvitse tehdä jokaiselle tukiasemalle erikseen. Nämä Thin Access Point -tukiasemat ovat myös edullisempia karsittujen ominaisuuksien ansiosta. Näitä tukiasemia on helppo ja nopea päivittää, koska kaikki konfiguroidaan kytkimen kautta. Kaapeloinnissa etua tuo AP300:n Power over Ethernet -ominaisuus eli virta kulkee tukiasemalle CAT5-verkkokaapelia pitkin.

AP300-tukiasema tukee myös niin sanottua Dual-radio-ominaisuutta eli langattomalta päätteeltä voidaan käyttää valinnan mukaan joko a-standardin mukaista 5 GHz:n taajuutta tai b- ja g-standardien mukaista 2,4 GHz:n taajuutta (Symbol 2 2006). Tämä ominaisuus on toimeksiantajan toimitiloissa hyödyllinen, sillä laitekanta on vaihtelevaa. Toisessa laitteessa saattaa olla uudempi verkkokortti ja toisessa vanhempi. Vanhemmat verkkokortit eivät välttämättä pysty käyttämään 5 GHz:n taajuutta. Symbol AP300 tukiasemista voi lukea lisää osoitteessa: www.symbol.com/products/wireless/ap_300_ap.html.

4.4 Verkon suunnitelma ja rakenne

Langaton verkkosegmentti haluttiin sijoittaa erilleen kiinteästä lähiverkosta, palomuurin ulkopuolelle. Tämä ratkaisu lisää tietoturvaa kiinteälle lähiverkolle ja sen palveluille. Suunnittelimme toteutettavaksi kaksi eri WLAN-verkkoa. Toinen WLAN henkilökunnalle ja toinen vieraille. Verkkojen oikeita nimiä ja tunnisteita en tule mainitsemaan toimeksiantajan toiveesta. Symbol AP300 -tukiasemia tähän WLAN-verkkoon suunniteltiin asennettavaksi kaksi. Kahden tukiaseman uskottiin kattavan hyvin toimiston hieman alle tuhannen neliömetrin tilan. Tukiasemien sijoittelu on esitelty tarkemmin aliluvussa 4.6 *Tukiasemien sijoittelu toimitiloissa*. Molemmista tukiasemista tarjotaan pääsy molempiin WLAN-verkkoihin (henkilökunta ja vieraat). Tukiasemien sisältämän Dual-radio-ominaisuuden ansiosta molemmat tukiasemat tarjoavat sekä 2,4 GHz:n siirtotaajuutta (b/g) että 5 GHz:n siirtotaajuutta (a). Näin jää kannettavan laitteen valittavaksi kumpaa taajuutta käyttää.

Kuva 4.1 esittää verkon rakennetta suhteessa kiinteään lähiverkkoon ja Internetiin. Käytännössä WLAN-kytkin tullaan siis kytkemään suoraan ISP (Internet Service Provider) -reitittimeen.



Kuva 4.1. Verkon rakenne

4.5 Tietoturva

Tietoturvallisuus on WLAN-verkon kohdalla tärkeä seikka. Pidän luotettavimpina ratkaisuvaihtoehtoina WPA2/802.11i menetelmään pohjautuvaa ratkaisua yhdistettynä 802.1x-järjestelmään sekä WPA-tekniikalla salattua verkkoa yhdistettynä VPN-ratkaisuun. 802.11i-standardiin pohjautuva WPA2 on pitkälle kehitetty tietoturvan osalta. Sen tarjoama AES-salaus tunnetaan yleisesti turvallisena algoritmina, jota on vaikea murtaa. Koska tämä WLAN-verkkosegmentti sijaitsee kiinteän lähiverkon palvelinresurssien ja palomuurin ulkopuolella, henkilökunnan WLAN-verkon tietoturvaratkaisuksi valittiin WPA yhdistettynä VPN- ratkaisuun. Langaton verkko salataan WPA-TKIP-menetelmällä ja käyttäjät ottavat yhteyden Internetin kautta kiinteään lähiverkkoon VPN-tunnelin läpi. VPN-ratkaisu tarjoaa vahvan liikenteen salauksen ja se ei vaadi kannettavan laitekannan päivittämistä. Se on laitekantaan nähden edullisin, mutta samalla luotettavin tarpeeseen sopivista menetelmistä.

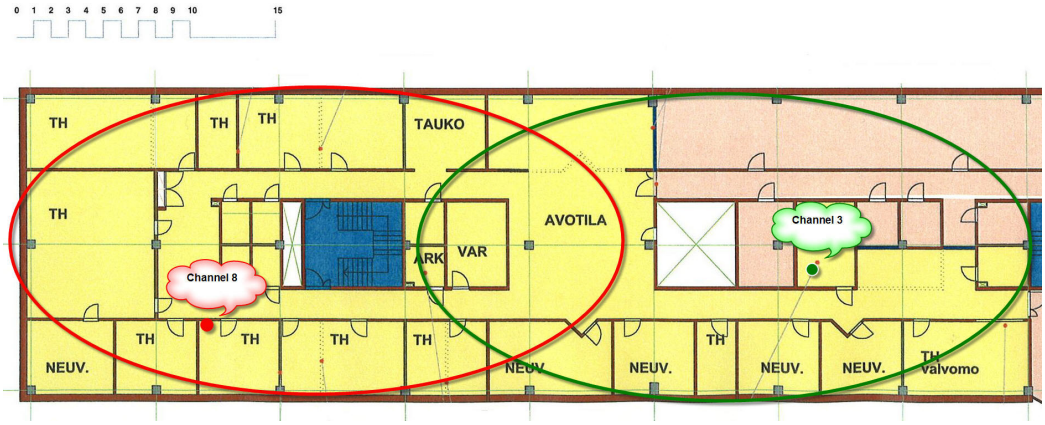
Myös vierasverkon käyttäjille sallitaan pääsy internetiin. Vierasverkkoakaan ei tosin ole syytä jättää liian alhaiselle tietoturvan tasolle. Vierasverkkoon valittiin verkon salausmenetelmäksi myös WPA-TKIP, sillä se toimii yhteen vanhemman laitekannan kanssa. Vierailijalle annetaan tarvittaessa verkkoon pääsyä varten usein vaihdettava WPA-avain, jolla hän voi assosioitua vierasverkkoon.

Tulemme noudattamaan myös erilaisia tietoturvakäytäntöjä antaaksemme turvaa verkolle. Esimerkiksi tukiasemat ovat hyvin suojatut fyysisellä tasolla, sillä toimitiloihin on pääsy vain henkilökunnalla. Vierailijat kulkevat henkilökunnan jäsenen valvomina, joten heitä ei pidetä uhkana. Myös se, että asetukset on määritelty lukitussa palvelinhuoneessa sijaitsevalle kytkimelle, parantaa tietoturvaa. Myös yrityksen kiinteä lähiverkko turvataan sijoittamalla WLAN-verkko erilleen palomuurin ulkopuolelle.

4.6 Tukiasemien sijoittelu toimitiloissa

Tukiasemien haluttiin kattavan mahdollisimman hyvin avotila, neuvotteluhuoneet sekä toimitilan päätyhuoneet (kuvassa 4.2 vasen pääty). Kuvaan 4.2 on ympyröity alueet, jotka haluttiin vähintään kattaa. Todellisuudessa tukiasemien kattamat alueet ulottuvat laajemmalle alueelle ja tukiasemien alueet menevät päällekkäin. Tästä syystä oli valittava tukiasemille b/g-radioverkon osalta kanavat, jotka ovat tarpeeksi kaukana toisistaan. Tässä tapauksessa väliin jää 5 kanavaa. Kartoitimme rakennuksessa muita käytössä olevia WLAN-verkkoja Netstumbler-ohjelman avulla. Saimme tällä tavoin tietoa, mitä kanavia muilla kuuluvilla WLAN-verkoilla on käytössään. Pyrimme käyttämään kanavia, jotka ovat vähintään kahden kanavan ”etäisyydellä” omista kanavistamme. Mm. kanavat 1 ja 6 olivat käytössä muissa verkoissa. Valitsimme alussa kanavat 8 ja 13, mutta kanava 13 ei kuulunut tarpeeksi voimakkaasti tukiaseman välittömässä läheisyydessäkään. Tätä ei lähdetty sen pidemmälle tutkimaan ajan puutteen vuoksi, vaan otimme sen sijaan käyttöön kanavan 3. Tukiasemien a-radioverkon osalta kanavasuunnittelua ei tarvitse tehdä, sillä kanavat eivät mene päällekkäin 5 GHz:n alueella. Tässä verkossa toistaiseksi vain pari uusinta kannettavaa tietokonetta pystyy hyödyntämään a-standardin mukaista taajuutta. Vanhempaa laitekantaa pyritään päivittämään mahdollisuuksien mukaan lähitulevaisuudessa, jotta se tukisi myös häiriöttömämpää a-standardia.

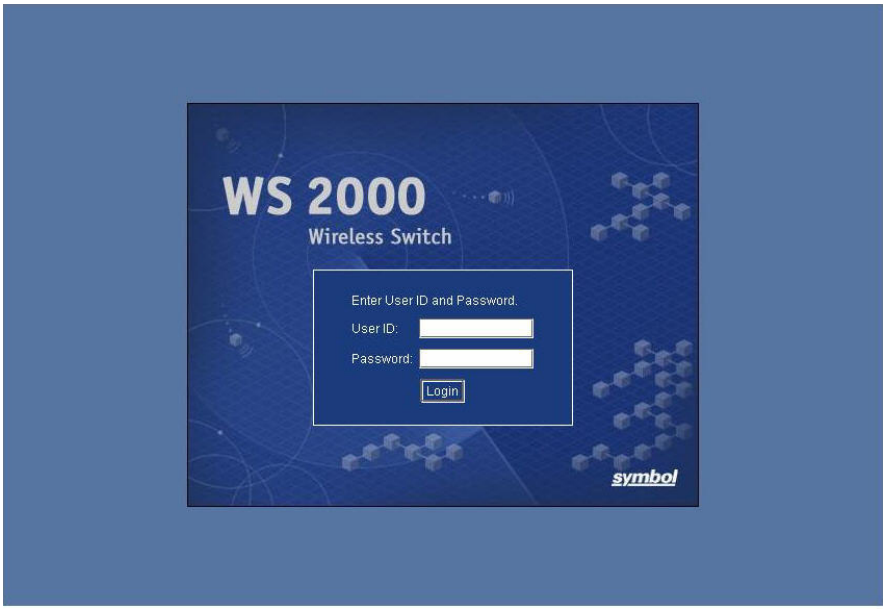
Itselleni heräsi kanavasuunnittelun yhteydessä kysymys, joka on tutkittava muiden jatkokehitystoimenpiteiden yhteydessä. Koska WLAN-kytkimessä on Roaming-ominaisuus, miten se toimii, jos kaksi verkkoa kuuluu samassa tilassa yhtä vahvasti eri kanavilla? Roaming siis mahdollistaa kannettavan tietokoneen liikuttelun eri kanavien kuuluvuusalueella ilman, että verkkoon täytyy kirjautua uudelleen yhteyskatkosten vuoksi.



Kuva 4.2 Tukiasemat toimitilassa

4.7 WLAN konfigurointi

WS2000 kytkintä konfiguroitiin web-liittymän kautta. Selaimella otettiin yhteys laitteen IP-osoitteeseen, joka on oletuksena 192.168.0.1. Kuvassa 4.3 on näkymä kirjautumisikkunasta.

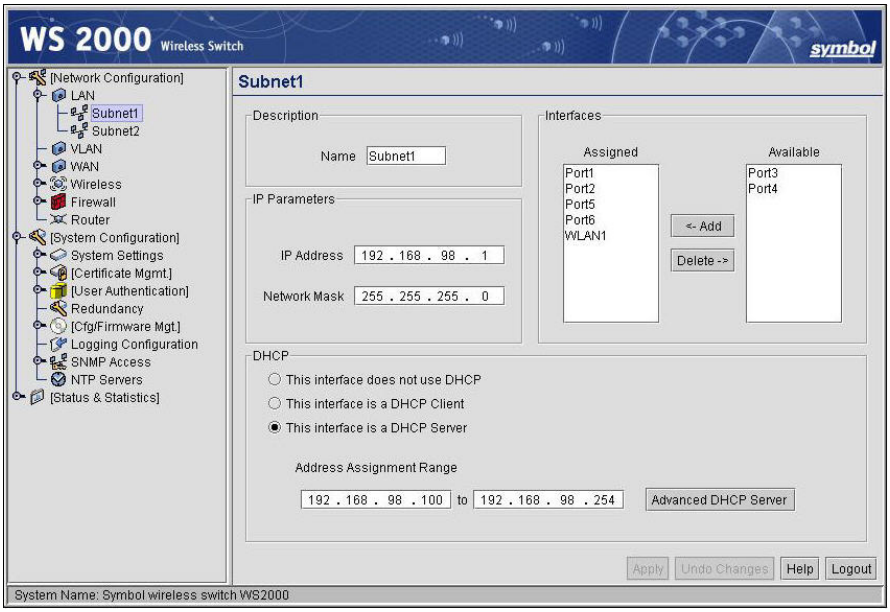


Kuva. 4.3 WS2000-kytkimen hallintakonsoliin kirjautuminen

Tärkeää on valita aloittaessa oikeat maa-asetukset. Näiden mukaan laite säätää automaattisesti erilaiset asetukset, kuten käytettävissä olevien kanavien määrän.

Käyttöliittymä listaa näkymän vasempaan reunaan valikot, joissa asetukset määritetään. Aloitimme konfiguroinnin valikossa *LAN,* jossa määritetään aliverkoille kuvaavat nimet, IP-osoitteet ja portit. Konfiguroimme tämän hetken tarpeeseen kaksi aliverkkoa, jotka liitetään kahteen eri WLAN-verkkoon. Kun kaksi aliverkkoa on otettu käyttöön, päästään konfiguroimaan näitä aliverkkoja. IP-osoitteet, aliverkkomaskit, portit sekä DHCP-asetukset määritetään aliverkkokohtaisesti. Käyttöönotetuissa aliverkoissa käytettiin valintaa ”*This interface is a DHCP server*”, koska IP-osoitteet jaetaan tältä laitteelta. Toinen vaihtoehto olisi hakea ne joltakin ulkoiselta DHCP-palvelimelta (DHCP Relay), mutta tässä toteutuksessa tätä ei tulla käyttämään.

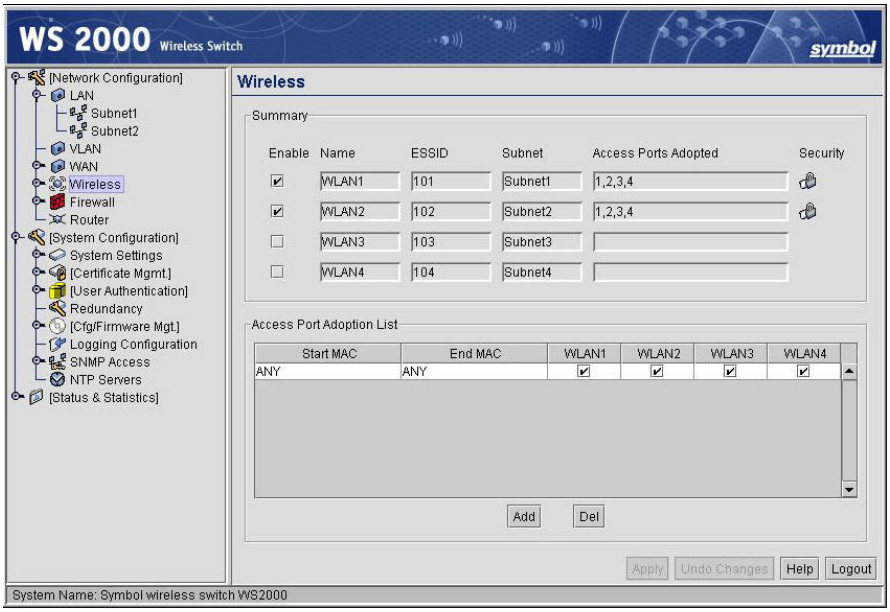
”Interfaces”-otsikon alla määritetään konfiguroitavaan aliverkkoon kuuluvat fyysiset portit ja WLAN-verkot. Jätimme fyysiset portit numero 3 ja 4 liittämättä kumpaankaan verkkoon, sillä niihin ei kytketä vielä tukiasemia. Ylimääräiset portit tultaneen ottamaan käyttöön, jos tukiasemia hankitaan jossakin vaiheessa lisää. Kuva 4.4 kuvaa LAN-valikon alta löytyvää aliverkon konfigurointinäkymää.



Kuva 4.4 LAN-valikko ja aliverkkoasetukset

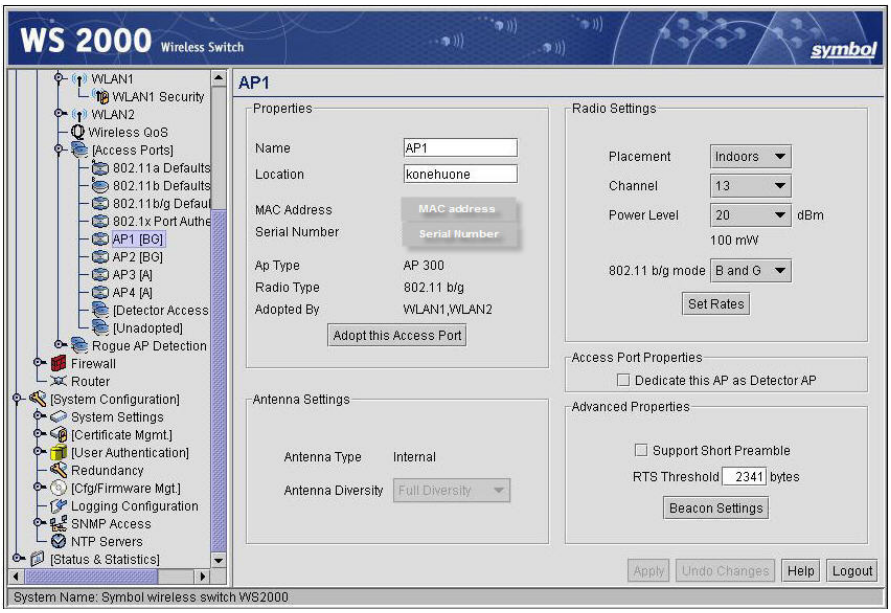
Huom! Kaikki kuvakaappaukset sisältävät kuvitteelliset SSID-tunnisteet ja verkkojen nimet sekä osoitteet toimeksiantajan toiveesta lukuun ottamatta kuvia 4.9 sekä 4.10 (näissä osoitteet on piilotettu). Muihin kuviin oikeat nimi- ja osoiteasetukset on vaihdettu kuvakaappausten jälkeen.

Seuraavaksi asetuksia määritettiin valikossa *Wireless*. Perusnäkymässä näkyvät listattuna kaikki WLAN-verkot, joita laite tukee. Tässä tapauksessa käyttöön on otettu vain kaksi. Laite ilmoittaa myös portit 3 ja 4 kuuluvaksi WLAN-verkkoihin, vaikka ne aliverkkojen konfiguroinnissa jätettiin lisäämättä. Tässä näkymässä tämä tarkoittanee kuitenkin, että kaikki portit tarjoavat automaattisesti näitä verkkoja, vaikka eivät olekaan käytössä. Kun uusia tukiasemia liitetään vapaisiin portteihin, on niillä heti valmius jakaa automaattisesti pääsyä molempiin verkkoihin. Tosin portit täytyy käydä silti asettamassa käyttöön aliverkkokohtaisesti, joten tämä ominaisuus hieman kummastutti. Kuva 4.5 kuvaa Wireless-valikon perusnäkymää.



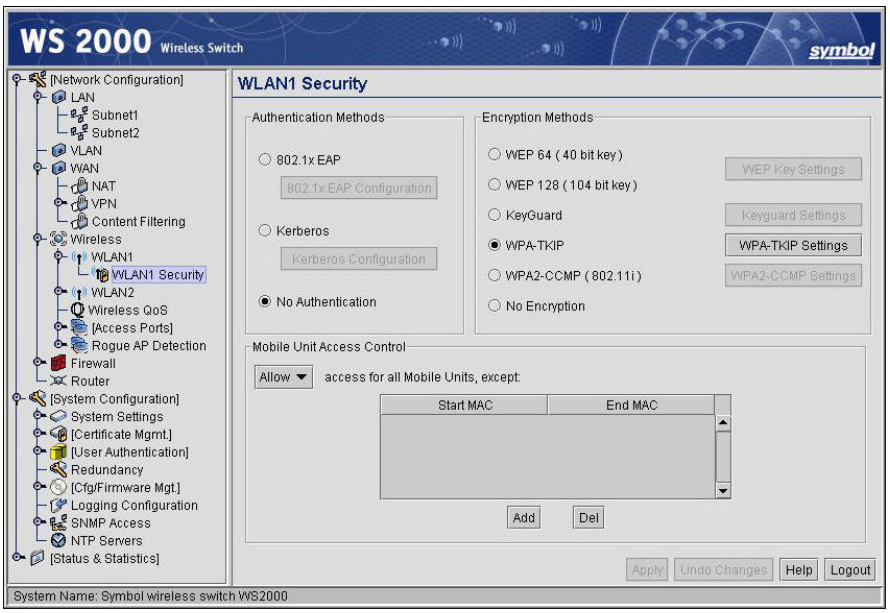
Kuva 4.5 Wireless perusnäkymä

Wireless-valikossa määritettiin myös tukiaseman radioporttien asetukset. Käyttöliittymä listaa tässä tapauksessa neljä porttia, kaksi yhtä tukiasemaa kohden (AP1 [BG], AP2 [A] jne.). Kummassakin tukiasemassa on niin sanottu looginen portti sekä a- että b/g-standardien mukaisille ”radioille”. Tätä kutsutaan Dual-radio-ominaisuudeksi (ks. 4.4 Wlan-kytkin ja tukiasemat). Kaikilla porteilla on oma MAC (Media Access Control) -osoite eli käytännössä yhdellä tukiasemalla on kaksi MAC-osoitetta, molemmille ”radioille” (a ja b/g). Kuva 4.6 kuvaa yhden radioportin konfigurointinäkymää.



Kuva 4.6 Yhden radioportin konfigurointinäkymä

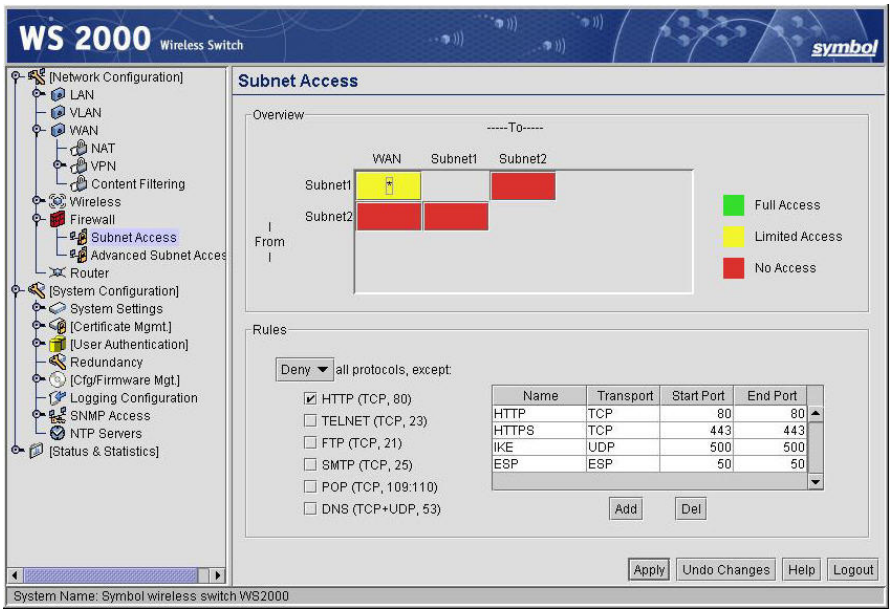
Wireless-valikossa määritettiin myös WLAN kohtaisesti salausasetukset. Molemmat WLAN-verkot konfiguroitiin käyttämään WPA-TKIP-salausta. Tämä valinta asetettiin ”Encryption Methods” -otsikon alla. Kun haluttu salausmenetelmä oli valittu, päästiin asettamaan salaukseen käytettävä salausavain valikossa *WPA-TKIP Settings.* Autentikointiasetuksiin (”Authentication Methods”) ei tehty määrityksiä, sillä käyttäjää ei autentikoida 802.1x-menetelmän eikä ulkoisen käyttäjätietokannan avulla. Käyttäjä pääsee WLAN-verkkoon WPA-avaimella. Kuva 4.7 esittää salausasetusten näkymää verkon WLAN1 kohdalla. Verkon WLAN2 asetusnäkymä on identtinen, tosin WPA-salausavain ei ole sama.



Kuva 4.7 WLAN1 salausasetusnäkymä

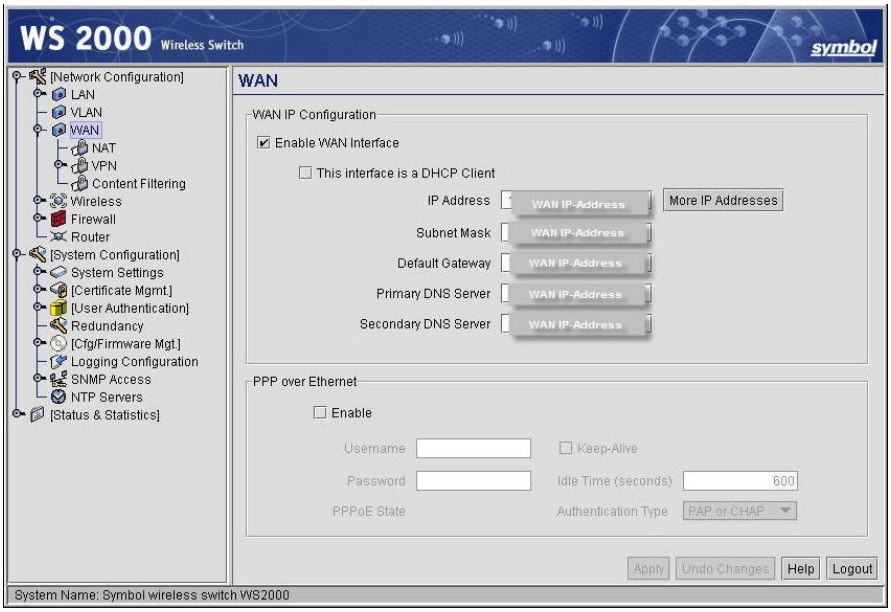
Seuraavat asetukset määritettiin *Firewall*-valikossa. Tässä valikossa määritetään kytkimen palomuurin asetuksia Määritykset konfiguroitiin aliverkkokohtaisesti alavalikossa *Subnet Access*. Aliverkon palomuuriasetuksiin päästiin valitsemalla ”alue” hiirellä otsikon ”Overview” alla. Kuvassa 4.8 voidaan nähdä Subnet1:n (WLAN1) asetukset. Määritetty ”alue”, Subnet1:stä WAN (Wide Area Network) -portille, on merkitty keltaisella (Limited Access), sillä pääsyä on rajoitettu. Rajoitukset ja säännöt voidaan nähdä alapuolella otsikon ”Rules” alla. Kaikki muu liikenne, paitsi http-liikenne, kielletään (Deny). Oikealla ruudukossa on tehty vielä tarkempia määrityksiä protokollien ja niiden porttien suhteen. Jotta VPN-tunnelin muodostus onnistuu, oli sallittava myös IKE- ja ESP-protokollille pääsy WAN-portille.

Subnet Access -näkymästä voi myös todeta, ettei Subnet1:stä (WLAN1) anneta pääsyä Subnet2:een (WLAN2). Kuvakaappaus näkymästä on otettu testivaiheessa, joten Subnet2:een ei ole tehty vielä määrityksiä sallittujen protokollien suhteen. Tällöin Subnet2:n ja WAN-portin välinen ”alue” merkitään punaisella (No Access). Tämäkin alue tulee muuttumaan keltaiseksi, kun konfigurointi on suoritettu. Tästä verkosta tullaan antamaan pääsy ainoastaan http- ja https (HyperText Transfer Protocol Secure) -protokollille.



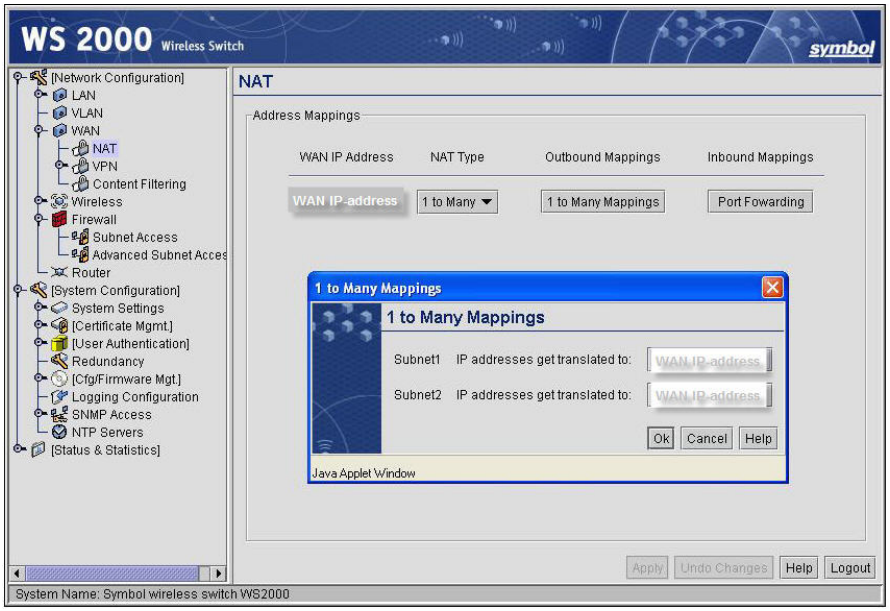
Kuva 4.8 Palomuuriasetukset Subnet1 (WLAN1)

Yhteydet ulkoverkkoon määritettiin valikossa *WAN*. Käytännössä WLAN-kytkimelle syötettiin ISP-reitittimen IP-osoite, aliverkkomaski, oletusyhdyskäytävä sekä DNS (Domain name system) -palvelimien osoitteet. Kuvassa 4.9 on näkymä WAN-asetuksista. IP-osoitteet on tässä piilotettu, sillä kuvakaappaus on otettu WLAN-verkon käyttöönoton jälkeen. Oikeita IP-osoitetietoja ei haluta esittää julkisesti.



Kuva 4.9 WAN-asetukset

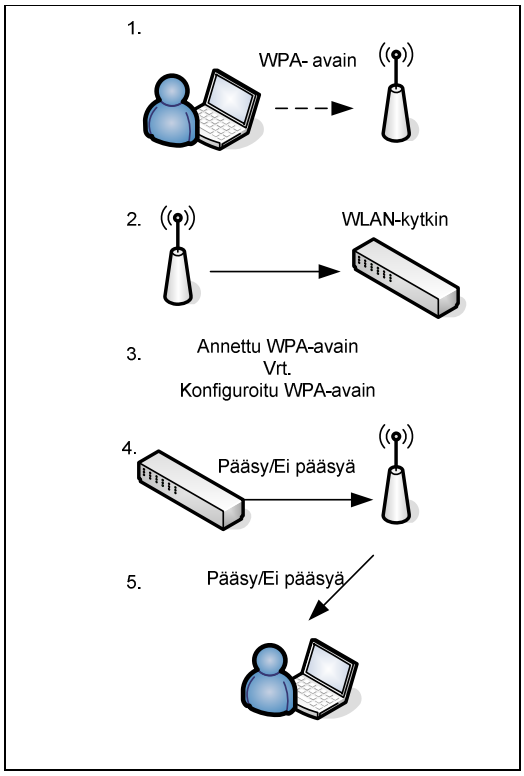
Kun WAN-valikossa oli asetettu ISP-reitittimen IP-asetukset, päästiin tarkistamaan NAT (Network Address Translation) -asetuksia. Kuva 4.10 esittää näkymää NAT-asetuksista. Tyypiksi valittiin ”1 to Many” eli yksi osoite pitää takanaan useita WLAN-verkkojen laitteiden IP-osoitteita. Tyypin perusteella otsikon ”Outbound Mappings” alle asettuu ”1 to Many Mappings”. Tämän valikon takaa avautuu ikkuna, joka näyttää, että kummankin aliverkon IP-osoitteet käännetään Internetiin mennessä WAN-portin osoitteeksi. IP-osoitteet on tässäkin piilotettu, sillä kuvakaappaus on otettu WLAN-verkon käyttöönoton jälkeen. Oikeita IP-osoitetietoja ei haluta esittää julkisesti.



Kuva 4.10 NAT-asetukset

4.8 WLAN-yhteyden prosessit

Henkilökunnan WLAN-verkossa voidaan katsoa tapahtuvan kahta eri ”yhteys-prosessia”. Ensimmäinen on langattoman käyttäjän liittyminen WLAN-verkkoon (assosioituminen). Tämä ensimmäisen prosessi tapahtuu tietysti myös vierasverkon puolella. Kummastakin WLAN-verkosta (henkilökunnan sekä vieraiden) tarjotaan vain pääsy Internetiin. Tarkastellaan kuvan 4.11 avulla mitä vaiheita ensimmäinen prosessi sisältää.



Kuva 4.11 Liittyminen WLAN-verkkoon

1. Käyttäjälle on annettu tiedoksi WLAN-verkon WPA-avain. Kannettavalla tietokoneella avataan langaton yhteys esimerkiksi Windowsin oman langattoman ”liittymän” kautta. Windows pyytää liittymisen yhteydessä WPA-avaimen.

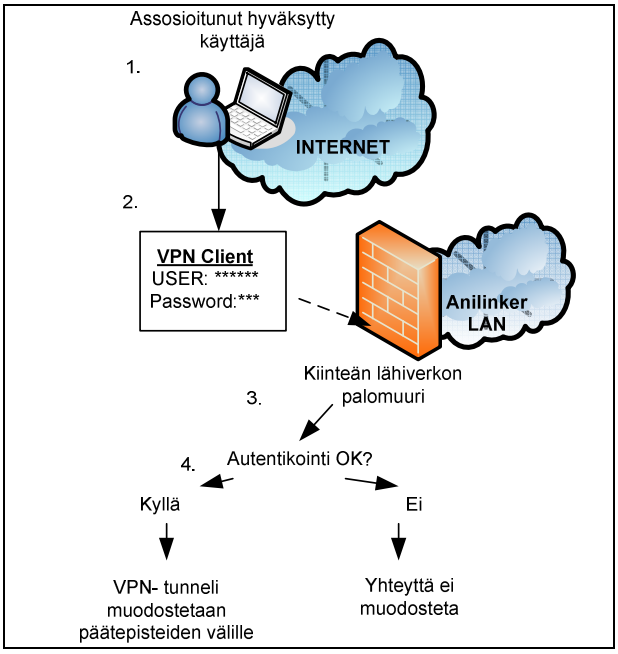
2. Tukiasema ”tarkistaa” WPA-avaimen oikeellisuuden WLAN-kytkimeltä.

3. WLAN-kytkin ”vertaa” saatua avainta konfiguroituun avaimeen.

4. Mikäli langattomalta käyttäjältä saatu avain täsmää, ilmoittaa WLAN-kytkin tiedon tukiaseman kautta käyttäjälle.

5. Avaimen ollessa oikea käyttäjä assosioidaan WLAN-verkkoon. Avaimen ollessa väärä, pääsy evätään.

Toinen prosessi tapahtuu, kun henkilökuntaan kuuluva langaton käyttäjä haluaa saada yhteyden Anilinker Oy:n kiinteään lähiverkkoon. Käydään tätä prosessia läpi kuvan 4.12 avulla.



Kuva 4.12 VPN-yhteyden muodostus lähiverkkoon

1. WLAN-verkkoon assosioituneella käyttäjällä on pääsy Internetiin.

2. Käyttäjä on asentanut langattomaan tietokoneeseensa VPN Client - ohjelman. Ohjelmana tulee käyttää palomuurin tarjoamaa CheckPointia. Client-ohjelmalla otetaan yhteys kiinteän lähiverkon palomuurin julkiseen IP-osoitteeseen ja samalla annetaan henkilökohtainen tunnus/salasana-pari Client-ohjelman osoittamiin kenttiin.

3. Palomuurissa sijaitsee oma käyttäjätietokanta, jota vasten Client-ohjelmalle annetut tunnukset autentikoidaan.

4. Autentikoinnin onnistuttua ja käyttäjän tunnistauduttua luvalliseksi, voidaan muodostaa VPN-tunneli. VPN-tunnelin muodostumisperiaatteet on kuvattu aiemmassa luvussa 4. *WLAN ja tietoturva*. Jos autentikointi epäonnistuu tai tunnus/salasana-pari ei löydy palomuuriin määritellyistä käyttäjätiedoista, tunnelia ei muodosteta eikä luvaton käyttäjä pääse kiinteään lähiverkkoon.

4.9 Kohdattuja ongelmia

Tämä WLAN-projekti sujui turhankin kivuttomasti, mutta pariin pikku ongelmaan törmättiin matkan varrella. Ensimmäinen ongelma WLAN-kytkimen konfiguroinnissa ilmeni toisella kirjautumisella laitteelle. Ensimmäisen kirjautumisen aikana laite pyytää aina vaihtamaan uuden administrator-salasanan oletuksen päälle. Käyttöliittymä sallii 11 merkkiä pitkän salasanan käytön, joten käytin koko sallitun merkkirajoituksen hyväkseni. Toisella kirjautumisella laite ei enää hyväksynytkään 11 merkkiä sisältävää salasanaa, vaan salli kirjoittaa kenttään vain 10. Tämä saatiin kuitenkin ratkaistua ottamalla telnet-yhteys laitteelle ja vaihtamalla komentorivin kautta lyhyempi administrator-salasana. Tämä ei sen suurempi ongelma ole, mutta kummallinen ominaisuus kyllä.

Toinen ongelma ilmeni vaiheessa, jossa WLAN-kytkin kytkettiin ulkomaailmaan. Koska ISP-reitittimellä alkoivat loppua portit, asetettiin sen ja WLAN-verkon sekä muiden reitittimeen kytkettävien laitteiden väliin HP:n kytkin. Tämän toimenpiteen jälkeen alkoi liikenne Internetin kautta hidastella kaikissa kytkimen takana olevissa verkoissa. Tilanne johtui siitä, että ISP-reititin käytti kytkimen suuntaan half-duplex-moodia. Tällöin siis vain toinen pää pystyy lähettämään tietoa kerrallaan toisten kuunnellessa. Tilanne saatiin korjattua soittamalla Internet-palveluntarjoajalle, joka pyynnöstä konfiguroi ISP-reitittimen käyttämään full-duplex-moodia kytkimen suuntaan.

Muita ongelmia ei tässä toteutuksessa kohdattu. WLAN-verkot oli melko helppo konfiguroida WLAN-kytkimen graafisen käyttöliittymän kautta.

5 Pohdintaa

5.1 Arviointia onnistumisesta

Pidän tämän verkonrakennusprojektin onnistumista hyvänä siihen nähden, ettei itselläni ollut aloittaessa aiempaa kokemusta langattomista verkoista. Tavoitteena oli saada rakennettua langaton lähiverkko, joka on mahdollisimman tietoturvallinen. Tämä tavoite saavutettiin. Toteutukselle ei asetettu tarkempia tai kunnianhimoisempia tavoitteita, sillä langatonta verkkoa ei ollut aiemmin käytössä. WLAN-verkko kuuluu nyt riittävän hyvin toimitiloissa eli signaalin vahvuus riittää koko alueella. Tietoturva toteutettiin sekä vieraiden että henkilökunnan verkossa WPA-TKIP-menetelmällä. Henkilökunta pääsee tarvittaessa kiinteään lähiverkkoon VPN-tunnelia pitkin. Kiinteän lähiverkon tärkeitä resursseja suojellaksemme, WLAN-verkko toteutettiin erilleen kiinteästä verkosta.

Oma tavoitteeni oli tutustua WLAN-verkkojen teoriaan ja saada riittävä tietämys, jotta pystyn jatkossa tekemään ylläpidollisia toimia tai muutoksia toteutettuun verkkoon. Tutkimalla lähdekirjallisuutta ja prosessoimalla tätä opinnäyteraporttia olen perehtynyt WLAN-verkkojen perusteisiin. Koen nyt omaavani riittävästi tietämystä WLAN-verkkojen teoriasta ja uskon pystyväni langattoman verkon suunnitteluun ja toteutukseen myös uudestaan, mikäli tarpeen.

Haluaisin mainita myös muutaman sanan graafisen käyttöliittymän kautta konfiguroimisesta. Olen sitä mieltä, että graafisen käyttöliittymän kautta konfigurointi tuntui jopa liian helpolta verrattuna komentorivin kautta konfigurointiin. Tätä ennen olin itse käyttänyt ainoastaan komentorivipohjaa, joten ero tuntui itselleni melko suurelta. Tosin graafinen käyttöliittymä mielestäni nopeuttaa konfigurointia, sillä asetukset saadaan helposti käyttöön valitsemalla oikea asetusvaihtoehto.

Pidän tämän opinnäytetyön etuna verrattuna muihin vastaaviin opinnäytetöihin sitä, että saimme toteuttaa tämän verkon WLAN-kytkimen avulla. Muissa töissä verkot toteutettiin lähes poikkeuksetta pelkkien tukiasemien varaan. Oli mielenkiintoista toteuttaa tämä verkko hieman eri ”kaavan” mukaan ja nähdä mitä uudenmallinen WLAN-kytkin pitää sisällään. Laite osoittautuikin erittäin monipuoliseksi, mutta tällä kertaa monta hyvää ominaisuutta jätettiin myös käyttämättä. Uskon, että näitä ominaisuuksia tullaan ottamaan käyttöön tulevaisuudessa. Esimerkiksi 802.11i-salausmenetelmä otetaan mahdollisesti käyttöön sitten, kun kaikki henkilökunnan kannettavat tietokoneet saadaan vaihdettua uudempiin.

Verkon jatkokehitykseen sain kaksi pähkinää purtavaksi. Olisi hyvä miettiä, voitaisiinko WLAN-verkkoon assosioituva käyttäjä autentikoida palomuurin VPN-käyttäjätietokantaa vasten. Tällöin verkkototeutus tulisi muuttaa siten, että pääsy WLAN-verkkoon tapahtuisi vain VPN-tunnelin kautta. Uskon, että tämä saatai-

siin ehkä onnistumaan 802.1x-ominaisuutta hyväksikäyttäen. Kaikki liittymispyynnöt ohjattaisiin ulkoisen tietokannan (palomuuri) IP-osoitteeseen. Tosin ennen tätä jatkokehitystoimenpidettä on selvitettävä tukeeko käytössä oleva palomuuri tällaista ominaisuutta.

Toinen pohdittava aihe on salauksen käyttö. Tällä hetkellä yhteys salataan kahdesti, jos otetaan yhteys VPN-tunnelilla lähiverkkoon. WLAN-yhteys salataan ensin WPA-TKIP-menetelmällä. Kun otetaan VPN-yhteys, salataan WPA-TKIP-menetelmällä salattu yhteys lisäksi ESP-protokollalla. Olisi hyvä pohtia, mitä haittaa tästä tuplasalauksesta mahdollisesti on. Tietoliikenne saattaa esimerkiksi hidastua. Tällä hetkellä WPA-salausta halutaan kuitenkin käyttää, sillä käyttäjät saattavat käyttää pelkästään Internetiä. Tästä johtuen katsottiin, että tällä hetkellä on tarpeen käyttää myös WPA-TKIP-salausta. Päätimme toimeksiantajan kanssa kuitenkin tarkkailla tilannetta. Jos ilmenee, että tuplasalaus hidastaa verkon toimintaa, on salaus suunniteltava uudelleen. Toistaiseksi ongelmaa ei ole havaittu.

5.2 Lähteistä

Koen onnistuneeni hyvin lähdevalinnoissa. Käytin opinnäytetyöni pohjana kolmea kirjallista niin sanottua päälähdettä; Puskan ”Langattomat lähiverkot” (2005), Hovatan, Kiviniemen ja Somiskan ”WLAN-tekniikat ja -käyttösovellutukset toimitilakiinteistössä” (2005) sekä Geierin ”Langattomat verkot: Perusteet” (2005). Nämä kolme teosta kahlasin lävitse lähes kannesta kanteen, koska ne tarjosivat mielestäni parhaan informaation, joka oli helppo ymmärtää ja sisäistää. Tarkoitukseni oli alussa valita luotettavia, asiantuntevia ja uusia lähteitä. Mielestäni nuo kolme teosta edustavat juuri tällaisia lähteitä, koska kirjoittajina ovat alansa asiantuntijat ja kirjat ovat melko tuoreita. Tosin kehitys langattomissa verkoissa menee eteenpäin jatkuvasti, joten muutaman vuoden päästä nämäkin saattavat jo sisältää vanhaa informaatiota.

Muut lähteet olivat lähinnä täydennystä ja tarkennusta päälähteistä hankittuun tietoon. Jäljitin kiinnostavia lähteitä lukemalla samaan aihealueeseen liittyviä opinnäytetöitä ja niiden lähdeluetteloita. Muun muassa hyödyllisiä sähköisiä artikkeleita löytyi tällä tavalla. Sattumalta löytyi myös mielestäni erinomainen Jim Geierin artikkeleita sisältävä sivusto www.wirelessnetworkingacademy.com. Sivusto tarjosi paljon sellaista informaatiota, jota en löytänyt yhtä selkeässä muodossa muualta.

Pyrin välttämään epäluotettavien lähteiden käyttöä pääasiallisena tietolähteenä ja tässä mielestäni onnistuinkin hyvin. Esimerkiksi Wikipediaa käytin vain tarkistaakseni vuosilukuja Ethernetin kehityksessä, joka ei ollut tämän työn pääaiheen kannalta kriittinen tieto. Arvioin tarkkaan mitä sähköistä lähdettä haluan käyttää työssäni tietolähteenä.

6 Yhteenveto

Langattomia verkkoja on alettu ottamaan käyttöön myös yrityksissä. Parannetut ominaisuudet, kuten tiedonsiirtonopeudet ja tietoturva, ovat alkaneet voittaa yritysmaailman verkkotukihenkilöiden luottamusta.

WLAN-verkon suunnittelussa ja toteutuksessa on otettava huomioon erilaisia seikkoja. Jokainen WLAN-verkko toteutetaan ympäristön ominaisuuksien mukaan. Erityisesti kanavasuunnittelu tulee työstää hyvin olosuhteissa, joissa on useita tukiasemia 2,4 GHz:n taajuudella. Tärkeä seikka on edelleen hieman kyseenalainen tietoturva. Nykyään tarjolla on parannettuja salaustekniikoita, kuten WPA2- sekä VPN-ratkaisun hyödyntäminen langattomassa verkossa. On olemassa myös erilaisia tietoturvakäytäntöjä, joita on hyvä noudattaa. Esimerkiksi sijoittamalla WLAN-verkko kiinteän lähiverkon ulkopuolelle, saadaan turvaa myös kiinteän verkon resursseille.

Omassa opinnäytetyössäni esittelen tamperelaiselle Anilinker Oy:lle toteutetun WLAN-verkon ratkaisuja. En ollut missään vaiheessa törmännyt langattomiin lähiverkoihin ennen tätä opinnäytetyötä. Sain toimeksiannon toteuttaa WLAN-verkon yrityksen toimitiloihin syyskuun 2006 alussa. Projektin aloitusvaihe kesti pari kuukautta, jonka jälkeen oli hankittu laitteiston rahoitus sekä tilattu laitteet. WLAN-verkko sovittiin toteutettavaksi Symbol WS2000 WLAN-kytkimellä ja kahdella Thin Access Point -tukiasemalla. WLAN-kytkimellä verkkoa voidaan hallita keskitetysti eikä tukiasemia tarvitse tällöin konfiguroida yksitellen.

Tämä opinnäytetyö onnistui mielestäni hyvin ja asetetut tavoitteet saavutettiin. Luonnehtisin verkkototeutusta haasteellisuudeltaan keskinkertaiseksi. Verkon tietoturva saatiin kuitenkin ratkaistua riittävän turvalliseksi. Tilanteeseen nähden edullisimmaksi ja toimivimmaksi ratkaisuksi katsottiin WPA-TKIP-salaus ja VPN-yhteyden käyttö otettaessa yhteys kiinteän lähiverkon resursseihin. WLAN-verkon kehityskohteita ei kirjattu vielä tässä vaiheessa virallisesti ylös. Toteuttajat luottavat siihen, että kehityskohteet selvinnevät käyttäjäkokemusten kautta. Itse haluan nimetä kehityskohteiksi VPN-yhteyden tuplasalaus seikan selvittämisen, käyttäjäautentikoinnin toteuttamisen palomuurin tietokantaa vasten, erilaiset käyttöönottamatta jääneet WLAN-kytkimen lisäominaisuudet, kuten SNMP (Simple Network Management Protocol) -ominaisuuksien hyödyntäminen sekä lokiseurannan toteuttamisen suunnittelu. Näistä aiheista voisi saada jopa aikaan toisen opinnäytetyön.

Tehdessäni tätä opinnäytetyötä törmäsin myös toiseen aiheeseen, josta voisi saada aikaan mielenkiintoisen opinnäytetyön. Mielestäni WLAN-verkkojen todellisia tiedonsiirtonopeuksia ja erilaisten fyysisten esteiden vaikutusta nopeuteen olisi hyvä tutkia käytännössä.

Lähteet

Geier, Jim 2005 **1**. Langattomat verkot: Perusteet. Helsinki: Edita Prima Oy.

Geier, Jim **2A** 2005. Making the Choice 80211a or 80211g .[online] [viitattu 15.12.2006] http://www.wirelessnetworkingacademy.com/learning_center/tutorials/Making_the_Choice_80211a_or_80211g.htm

Geier, Jim **2B** 2005. Assigning 802.11b Access Point Channels.[online] [viitattu 15.12.2006] http://www.wirelessnetworkingacademy.com/learning_center/tutorials/Assigning_80211b_Access_Point_Channels.htm

Geier, Jim **2C** 2005. Implementing Multiple SSIDs.[online] [viitattu 16.12.2006] http://www.wirelessnetworkingacademy.com/learning_center/tutorials/Implementing_Multiple_SSIDs.htm

Geier, Jim **2D** 2005. WPA Security Enhancements.[online] [viitattu 27.2.2007] http://www.wirelessnetworkingacademy.com/learning_center/tutorials/WPA_Security_Enhancements.htm

Heinonen, Arsi & Hovatta, Tauno & Hummelin, Harri 2005. Kiinteistöjen lähiverkot. Espoo: Sähköinfo Oy.

Hovatta, Tauno & Kiviniemi, Jussi & Somiska, Jukka 2005. WLAN-tekniikat ja -käyttösovellutukset toimitilakiinteistössä. Espoo: Sähköinfo Oy.

IEEE-SA 2005. Networking Standards For Advanced Telecommunications. [online][viitattu 20.11.2006] http://standards.ieee.org/announcements/bkgnd_802stds.html

IEEE-SA 2006. IEEE Std 802.11h™-2003 Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specificationsAmendment 5: Spectrum and transmit power management extensions in the 5 GHz band in Europe. [online] [viitattu 18.12.2006] http://stdsbbs.ieee.org/all_desc/lanman/restricted/802.11h-2003.html

Jaakohuhta, Hannu 2000. Lähiverkot: Ethernet. Helsinki: IT Press.

Puska, Matti 2005. Langattomat lähiverkot. Helsinki: Talentum.

Reiss, Markku 2006. Langaton lähiverkko 60 prosentilla yrityksistä. [online][viitattu 5.9.2006].
http://www.itviikko.fi/page.php?page_id=15&news_id=200611522

Seppänen, Lasse. Langaton lähiverkko: Wireless Local Area Network (WLAN) IEEE 802.11. [online] [viitattu 10.12.2006]
http://trade.hamk.fi/~lseppane/courses/wlan/doc/Materiaali.pdf

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

Symbol **1** 2006. WS2000 Wireless Switch from Symbol. [online] [viitattu 27.12.2006]
http://www.symbol.com/ws2000

Symbol **2** 2006. AP300 Wireless Access Port from Symbol [online] [viitattu 27.12.2006]
http://www.symbol.com/products/wireless/ap_300_ap.html

Wikipedia – Vapaa tietosanakirja. Ethernet. [online][viitattu 15.10.2006]
http://fi.wikipedia.org/wiki/Ethernet