Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Antti Dufva

Langattoman lähiverkon käyttöönotto Sweco Industry Oy:ssä

Insinöörityö

Ohjaaja: IT-asiantuntija Juhani Inkiläinen
Ohjaava opettaja: yliopettaja Matti Puska

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä Otsikko Sivumäärä Aika	Antti Dufva Langattoman lähiverkon käyttöönotto Sweco Industry Oy:ssä 38 sivua 8.5.2010
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja Ohjaava opettaja	IT-asiantuntija Juhani Inkiläinen yliopettaja Matti Puska

Tämä insinöörityö käsittelee langattoman lähiverkon suunnittelun ja toteutuksen yritys ympäristössä. Työn tilaajana toimii Sweco Industry Oy.

Tänä päivänä langattomat verkot ovat käytössä useissa eri käyttötarkoituksissa. Langaton lähiverkkoteknologia on hyvin laajasti levinnyt kannettaviin tietokoneisiin ja mobiili-laitteisiin. Langattomalla teknologialla on helppo tarjota verkkoyhteys tiloihin, joissa kiinteää kaapelointia ei ole tai sen käyttö olisi hankalaa. Langaton lähiverkko on myös yleinen tapa toteuttaa verkkoyhteys neuvotteluhuoneisiin, joissa voi olla monenlaisia käyttötarpeita, niin yrityksen työntekijöillä, kuin vieraillakin.

Työn tavoitteena oli toteuttaa langaton lähiverkkojärjestelmä, joka pystytään yhdistämään yrityksen käytössä oleviin tietojärjestelmiin.

Työn kirjallisessa osassa käydään läpi langattomien lähiverkkojen teknologiat ja tietoturva-ominaisuudet. Työn toteutusosassa käydään läpi langattoman lähiverkon suunnittelu, mitä toimenpiteitä ja laitteita se vaatii, sekä verkon rakentaminen ja käyttöönotto, siten että ne vastavat yrityksen tarpeita.

Työn lopputuloksena syntyi WLAN-järjestelmä, joka mahdollistaa yritysten työntekijöiden turvallisen ja helpon kytkeytymisen yrityksen verkkoon, sekä että vierailijoiden verkko-yhteyden neuvotteluhuoneissa. Tämä mahdollistaa vierailijaverkon käytön laajentamisen kaikkiin yrityksen toimipisteisiin.

Hakusanat	langaton lähiverkko, WLAN-käyttöönotto, 802.11, yrityskäyttö, vierasverkko

Helsinki Metropolia University of Applied Sciences Abstract

Author Title Number of Pages Date	Antti Dufva Implementing WLAN in Sweco Industry Oy 38 pages 8 May 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Juhani Inkiläinen, ICT Specialist Matti Puska Title Principal Lecturer

Assigned by Sweco Industry Oy, the purpose of this thesis project was to implement a wireless local-area network (WLAN) at their facility.

Nowadays wireless networks are applied to many different uses. WLAN technologies are very widespread in laptops and mobile devices. WLAN technology can provide easy network access in locations where fixed wiring does not exist or it would be difficult to use. WLAN is also a common way to implement network access to conference rooms with a wide range of user needs from corporate to guest users. The goal was to implement a WLAN system which could combine the company's existing data systems.

The theory part of the thesis is concerned with WLAN technologies and security features. The practical part focuses on planning and implementing a WLAN as well as the operations it needs and the devises it requires to cover business use requirements.

The final result was a WLAN system, which allows the employees a secure and simple connection in the corporate network, as well as guest users a network connection to the negotiating rooms. This allows the guest network to be extended to all company offices.

Keywords	wireless networks, WLAN-implementation, 802.11, business use, guest network

Sisällys

Lyhenteet

AES	Advanced Encryption Standard; salausmenetelmä
BBS	Basic Service Set; peruspalveluverkko
DHCP	Dynamic Host Configuration Protocol; IP-osoitteiden jakeluprotokolla
EAP	Extensible Authentication Protocol; tunnistusprotokolla
EDCA	Enhanced Distributed Channel Access; palvelunlaadusta ja pakettien luokittelusta vastaava protokolla
HCF	Hybrid Coordination Function; kanavalle pääsyn koordinointifunktio
IEEE	Institute of Electrical and Electronics Engineers; standardointijärjestö
IBBS	Independent BBS; ifrastruktuuriverkko
IP	Internet Protocol; internetissä käytettävä pakettimuoto
IAS	Internet Authentication Service; tunnistuspalvelu
LAN	Local Area Network; lähiverkko
MAC	Media Access Control; siirtokerroksen alin kerros
MPLS	Multiprotocol Label Switching; lippuinformaatiota käyttävä tiedonsiirtotapa
OSI	Open Systems Interconnection; tietoliikenteen referensimalli
PoE	Power over Ethernet; virransyöttötapa lähiveverkossa
PSK	PreShared Key; esijaettu avain
QoS	Quality of Service; liikenteen luokittelu
RADIUS	Remote Authentication Dial-in User Service; tunnistamisen ja valtuuksien määrittelyyn käytettävä palvelu

SNMP	Simple Network Management Protocol; verkkojen hallinnassa käytettävä tietoliikenneprotokolla
SSL	Secure Sockets Layer; liikenteen salaustapa
SSID	Service Set Identifier; langattoman verkon nimi
TKIP	Temporal Key Integrity Protocol; automaattisen avainten uusimisen mahdollistava protokolla
TLS	Transport Layer Security; salausprotokolla
VLAN	Virtual LAN; virtuaali lähiverkko
VoIP	Voice over IP; IP-puhe
VPN	Virtual Private Network; virtuaalinen yritysverkko
WEP	Wireless Equivalent Privacy; langattoman lähiverkon salaustekniikka
WPA	Wireless Fidelity Protected Access; langattoman lähiverkon salaustekniikka
WPA2	WPA versio 2; langattoman lähiverkon salaustekniikka
WLAN	Wireless LAN; langaton lähiverkko
VoWLAN	Voice over WLAN; IP-puhe langattomassa lähiverkossa

1 Johdanto

Tämä työ on tehty Sweco Industry Oy:lle. Työn aiheena oli suunnitella ja toteuttaa langaton lähiverkko osaksi Sweco Industry Oy:n jo olemassa olevaa verkkoa.

Langattoman lähiverkon avulla voidaan tarjota asiakkaille ja liikekumppaneille helppo ja nopea pääsy Internetiin. Sen avulla voidaan myös tarjota yrityksen työntekijöille mahdollisuus kytkeytyä langattomasti Sweco Industry Oy:n lähiverkkoon, mikä mahdollistaa tehokkaan työskentelyn myös henkilökohtaisen työpisteen ulkopuolella.

Työn kirjallisessa osassa esitellään langattoman lähiverkon tekniset ominaisuudet sekä siihen liittyvä tietoturva.

Työn toteutusosassa esitellään, miten langaton lähiverkko toteutettiin Sweco Industry Oy:n tiloihin ja mitä toimenpiteitä ja laitteita se vaati. Tässä osassa kerrotaan myös, miten langaton lähiverkko otettiin käyttöön osaksi yrityksen olemassa olevaa verkkoa.

2 Langaton lähiverkko

2.1 Langattomien lähiverkkojen periaate

Langattomalla lähiverkolla tarkoitetaan tiedonsiirtoa ilman fyysistä tietoverkkoa tietokoneiden välillä. Sen avulla mahdollistetaan joustava liittyminen verkossa oleviin palveluihin, ja vapaus liikkua ja tehdä töitä eri paikoissa. Nykyään langattomista verkoista on tullut näkyvämpi osa jokaisen ihmisen arkipäivää. [1.]

Langattoman verkon avulla tapahtuva langaton viestintä ei kuitenkaan ole uusi keksintö. Ensimmäisiä merkkipaaluja langattomasta viestinnästä oli intiaanien käyttämät savumerkit. Niiden avulla saatiin välitettyä viestejä pitkienkin välimatkojen päähän. Langatonta viestintää käytetään hyväksi myös matkapuhelimissa, joiden käyttö on yleistynyt maailmanlaajuiseksi. [1.]

Langattomat verkot käyttävät viestisignaalien eli informaatiosignaalien siirtotienä ilmatietä. Informaatiosignaalit voivat kulkea pitkiäkin matkoja, mutta etäisyyden kasvaessa signaalin voimakkuus heikkenee. Kaavassa 1 on esitetty ilman vapaan tilan vaimennussuhde (L):

$$L = \left(\frac{4\Pi d}{\lambda} \right)^2, \tag{1}$$

jossa d on etäisyys ja λ on aallonpituus.

Signaalien laatuun vaikuttavat vaimennussuhteen lisäksi ilmatiellä esiintyvät esteet, jotka heikentävät ja hajottavat signaalien voimakkuutta ja kantavuutta.

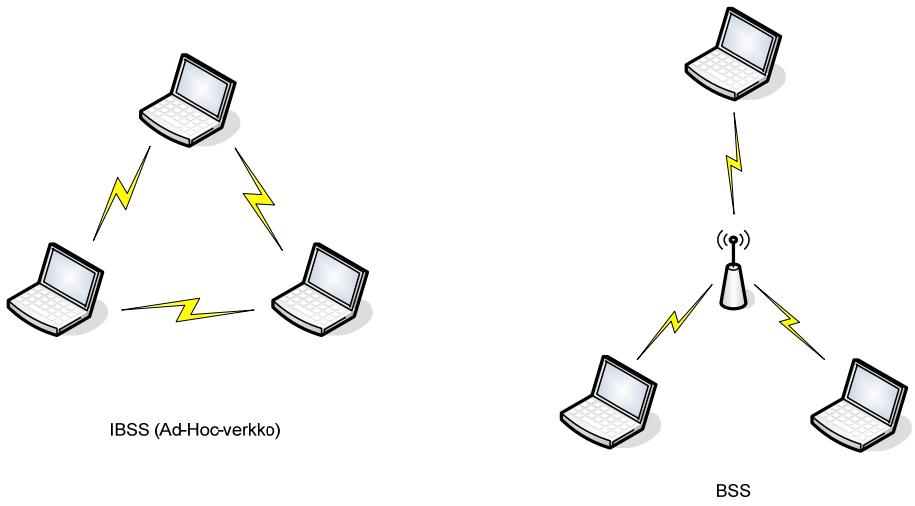
Jotta langattomassa verkossa voidaan suorittaa tiedonsiirtoa, tarvitaan yhteys lähde- ja kohdekoneen välille. Tämän yhteyden luomiseksi tarvitaan kuljetus- ja istuntokerroksen toimintoja. Näiden kerrosten ominaisuuksista sekä verkon rakenteesta kerrotaan tarkemmin luvussa 2.2.

Jotta tietokonelaitteella voidaan kytkeytyä ja käyttää langatonta verkkoa, täytyy siinä olla langaton verkkosovitin eli verkkokortti. Verkkokortin toiminnan määrittelevät käytössä olevat verkkostandardit. Langattoman lähiverkon ja langattoman verkkokortin on toimittava saman standardin mukaisesti. 2.3 IEEE 802.11 -standardit kappaleessa on esitelty tarkemmin yleisimmät käytössä olevat langattoman verkon standardit. [1.]

2.2 Langattomien verkkojen rakenne

Tietokonelaitteet toimivat langattomassa verkossa asiakaspäätteinä. Asiakaspäätteinä voi toimia esimerkiksi kannettava tietokone, kämmentietokone, matkapuhelin, pöytätyöasema sekä tulostin [1]. IEEE 802.11-protokollassa määritellään kaksi erityppistä verkkotopologiaa [2; 3]. Asiakaspäätteet yhdistyvät dynaamisesti langattoman verkon soluihin tai perusarkkitehtuuriin BBS (Basic Service Set). [2.]

Ensimmäinen malli on IBSS (Independent BBS) eli ad hoc -verkko (tilapäisverkko) (kuva 1, vasemmanpuoleinen kuva). IBSS-verkossa lähettäjä- ja vastaanottajalaite muodostavat suoran yhteyden MAC (Media Access Control) -verkkokerroksella ja kommunikoivat keskenään. IBSS-verkkoa käytetään yleensä lyhyen aikaan jotain tiettyä käyttötarkoitusta varten. IBSS ei tarjoa minkäänlaisia yhteyksiä ulkoisiin verkkoihin. Tästä johtuen kaikki liikenne on siihen kytkettyjen laitteiden välistä. Laitteet voivat olla saman IBSS-verkon jäseniä näkemättä toisiaan. Standardi kieltää laitteita toimimasta kytkimenä tai välittäjänä osapuolten välillä. [2; 3.]



Kuva 1. IBSS- ja BSS-verkkotopologiat.

Toinen malli on infrastuktuuri-BSS (k 1, oikeanpuoleinen kuva), joka perustuu tukiasemaan, ja on asiakas-palvelintyyppinen ratkaisu [2; 3]. BSS muodostuu kiinteästä tukiasemasta, joka operoi tietyllä kanavalla. BSS:ssä on tukiasema (AP, Access Point), joka hallitsee ja välittää liikenteen solussa. Tukiasemien avulla yhdistetään langattomat viestisignaalit lankaverkkoon. Tukiasemat sisältävät langattoman verkkoliitännän, joka toimii samalla standardilla muiden langattoman verkon laitteiden kanssa.[1.]

2.3 IEEE 802.11 -standardit

IEEE 802.11

Vuonna 1997 IEEE:n (Institute of Electrical and Electronics Engineers) julkaisema 802.11 on yleisin langattomien lähiverkkojen standardi tällä hetkellä. Standardilla katetaan OSI-mallin kaksi alinta kerrosta: siirtoyhteyskerroksella toimiva yhteisen siirtotien varausmenetelmä (MAC) sekä fyysinen kerros. Standardin enimmäisnopeudeksi määritetty bittinopeus on 2 Mbps, ja se toimiin 2,4 GHz:n taajuusalueella. Standardi määrittelee välitystekniikoiksi infrapunan ja radiotien. Tällä hetkellä ei kuitenkaan ole käytössä infrapunatekniikkaan perustuvia laitteita, vaan kaikki toimivat radiotaajuudella. [1; 4.]

Standardiin on tehty useita eri versiota, jotka kaikki käyttävät radiotien taajuuskaistoja 2,4 tai 5 GHz. Eri versiot eivät ole kaikilta osin täysin yhteensopivia. [1.]

Fyysisen kerroksen standardit

Fyysisen kerroksen standardit määrittelevät laitteiden käyttämät taajuudet, kanavat ja niiden leveydet ja verkon nopeusluokat.

IEEE802.11a

Vuonna 1999 julkaistu 802.11a käyttää 5 GHz:n radiotaajuusaluetta. 5 GHz mahdollisti verkkoyhteyksien bittinopeuden noston aina 54 Mbps:ään asti. Standardiin pohjautuvat laitteet tulivat markkinoille vasta 2001 johtuen tarvittavien piirien kehittämisen hankaluudesta. [1; 5.]

IEEE802.11b

802.11b hyväksyttiin IEEE:an toimesta samaan aikaan 802.11a:n kanssa, ja 802.11b standardiin pohjautuvia laitteita oli saatavana jo vuonna 1999. Tämän johdosta standardi yleistyi 802.11a:ta nopeammin. Standardi toimii 2,4 GHz:n taajuuskaistalla, ja sen suurin mahdollinen verkkoyhteyden bittinopeus on 11 Mbps. [1; 5.]

Standardin etuna on hyvä kantomatka, sisätiloissa voidaan päästä jopa 100 metrin kantamaan. Tämä vähentää lähiverkkoon tarvittavien tukiasemien määrää. Heikkouksina voidaan pitää käytettävää 2,4 GHz:n radiotaajuusaluetta, sillä monet laitteet, kuten mikroaaltouuni ja langaton puhelin, käyttävät tätä vapaasti käytössä olevaa radiotaajuusaluetta. [1.]

IEEE802.11g

Vuonna 2003 julkaistu versio IEEE802.11g käyttää samaa taajuutta kuin b-versio ja toimii a-version käyttämillä nopeuksilla. Koska 802.11g on yhteensopiva b-version kanssa, voidaan niihin pohjautuvia laitteita käyttää samassa verkossa. Kun

verkkoyhteyden bittinopeus kasvaa suuremmaksi kuin 11 Mbps, se ylittää b-version mukaisten laitteiden suorituskyvyn. Näillä nopeuksilla käytetään pelkästään 802.11g-standardia. [1; 5.]

IEEE802.11n

802.11n-version avulla parannetaan b- ja g-versioiden suorituskykyä. Standardi käyttää useampaa antennia ja kanavaa samanaikaisesti. Tämän johdosta saadaan pidennettyä kantamaa ja lisättyä verkkoyhteyden nopeutta. IEEE hyväksyi tämän standardin syyskuussa 2009. [5; 6.]

Laajennukset ja lisäosat

Lisäosilla on parannettu langattoman lähiverkon ominaisuuksia sekä tietoturvan että liikkuvuuden osalta. Laajennuksia voidaan liittää yksittäin tai yhdessä fyysisen kerroksen standardeihin.

IEEE 802.11e

IEEE 802.11e on vuonna 2005 hyväksytty QoS-laajennus (Quality of Service, palvelunlaatu) langattomaan lähiverkkoon. Laajennus tarjoaa parannettuja MAC-ominaisuuksia: EDCF (Enhanced Distributed Channel Access), HCF (Hybrid Coordination Function) sekä QoS-merkinantoa ja uusia kehyksiä QoS-tuella. 802.11e standardista hyödytään paljon VoWLAN (Voice over WLAN) -ratkaisuissa, jotka ovat erittäin viivekriittisiä. [5; 7.]

IEEE 802.11i

802.11i-standardin tietoturvallisuuden puutteita saadaan parannettua ottamalla käyttöön vuonna 2004 hyväksytty 802.11i-standardi. Standardi määrittelee seuraavat asiat: tietoturvaan ja päätelaitteiden liikkuvuuteen liittyvät parannukset, luotettava salausavainten hallinta ja vahvan AES-salaus (Advanced Encryption Standard). [2; 5.]

IEEE 802.11r

IEEE 802.11r -standardilla parannetaan liikkuvuutta WLAN-verkossa. Standardi mahdollistaa alle 50 millisekunnin viiveen käyttäjän vaihtaessa tukiasemaa. Näin pystytään tarjoamaan katkeamaton yhteys esim. VoIP-palveluiden (Voice over IP) -käyttäjille, heidän liikkuessaan WLAN-verkon alueella. [8.]

IEEE 802.11s

802.11s-laajennus tulee pitämään sisällään tuen mesh-verkoille, mikä mahdollistaa tukiasemien liittämisen verkkoon ilman erillistä verkkokaapelointia. Tämä helpottaa verkkoyhteyksien luomista tiloihin, joissa ei ole valmiiksi tehtyä verkkokaapelointia. [9.]

3 Tietoturva

3.1 Langattoman verkon tietoturva yleisesti

Langattoman verkon tietoturvariskit ovat pääsääntöisesti samat kuin perinteisen langallisen verkon. Langattomuudesta johtuen verkkoon voidaan kytkeytyä ilman fyysistä pääsyä, mikä on ollut helpoin tapa rajata verkon käyttö. Tämän vuoksi yrityksen verkosta voidaan yrittää varastaa tietoja, käyttää eri sovelluksia tai keskeyttää verkon toiminta kokonaan tai osittain (kuva 2). [2; 10.]

Kuva 2. Langattoman verkon uhat: verkon tarkkailu, luvaton käyttö ja palvelunesto [10].

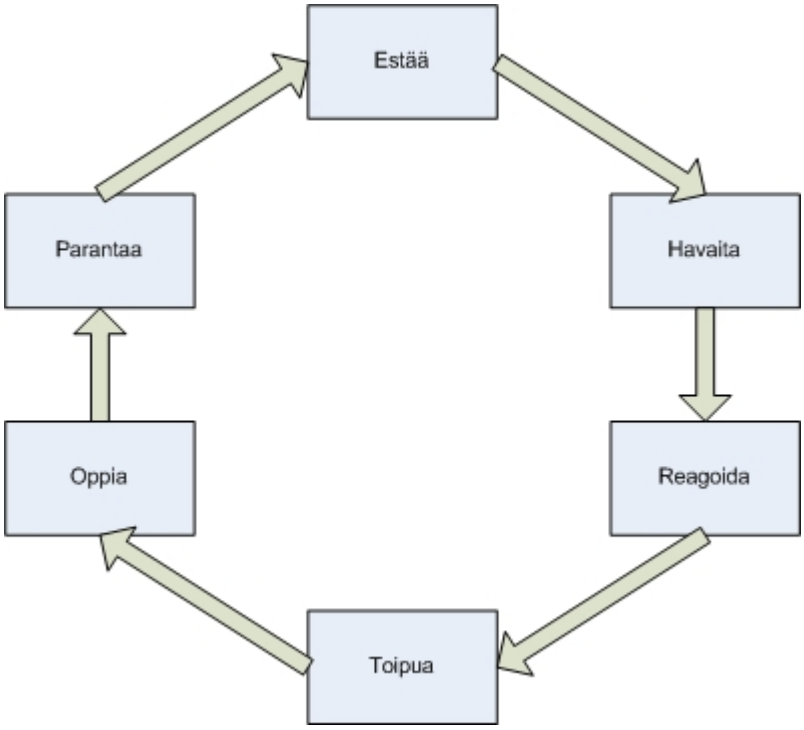
Langattomissa lähiverkoissa käytetty standardi 802.11 ei takaa riittävää tietoturvaa verkossa. Tämän vuoksi sitä on yritetty parantaa monilla eri lisäosilla. Yksi toimivimmista parannuksista on kesällä 2004 hyväksytty IEEE 802.11i -standardi, joka takaa luotettavan salausmenetelmän. [2.]

Langattoman verkon tietoturvaa voidaan parantaa seuraavien kuuden turvapalvelun avulla:

- tiedon luottamuksellisuus (Confidentiality)
- tiedon eheys (Integrity)
- todennus (Authentication)
- kiistämättömyys (Non-repudiation)
- pääsynvalvonta (Access Control)
- käytettävyys (Availability) [11.]

Tiedon luottamuksellisuuden avulla sähköisen tiedon käytettävyys rajoitetaan vain tietyille henkilöille. Käyttöoikeudet määritellään jokaiselle henkilölle erikseen käyttöoikeusryhmien mukaisiksi. *Tiedon eheydellä* varmistutaan siitä, että tietoa ei ole muutettu ulkopuolisten, ei-valtuutettujen toimesta tiedonsiirron aikana. Tiedon muuttumisella tarkoitetaan tässä tapauksessa vahingossa muuttunutta tai tahallisesti muutettua tietoa. *Todennuksen* avulla varmistetaan kommunikointikumppanien identiteetti. Sen avulla voidaan todentaa tehdyt toimenpiteet jälkikäteen. Huomattavaa on, että tiedon todennuksella parannetaan myös tiedon eheyttä. *Kiistämättömyydellä* varmistetaan tietojen, toimenpiteiden ja käyttäjien aitoudet. *Pääsynvalvonnan* avulla rajoitetaan henkilöiden pääsyä tietoihin. *Käytettävyydellä* varmistetaan, että oikeutetuilla henkilöillä on mahdollisuus käyttää verkkopalveluja tarvittaessa. [11.]

Riittävän tietoturvan aikaansaamiseksi on yrityksen määriteltävä tietoturvapolitiikka. Yrityksen tietoturvan ajan tasalla pitäminen vaatii jatkuvia toimia. Kuvassa 3 on esitetty yksi toimintamalli tietoturvan jatkuvasta kehittämisestä. [1; 4; 11.]



Kuva 3. Tietoturvapolitiikan kehittäminen käytössä.

Olemassa olevan tietoturvapolitiikan avulla pyritään turvaamaan verkon ja verkkopalveluiden toiminta väärinkäytöksiltä ja hyökkäyksiltä. Järjestelmien toimintaa ja turvatasoa seurataan jatkuvasti ja häiriötilanteen sattuessa reagoidaan välittömästi. Nopean toiminnan avulla häiriötilanteen jälkeen saadaan järjestelmä toipumaan häiriöistä. Tämän jälkeen täytyy ymmärtää, mitä on tapahtunut ja minkä takia, jotta voidaan parantaa tietoturvapolitiikkaa. Tietoturvapolitiikan kehittäminen ei kuitenkaan saa jäädä pelkästään häiriöistä oppimiseen, vaan sitä pitää myös omatoimisesti kehittää. [1; 4; 11.]

3.2 Langattoman verkon suojausmenetelmät

WEP-protokolla (Wired Equivalent Privacy) on 802.11-standardin määrittelemä turvamekanismi, jolla pyritään turvaamaan verkkoliikenteen luottamuksellisuus. Tämä perustuu maksimissaan 128-bittisen jaetun avaimeen käyttöön, jonka salausalgoritmi perustuu RSA-yhtiön (Rivest, Shamir and Adleman) RC4-salausalgoritmiin. Tämän takia WEP-salaus on helposti murrettavissa. WEP ei tarjoa varsinaisesti käyttäjien

luotettavaa tunnistusta, koska käytetään jaettua avainta. Tunnistusta voidaan parantaa määrittelemällä tukiasemille sallittujen MAC-osoitteiden listat, joista liikennöinti on sallittua. MAC-osoitteet ovat kuitenkin helposti muutettavissa, joten niiden käyttö tuo vain nimellistä turvallisuutta verkkoon, ja niitä on hankala ylläpitää useiden tukiasemien ympäristössä. MAC-osoitelistojen käyttö ei ole 802.11-standardin mukaista. [2; 12.]

WPA-protokolla (Wireless Fidelity Protected Access) on kehitetty ennen varsinaista 802.11i-standardia parantamaan langattomien verkkojen tietoturvaa ja korjaamaan WEP-prokollan puutteita. WPA sisältää salausavaimen automaattisen uusimisen sekä käyttää pakettikohtaisia salausavaimia. TKIP (Temporal Key Integrity Protocol) huolehtii pakettien salauksesta käyttäen RC4-salausalgoritmia. Viestien eheyden tarkistamiseen käytetään lisäksi MIC-ominaisuutta (Message Integrity Code). WPA sisältää 802.1x-todennuksen ja tukee myös käyttäjien luotettavaa tunnistamista hyödyntäen EAP (Extensible Authentication Protocol) -protokollaa ja RADIUS (Remote Authentication Dial-in User Service) -ympäristöä. Tätä kutsutaan WPA Enterprise -tilaksi. WPA-ympäristössä on mahdollista käyttää etukäteen jaettua aloitusavainta PSK:tä (PreShared Key). Tätä kutsutaan WPA Personal -tilaksi. [12; 13; 14.]

WPA2-protokolla eli 802.11i-standardi sisältää parannuksia WPA-protokollaan. Salausalgoritmiksi on päivitetty AES käyttäen Counter Mode-Cipher Block Chaining- (CBC) ja Message Auhtentication Code (MAC) -protokollaa (CCMP), mikä tarjoaa tiedon luottamuksellisuuden, alkuperän ja eheyden varmistuksen. WPA2 on myös Presonal -tila, jossa voidaan käyttää PSK:tä sekä Enterprice-tila käyttäen 802.1x:ää. [2; 15; 16.]

IEEE 802.1x-standardissa määritellään tapa tunnistaa verkkoon liittyvät asiakkaat portti- ja käyttäjäkohtaisesti. Tunnistustapaan kuuluvat asiakaskoneen verkkokortti (Supplicant), tukiasema (Authenticator) ja todennuksen tekevä palvelin (Authentication Server). [12;17.]

EAP on pohjimmiltaan kuljetuskerroksen protokolla, joka tukee useita todennustapoja. EAP:aa käytetään yleensä siirtokerroksella, esimerkiksi Point-to-Point -protokollan

(PPP), tai IEEE 802:n päällä eikä se tarvitse toimiakseen IP:tä. Taulukossa 1 on esitetty langattomien verkkojen kanssa yleisesti käytettyjen EAP-tapojen eroavaisuuksia. [18; 19.]

Taulukko 1. EAP-versioiden erot [20].

	EAP-MD5	**LEAP**	**EAP-TLS**	**EAP-TTLS**	**PEAP**
Server Authentication	None	Password Hash	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Password Hash	Public Key (Certificate or Smart Card)	CHAP, PAP, MS-CHAP(v2), EAP	Any EAP, like EAP-MS-CHAPv2 or Public Key
Dynamic Key Delivery	No	Yes	Yes	Yes	Yes
Security Risks	Identity exposed, Dictionary attack, Man-in-the-Middle (MitM) attack, Session hijacking	Identity exposed, Dictionary attack	Identity exposed	MitM attack	MitM attack; Identity hidden in Phase 2 but potential exposure in Phase 1

EAP-versiot

EAP-MD5 -todentamistapa tarjoaa yhdensuuntaisen salasanapohjaisen asiakkaan tunnistamistavan. Tämän todentamistavan heikkoutena voidaan pitää sitä, ettei se tarjoa salausavaimia. [2.]

LEAP (Lightweight EAP) on Ciscon kehittämä ja standardisoima EAP-todentamismenetelmä. LEAP tarjoa molemminpuolisen todentamisen ja dynaamisen salausavainten vaihtomekanismin, mutta avainten vaihto perustuu jaettuun avaimeen. [18.]

EAP-TLS käyttää TLS-protokollaa (Transport Layer Security) tarjoten molemminpuolisen julkisen avaimen, joka on varmenteeseen pohjautuva todentamistapa, sekä salausavainten vaihdon. Asiakkaan ja palvelimen sertifikaattien täytyy olla sellaisen varmennepalvelimen allekirjoittamia, johon kumpikin luottaa. [2; 18.]

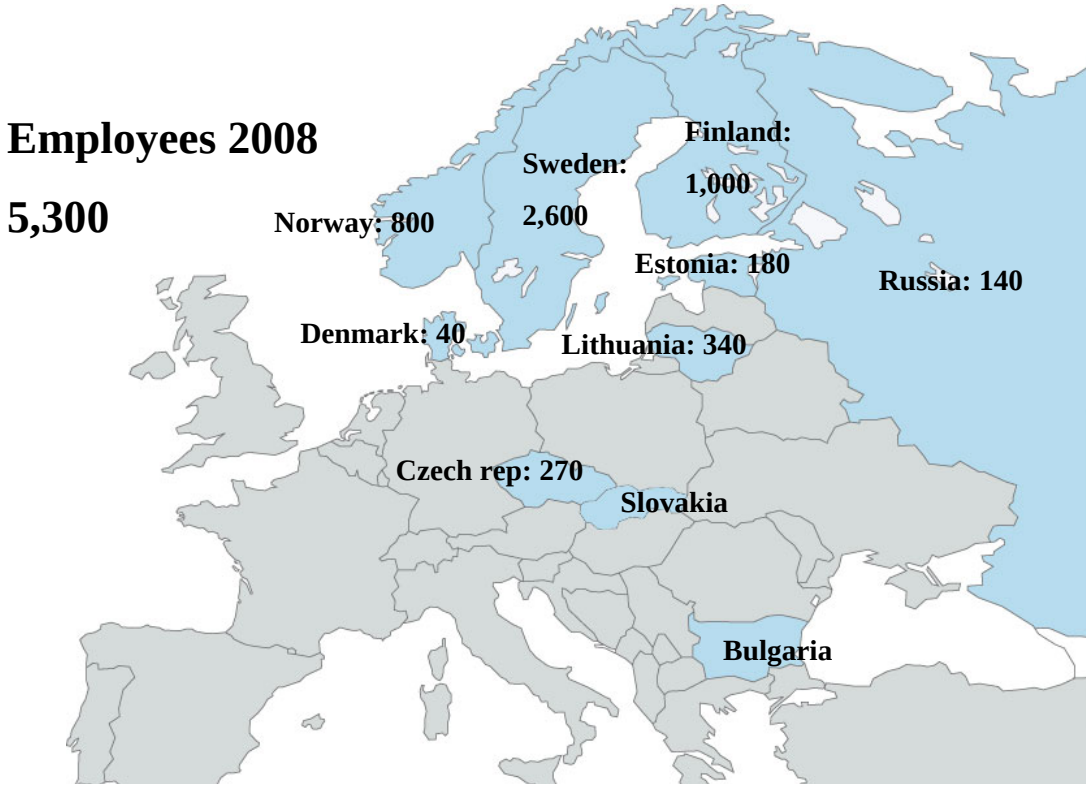
EAP-TTLS:ää (EAP Tunneled TLS) voidaan pitää EAP-TLS:n ja perinteisen salasanapohjaisen todentamistavan yhdistelmänä, jossa ensin luodaan turvallinen TLS-tunneli palvelimelle, jonka jälkeen asiakas tunnistetaan. EAP-TTLS muistuttaa paljolti PEAP:a (Protected EAP). [2; 18.]

PEAP mahdollistaa asiakkaiden tunnistamisen ilman niiltä vaadittavia varmenteita. PEAP lisää TLS-kerroksen EAP:n päälle, palvelin tunnistetaan julkisen avaimen varmenteella, jonka jälkeen asiakaan ja palvelimen väliset EAP viestit paketoidaan TLS:n sisään. [18.]

4 Työn tavoitteet

4.1 Taustat

SWECO on kansainvälisesti toimiva tekninen asiantuntijayhtiö, ja sen pääkonttori sijaitsee Tukholmassa Ruotsissa. Sweco-konserni työllistää yhteensä 5 300 henkilöä kymmenessä maassa (kuva 4). Konsernin liikevaihto on noin 483 miljoonaa euroa. [21.]



Kuva 4. Maat, joissa Sweco-konsernilla on toimipisteet [21].

Työn tekohetkellä Suomessa oli kolme Sweco-konserniin kuuluvaa yritystä: Sweco Industry Oy, Sweco CMU Oy ja Sweco Paatela Architects Oy. Kuvassa 5 on esitetty Sweco-konserniin kuuluvien yritysten toimipisteiden sijainti Suomessa. [21.]

Kuva 5. Toimipisteiden sijainti kartalla [21].

Sweco Industry Oy:n verkko koostuu pääkonttorista Vantaalla sekä useista aluetoimipisteistä ympäri Suomea. Toimipisteet on kytketty toisiinsa MPLS-VPN (Multiprotocol Label Switching-Virtual Private Network) -yhteydellä. Myös muut Suomessa toimivat Sweco-konsernin yritykset on kytketty aluetoimistojen tapaan MPLS-VPN -yhteydellä Sweco Industryn verkkoon. [21.]

Toimipisteiden työntekijämäärä vaihtelee noin 10 hengestä 300 henkeen. Henkilömäärä vaikuttaa oleellisesti tarvittavien tukiasemien määrään toimistoissa, joissa langaton verkko otettiin täysipainoisesti tuotantoympäristön käyttöön. [21.]

Yrityksen toimipisteissä tehdään töitä pääsääntöisesti paikalliselle levypinnalle. Tämä aiheuttaa verkkoliikenteen kasvua, kun kaikki liikenne langattoman verkon päätelaitteen ja levypalvelun kautta kiertää yhden WLAN-kytkimen kautta.

Ennen projektin aloittamista yrityksessä oli olemassa yhden tukiaseman laajuinen langaton vierailijaverkko. Tämän verkon peittoalue oli yrityksen koulutustila. Sen kautta oli mahdollista kytkeytyä yrityksen vierasverkkoon, josta oli mahdollista päästä Internetiin. Langattoman verkon käyttö oli hyvin vähäistä, mikä johtui langattoman verkon pienestä peittoalueesta.

4.2 Langattoman lähiverkon tarpeet yrityksessä

Sweco Industry Oy:n tuotanto-osasto halusi vierailijoiden käyttöön langattoman verkkoyhteyden, jonka avulla asiakkaat pääsisivät käyttämään helposti ja vaivattomasti Internetiä eri liiketoimipisteistä. Langattoman verkon käyttöä puolsi myös se, että Swecon sisäiseen verkkoon ei saa kytkeä ulkopuolisia koneita, eikä kaikissa toimipisteissä ole mahdollista käyttää käytössä olevaa ”langallista” vierasverkkoa.

Verkon kohderyhmäksi valittiin tuotanto-osastojen tarpeen perusteella vierailijat. Vierailijoiden lisäksi määriteltiin myös yrityksen työntekijät mahdollisiksi käyttäjiksi. Vierasryhmälle verkon käyttöä rajoitettiin yrityksen tietoturvapolitiikan mukaisesti olemassa olevaan vierasverkkoon. Työntekijöille haluttiin tarjota pääsy yrityksen sisäverkkoon, mikä vaatii yrityksen tietoturvapolitiikan mukaisen salauksen ja tunnistamisen.

Langattoman verkon keskitettyä hallintaa pidettiin oleellisena osana langattoman verkon ylläpidon osalta. Keskitetyn hallinnan avulla helpotetaan verkon hallintaa, valvontaa ja ylläpitoa.

Järjestelmän haluttiin mukautuvan yrityksen mahdollisien tulevaisuuden tarpeiden mukaisiksi. Tällaisia tarpeita voivat olla muun muassa mahdolliset mobiilipäätelaitteet ja VoWLAN (Voice over WLAN). Myös mahdolliset uudet toimipisteet vaativat järjestelmältä mukautumista niiden tarpeisiin.

Suunnittelun alussa määritettiin langattoman verkon peittoalue. Peittoalueen haluttiin kattavan yrityksen edustustilat, joissa vierailijoilla olisi tarpeellista käyttää verkkoa. Tällaisiksi tiloiksi määriteltiin neuvotteluhuoneet Vantaalla, Kuopiossa, Oulussa,

Lappeenrannassa, Pietarsaaressa, Anjalankoskella, Varkaudessa ja Tampereella. Vantaalla valittiin näiden tilojen lisäksi IT-, sauna- ja koulutustilat peittoalueen piiriin. Vantaalla tällaisia tiloja oli kahdessa rakennuksessa ja useassa eri kerroksessa.

Käyttäjämäärät vaihtelivat toimipisteiden koon mukaan noin kymmenestä käyttäjästä 100 käyttäjään ja yhteysnopeudet vaihtelivat käyttäjämäärien mukaan 4/4 Mbps:sta 10/10 Mbps:iin. Neuvotteluhuoneet sijaitsivat muutamissa toimistoissa hyvin kaukana toisistaan, ja tällöin jouduttiin varautumaan kahden WLAN-tukiaseman sijoittamiseen toimistoon. Viidessä toimistossa työskenteli paikallinen tukihenkilö.

5 Toteutus

5.1 Järjestelmän valinta

Yrityksen olemassa oleva verkko oli toteutettu Nortelin laitteilla. Pysyminen saman laitevalmistajan laitteistossa oli luontevaa. Valintaa tuki myös yrityksen laitetoimittajan saamat positiiviset kokemukset Nortelin tarjoamista WLAN-ratkaisuista.

Standardiksi, jolla langaton lähiverkko toteutettiin, valittiin IEEE 802.11g, joka oli valintahetkellä tuorein virallinen langattomien lähiverkojen standardi. 802.11g sisältää tuen myös vanhemmalle 802.11b-standardille. Käytössä olevista kannettavissa tietokoneissa on 802.11b/g-standardin mukaiset verkkosovittimet, mikä tuki myös käytettävän standardin valintaa.

Langattoman lähiverkon hallinnan helpottamiseksi haluttiin ratkaisu, joka tarjoaa yhden hallintapisteen kaikkien tukiasemien asetusten hallintaa varten. Verkon ylläpito olisi muodostunut hyvin hankalaksi, jos verkkoon tehtävät muutokset pitäisi tehdä kaikille tukiasemille. Valitussa mallissa muutokset tehdään hallintakytkimelle, joka julkaisee ne tukiasemille.

Seuraavassa esitellään valittujen komponenttien tärkeimmät ominaisuudet.

WLAN Security Switch 2380

WLAN-kytkintä kutsutaan usein myös WLAN-kontrolleriksi. WLAN-kytkimellä hallitaan ja tehdään asetuksia langattomaan lähiverkkojärjestelmään kuuluville tukiasemille. Tämä mahdollistaan kaikkien toimintojen, kuten salauksen purun, siirtämisen WLAN-kytkimelle. Kun kytkin hallitsee kaikkea langattoman verkon toimintaa, ylläpito, muutokset, päivittäminen ja valvonta voidaan tehdä keskitetysti yhdestä pisteestä. [22.]

Langattoman lähiverkon hallintaan valittiin WSS (WLAN Security Switch) 2380, koska se on järein kytkin 2300-tuoteperheessä ja se on suunniteltu suuryritysten käyttöön tietokeskusten yhteydessä. Kytkimeen voidaan liittää 40 tukiasemaa ja se voidaan lisensoida aina 120 tukiasemaan asti, kun taas WSS 2360 -mallin kytkimeen voidaan liittää korkeintaan 12 tukiasemaa ja WSS 2350 -malliin vain kolme tukiasemaa. Kun verkko toteutettiin yhdellä WSS 2380 -kytkimellä, verkon rakenne pysyi yksinkertaisempana, koska se muodostui tukiasemista ja yhdestä hallintakytkimestä. Muilla vaihtoehdoilla olisi pitänyt käyttää useampaa kytkintä, joiden sijoittaminen eri toimipisteisiin ei olisi ollut mahdollista, koska kytkimelle pitää tuoda langattomasti levitettävät virtuaaliverkot. Tämä ei ollut mahdollista muualla kuin pääkonttorissa. [23.]

WLAN Access Point 2330A

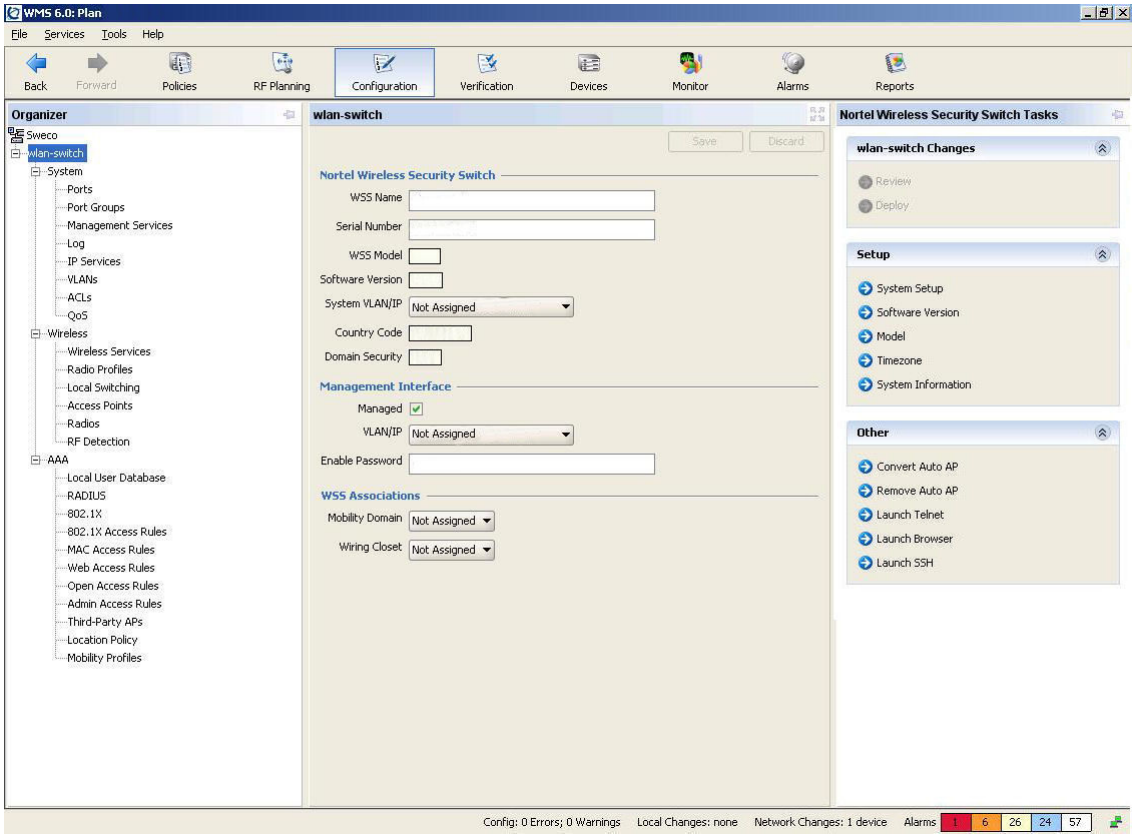
WLAN 2330A -tukiasema on monimuotomalli, jossa on kaksi radiota, yksi 802.11a:lle ja toinen 802.11b/g:lle. Vaihtoehtona olisi ollut tukiasema 2330, jossa olisi ollut vain 802.11b/g-radio. 2330A valittiin käytettäväksi kahden radion takia, koska se mahdollistaa paremman langattoman lähiverkon suunnittelun ja verkon nimelliseksi bittinopeudeksi saadaan 2 x 54 Mbps. Näitä tukiasemia hallitaan WLAN-kytkimellä. Tukiasemia voidaan lisätä suurikin määrä luomatta ylläpitäjille ylimääräistä kuormaa. Tukiasemat ovat helposti asennettavissa toimistoon, ja ne muistuttavat tavallisia palohälyttimiä (kuva 6). Tukiasemat voidaan kytkeä joko suoraan WLAN-kytkimeen tai Layer2- tai Layer3-verkkoyhteydellä. Tukiasemien virransyöttö tapahtuu 803.3af Power over Ethernet -tekniikalla, joten niille ei tarvitse järjestää erillistä sähkönsyöttöä. [23.]

Kuva 6. Nortel WLAN Access Point 2330A.

WLAN Management System

WLAN-järjestelmään hallintaan valittiin WMS-ohjelmisto (WLAN Management System), koska sen avulla voidaan viedä koko WLAN-käyttöönottoprojekti läpi. Käyttöönottoprojekti sisältää koko suunnitteluvaiheen, radioiden sijoittelun, asetusten määrittämisen, vianselvityksen ja valvonnan. WMS-hallintaohjelmaan voidaan tuoda myös CAD-, JPEG- ja GIF-kuvia. Kuvien avulla voidaan sijoitella radioita ja arvioida rakenteista aiheutuvia vaimennuksia radiosignaaleihin. Vaihtoehtona olisi ollut käyttää WLAN-kytkimen komentokehotehallintaa, mutta siitä olisi puuttunut mahdollisuus verkkosuunnitteluun ja verkon toiminnan valvonta olisi ollut huomattavasti hankalampaa. Kuvassa 7 näkyy WMS hallintaohjelmiston muodostama näkymä järjestelmän tilasta. [23.]

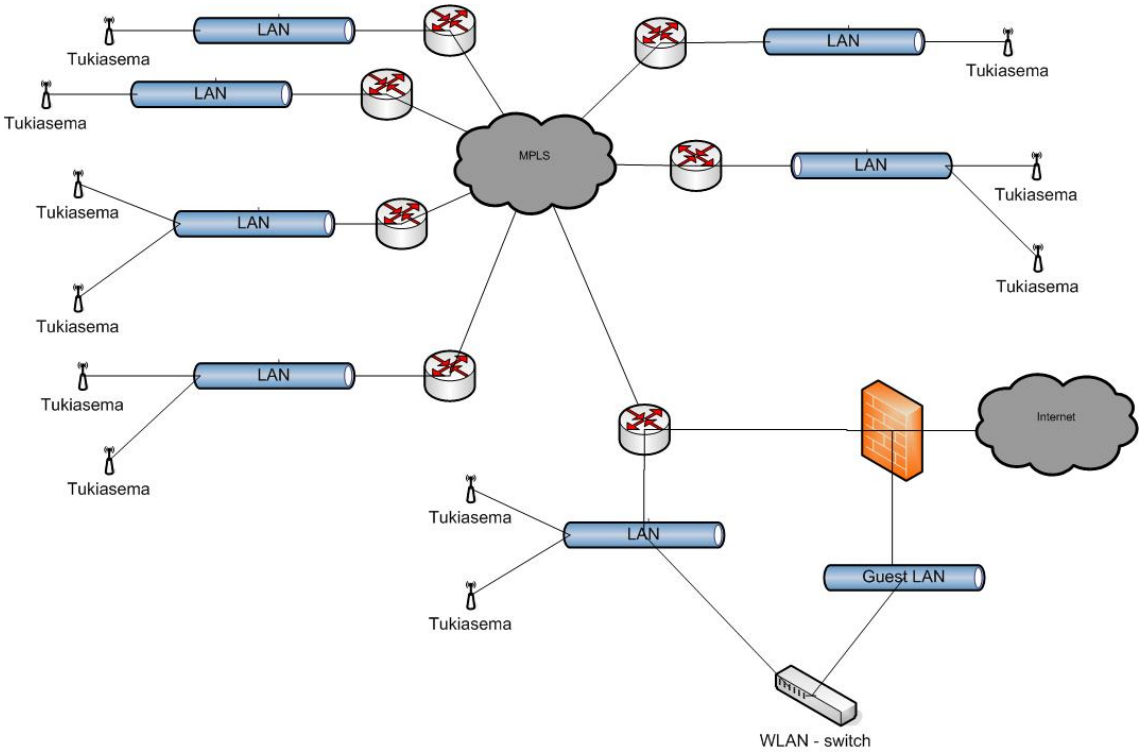
Hallintaohjelmistolla luodaan verkkopalveluita, jotka sisältävät verkon asetukset ja julkaisemisen. Jokainen langaton verkkopalvelu sisältää todentamistavan (802.1x, www-kirjautuminen, MAC osoite tunnistus tai avoin pääsy) ja mahdollisen liikenteen salausmenetelmän (802.11i:n, WPA:n, WEP:n tai suojaamattoman verkon). WMS-ohjelmisto vaati toimiakseen Windows Server 2003:n, Windows XP:n, Windows 2000:n tai Linuxin. [24.]



Kuva 7. WMS-hallintaohjelmiston järjestelmän asetukset.

5.2 Nortel WLAN -asennus

Nortel Security Switch kytkettiin kuvan 8 osoittamalla tavalla: toinen verkkoliitäntä yrityksen sisäverkkoon ja toinen käytössä olevaan vierasverkkoon. Tämä malli valittiin, koska WLAN-kytkimen piti kyetä käsittelemään virtuaaliverkkoja. Tukiasemat kytkettiin sisäverkkoon, ja ne hakevat IP-osoitteen DHCP-palvelimelta (Dynamic Host Configuration Protocol). Tukiasemat kytkeytyvät kakkos- ja kolmoskerroksen verkkoyhteyden kautta WLAN-kytkimeen.



Kuva 8. Looginen verkkokuva WLAN-järjestelmästä.

Langattoman verkon hallintaa ja suunnittelua varten pystytettiin Windows 2003 -palvelin, johon asennettiin WLAN Management Software. Tätä sovellusta käytettiin tukiasemien sijoittelun suunnittelussa kattamaan eri toimipisteiden WLAN-verkkotarpeen.

5.3 Langattoman verkon asetukset

Radiosuunnittelu

Radiosuunnittelulla varmistettiin langattoman verkon toiminta. Suunnitelmasta nähdään miten tukiasemat kannattaa sijoittaa ja miten radiokanavia voi käyttää. Langattoman verkon toteuttaminen aloitettiin WMS-ohjelmiston RF Planning -osiolla, johon luotiin verkkosuunnitelma (Nework Plan). Suunnitelmaan määritettiin verkon nimi, maakoodi ja käytettävät radiokanavat. 802.1b/g-verkon kanaviksi valittiin 1, 3, 9 ja 13, koska haluttiin käyttää neljää kanavaa. Tämä mahdollisti sen, että verkko mukautui mahdollisimman hyvin yrityksen tarpeisiin. Vierekkäisten tukiasemien käyttämien

kanavien tulee olla mahdollisimman kaukana toisistaan, jotta tukiasemat eivät häiritsisi toisiaan. Taulukossa 2 on esitetty käytettävät radiotaajuudet ja kanavat.

Taulukko 2. Vapaasti käytettävät 2,4 GHz taajuusalueen kanavat [12.]

Numero		**Keskitaajuus MHz**
EU	**USA**	
1	1	2 412
2	2	2 417
3	3	2 422
4	4	2 427
5	5	2 432
6	6	2 437
7	7	2 442
8	8	2 447
9	9	2 452
10	10	2 457
11	11	2 462
12		2 467
13		2 472

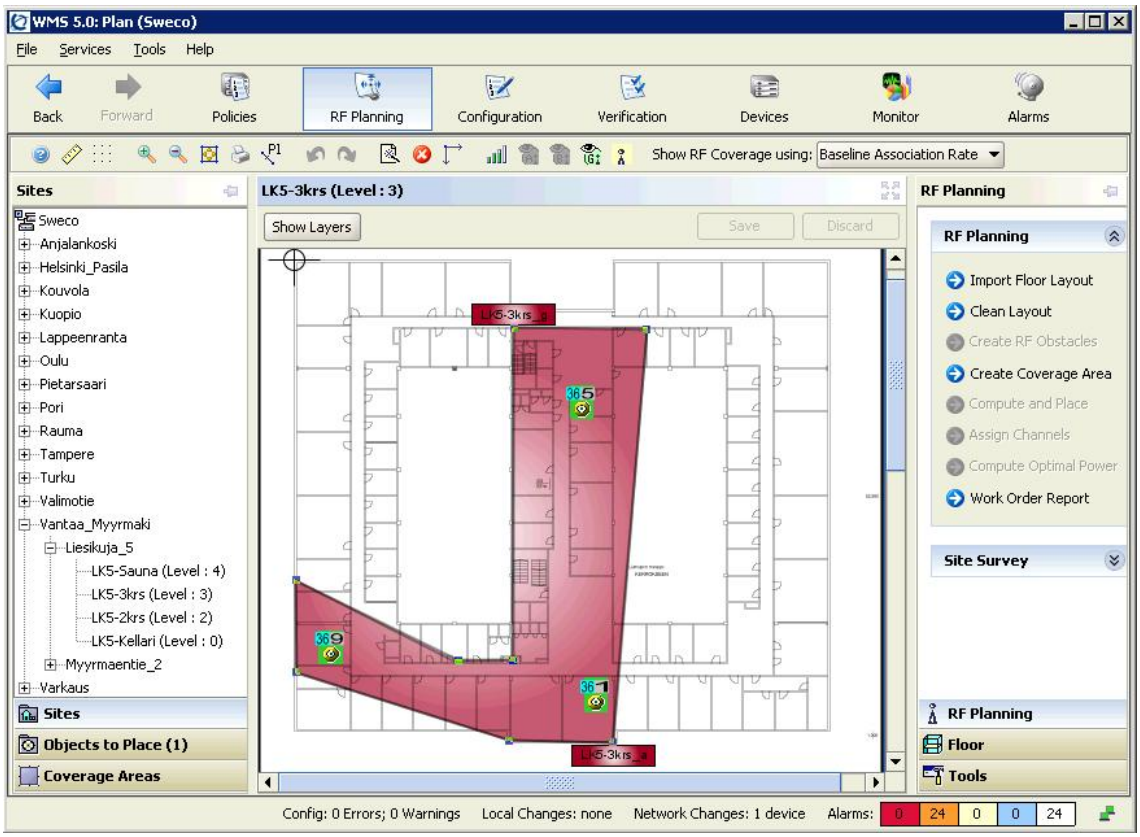
WLAN Management Softwaren RF Planning -osioon luotiin ensin paikkakunnat (kaupunki tai kunta jossa toimisto sijaitsee), jotta paikkakunnille voitiin luoda rakennus. Rakennukseen määriteltiin siinä olevat kerrokset. Tämän jälkeen liitettiin yrityksen käytössä oleviin kerroksiin niiden pohjapiirustukset, mikäli ne olivat käytettävissä. Näin päästiin määrittämään kerrokseen WLAN-peittoalue 802.1a- ja 802.1b/g-standardeille sekä sijoittamaan haluttu määrä tukiasemia kattamaan haluttu peittoalue. RF Planning ohjelma osaa laskea jossain määrin rakenteiden aiheuttamia vaimennuksia. Taulukossa 3 on esitelty joitain yleisiä AutoCAD-kerrosten nimiä.

Taulukko 3. Yleisiä AutoCAD kerrosten nimiä [24.]

AutoCAD Layer	**Name Commonly Represents...**
glaz	windows
scol	steel columns
p-fixt	bathroom
p-part	bathroom stall partitions
ext	exterior
int	interior

Kuvassa 9 on esitetty Sweco Industryn pääkonttorin kolmanteen kerrokseen tarvittava peittoalue. Peittoalueeseen liitettiin haluttu määrä tukiasemia. Tässä tapauksessa niitä tarvittiin kolme kappaletta tarjoamaan haluttu palvelutaso käyttökohteissa. Kuvassa

olevista tukiasemista kaksi sijoitettiin neuvotteluhuoneisiin, joista oli helppo saada verkkoyhteys ja jotka tarjosivat huomaamatoman sijainnin ja hyvän peittoalueen haluttuun tilaan. Kolmas tukiasema sijoitettiin ristikytkentätilaan, koska sen läheisyydessä olevat neuvotteluhuoneet haluttiin langattoman lähiverkon piiriin ja tukiasema oli erittäin helppo sijoittaa ristikytkentätilaan.



Kuva 9. RF Planning -kuva pääkonttorin kolmannesta kerroksesta.

Verkkoa suunniteltaessa törmättiin mittayksikköongelmaan, vaikka WMS-ohjelmisto tukee metrijärjestelmän mittayksiköitä. Tämä aiheutti mielenkiintoisia tilanteita. Yhdessä tapauksessa suunnitteluosio näytti, että yksi tukiasema pystyisi tarjoamaan täyden 54 Mbps:n bittinopeuden lähes 100 x 100 metriä olevaan tilaan.

Suunnitteluohjelman kykyä laskea rakenteiden vaimennuksia järjestelmään tuoduista AutoCad piirustuksista ei pystytty hyödyntämään, koska olemassa olevat piirustukset olivat hyvin monimutkaiset ja sisälsivät paljon tähän käyttötarkoitukseen sopimatonta tietoa. Vaikka tämmöinen ongelma havaittiin, ohjelmasta oli kuitenkin suurta hyötyä

verkon suunnittelussa. Rakennusten ja kerrosten pohjapiirustukset saatiin tuotua järjestelmään ja suunnitelma toimi oleellisena osana langattoman verkon dokumentaatiota, mikä auttoi ylläpitoa.

Asetusten määrittäminen

Langattomaan verkkoon määritettiin ensin kaksi eri palveluprofiilia, koska vierailijat haluttiin yrityksen tietoturvapolitiikan mukaan erottaa yrityksen omista koneista. Ensimmäinen oli vierailijoille tarkoitettu ja toinen työntekijöille tarkoitettu palvelu.

Palveluprofiilien luonnin jälkeen järjestelmään tehtiin kolme radioprofiilia: yksi oli tarkoitettu pelkästään vieraille, toinen pelkästään työntekijöille ja kolmannen profiilin kautta oli mahdollista päästä kumpaankin. Näin pystyttiin valitsemaan tukiaseman ja RF Planning -osiossa tehtyjen WLAN-peittoalueiden perusteella, mistä oli mahdollista kytkeytyä mihinkin verkkoon. Käytetyissä 2330A mallin WLAN-tukiasemissa oli kaksi erillistä radiota (802.11a ja 802.11b/g), joten yhteen tukiasemaan voitiin määrittää käyttöön kaksi eri radioprofiilia.

Vieraita varten määritettiin vierasverkkopalvelu, joka sisältää www-kirjautumisen. Näin saatiin rajoitettua verkkoon pääsyä, ja verkon käyttäjien valvonta helpottui. Vierasverkkopalvelun kautta pääsi yrityksessä käytössä olevaan vierasverkkoon. Vierasverkon SSID (Service Set Identifier) -jakelu jätettiin toimimaan, jotta vierailijoiden oli helpompi kytkeytyä verkkoon. Verkon sai käyttöön yhdistämällä tietokoneen SWECO-Guest SSID:llä olevaan langattomaan verkkoon. Tietokone sai verkosta IP-osoitteen, jonka jälkeen tietokoneesta lähtevä liikenne ohjattiin kirjautumissivulle. Kirjautuminen tapahtui vierailijalle luodun käyttäjätunnus-salasanaparin avulla, ja se oli suojattu SSL-salauksella (Secure Sockets Layer). Tätä varten WLAN-kytkimelle hankittiin julkinen SSL-varmenne, johon vierailijoiden tietokoneet luottivat.

Langattomaan verkkoon luotiin palvelu myös yrityksen työntekijöille. Tämän verkkopalvelun suojaamiseen kiinnitettiin erityistä huomiota, koska verkon käyttöönoton jälkeen yrityksen sisäverkkoon voisi päästä myös yrityksen ulkopuolelta.

Radioiden signaalit kuuluvat rakennusten rakenteiden läpi, vaikka niiden sijanteihin ja lähetystehoihin kiinnitettiin juuri tämän takia huomiota. Verkkoon pääsyä varten pystytettiin RADIUS-palvelu, jonka alustana toimi Windows 2003 -palvelin ja tähän lisättiin IAS-palvelu (Internet Authentication Service). Tuotantoverkosta otettiin SSID:n mainostus pois päältä, vaikkei se olekaan mikään varsinaista tietoturvaa lisäävä tekijä. Useimmat Windows-koneet eivät kuitenkaan osaa näyttää ilman eritystoimenpiteitä tällaisen verkon SSID-tunnusta.

5.4 Langattoman lähiverkon pilotointi

Ennen pilotointia verkon toimivuutta ja käytettävyyttä testattiin pääkonttorissa kannettavilla tietokoneilla ja kännyköillä, joissa oli WLAN-ominaisuus. Näin varmistuttiin, että verkkoon kytkeytyminen ja todennus toimivat sekä liikennöinti haluttuihin palveluihin onnistuu. Tämän perusteella voitiin todeta, että verkko toimi odotetulla tavalla ja verkon pilotointi voitiin aloittaa.

Pilotointiin valittiin noin kymmenen hengen testiryhmä. Ryhmä koostui pääasiassa ICT-organisaation työntekijöistä useilla eri paikkakunnilla. Mukana oli myös pari yrityksen ulkopuolista käyttäjää, jotka työskentelivät yrityksen tiloissa käyttäen omiaan koneitaan, joita ei saanut kytkeä yrityksen tieturvapolitiikan mukaan sisäverkkoon. Tämä ratkaistiin tarjoamalla heille pääsy WLAN-järjestelmän kautta vierasverkkoon.

Pilotoinnissa havaittiin, että joissain tilanteissa, kun käytössä oleva päätelaite tukee 802.11a/b/g-standardeja, kone kytkeytyy 802.11a-verkkoon, vaikka kyseinen verkko ei olisi signaalin voimakkuudeltaan paras. Muuten verkko toimi täysin odotetulla tavalla. Vierasverkkoa käyttäneet ulkoiset henkilöt antoivat parhaan tuloksen verkon luotettavasta käytettävyydestä, vaikka heillä olikin kiinteä työpiste eivätkä näin ollen käyttäneet verkkoa eri paikoista. Heiltä saadun palautteen perusteella saatiin yhteyden aikakatkaisuun liittyvät parametrit säädettyä vastaamaan haluttuja arvoja. Tämän jälkeen voitiin asentaa loputkin tukiasemat niihin toimistoihin, joissa ei työskennellyt paikallista IT-tukihenkilöä. Asennuksen jälkeen julkaistiin verkon käyttöönotosta kertova tiedote.

5.5 Käyttöönotto

Onnistuneen pilotin jälkeen pystyttiin langaton verkko ottamaan täysipainoisesti käyttöön tuotannossa. Loppuihin toimistoihin toimitettiin tukiasemat huoltokäyntien yhteydessä. Langattoman verkon käyttöönotossa pääpaino asetettiin vierasverkon toiminnan varmistamiseksi, koska vieraille haluttiin tarjota positiivinen käyttökokemus verkon toiminnasta ja näin ollen myös yrityksen toiminnasta. Vierasverkkoon otettiin käyttöön vain 802.11b/g-standardin mukaiset radiot, koska sisäverkolle haluttiin enemmän kapasiteettia ja pilotissa oli havaittu, että jotkin päätelaitteet kytkeytyvät 802.11a-verkkoon, vaikkei se olisi laadultaan paras. Vierasverkon käyttöönotosta julkaistiin liitteen 1 mukainen tiedote. Yrityksen langattomaan sisäverkkoon otettiin käyttäjiä heidän tarpeittensa mukaan.

6 Ylläpito

Käyttö

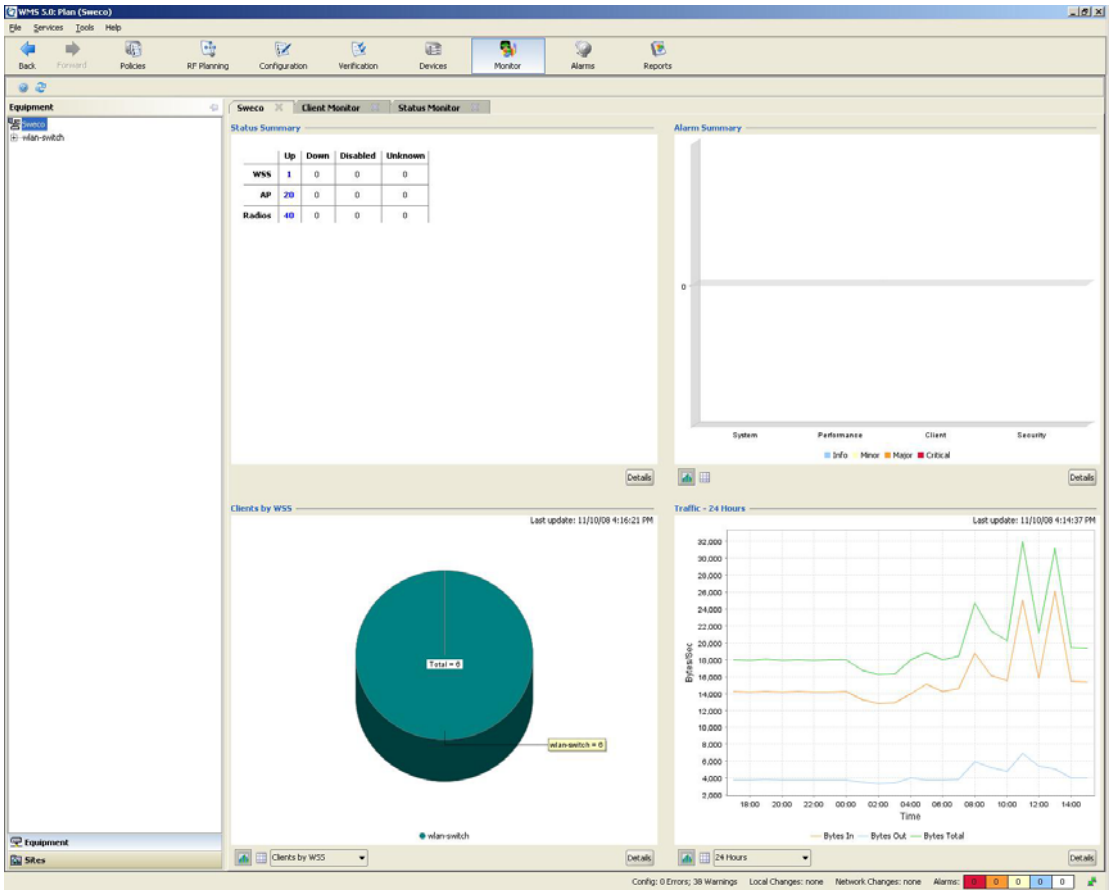
Vieraille luotiin tunnukset WLAN-verkon käyttöä varten Nortel Guest Pass -sovelluksella. Ihanteellisin vaihtoehto tunnusten luomiseen olisi yrityksen vastaanotossa, mutta tämä ei ollut mahdollista, koska läheskään kaikissa toimistoissa ei ole vastaanottovirkailijaa. Todettiin myös, että tunnusten luominen pääkonttorin vastaanotossa kuormittaisi liikaa siellä työskenteleviä henkilöitä. Tunnusten luomisessa päädyttiin ratkaisuun, jossa vieraan isäntä pyytää helpdeskistä tunnukset vierailleen viimeistään päivää ennen käyttötarvetta. Nortel Guest Pass -sovelluksen asentamisesta ja käytöstä on laadittu seikkaperäiset käyttäjän ohjeet, jotka ovat yrityksen ICT-organisaation hallussa.

Yrityksen sisäverkon käyttö on toteutettu 802.1x:n pohjalta, ja se edellyttää käyttäjän ja käytettävän tietokoneen kuulumista käytön mahdollistaviin aktiivihakemiston suojausryhmiin. Suojausryhmien hallinnointi on yrityksen ICT-organisaation vastuulla. ICT määrittelee myös tarvittavat asetukset kannettavan tietokoneen WLAN-profiiliin. Tätä varten laadittiin ohjeet verkkoasetusten luomiseksi, niin Intelin WLAN-

hallintaohjelmistolle, kuin Windows XP:n omalle langattomien verkkojen hallintaohjelmistolle.

Monitorointi

WMS-ohjelmisto valvoo langattoman verkon tilaa ja ohjelmisto kokoaa selkeään käyttöliittymään yhteenvedon verkon tilasta kuvan 10 tapaan sekä vastaanottaa laitteilta SNMP (Simple Network Management Protocol) -raportteja.



Kuva 10. WMS hallintaohjelmiston raportointi osio.

WMS-ohjelmisto määritettiin lähettämään kaikista Major- ja Critical- tason tapahtumista sähköpostia verkon ylläpidolle. Näin ylläpito saa välittömästi tiedon verkossa olevista ongelmista ja pystyy reagoimaan niihin mahdollisimman nopeasti.

Vikatilanteet

Mahdollisen vikatilanteen ilmetessä tulee selvittää tarkkaan, mitä langattoman verkon osa-aluetta se koskee. Onko kyseessä vain yksittäisen käyttäjän verkkoon liittymistä koskeva ongelma, jonkin tukiaseman toimintahäiriö vai laajemmin verkkoa koskeva häiriö. Vian selvitystä varten myös langattoman verkon laitteita valvotaan verkonvalvontaohjelmistolla. Näin saadaan ilmoitus, mikäli jokin tukiasema tai peräti WLAN-kytkin lakkaa toimimista ja voidaan ryhtyä tarvittaviin toimenpiteisiin vian ratkaisemi-seksi.

Kehitys- ja laajennusmahdollisuudet

Järjestelmän toiminnallisuuden turvaamisen kannalta olisi erittäin suotavaa kahdentaa WLAN-kytkin. Järjestelmää on mahdollista laajentaa usealla eri tavalla, esimerkiksi luomalla oma WLAN-palvelu VoIP-laitteille ja mobiilikäyttäjille. Luomalla oman WLAN SSID:n VoIP-käyttöä varten liikenteen priorisointi helpottuu valmiiden QoS-profiilien avulla. Järjestelmään voidaan tämänhetkisellä lisenssillä liittää 40 WLAN-tukiasemaa ja mikä laajennettavissa aina 120 tukiasemaan pelkästään lisenssi-päivityksillä.

7 Yhteenveto

Työn tarkoituksena oli suunnitella ja toteuttaa langaton lähiverkko tarjoamaan langaton verkko yrityksen vierailijoille sekä tarjoamaan yrityksen tietoturvapolitiikan vaatimukset täyttävä langaton verkkoyhteys yrityksen työntekijöille. Nämä tavoitteet toteutuivat odotusten mukaisesti ja työn ansiosta yrityksellä on käytössä toimiva langaton lähiverkko ratkaisu.

Työn kirjallisessa osassa käsiteltiin langattomia lähiverkkoja teknologioiden ja tietoturvan osalta pyrkien tuomaan selkeästi esille niiden erot.

Työn käytännön osuus sujui mukavasti. Vaikkei pohjapiirustuksia pystytty tuomaan täysin yhteensopivassa muodossa suunnitteluohjelmaan, verkon suunnittelu ja toteutus sujui hyvin koulussa opittujen tietojen pohjalta. Selkeän aikataulun puuttuminen työn aloitusvaiheessa aiheutti työn venymistä melko pitkäksi, mutta työ saatiin päätettyä kunnialla.

Tulevaisuudessa langatonta lähiverkkoa voidaan laajentaa helposti lisäämällä tukiasemia, koska WLAN-kytkin tukee nykyisellä lisenssillä niitä 40 kpl:seen asti.

Lähteet

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

2 Bing, Benny. Wireless Local Area Networks. New York, Wiley-Interscience, 2002.

3 Granlund, Kaj. Langaton tiedonsiirto: langattoman tiedonsiirron peruskirja. Jyväskylä, Docendo, 2001.

4 Puska, Matti. Langattomat lähiverkot. Jyväskylä, Gummerus Kirjapaino Oy, 2005

5 IEEE 802.11 Official Timelines. (WWW-dokumentti.) the Institute of Electrical and Electronics Engineers, Inc. (IEEE). http://www.ieee802.org/11/Reports/802.11_Timelines.htm. Luettu 18.2.2010.

6 Hämäläinen, Perttu. Wlan on nyt virallisesti nopea. Tietokone nro 9/2009, s.25.

7 Ganz, Aura. Multimedia wireless networks Technologies, Standards, and QoS. New Jersey, Prentice Hall PTR, 2004.

8 IEEE standardises fast Wi-Fi roaming - Techworld.com. (WWW-dokumentti.) Techworld. http://news.techworld.com/mobile-wireless/103501/ieee-standardises-fast-wi-fi-roaming. Luettu 18.2.2010.

9 MeshWLAN.com - Information about WLAN MESH Wireless Networks. (WWW-dokumentti.) MeshWLAN http://www.meshwlan.com. Luettu 18.2.2010.

10 Anurag Kumar, D. Manjunath, Joy Kuri. Wireless networking. Amsterdam, Morgan Kaufmann/Elsevier, cop, 2008

11 Paavilainen, Juhani. Tietoturva. Jyväskylä, Gummerus Kirjapaino Oy, 1998.

12 Hakala, Mika. Tietoverkon rakentaminen. Jyväskylä, Docendo, 2005.

13 The Cable Guy - March 2003. (WWW-dokumentti.) Microsoft. http://technet.microsoft.com/en-us/library/bb877996.aspx. Luettu 20.2.2010.

14 Windows XP:n WPA (Wi-Fi Protected Access) -tietoturvapäivityksen yleiskatsaus. (WWW-dokumentti.) Microsoft. http://support.microsoft.com/kb/815485/fi. Luettu 20.2.2010.

15 The Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2 is available. (WWW-dokumentti.) Microsoft. http://support.microsoft.com/kb/893357. Luettu 20.2.2010.

16 The Cable Guy - May 2005. (WWW-dokumentti.) Microsoft. http://technet.microsoft.com/en-us/library/bb878054.aspx. Luettu 20.2.2010.

17 Authentication and Authorization: The Big Picture with IEEE 802.1X. (WWW-dokumentti.) Information Security Reading Room. http://www.sans.org/reading_room/whitepapers/authentication/authentication_and_authorization_the_big_picture_with_ieee_802_1x_123?show=123.php&cat=authentication. Luettu 22.2.2010.

18 EAP Methods for 802.11 Wireless LAN Security. (WWW-dokumentti.) International Engineering Consortium. http://www.iec.org/online/tutorials/eap_methods/index.asp. Luettu 15.11.2009.

19 The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network Access. (WWW-dokumentti.) Microsoft. http://download.microsoft.com/download/4/4/7/447404a7-c373-4bf4-9c77-daee54b1f6fc/PEAP.doc. Luettu 22.2.2010.

20 EAP Overview (WWW-dokumentti.) Openloop Technologies. http://www.openloop.com/education/classes/sjsu_engr/engr_networksecurity/preso/eap/EAP_Overview.ppt. Luettu 22.2.2010.

21 Sweco Industry Oy:n intranet-sivusto. (WWW-dokumentti.) Luettu 9.1.2009,

22 Sridhar, T. Wireless LAN Switches - Functions and Deployment. (WWW-dokumentti.) http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/wireless_lan_switches.html. Luettu 25.4.2010.

23 Solutions Brief Nortel WLAN 2300. (WWW-documentti.) Nortell Networks. http://products.nortel.com/go/product_assoc.jsp?segId=0&parId=0&prod_id=52544&locale=en-US&rend_id=FB. Luettu 11.7.2008.

24 Nortel WLAN Mangement Software 2300 Series User Guide. Santa Clara, Great America Parkway, 2007.

Liite 1: Tiedote Langattoman vierasverkon käyttöönotosta

ADuf

Langaton vierasverkko

Olemme ottaneet käyttöön langattoman verkkoratkaisun jonka avulla voimme tarjota vieraille langattoman verkkoyhteyden. Verkon peittoalue on tällä hetkellä neuvotteluhuoneet Vantaalla, Kuopiossa, Oulussa, Lappeenrannassa, Pietarsaaressa, Anjalankoskella, Varkaudessa ja Tampereella.

Langattoman verkon käyttöä varten vierailija tarvitsee tunnukset, jotka isännän tulee tilata Helpdeskistä viimeistään päivää ennen tunnusten käyttötarvetta. Tunnukset lähetetään sähköpostilla isännälle. Tunnus on henkilökohtainen ja voimassa yhden päivän.

Lisätietoja:
Antti Dufva
antti.dufva@sweco.fi

SWECO Industry **Oy**
Liesikuja 5
P.O. Box 31
FI-01601 Vantaa, Finland
Telephone +358 9 530 91
Fax +358 9 530 9323

SWECO Industry Oy
VAT FI03509419
Domicile Vantaa
Bank SEB 330100-01116672
Email firstname.lastname@sweco.fi
www.sweco.fi