STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

KONSERNINLAAJUISEN WLAN-VERKON SUUNNITTELU

Työn tekijä: Iiro Mäkinen
Työn valvoja: Jukka Louhelainen
Työn ohjaaja: Markku Kuronen

Työ hyväksytty: __. __. 2006

Jukka Louhelainen
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin Ahlstrom Oyj:n Helsingin yksikölle. Haluan kiittää projektissa auttamassa olleita, koko Ahlstrom Oyj:n mainiota Corporate IT tiimiä, sekä erityisesti IT Network Specialist Ville Laaksosta ja IT Development Manager Markku Kurosta.

Helsingissä 9.9.2006

Iiro Mäkinen

STADIA
HELSINGIN AMMATTIKORKEAKOULU

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Iiro Mäkinen	
Työn nimi: Konserninlaajuisen WLAN-verkon suunnittelu	
Päivämäärä: 9.9.2006	Sivumäärä: 53 s. + 2 liitettä
Koulutusohjelma: Tietotekniikka	Suuntautumisvaihtoehto: Tietoliikennetekniikka
Työn valvoja: lehtori Jukka Louhelainen Työn ohjaaja: IT Development Manager Markku Kuronen	

Tässä insinöörityössä tutustuttiin WLAN-verkkoihin, sekä varsinkin niiden integroimiseen osaksi yrityksen tietoverkkoa. Työ tehtiin Ahlstrom Oyj:n tilauksesta.

WLAN-verkot mahdollistavat käyttäjälleen paremman liikkuvuuden mm. kannettavaa tietokonetta käytettäessä eivätkä sido käyttäjää kiinteän yhteyspisteen viereen. Tästä on yrityskäytössä hyötyä mm. kokouksissa ja neuvotteluissa. Myös vierailijoille tästä on hyötyä, mikäli yritys pystyy tarjoamaan heille palvelun päästä verkkoon.

LWAPP on tekniikka, joka mahdollistaa suurien langattomien verkkojen hallinnoimisen ja valvomisen yhdestä paikasta tai laitteesta käsin. Tästä on hyötyä, mikäli tukiasemien lukumäärä on suuri ja verkko laaja.

Tutkimus aloitettiin selvittämällä WLAN-verkkojen historiaa sekä esittelemällä eri standardit. Tämän jälkeen tutustuttiin radiotiellä tapahtuviin siirtotekniikoihin ja eri modulaatiomenetelmiin. Myös WLAN-verkon siirtotietä sekä erilaisia WLAN-verkoissa käytettäviä antenneja tarkasteltiin työssä. WLAN-verkkojen tietoturvallisuus, kuten uhat ja salausmenetelmät olivat keskeisessä asemassa työtä tehtäessä.

Tulevaan CAPWAP-protokollaan luotiin katsaus työssä. Vahvin ehdokas protokollaksi on Ciscon kehittämä LWAPP, mutta myös sen kilpailijoita tarkasteltiin lyhyesti.

Työn lopuksi suunniteltiin Ahlstrom Oyj:lle konserninlaajuinen WLAN-standardi, jota tullaan käyttämään yrityksen konttoreissa ympäri maailman. Systeemi mahdollistaa sekä yrityksen työntekijöille vahvalla salauksella muodostetun langattoman yhteyden luomisen inter- ja intraverkkoihin, että yrityksen vierailijoille internet-yhteyden. Tämä on toteutettu käyttämällä useita SSID:tä joille on luotu erilaiset toimintaperiaatteet.

Avainsanat: WLAN, langaton lähiverkko, Wi-Fi, LWAPP, CAPWAP

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name: Iiro Mäkinen

Title: Designing of a Corporate-Wide WLAN solution

Date: September 9 2006 Number of pages: 53 + 2 appendix

Department: Information Technology

Study Programme: Telecommunications

Instructor: Jukka Louhelainen, Lecturer

Supervisor: Markku Kuronen, IT Development Manager

The purpose of this graduate study was to evaluate the use of WLAN networks and especially the integration of them as a part of a corporate network. The study was assigned by Ahlstrom Corporation.

Wireless networks enable better mobility for their users for example when using laptops, as they do not bind the user to a fixed network access point. For corporations, this is particularly beneficial in meetings and negotiations. Also corporate visitors can benefit from this as they can connect their laptop in the WLAN facility provided by the corporation.

The aim of this study was to examine the history of wireless networks and present different WLAN standards. Another objective was to study transmission techniques which occur in radio waves and different modulation techniques. Also different types of radio antennas, which are used with WLANs have been presented in this study. Security in wireless networks, such as hazards and encryption methods, has been discussed extensively.

The new forthcoming IETF draft protocol, CAPWAP, was evaluated in this study. The strongest and most likely candidate is LWAPP developed by Cisco, but also its competitors were studied.

Based on the findings of this study, a corporate-wide WLAN solution was designed for Ahlstrom Corporation, which will be used at the corporate offices throughout the globe. The system empowers the employees with Internet and intranet access with strong encryption and corporate visitors with Internet access. This was accomplished by using multiple SSIDs with each having different policies.

Keywords: WLAN, wireless local-area network, Wi-Fi, LWAPP, CAPWAP

SISÄLLYS

LYHENNELUETTELO

ACK	Acknowledgement code; tiedonsiirrossa käytettävä merkinantokoodi
AES	Advanced Encryption Standard; tehokas salausalgoritmi
AP	Access Point; tukiasema
ARP	Address Resolution Protocol, MAC-osoitteen löytämiseen käytetty protokolla
BBS	Basic Service Set; yhden tukiaseman infrastruktuurinen verkko
BPSK	Binary Phase Shift Keying; tiedonsiirrossa käytettävä modulaatio-tekniikka
CCK	Complement Code Keying; tiedonsiirrossa käytettävä koodaus-tekniikka
CFP	Contention Free Period; aika joka käytetään keskitettyyn hallintaan
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; MAC-osakerroksen protokolla langattomassa tiedonsiirrossa
CSMA/CD	Carrier Sense Multiple Access with Collision Detection; MAC-osakerroksen protokolla kiinteässä verkossa
CTS	Clear to Send; langattoman tiedonsiirron merkinantoa
dBi	Antennivahvistus desibeleinä
DCF	Distributed Coordination Function; langattoman tiedonsiirron toimintatapa
DECT	Digital Enhanced Cordless Telecommunications; langaton digitaalinen puhelinjärjestelmä
DES	Data Encryption Standard; salausalgoritmi
DHCP	Dynamic Host Configuration Protocol; protokolla joka jakaa IP-osoitteita verkoissa
DIFS	Interframe Space; aikaviive
DNS	Domain Name System; muuttaa verkkotunnukset IP-osoitteiksi
DoS	Denial of Service; palvelunestohyökkäys, verkkopalveluihin kohdistuva hyökkäys
DSSS	Direct Sequence spread spectrum; suorasekvenssihajaspektri
DTE	Data Terminal Equipment; päätelaite
EIFS	Extended InterFrame Space; pisin WLAN-laitteiden käyttämä viive
EIRP	Effective Isotropic Radiated Power; isotrooppinen lähetysteho

ETSI	European Telecommunications Standards Institute; eurooppalainen telealan standardisoimisjärjestö
ESS	Extended Service Set; useammasta BBS:stä muodostuva verkko
EWC	Enhanced Wireless Consortium; Intelin vetämä konsortio joka suunnittelee WLAN-tekniikoita
FHSS	Frequency-hopping Spread Spectrum; taajuushyppelyhajaspektri
HIPERLAN	High Performance Radio Local Area Network; ETSIn määrittelemä langaton lähiverkko -standardi
HR/DSSS	High Rate Direct Spread Spectrum; nopea suorasekvenssihajaspektri
HTTP	Hypertext Transfer Protocol; selaimen tiedonsiirtoprotokolla
IAPP	Inter Access Point Protocol; tukiasemien välillä toimiva protokolla
IEEE	the Institute of Electrical and Electronics Engineers; kansainvälinen sähköinsinööriliitto
IETF	Internet Engineering Task Force; internet protokollien standardointijärjestö
IPS	Intrusion Prevention System; palomuuriratkaisu
ISM	Industrial, Scientific and Medical; vapaa taajuuskaista teollisuuden, tieteen ja lääketieteen käyttöön
ISO	International Organization for Standardization; kansainvälinen standardisoimisjärjestö
LWAPP	Light Weight Access Point Protocol; hallittavien tukiasemien ja kontrollereiden välillä käytettävä protokolla
MAC	Medium Access Control layer; OSI:n tiedonsiirtokerroksen osakerros
MAC	Medium Access Control address; verkon päätelaitteen osoite
NAV	Network Allocation Vector; Ajastintekniikassa käytettävä ajastin
OFDM	Orthogonal Frequency Division Multiplexing; ortogonaalinen taajusjakomultipleksointi
PCF,	Point Coordination Function; langattoman tiedonsiirron toiminatapa
PIFS	Point Coordination InterFrame Space; tukiasemien käyttämä viive
PoE	Power over Ethernet; ethernet-kaapeloinnin kautta toteutettu virransyöttö
POP3	Post Office Protocol 3; sähköpostin hakemiseen tarkoitettu protokolla
QAM	Quadrature Amplitude Modulation; amplitudimodulaatio-tekniikka
QoS	Quality of Service; palvelun laatu

QPSK	Quadrature Phase Shift Keying; tiedonsiirrossa käytettävä modulaatiotekniikka
RC4	Rivest Cipher 4; salausalgoritmi jota käytetään WEP:ssä
REAP	Remote Edge Access Point; Verkon reunalla sijaitseva tukiasema
RF	Radio Frequency; radiotie
RSSI	Received Signal Strength Indicator; vastaanotetun signaalin voimakkuus
RTS	Request to send; langattoman tiedonsiirron merkinantoa
RRM	Radio Resource Management; radiotiellä käytettyhallintaprotokolla
SARP	Secure Address Resolution Protocol; suojattu ARP-protokolla
SIFS	Short Interframe Space; odotusaika langattomassa tiedonsiirrossa
SSDI	Service Set Identifier; langattoman verkon tunnus, nimi
SSH	Secure Shell; tiedonsiirtojärjestelmä
TDMA	Time Division Multiple Access; aikajakokanavointi tekniikka
TKIP	Temporal Key Integrity Protocol; langattoman lähiverkon salaustekniikka, tehokkaampi kuin WEP
VLAN	Virtual Local Area Network; virtuaalinen lähiverkko
VoIP	Voice Over Internet Protocol; IP-verkon yli oleva puheliikenne
WEP	Wired Equivalent Privacy; langattoman lähiverkon salaustekniikka
Wi-Fi	Wireless Fidelity; langattomien verkkolaitteiden valmistajien liittouma
WLAN	Wireless Local Area Network; langaton lähiverkko
WPA	Wi-Fi Protected Access; langattoman lähiverkon salaustekniikka
WPA2	Wi-Fi Protected Access 2; toinen nimitys standardille IEEE 802.11i

1 JOHDANTO

Langattoman lähiverkon yleistyttyä ovat myös yritykset siirtymässä pikkuhiljaa käyttämään tätä ratkaisua. Houkutus siirtyä käyttämään langattomia ratkaisuja on suuri, vaikka tiedonsiirtonopeudet eivät pärjääkään perinteiselle kiinteälle verkolle. Esimerkiksi kokoustiloissa tai kotona pääsy verkkoon tai internetiin kannettavalla tietokoneella helpottuu huomattavasti, kun infrastruktuuri ei ole enää esteenä liikkuvuudelle, vaan yhteys voidaan muodostaa langattomasti.

WLAN- tai Wi-Fi-verkkojen suurimpana ongelmana on ollut tietoturvallisuus. Verkkojen siirtotienä käytetään radiokerrosta, joka on fyysisesti avoin kaikille. Tämän takia siirtyminen langattomien verkkojen käyttöön yritystasolla onkin ollut kyseenalaista. Pääsyä internetiin on kyllä tarjottu, mutta pääsyä yrityksen sisäverkkoon on kuitenkin pyritty rajoittamaan WLAN-ratkaisuilla.

IEEE 802.11 - suosituksen ensimmäinen standardi saatiin hyväksytettyä vuonna 1997, ja sitä on seurannut monta laajennusta. Ensimmäisen standardin tarjoama tiedonsiirtonopeus 1 -2 Mbit/s on moninkertaistunut vuosien saatossa ja vuoden 2006 tammikuussa IEEE (the Institute of Electrical and Electronics Engineers) hyväksyi uuden IEEE 802.11n -luonnoksen, joka lupaa tiedonsiirtonopeudeksi huimat 600 Mbit/s. Toinen asia, mihin uusissa standardeissa keskitytään, on tietoturvan parantaminen.

Tässä työssä keskitytään WLAN-verkon rakentamiseen yrityksen konttoreihin ympäri maailmaa, käyttäen Airespacen kehittämää LWAP (Light Weight Access Point) -protokollaa, joka mahdollistaa WLAN-verkon keskitetyn hallinnan. Tämä tehtiin Ahlstrom Oyj:lle tilauksesta. Lisäksi tutustutaan lähemmin langattoman verkon toimintaan ja standardiin, sekä laitteistoon joka vaaditaan langattoman verkon ylläpitämiseen.

2 WLAN-STANDARDIT

Kun langattomia lähiverkkoja lähdettiin aluksi kehittelemään, oli olemassa monia eri suljettuja protokollia ja eri verkkoja eri käyttötarkoituksiin, mutta 1990-luvun lopussa niille kehitettiin standardit IEEE:n ja ETSI:n toimesta. Suurin näistä oli IEEE 802.11, johon on tullut suurimpina laajennuksina IEEE 802.11a, IEEE 802.11b ja IEEE 802.11g. ETSI:n standardina on julkaistu HIPERLAN ja HIPERLAN II. /1, s. 230./

2.1 IEEE 802.11

IEEE802.11:n ensimmäinen versio hyväksyttiin vuonna 1997 ja paranneltu versio vuonna 1999. Suositus määrittelee kaksi erityyppistä topologiaa: vertaisverkko eli Ad-Hoc ja tukiasemaan eli access pointiin perustuva asiakas/palvelin-tyyppinen verkko. Standardi tukee nopeuksia 2 Mbit/s saakka, ja se toimii 2,4 ja 5 GHz:n ISM (Industrial Scientific Medical) alueilla radiotaajuudella. Standardi on myös määritelty infrapuna-alueelle välillä 850 – 950 nm.

IEEE802.11 käyttää hyväkseen radiotaajuudella sekä suorasekvenssihajaspektriä, DSSS (Direct Sequence Spread Spectrum), että taajuushyppelyä, FHSS (Frequency Hopping Spread Spectrum). (Effective Isotopic Radiates Power). /1, s. 230 - 235./

2.2 IEEE 802.11a

IEEE 802.11a:n kehitystyö käynnistyi vuoden 1997 aikana ja se valmistui vuoden 1999 aikana. Laajennuksesta käytetään nimitystä OFDM PHY (Orthogonal Frequency Division Multiplexing), ja se sallii jopa 54 Mbps:n siirtonopeuden 5 GHz:n taajuusalueella. IEEE 802.11a:n vaatima kaistanleveys on 16,6 MHz ja niitä on kahdeksan kappaletta välillä 5,1 – 5,8 GHz. /1, s. 238./

2.3 IEEE 802.11b

Toinen laajennus IEEE 802.11 -tekniikkaan on IEEE 802.11b, joka tukee nopeuksia 11 Mbps:ään saakka 2,4 GHz:n ISM-alueella. Tarkemmin välillä 2,4- 2,485 GHz. Suosituksesta käytetään myös nimitystä HR/DSSS (High Rate/ Direct Sequence Spread Spectrum). Suositus määrittelee tavan, jolla huonoissa olosuhteissa voidaan datasiirtonopeutta pudottaa 1 tai 2 Mbps:ään. Näin järjestelmä voi tukea myös vanhemman IEEE 802.11:n mukaisia nopeuksia. Linjalla siirtyvä sanoma on kentiltään identtinen DSSS-peruskehyksen kanssa. /1, s. 240./

2.4 IEEE 802.11g

IEEE 802.11g on laajennus IEEE 802.11 -standardiin ja se tukee nopeuksia 54 Mbps:ään saakka. Standardi toimii myös 2,4 GHz:n ISM-alueella ja käyttää samaa modulaatiotapaa kuin IEEE 802.11b. Näin ollen se on yhteensopiva b-standardin kanssa. G-standardi käyttää samaa tekniikkaa kuin a-standardi, eli OFDM:ia. /14./

2.5 IEEE 802.11n -luonnos

Vuonna 2003 perustettu IEEE:n 802.11n -työryhmä valmistelee uutta standardia. Syynä tähän uuteen standardiin on nopeuskehityksen ohella WLAN-verkkojen laajentuminen mm. langattomiin VoIP-toteutuksiin sekä kulutuselektroniikkatuotteiden välisiin yhteyksiin. Palvelunlaatu on keskeisenä kehityksen kohteena standardissa. /4, s. 127./

Tuore IEEE 802.11n -ehdotus lupaa nopeuden nousevan jopa 600 Mbps:ään ja siinä on tuki neljälle antennille. Sen MAC-osaa halutaan vielä kehittää niin että käyttäjälle voitaisiin taata aina vähintään 100 Mbps:n nopeudet. Se tukee yhteyksiä sekä 2,4 että viiden gigahertsin taajuuksilla. Standardi tulee tukemaan usean yhtäaikaisen kanavan hyödyntämistä. Luonnos tukee sekä 20 että 40 MHz:n kanavia. Standardin ensimmäinen luonnos hyväksyttiin EWC-määrityksen pohjalta tammikuussa 2006 ja sen odotetaan saavan lopullisen muodon vuonna 2007. /19./

2.6 Muita IEEE 802.11 –standardeja

Edellä mainittujen standardien lisäksi IEEE on julkaissut seuraavat standardit.

- 802.11e, sisältää palvelunlaatuun (QoS) ja suorituskykyyn liittyviä parannuksia
- 802.11f, määrittelee WLAN-liityntäpisteiden välisen liikennöinnin. Se käyttää hyväkseen tähän IAPP protokollaa (Inter Access-Point Protocol)
- 802.11h, määrittelee lisämääritykset 5 GHz:n taajuuden käytölle Euroopassa
- 802.11i, sisältää tietoturvaan liittyviä parannuksia, käytetään myös nimeä WPA2
- 802.11j, sisältää Japania koskevia laajennuksia /4, s. 47/
- 802.11s, tarkoituksena WLAN-tukiasemien muodostaminen suureksi silmukkaverkoksi, käytettäneen kaupunkiverkkojen suunnittelussa.

2.7 HIPERLAN

HIPERLAN (High Performance Radio LAN) on ETSI:n (European telecommunications Standards Institute) määrittelemä standardi. HIPERLAN-standardiperhe käsittää neljä eri versiota.

HIPERLAN/1:n suunnittelu alkoi vuonna 1991 ja standardi hyväksyttiin vuonna 1996. Sen suurin mahdollinen tiedonsiirtonopeus on 23,5 Mbit/s ja se käyttää 5 GHz:n taajuutta. Se käyttää tiedonsiirtoon viittä kanavaa välillä 5,15 - 5,35 GHz

HIPERLAN/2-standardi hyväksyttiin helmikuussa 2000. Standardi käyttää 5 GHz:n taajuutta ja tiedonsiirtonopeus on 54 Mbit/s. 2-versiossa on keskitytty myös tietoturvan parantamiseen. Tiedon kryptaamiseen käytetään DES- ja 3DES-algoritmeja. /13./

2.8 HomeRF

HomeRF-standardi on kehitelty DECT (Digital Enhanced Cordless Telephone) -standardin pohjalta. Standardin tavoitteena on ollut puheen- ja datansiirto, mutta IEEE802.11 standardi on selvästi suositumpi. HomeRF käyttää CSMA/CD-tekniikkaa (Code Division Multiplex Access/ Collision Detection) datapakettien siirtoon ja TDMA-tekniikkaa (Time Division Multiple Access) äänen ja kuvan siirtoon. HomeRF mahdollistaa datansiirtonopeudet 2,4 GHz:n taajuudella 1,6 Mbps:ään saakka. HomeRF:n seuraaja HomeRF2 mahdollistaa siirtonopeuden 10 Mbps:ään saakka. Molemmat HomeRF-tekniikat käyttävät FHSS-tekniikkaa fyysisellä tasolla. /2, s. 34 - 35./ (Kuva 1.)

Standardi	Max. nopeus	Todellinen nopeus	Kantama (noin)	Käytetty taajuusalue	Liityntä ilmatiehen	QoS
IEEE 802.11	2 Mbps	2 Mbps	~200 m	2.4 GHz	FHSS	-
IEEE 802.11a	54 Mbps	31 Mbps	80 m	5 GHz	OFDM	-
IEEE 802.11b	11 Mbps	6 Mbps	~200 m	2.4 GHz	DSSS	-
IEEE 802.11g	54 Mbps	~20 Mbps	~200 m	2.4 GHz	OFDM/ DSSS	-
HomeRF2	10 Mbps	6 Mbps	50 m	2.4 GHz	FHSS	ON
ETSI HiperLAN/2	54 Mbps	54 Mbps	80 m	5 GHz	OFDM	ON

Kuva 1. Standardien vertailua /3/

2.9 Wi-Fi-määritys

Wi-Fi (Wireless Fidelity) on Wi-Fi Alliancen perustama tavaramerkki. WI-Fi käsittää langattomat verkkotuotteet jotka perustuvat IEEE 802.11 -standardiin. Se on perustettu siksi että se on käyttäjäystävällisempi nimitys standardille. Alun perin Wi-Fi-nimen piti käsittää vain IEEE 802.11b -standardi, mutta sitä on laajennettu myöhemmin käsittämään myös IEEE 802.11a ja -g standardit.

3 WLAN-RADIOTAAJUUDELLA TOIMIVAT SIIRTOTEKNIIKAT

Yleensä kun puhutaan radiotaajuisesta siirtotekniikasta, niin sekoitetaan keskenään modulaatio- ja siirtotekniikat. Näiden ero on se että hajaspektri-tekniikka jakaa informaation monilla eri kanavilla ja modulaatiotekniikka moduloi informaation jokaisen kanavan yli. IEEE 802.11 -standardi sisältää lisäksi mahdollisuuden käyttää infrapuna-aluetta tiedonsiirtoon, mutta se on epäkäytännöllistä siitä syystä että näköyhteyden on säilyttävä.

Siirtotekniikoita ovat:

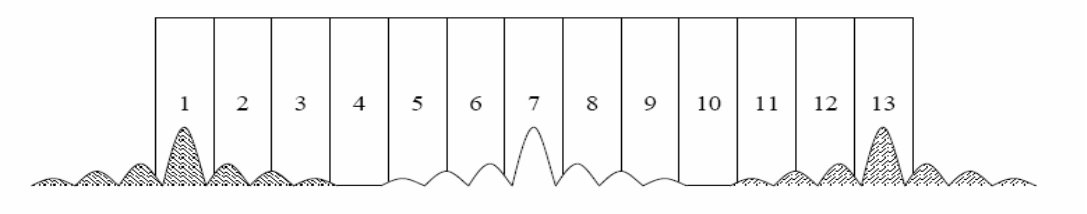
- DSSS (Direct Sequence Spread Spectrum eli suorasekvenssihajaspektri)
- FHSS (Frequency Hopping Spread Spectrum eli taajuushyppelyhajaspektri)
- CDMA (Code Division Multiplex Access eli koodijakokanavointi)
- OFDM (Orthogonal Frequency Division Multiplexing eli kantoaaltomodulointi)
- COFDM (Coded Orthogonal Frequency Division Multiplexing)

/2, s. 50./

3.1 DSSS ja FHSS

802.11-standardit käyttävät hajaspektritekniikoita. On siis olemassa kaksi erilaista hajaspektritekniikkaa, joita 802.11- ja 802.11b-standardit käyttävät, DSSS ja FHSS. Näiden suurin ero käytännössä on se että DSSS on suorituskyvyltään parempi ja FHSS on vastustuskykyisempi häiriöille. /2, s. 50/

FHSS ja DSSS tukevat molemmat nopeuksia 1 ja 2 Mbps. Tämän lisäksi DSSS tukee nopeuksia aina 11 Mbps:ään saakka. 802.11 DSSS standardi käyttää 11 eri kanavaa USA:ssa, 13 kanavaa Euroopassa ja 14 Japanissa. Tässä tulee tämän tekniikan epäkohta esiin. Näistä kanavista ainoastaan kolmea pystytään käyttämään yhtä aikaa johtuen siitä että kanavat ovat toistensa kanssa hieman päällekkäin. (Kuva 2.)



Kuva 2. Siirtonopeuden ollessa maksimissa, vain kolmea kanavaa voidaan käyttää

Hajaspektritekniikkaa käytettäessä verkon kapasiteetti jakautuu automaattisesti käyttäjien kesken ja erillisiä synkronointimenetelmiä ei tarvita. DSSS käyttää 22 MHz:n taajuuskaistoja.

Taajuushyppelyhajaspektritekniikka, FHSS, hyödyntää siis taajuushyppelyä, eli käyttää lähetyksessään yhtä taajuutta kerrallaan ja hyppii edestakaisin kaikkien taajuuksien välillä. FSHH käyttää 79 kanavaa Euroopassa. Se sietää hyvin häiriöitä, koska yhdellä kanavalla ei viivytä pitkään kerrallaan.

FHSS vaatii MAC (Medium Access Control) -kerrokselta enemmän kuin DSSS, koska sen täytyy tehdä kerroksella mm. kanavanvaihtojen tahdistus ja hyppyjen koordinointi. /6./

3.2 OFDM

OFDM-tekniikassa käytetään monia eri signaaleja, joille digitaalinen data jaetaan koko käytössä olevalle spektrin alueelle. Nämä signaalit sitten lähetetään samaan aikaan rinnakkain eri kantoaalloilla. Jokaisella kantoaallolla lähetettävä bitti on taajuudeltaan kapea, mikä tarkoittaa sitä että se on ajallisesti pidempi. OFDM:n hyvä puoli on se, että se mahdollistaa suuret nopeudet, joita käytetään mm. 802.11a- ja -g-standardeissa, hyödyntämällä koko taajuuskaistan spektri tehokkaasti. Tämän lisäksi se sietää hyvin impulssimuotoisia häiriötekijöitä, sekä monitie-etenemisestä aiheutuvia häiriöitä. Tekniikan heikkouksina mainittakoon, että se on erittäin herkkä taajuusvaihtelulle ja vaatii tarkan synkronoinnin. Lisäksi OFDM:n lähetysteho on pidettävä matalana, mutta lähetyspiikit ovat korkeita. /6./

4 WLAN-VERKON SIIRTOTIE

Kun vertaillaan langatonta verkkoa kiinteään verkkoon, niin nopeasti katsottuna näiden välillä ei esiinny suurempia eroja. Kun tarkastellaan lähemmin asiaa, niin päädytään siihen tulokseen, että langattoman verkon siirtonopeus on yleensä pienempi ja verkon käyttämä media, rf-taajuudet, on fyysisesti avoin kaikille. Jos mahdollisella salakuuntelijalla on tarvetta kuunnella verkkoa, niin hän ei tarvitse muuta kuin sopivan vastaanottimen, mm. WLAN-verkkosovittimen, kuunnellakseen liikennettä. Kiinteän verkon puolella tämä on huomattavasti vaikeampaa, koska tämä vaatisi fyysistä yhteyttä kuunneltavaan verkkoon. Langattomuudessa on kuitenkin muitakin ongelmia, joihin perehdytään seuraavassa. /1, s. 241./

4.1 Hidden station -ongelma

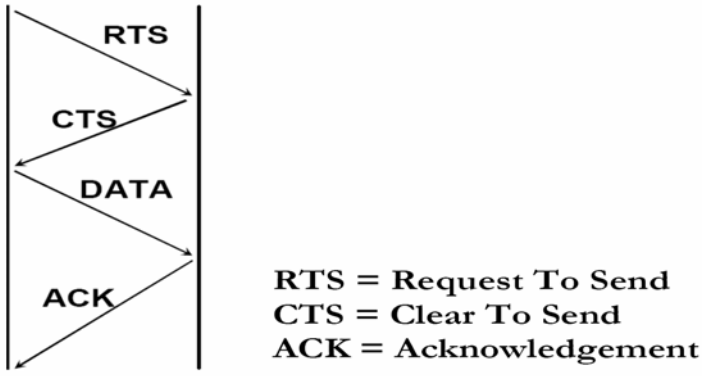
Langattomissa verkoissa voi infrastruktuurista johtuen syntyä tilanne, jossa pääteasemat ovat piilossa toisiltaan. Tätä ongelmaa kutsutaan nimellä ”Hidden station” tai ”hidden node”. Tämmöinen tilanne syntyy esimerkiksi yrityksessä, jossa on kolmessa kerroksessa toimistoja. Langaton tukiasema on sijoitettu toiseen kerrokseen, jotta peittoalue saataisiin kuulumaan kokonaisuudessaan yrityksen tiloihin. Kuitenkaan ensimmäisessä ja kolmannessa kerroksessa olevat työasemat eivät pysty havaitsemaan toisiaan, vaan ainoastaan tukiaseman toisessa kerroksessa, sillä niiden kantama ei riitä tähän. Näin ollen esimerkiksi ensimmäisessä kerroksessa oleva tietokone varustettuna WLAN-kortilla ei pysty havaitsemaan, mikäli kolmannessa kerroksessa oleva työasema on lähettämässä.

Tätä ongelmaa varten on kehitetty erilaisia tekniikoita joita käsitellään seuraavassa kappaleessa. /1, s. 242./

4.2 Kanavanvaraus WLAN-verkossa

Kanavanvaraus voidaan tehdä IEEE 802.11 -verkossa, joko keskitetysti PCF (Point Coordination Function) -menetelmää käyttäen, tai sitten hajautetusti käyttäen DCF (Distributed Coordination Function) -menetelmää. Nämä molemmat menetelmät voivat olla käytössä samanaikaisesti. Kaikkien IEEE 802.11 -standardin mukaisten laitteiden edellytetään hallitsevan molemmat tekniikat.

Kuittaukset tai niiden puuttuminen on ainoa keino valvoa törmäyksiä langattomassa verkossa. Jotta kuittaus olisi mahdollista kohdistaa oikein verkoissa joissa hallinta on hajautettu, niin tiedonsiirto muodostuu tapahtumista. Tapahtumaan sisältyy vähintään sanoman lähetys sekä siihen liittyvä kuittaus. Tätä kutsutaan kaksivaiheiseksi tapahtumaksi. Nelivaiheinen tapahtuma muodostuu datan ja kuittauksen lisäksi näitä ennen siirrettävän kanavanvaraussanoman RTS (Request To Send) ja varauksen kuittauksen CTS (Clear to Send). Kaksivaiheinen sanoma voidaan suorittaa välittömästi ilman kanavanvarausta, ja tätä käytetäänkin pienissä verkoissa, missä törmäyksien mahdollisuus on pieni. Kuormitetussa verkossa käytetään mieluummin nelivaiheisia sanomia, mikä pienentää törmäysriskiä. Verkossa toimivat laitteet sisältävät laskurin, joka määrittelee suurimman sellaisen sanoman, joka voidaan lähettää kaksivaiheisena tapahtumana. /1, s. 242 - 246./ (Kuva 3.)



Kuva 3. Nelinkertainen kättely /3/

4.3 Ajastintekniikka WLAN-verkoissa

Jokaisessa radiotiellä siirtyvässä sanomassa on kenttä, jolla ilmoitetaan menossa olevan tapahtuman kesto. NAV-ajastin (Network Allocation Vector) viritetään siirtämällä tämä tieto ajastimeen. Silloin kun NAV-ajastin on viritetty, laite ei saa lähettää sanomia. Vasta ajastimen lauettua tai kun linja on ollut vapaana tietyn ajan, lähetys on sallittua.

Tämä järjestelmä käyttää myös viiveitä, jotka ovat välttämättömiä, koska niiden avulla voidaan säädellä toimintaa verkossa. Viive estää laitetta aina lähettämästä ja kun protokollan eri osissa käytetään erilaisia viiveitä, saadaan verkko toimimaan halutulla tavalla. /1, s. 243./ Tässä käytetyn aikavälin pituus on FSHH:lla 50 µs ja DSSS:lla 20 µs /6/.

Viiveet:

- SIFS (Short InterFrame Space) on lyhyin viive. Sen kesto on FHSS 28 µs ja DSSS 10 µs. SIFS-viivettä käytetään saman tapahtumien sisällä siten, että kuittausten lähetettyihin sanomiin oletetaan saapuvan tämän ajan sisällä. Esim. Datan ja ACK-sanoman välillä.
- PIFS (Point Coordination InterFrame Space) on viive, jota tukiasemat käyttävät. Viiveen pituus on SIFS + yksi aikaväli µs, joka mahdollistaa sen että tukiasema voi ottaa siirtotien haltuunsa ennen verkossa olevia muita laitteita.
- DIFS (Distributed InterFrame Space) on viive, jota verkossa olevan päätelaitteen tulee odottaa ennen kuin se on oikeutettu lähettämään sanomaa siirtotielle. Sen pituus on SIFS + 2 aikaväliä.
- EIFS (Extended InterFrame Space) on viive, jota asema käyttää, mikäli se ei kykene tulkitsemaan verkosta tullutta sanomaa. Tämän avulla työasemaa estetään lähettämästä keskellä menossa olevaa tapahtumaa. EIFS on viiveistä pisin ja sen kesto on useita aikavälejä riippuen sanoman maksimipituudesta. /1, s. 243 - 244./

4.4 Törmäykset langattomassa verkossa

Törmäyksien havaitseminen langattomissa verkoissa on mahdollista. Kiinteässä verkossa (ethernet) siirtotietä kuunnellaan samalla, kun dataa lähetetään ja törmäys huomataan mikäli vastaanotettu data ei täsmää lähetetyn datan kanssa. Radiotietä käyttävässä langattomassa verkossa tällainen ratkaisu olisi kuitenkin erittäin kallis ja sen takia siihen ei ole päädytty.

Datan törmäys tuhoaa aina siirtotiellä olevat sanomat, joten voidaan lähteä siitä olettamuksesta, että perille mennyt sanoma ei ole törmännyt toiseen sanomaan. Pitää kuitenkin muistaa se seikka että virheellisesti perille mennyt sanoma ei ole välttämättä törmännyt, vaan virhe on voinut johtua muista syistä. IEEE 802.11 -standardissa on kuitenkin määritelty, että mikäli virheellinen sanoma vastaanotetaan, se tulkitaan törmäykseksi. Tämä on erittäin merkittävä seikka verrattuna kiinteään verkkoon, sillä kuittauksen tarpeellisuus tarkoittaa samalla sitä, että kaikki data mitä siirretään, niin päätyy myös vastaanottajalle, koska häneltä edellytetään kuittausta. Ero kiinteän verkon ratkaisuun verrattuna on merkittävä.

Törmäyksiä sattuu CSMA/CA-protokollassa, vaikka niitä pyritään välttämään. Törmäyksestä toipumisen edellytyksenä on, että molemmat osapuolet toimivat eri tavalla. Jos molemmat osapuolet yrittäisivät uusia sanomaa samalla menetelmällä, se johtaisi vain uudelleen törmäykseen. Tämän takia hyväksi käytetään ethernet-verkoista tuttua eksponentiaalista toipumista (exponential backoff). Tämä tekniikka perustuu siihen, että uudelleenlähetyksen ajankohta n valitaan satunnaisesti kahden luvun 0 ja i-1 väliltä. Laite voi jälleen lähettää sanoman kun n aikaväliä on kulunut. Eksponentiaalisuus saadaan siitä, että mikäli molemmat asemat törmäävät toistamiseen, niin yläraja i kaksinkertaistetaan edellisestä arvostaan. Alussa i = 1 ja ensimmäisen törmäyksen jälkeen valittavana on yksi aikaväleistä 0 ja 1. Seuraavan törmäyksen jälkeen valittavana on yksi aikaväleistä 0 - 3. Näin jatketaan, kunnes sanomat saadaan onnistuneesti lähetettyä tai törmäysten maksimimäärä ylittyy. IEEE 802.11 -standardin mukaan näin toimitaan, mikäli siirtotiellä on muuta liikennettä silloin, kun asema on lähettämässä sanomaa törmäysten jälkeen tai onnistuneen siirron jälkeen. Menettelyä ei käytetä, mikäli NAV on lauennut ja siirtotie ollut vapaana DIFS-viiveen ajan. /1, s. 241./

4.5 WLAN-verkon siirtotien hajautettu hallinta

CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) on tekniikka, millä sanomia lähetetään IEEE 802.11 -verkoissa. Tekniikka muistuttaa ethernet-verkoissa käytettyä CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) -tekniikkaa.

CSMA/CD-tekniikkaa ei voida kuitenkaan käyttää langattomissa verkoissa, sillä kuten aiemmin mainittiin, niin ei ole kustannuksellisista syistä järkevää valmistaa laitteita, jotka pystyvät kuuntelemaan ilmatietä samaan aikaan lähetyksen kanssa. Tästä syystä on kehitetty CSMA/CA-tekniikka.

Kanavanvaraus toimii seuraavasti nelivaiheisessa tapahtumassa:

Ensiksi laite haluaa lähettää sanoman ja kuulostelee, onko siirtotie vapaana ja pysyy myös vapaana DIFS-viiveen ajan. Mikäli muuta liikennettä ilmenee, laite siirtyy eksponentiaaliseen toipumismenettelyyn. Mikäli lähetys onnistuu, niin vapaalle siirtotielle lähetetään RTS-sanoma, johon odotetaan CTS-kuittausta SIFS-viiveen aikana. Mikäli kuittausta ei vastaanoteta, seurauksena on oletettu törmäys ja siirrytään eksponentiaaliseen toipumismenettelyyn. Mikäli kuittaus saapuu, niin laite on valmis lähettämään linjalle datasanomansa ja odottaa kuittausta SIFS-viiveen ajan. Jos kuittausta ei kuulu, niin sanoman oletetaan törmänneen ja se tulee lähettää uudelleen. Mikäli kuittaus saapuu, niin laite siirtyy eksponentiaaliseen toipumismenettelyyn. /1, s. 245./

4.6 WLAN-verkon siirtotien keskitetty hallinta

Keskitetystä hallinnasta käytetään nimitystä PCF (Point Coordination Function). Laitteiden osallistuminen tähän on tehty vapaaehtoiseksi ja ne voivat halutessaan käyttää edelleen DCF-menetelmää. Keskitettyä hallintaa kontrolloi tukiasema, josta käytetään tässä yhteydessä myös nimitystä PC (Point Coordinator). Syy siihen, miksi keskitettyä hallintaa halutaan käyttää, on se että tarvitaan vakaampaa datasiirtoa esimerkiksi kuvan- tai äänensiirtoon.

Keskitetyssä hallinnassa PC hoitaa kohtalaisen tasaisen datasiirron sitä tarvitseville työasemille. Tämä onnistuu sillä tavalla, että PC ottaa siirtotien haltuunsa käyttämällä suurempaa prioriteettiansa (PIFS). Tällöin se lähettää siirtotielle ns. Beacon-sanomassa tiedon keskitetyn hallinnan alkamisesta ja sen pituudesta. Tämän jälkeen verkon laitteet päivittävät tiedon NAV-ajastimiinsa.

Tämän jälkeen PC ryhtyy lähettämään kiertokyselyä keskitetyn hallinnan piirissä oleville laitteille. Koska tästä syntyvien kyselyjen ja niitä seuraavien toimenpiteiden välinen aika ei saa olla suurempi kuin SIFS-viive, eivät muut asemat pääse keskeyttämään toimenpidettä. Tässä varmistetaan se, ettei kukaan pääse ottamaan siirtotietä haltuun hajautetun hallinnan avulla. Kun kaikki kiertokyselyn kohteena olevat laitteet on käyty läpi, niin tukiasema vapauttaa liikenteen hajautetulle hallinnalle.

Aikaa, joka käytetään keskitettyyn hallintaan, sanotaan CFP:ksi (Contention Free Period). Kun kyselykierros päättyy, niin tukiasema lähettää CF-End-sanoman verkkoon ilmoittamaan, että siirtotie on vapaa. Yhden kyselykierroksen aikana voi siirtyä vain yksi datasanoma per asema. /1, s. 246./

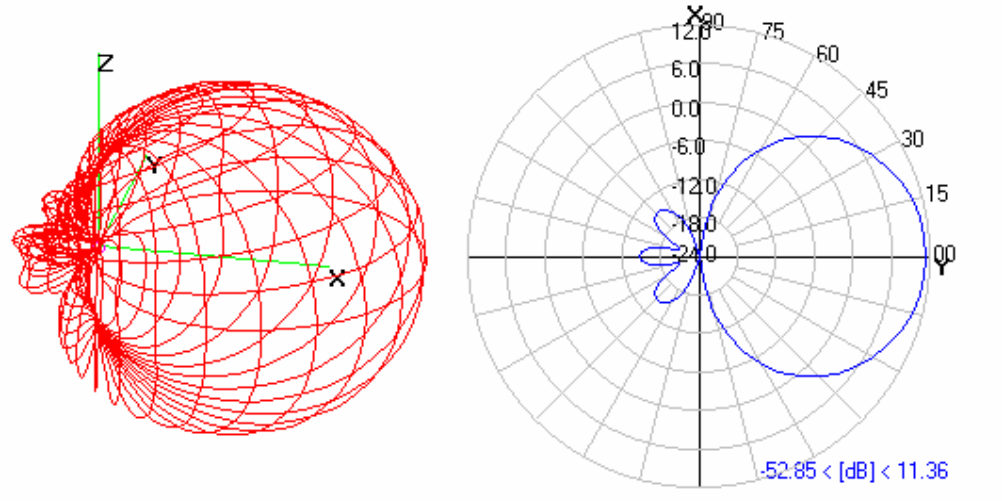
5 WLAN-ANTENNIT

WLAN-tuotteissa käytettävien antennien toimintaperiaate on se, että ne muuttavat sähköenergiaa sähkömagneettiseksi säteilyksi. Samaa antennia käytetään siis lähetykseen ja vastaanottoon, eli se muuttaa myös vastaanotettua säteilyä sähköiseksi signaaliksi. Käytännössä kaikkien antennien suuntakuvio on epäsymmetrinen, eli lähetetty teho yhteen suuntaan on suurempi kuin toiseen. Korkein vahvistus pyritään yleensä suuntaamaan alueelle, jossa on paljon käyttäjiä. Mikäli halutaan mahdollisimman suurta peittoa, niin valitaan ns. ympärisäteilevä antenni. Tällaisen antennin pystysuuntainen kuvio on kapea ja epäsymmetrinen. Lähetystehoa ei yleensä haluta tuhlata yläpuolelle, mutta alapuolelle muodostuva katvealue voi olla joissakin tapauksissa haitallinen. /4, s. 60./

Antennityypit WLAN-verkoissa

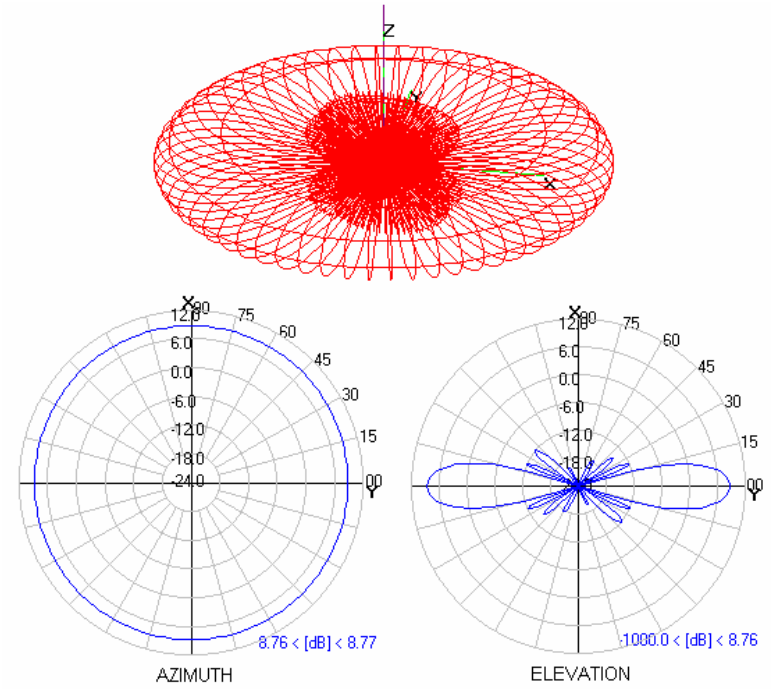
Yleisimmin käytössä olevia antenneja ovat suunta-antenni, Dipoli-antenni, ympärisäteilevä antenni, sektoriantenni ja lautasantenni. Nykyisin ovat yleistyneet myös verkkokorttien sisäiset antennit varsinkin kannettavissa tietokoneissa.

Suunta-antennit (Kuva 4.) on tarkoitettu esimerkiksi linkiksi kahden paikalla olevan tukiaseman väliin.

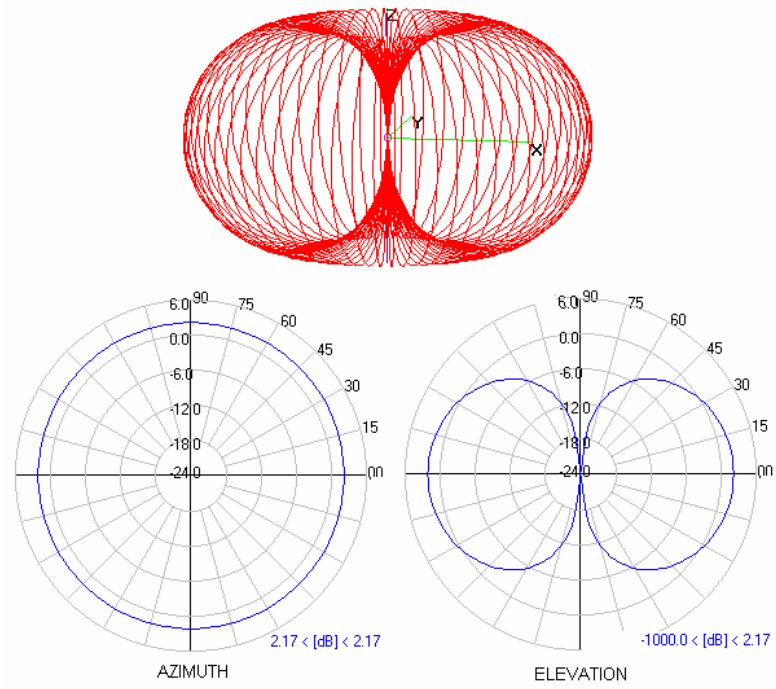


Kuva 4. Suunta-antennin säteilykuviot 3-ulotteisena ja x/y-akseleilla /23/

Ympärisäteilevät antennit (Kuva 5.) ovat ehkä yleisempiä antenneja toimisto/kotikäytössä. Ne säteilevät radioaallot tasaisesti joka puolelle antennia tasaisesti. dipoli-antennit (Kuva 6.) eroavat ympärisäteilevistä antenneista siinä, että niiden z/x -akselille muodostuva kuvio on erilainen kuin ympärisäteilevillä antenneilla. Se muodostaa nimensä mukaisesti dipolin eli kaksi keilaa.

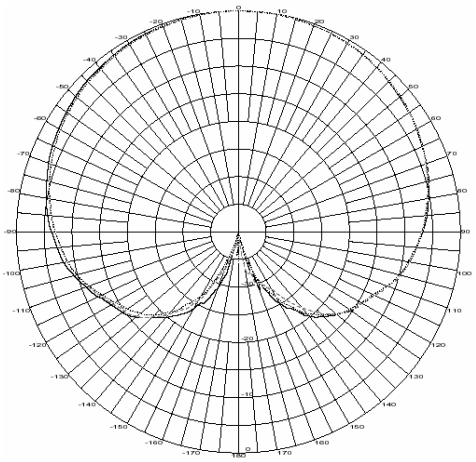


Kuva 5. Ympärisäteilevän antennin säteilykuviot /23/



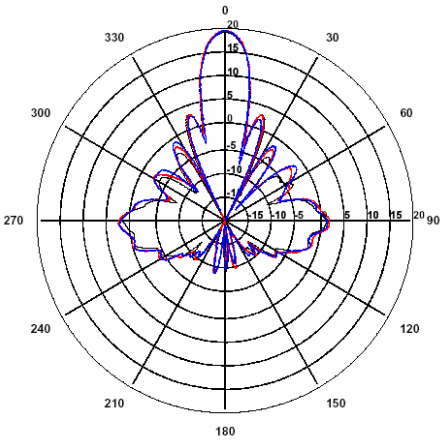
Kuva 6. dipoli-antennin säteilykuviot /23/

Sektoriantennit (Kuva 7.) ovat tarkoitettu sektorin muotoisen alueen peittoon ja ne ovat mainioita esimerkiksi rakennuksen nurkka-asennuksiin.



Kuva 7. Sektoriantennin säteilykuvio x/y-akseleilla /3/

Lautasantennit (Kuva 8.) on tarkoitettu mm. pitkien välimatkojen linkkeihin. Niiden suuntakuvio on hieman samanmuotoinen kuin suunta-antenneilla, mutta niiden vahvistus on huomattavasti suurempi.



Kuva 8. Lautasantennin säteilykuvio x/y-akseleilla /3/

6 WLAN VERKKOMALLIT

WLAN-verkko voi koostua joko tukiasemasta ja verkkokorteista, tai sitten pelkistä verkkokorteista. Mikäli verkko koostuu tukiasemasta johon käyttäjät liittyvät käyttäen langatonta verkkokorttia, niin kyseessä on infrastruktuuri-verkko. Mikäli taas verkko muodostuu pelkistä verkkokorteista, eikä käytössä ole tukiasemaa, kutsutaan verkkoa ad-hoc-tyyppiseksi.

6.1 Ad-Hoc-verkkomalli

Ad-hoc-tyyppistä verkkoa (Kuva 9.) käytettäessä ei tarvita ollenkaan tukiasemaa. Hyötypuolena tästä aiheutuu se, että verkon kustannukset laskevat. Suurena haittapuolena tässä on kuitenkin se, että ilman tukiasemaa tietokoneiden kantama jää pieneksi, koska kaikkien tietokoneiden täytyy olla yhteydessä toisiinsa.

Ad-hoc on hyödyllinen ratkaisu pieniin verkkoihin tai jos halutaan liittää kaksi tietokonetta toisiinsa. Tällöin verkko saadaan konfiguroitua nopeasti ja vaivattomasti. /16./

Kuva 9. Ad-Hoc verkon malli /16/

6.2 Infrastruktuuriverkko

Infrastruktuuriverkot voi jakaa kahteen ryhmään: BSS:ään (Basic Service Set) (Kuva 10.) ja ESS:ään (Extended Service Set) (Kuva 11.). Näistä BSS on yleisin WLAN-ratkaisu varsinkin kodeissa ja pienissä toimistoissa. Tässä ratkaisussa on vain yksi tukiasema, jonka kautta tietokoneet ovat yhteydessä lähiverkkoon.

Kuva 10. Infrastruktuuriverkko (BSS) /16/

BSS-tyypin verkko voidaan muuttaa ESS-tyypin verkoksi lisäämällä siihen tukiasemia. Näin ollen aliverkon muodostaa useampi kuin yksi BSD-verkko. Yleensä tässä mallissa jokainen tukiasema on yhteydessä langalliseen verkkoon, mutta on myös mahdollista yhdistää useampi tukiasema langattomasti toisiinsa, käyttäen tukiasemien siltaustoimintoja. Tämä mahdollistaa verkon peittoalueen kasvattamisen ja tietokoneet voivat olla yhteydessä toisiinsa pidempien matkojen päästä. /16./

Tekniikasta käytetään nimitystä roaming ja se mahdollistaa käyttäjän liikkumisen tukiaseman alueelta toisen tukiaseman peittoalueelle ilman, että käyttäjä huomaa tätä. /4./

Kuva 11. Infrastruktuuriverkko (ESS)

7 WLAN TIETOTURVALLISUUS

WLAN verkkojen yleistyttyä myös yksityiskäytössä, keskustelu niiden tietoturvasta on kiihtynyt. Uutisissa on ollut tapauksia, joissa esimerkiksi naapurin suojaamatonta WLAN-yhteyttä käyttämällä, on voitu kirjautua yrityksen taloushallintajärjestelmään siirtämään yrityksen varoja omalle tilille ja yritetty näin häivyttää jälkiä /7/. Langatonta liikennettä on erittäin helppo kuunnella. Tämä johtuu siitä seikasta, että siirtotie on kaikkien kuunneltavissa, mikäli käytössä on tarvittavat laitteet, eli käytännössä tietokone varustettuna langattomalla verkkokortilla. Tämä onkin muodostunut ongelmaksi esimerkiksi tavallisilla käyttäjillä, jotka haluavat kotiinsa langattoman verkkoyhteyden mutta eivät osaa konfiguroida laitteitansa niin että salaus olisi kunnossa. Langattomien verkkojen turvaksi on kehitelty monia salausmenetelmiä joihin tutustutaan tässä luvussa.

7.1 Tietoturvauhat

7.1.1 Liikenteen tarkkailu

Mikäli langatonta verkkoa ei ole lainkaan suojattu ja se lähettää SSID:tään radiotiellä, niin satunnaiselle nuuskijalle ei ole vaikea temppu tarkkailla suojaamattomia datapaketteja hakkerointityökaluilla (jokin ohjelma, esim. AirMagnet). Ohjelmat paljastavat täysin langattomien datapakettien sisällön ja nuuskijat voivat esimerkiksi seurata kaikkia verkon langattoman osuuden tapahtumia kymmenien metrien päässä langattoman lähiverkon sijainnista. Tämä tarkoittaa siis sitä että kaikki luottokorttitiedot, käyttäjätunnukset ja salasanat ovat alttiina hyökkäyksille.

Ratkaisu tähän ongelmaan on se, että langattoman tukiaseman ja asiakaslaitteen välillä tulee käyttää jonkinlaista salaustapaa. /5, s. 172./

7.1.2 Luvaton pääsy

Langattomien sovelluksien tarkkailu on helppoa johtuen jaetusta mediasta (Radiotie). Mahdollinen tunkeutuja kykenee helposti pääsemään langattoman verkon kautta esimerkiksi yrityksien palvelimiin, mikäli tietoturvallisuudesta ei ole huolehdittu. Tämä on rinnastettavissa murtovarkaan pääsyyn yrityksen tiloihin.

Vieläkin ilmenee tapauksia, joissa esimerkiksi yritykseen käyttöönotettu langaton verkko on otettu käyttöön ilman tukiasemien konfigurointia. Laitteissa on yleensä oletusarvoisesti kytketty salaus pois päältä ja ne tulisi aina konfiguroida tarpeiden mukaan käyttämään jotakin salausmenetelmää. Jos salausta ei ole, niin se mahdollistaa kenen tahansa pääsyn yrityksen verkkoon ja sitä kautta arkaluontaiseen dataan. /5, s. 172./

7.1.3 Välistävetohyökkäykset

Taitavat hakkerit kykenevät löytämään heikkouksia langattomista verkoista, johtuen verkkoprotokollien toimintatavoista. Yksi tämmöinen heikkous on välistävetohyökkäykset, jossa hakkeri laittaa valelaitteen asiakkaan ja tukiaseman väliin. Tämä ns. välistävetohyökkäys käyttää hyväkseen ARP (Address Resolution Protocol) -protokollaa, joka on käytössä kaikissa TCP/IP-protokollaa käyttävissä verkoissa.

ARP on protokolla jota verkkokortti käyttää selvittääkseen kohdeverkkokortin fyysisen eli MAC-osoitteen, jonka valmistaja on laittanut korttiin. Verkkokortti ymmärtää ja vastaa ainoastaan MAC-osoitteeseen. Ohjelmalla joka lähettää dataa, on tiedossa kohteen IP-osoite, mutta OSI-kerroksen alemmalla tasolla toimivan verkkokortin on käytettävä ARP:tä saadakseen selville sitä vastaavan fyysisen osoitteen. Se etsii sen lähettämällä yleislähetyksenä ARP-pyyntöpaketin, joka sisältää kohdeverkkokortin IP-osoitteen. Kaikki mediassa olevat laitteet kuulevat tämän pyynnön ja IP osoitteen omaava laite palauttaa ARP-paketin, joka sisältää sen MAC- ja IP-osoitteet. Tämän jälkeen lähettävä asema laittaa saamansa MAC-osoitteen lähettämänsä kehyksen kohdeosoitteeksi. Se myös tallentaa MAC-osoitteen ja IP-osoitteen taulukkoon määräajaksi.

ARP muodostaa tietoturvariskin joka johtuu ARP spoofing -toiminnosta. Esimerkkinä voisi toimia tilanne, missä verkkoon on kytketty ns. rosvotukiasema, mikä lähettää kysyjälle valheellisen ARP-vastauksen, missä on luvallisen laitteen IP-osoite ja luvattoman laitteen MAC-osoite. Tämän seurauksena kaikki verkon tukiasemat päivittävät ARP-taulukkonsa väärillä tiedoilla. Tämän seurauksena laitteet lähettävät kaikki pakettinsa luvattomalle laitteelle oikeiden osoitteiden sijasta. Tämän seurauksena hyökkääjä voi siepata dataa tai pahimmassa tapauksessa päästä yrityksen palvelimiin käsiksi.

Yksi ratkaisu ongelmaan on korvata ARP-protokolla SARP (Secure Address Resolution Protocol) -protokollalla. Se on laajennus joka tarjoaa erityisen tunnelin jokaisen asiakkaan ja tukiaseman välille. Tällä protokollalla toimivat laitteet eivät joudu osoitevääränn östen kohteeksi, sillä ARP-tauluja päivitetään vain laillisten vastausten perusteella. /5, s. 174 - 175./

7.1.4 DoS eli palvelunesto

Palvelunestohyökkäyksellä tarkoitetaan tilannetta, missä vihamielinen taho saa rampautettua tai kaadettua verkon. Tällainen hyökkäys tulisi aina ottaa huomioon tietoturvaa rakennettaessa, sillä riippuen tilanteesta, langattoman verkon toiminnan varmistaminen voi olla kriittistä. Esimerkiksi varastoissa joissa käytetään langattomia varastonhallintajärjestelmiä, verkon sulkeminen voi olla huomattavasti haitallisempaa, kuin mitä se olisi esimerkiksi langattoman kotiverkon tapauksessa.

Yksi palvelunestohyökkäyksen muodoista on väsytyshyökkäys. Tämä tarkoittaa sitä että verkko jumitetaan lähettämällä siihen isoja määriä datapaketteja. Suuri määrä liikennettä kuluttaa verkon resurssit ja seurauksena on yleensä verkon kaatuminen. Internetistä löytyy valmiita ohjelmia joilla hakkerit voivat tulvittaa langattoman verkon tehokkaasti. Hakkeri voi esimerkiksi suorittaa pakettipohjaisen väsytyshyökkäyksen lähettämällä hyödyttömiä paketteja palvelimelle verkon muilta tietokoneilta. Tämä syö kaistanleveyttä suuresti muilta käyttäjiltä.

Toinen tapa palvelunestohyökkäykseen erityisesti törmäystunnistusta käyttävissä langattomissa verkoissa on käyttää erittäin voimakasta radiosignaalia, joka ottaa ilmatien hallintaansa ja samalla tekee tukiasemista ja verkkokorteista käyttökelvottomia. IEEE 802.11:n kaltaiset protokollat ovat haavoittuvaisia tällaiselle, koska ne ovat ”kohteliaita” ja antavat vihamielisen signaalin pitää siirtotietä hallussaan miten kauan tahansa. Tällaiseen hyökkäykseen tarvitaan kuitenkin erittäin tehokas lähetin, jonka täytyy olla lähellä verkkoa, joka sitten mahdollistaa myös sen löytämisen helpommin mm. verkkoanalysaattorilla.

Langattomaan verkkoon kohdistuva palvelunestohyökkäys voi olla myös tahaton. Esimerkiksi 2,4 GHz:n taajuudella toimiva 802.11b ottaa herkästi häiriötä esimerkiksi mikroaaltouuneista, bluetooth-laitteista ja DECT-puhelimista. /5, s. 176 – 177./

7.1.5 Valetukiasema

Valetukiasemalla eli rosvotukiasemalla tarkoitetaan langatonta tukiasemaa, joka lisätään yrityksen kiinteään verkkoon ilman päällä olevia suojauksia. Se voi esimerkiksi olla jonkun työntekijän itse lisäämä henkilökohtainen tukiasema tai sitten jonkun mahdollisen pahaa tahtovan tahon lisäämä. Tämän takia yrityksen olisi syytä skannata tasaisin väliajoin liiketilat tietoturvallisuuden parantamiseksi. /5, s. 193./

7.2 Salausmenetelmät

7.2.1 Pääsylistat eli MAC-suodattimet

Yksi yksinkertainen keino rajoittaa ulkopuolisten käyttäjien pääsyä kiinni tukiasemaan on määrittää tukiasemalle lista MAC-osoitteista (Medium Access Control) joille on verkkoon pääsy sallittu. Tämän menetelmän huono puoli on siinä, että ylläpitäjän on naputeltava jokainen MAC-osoite erikseen tukiasemalle. Tietoturvallisesti tätä ei tule pitää kovin luotettavana, sillä nykyisistä verkkokorteista pystyy MAC-osoitetta muuttamaan ja ne kulkevat selväkielisissä paketeissa vaikka data olisikin salakirjoitettu. Mahdollisen hyökkääjän on mahdollista selvittää kuunteluohjelmalla jokin verkossa ole MAC-osoite ja muuttaa oma verkkokorttinsa käyttämään sitä.

7.2.2 WEP – Wired Equivalent Privacy

WEP on ensimmäinen salausmenetelmä mikä on implementoitu IEEE 802.11 -standardiin. Sen tarkoitus oli mahdollistaa yhtä hyvä tietoturva kuin mitä kiinteässä verkossa ja estää salakuuntelijoiden pääsy verkkoon. WEP perustuu salaiseen avaimeen mikä alun perin oli 64 (40+24)-bittinen. Myöhemmin IEEE 802.11b ja -g -standardien myötä mahdollistui myös 128

(104+24)-bittisten salausavaimien käyttö. Käytettävä salainen avain kryptaa lähetettävän tiedon ja pyrkii takaamaan sen eheyden. /9/

WEP toimii kohtuullisen hyvin langattoman verkon turvana ja estää useimmissa tapauksissa esimerkiksi naapureilta oman langattoman verkon käytön. Esimerkiksi kotikäytössä missä yleensä ei ole käytössä kriittisiä tietoja, voidaan mahdollisesti käyttää WEP-salausta, mikäli muita vaihtoehtoja ei ole tarjolla. WEP Käyttää hyväkseen RC4-salausalgoritmia, jossa on havaittu joitakin puutteita. Sen alustusvektorit ovat vain 24 bitin mittaisia, joten samankaltaisuus havaitaan niissä helposti. Ne myös lähetetään salaamattomana jokaisessa kehyksessä. Kuviteltu hyökkääjä saa siis avaimen selville, mikäli kuuntelee tietoliikennettä tarpeeksi kauan ja seuraamalla samankaltaisia alustusvektoreita ja laskemalla niistä avaimen. Siirrettävät datamäärät vaikuttavat siihen kuinka nopeasti avain on murrettavissa. /9/. Mikäli WEP:llä haluttaisiin pitää tietoturva jonkinasteisessa kunnossa, niin salausavainta tulisi vaihtaa säännöllisin väliajoin. Tämä koetaan kuitenkin yleisesti kohtuullisen hankalaksi, varsinkin jos kyseessä on kotikäyttäjä, jolle esimerkiksi laajakaistan asentaja on käynyt konfiguroimassa laitteet toimintaan. Ongelmia aiheuttaa myös se, että jokaiseen laitteeseen pitäisi erikseen käydä vaihtamassa salasana.

Puutteista huolimatta kannattaa muistaa että WEP-salaus on kuitenkin tehokkaampi kuin ei salausta ollenkaan. Se riittää mainiosti monille kotikäyttäjille, joiden verkossa ei liiku erittäin salaisia tietoja. Se riittää myös estämään useimmissa tapauksissa naapuria käyttämästä ”ilmaista” internetyhteyttä

7.2.3 RADIUS (Remote Authentication Dial In User Service) -protokolla

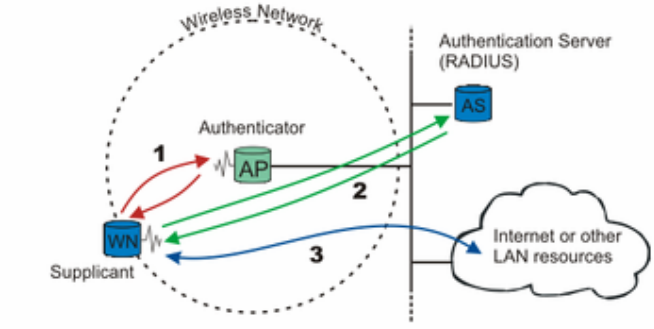
RADIUS-protokolla on aikoinaan suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen. Nykyään sitä käytetään myös langattomien lähiverkkojen salauksen yhteydessä. Mikäli halutaan käyttää AAA (authentication, authorization and accounting) -palveluita, niin lähiverkolla on oltava RADIUS-palvelin, johon kytkimet ja tukiasemat ottavat yhteyttä RADIUS-protokollalla. Palvelimen ja verkkolaitteiden välille pitää konfiguroida oma salasana jokaista palvelin/verkkolaite-yhteyttä varten. RADIUS-palvelin voi si-

sältää tietokannan, jossa käyttäjänimiä ja salasanoja säilytetään. Se osaa myös käyttää hyväkseen jo olemassa olevia käyttäjänimi/salasana-tietokantoja. /9./

7.2.4 802.1X – porttikohtainen autentikointi

Edistysaskel langattomien verkkojen tietoturvaan oli vuonna 2001 julkaistu IEEE 802.1X, joka mahdollisti autentikoinnin. IEEE 802.1X käyttää asiakkaan tunnistukseen protokollaa nimeltä EAP (Extensible Authentication Protocol), jota käytetään asiakkaan ja autentikaattorin välisessä autentikointitiedon siirrossa. /9./

802.1x liikenne käynnistyy kun autentikoimaton langaton yhteyslaite yrittää muodostaa yhteyttä tukiasemaan. Tukiasema vastaa laitteelle avaamalla portin, jossa sallitaan vain EAP-paketit asiakkaalta autentikointipalvelimelle, joka sijaitsee yleensä kiinteän verkon puolella. Tukiasema estää kaiken muun liikenteen, kuten http, DHCP ja POP3-paketit, siihen asti, kunnes se voi varmistaa langattoman laitteen identiteetin autentikointipalvelimen (RADIUS-palvelin) kanssa. Kun autentikointi on suoritettu ja asiakas tunnistettu, tukiasema avaa liikenteen muun tyyppiselle liikenteelle autentikointipalvelimen ilmoittamien oikeuksien mukaisesti. (Kuva 12.)



Kuva 12. 802.1X:n toimintaperiaate RADIUS-palvelimen avulla

7.2.5 TKIP – temporal Key Integrity Protocol

TKIP on päivitys langattomien verkkojen tietoturvaan ja erityisesti WEP-salaukseen. Sitä kutsuttiin alun perin myös WEP2:ksi. TKIP on ratkaisu, joka korjaa WEP:n sisältämän avaimien uudelleenkäytön ongelman. Useimmissa uusissa WLAN-tuotteissa TKIP on jo vakio-ominaisuutena mukana. TKIP käyttää salaamiseen WEP:n lailla RC4-algoritmia. Suurin ja keskeisin ero TKIP:n ja WEP:n välillä on se, että TKIP vaihtaa tilapäisen avaimen aina 10000 paketin välein. Tämä parantaa merkittävästi verkon tietoturvaominaisuuksia. TKIP:n etu on se että sen käyttöönottoon riittää yleensä jo pelkät ohjelmistopäivitykset jo käytössä oleviin laitteisiin. TKIP on kuitenkin vain tilapäinen ratkaisu, sillä useimmat asiantuntijat ovat sitä mieltä että tarve vieläkin vahvemmalle salaukselle on olemassa. /5, s. 183 - 184./

7.2.6 WPA – Wireless Fidelity Protected Access

WPA-tekniikkaa alettiin kehittää WEP-salauksen ongelmien paljastuttua. WPA sisältää 802.11i (eli WPA2) -standardin ominaisuuksia ja on yhteensopiva nykyisten ja myös tulevien laitteiden kanssa. WPA:ssa WEP-salauksen heikot aloitusvektorit on korvattu paremmilla ratkaisuilla. Tämän lisäksi salausavainta vaihdetaan automaattisesti 10 000 paketin välein. WPA käyttää hyväkseen TKIP-salausta (Temporal Key Integrity Protocol) joka mahdollistaa salausavaimen hajautuksen parantaen näin tietoturvaa. TKIP käyttää liikenteen salaukseen RC4-algoritmia sillä erolla WEP:iin, että salausavaimen pituus on 128 bittiä. /9./

WPA:sta on olemasta eri tarkoituksiin kaksi eri toimintamoodia:

- WPA-PSK (Pre-Shared Key) on tarkoitettu kotikäyttöön. Siinä tukiasemaan kirjaudutaan määriteltyä salasanaa käyttäen jonka jälkeen yhteys tukiaseman ja käyttäjän välillä on suojattu.
- 802.1X on suurissa yrityksissä käytettävä ratkaisu jossa RADIUS-palvelinta ja EAP:ia (Extensible Authentication Protocol) käyttämällä saadaan erittäin korkea tietoturvan taso ja keskitetty hallinta käyttäjätunnistukselle. /10./

7.2.7 WPA2 – Wireless Fidelity Protected Access versio 2

WPA2 on langattomien verkkojen uusin tietoturvastandardi, joka tunnetaan myös IEEE 802.11i -standardina. Siinä määritellään 802.1X:n kaltainen todennus ja avaintenhallintakäytäntö sekä entistä tehokkaammat tiedonsalausmenetelmät. WPA2 tarjoaa samat ratkaisut kuin aikaisemmin kehitelty WPA-standardi, mutta tämän lisäksi se antaa mahdollisuuden käyttää kokonaan uudenlaista salausmekanismia AES:aa (Advanced Encryption Standard) RC4:n tilalla. AES mahdollistaa eripituisten salausavaimien käytön, vaihtoehtoina 128-, 192-, ja 256-bittiset avaimet. /9./

Niin kuin WPA niin myös WPA2 mahdollistaa kaksi eri toimintamoodia:

- WPA2-Personal on suunniteltu kuluttajille ja on vastaavanlainen WPA-PSK:n kanssa. Se käyttää AES-algoritmia salaukseen ja siinä tukiasemaan kirjaudutaan käyttäen ennalta määrättyä salasanaa.
- WPA2-Enterprise on yrityskäyttöön tarkoitettu, ja se käyttää AES-algoritmia salaukseen ja tunnistaa käyttäjät EAP:n avulla. /11./

Wi-Fi Alliance on ilmoittanut, että 13.3.2006 lähtien uusien Wi-Fi-merkintää käyttävien laitteiden on tuettava WPA2-standardia. /11./

8 CAPWAP ELI CONTROL AND PROVISIONING OF WIRELESS APS

CAPWAP on IETF:n protokollaluonnos jota käytetään langattomien tukiasemien keskitettyyn hallintaan. Tähän tarkoitukseen on kehitelty eri yrityksien toimesta erilaisia protokollia, jotka yhdistävät ns. ”thin-edge” tai ”light weight” -tukiasemat WLAN-kontrolleriin. Protokollan avulla olisi tarkoitus huolehtia roamingista, rosvotukiasemien havaitsemisesta ja estämisestä, kanavanvarauksesta, redundanssista sekä virranjakamisesta. /22./

Näistä jo kehitetyistä protokollista käytetyin lienee tällä hetkellä mm. Cisco Systemsin käyttämä LWAPP eli Light Weight Access Point Protokolla. Siitä kaavaillaan myös runkoa lopulliselle IETF:n CAPWAP standardille. /25./

Capwap protokollakandidaatteja ovat seuraavat

LWAPP "Light weight Access Point Protocol"

Ensimmäinen capwap protokolla joka esitteli alkuperäiset ratkaisut autentikoinnille, käyttäjän datan enkapsulointiin sekä hallinnan ja konfiguroinnin tarpeisiin. Tässä työssä tutustuttiin lähinnä LWAPP protokollaan, johtuen laitevalinnoista. Protokollasta lisää seuraavassa kappaleessa.

SLAPP "Secure Light Access Point Protocol"

SLAPP käyttää tunnettuja teknologioita, kuten GRE:a (Generic Route Encapsulation) jota käytetään datan tunneloimiseen Access Controllerin (WLAN-kontrolleri) ja WTP:n (Wireless Termination Point) välillä, ja DTLS:a (Datagram Transport Layer Security) jota käytetään kontrollikanavan siirtoon.

CTP "CAPWAP Tunneling Protocol"

CTP:n merkittävä ominaisuus on SNMP:n käyttö konfigurointi- ja hallintamäärityksessä, jotka se enkapsuloi kryptatulle kontrollikanavalle.

WICoP "Wireless LAN Control Protocol"

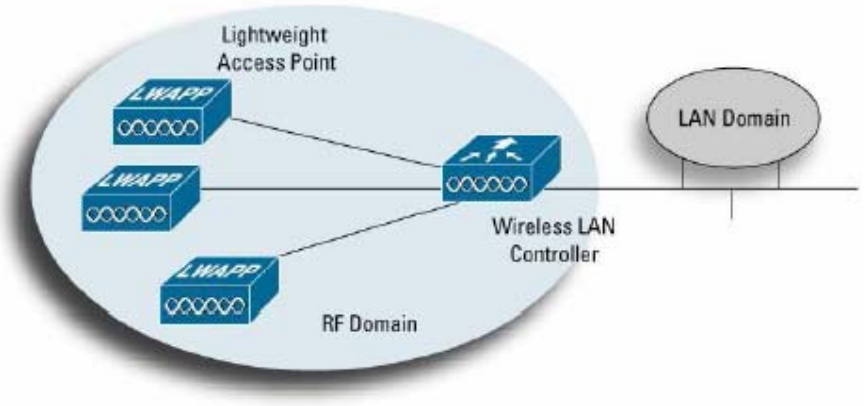
WICoP protokolla perustelee uuden systeemin WLAN systeemien löytämiseen, konfigurointiin ja hallintaan. Protokolla määrittelee selkeän havaitsemismekanismin joka integroi siihen WTP-AP yhteyksien neuvottelun. /26./

9 LWAPP-PROTOKOLLA JA KESKITETTY HALLINTA

Airespacen, Ciscon ja NTT Docomon insinöörit esittelivät huhtikuussa 2003 luonnoksen LWAPP:sta eli Light Weight Access Point -protokollasta. Protokollan kehittely perustuu ajatukseen, että langattomat tukiasemat (access point) voisivat toimia verkossa kuin pääsynvalvontaserverit (Network Access Server). /21/ Mukana kehityksessä oli myös D-Link. Perimmäinen filosofia tässä on D-Link Suomen myyntijohtaja Anssi Eskolan mukaan se, että voitaisiin siirtää ”äly” kytkimiin. Tämä myös mahdollistaisi nopeamman roamingin tukiasemien välillä. Lisäksi verkon hallinta yksinkertaistuisi huomattavasti, kun päivitykset, ylläpito ja valvonta voitaisiin hoitaa niin kuin kiinteissä verkoissa. /24./

9.1 Light Weight Access Point Protokolla

Varsinkin suuret yritykset jotka haluavat tarjota työntekijöilleen sekä vierailijoilleen langattoman verkon käyttömahdollisuutta ovat siirtymässä keskitettyyn hallintaan. Lightweight tukiasemien avulla toteutetuissa systeemeissä, WLAN-kontrolleri hoitaa tukiasemien normaalisti toteuttamat tehtävät kuten pääsynhallinnan, tietoturvahallinnan sekä QoS:n. Tämän tekniikan edut ovat huomattavan käteviä varsinkin silloin, jos yrityksellä on useita tukiasemia ympäri yrityksen tiloja eri paikkakunnilla. (Kuva 13.)



Kuva 13. Keskitetty hallinta toteutettuna WLAN-kontrollerilla ja LWAPP:lla

Perinteinen WLAN-ratkaisu perustuu siihen, että tukiasema vastaa liikenteen jakamisesta, radiotien kontrolloimisesta, tietoturvasta, sekä muista liikenteenohjaustehtävistä. Tästä seuraa siis se että mikäli yksittäisiä tukiasemia hallitaan ilman erillisiä etähallintalaitteita, niin se nostaa kustannuksia ja henkilöstömäärää. Lisäksi esimerkiksi DoS eli Denial of Service on vaikea havaita koko WLAN-verkossa. Tämä vaikeuttaa myös optimoidun reaaliaikaisen liikenteen jakamisen (load balancing) langattomassa verkossa. Verkon käyttäjät eivät voi suorittaa nopeita verkon vaihtoja (handoffs), mitä vaaditaan esimerkiksi puheen ja kuvan reaaliaikaisessa välityksessä. Fyysisen riskin menetelmässä aiheuttaa myös jos jokin tukiasema varastetaan paikaltaan. /20./

Standardisoiminen

Koska markkinoille tulee jatkuvasti uusia laitteita, jotka käyttävät keskitettyä WLAN-hallintaa, on tarvetta luoda näille standardi, jotta eri valmistajien laitteet voisivat kommunikoida keskenään. LWAPP-malli on tällä hetkellä odottamassa IETF:n hyväksymistä sitä standardiksi. Tavoite on että LWAPP:sta tulisi standardoitu protokolla tukiasemien ja WLAN-systeemien (reitittimet, kontrollerit, kytkimet, jne.) välille. Aloitteen tavoitteet ovat seuraavat.

- Vähentää tukiasemissa tapahtuvaa liikenteen prosessointia, vapauttaen niiden tehot keskittymään langattomien laitteiden pääsyn takaamiseen verkkoon.
- Mahdollistaa järjestelmä jossa liikenteen hallinta, autentikointi, tiedon enkryptaus, tietoturvan ja QoS hallinta voidaan toteuttaa keskitetysti koko WLAN systeemissä.
- Tarjota yleinen tapa tiedon enkapsulointiin ja kuljetukseen eri tukiasemien valmistajille, joko layer 2 -tasoa käyttäen, tai IP-pohjaisesti reititetyssä verkossa

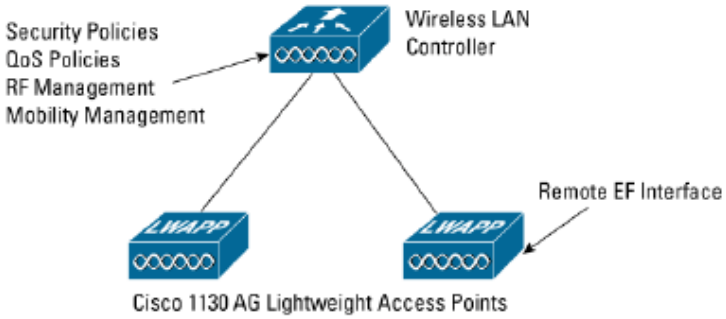
LWAPP-malli mahdollistaa seuraavat toiminnot:

- Tukiasemien havaitseminen, informaation vaihto sekä laitteiden konfigurointi
- Tukiasemien sertifikointi ja ohjelmistopohjainen hallinta
- Datapakettien enkapsulointi, fragmentointi ja formatointi
- Kommunikoinnin hallinta tukiaseman ja WLAN-systeemilaitteen välillä

Standardin toteutuminen antaisi asiakkaille mahdollisuuden valita tukiasemat ja WLAN-systeemilaitteet varmistamalla niiden yhteensopivuuden. /20./

9.2 LWAPP käytännössä

Kun LWAPP ensimmäisen kerran julkaistiin vuonna 2002, niin se vallankumouksellisesti muutti tavan jolla WLAN laitteita hallittiin. Konseptia kutsutaan nimellä ”split-MAC” (Kuva 14.) ja se tarkoittaa tapaa millä voidaan 802.11:n reaaliaikaiset piirteet erotella hallinnollisista piirteistä. Toisin sanoen reaaliaikainen datakehyksien vaihto sekä erinäiset reaaliaikaiset MAC-osoitteiden hallinnat voidaan toteuttaa tukiasemassa. Samalla autentikointi, tietoturvahallinta ja liikkuvuuden hallinta suoritetaan WLAN-kontrollerissa. Cisco Centralized WLAN solution oli ensimmäinen keskitetty hallintasysteemi joka käytti ”split-MAC”-ominaisuutta. /15./



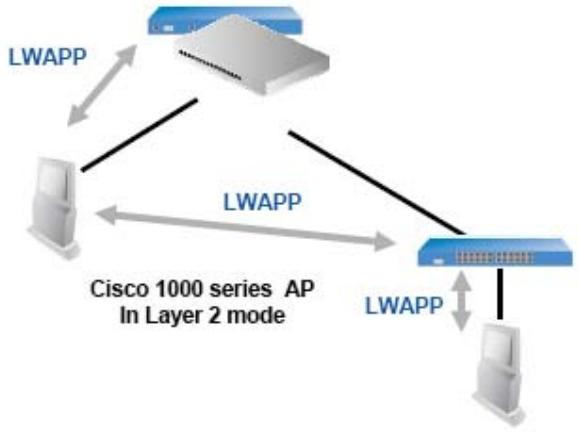
Kuva 14. Split-MAC toimintaperiaate toteutettuna Ciscon laitteilla /15/

LWAPP tarjoaa siis systeeminlaajuisen radiotaajuuksien hallinnan mikä pitää sisällään kanavien varauksen, lähetystehon määritykset sekä liikenteen ta-

soittamisen. Se käyttää AES-algoritmia liikenteen kryptaukseen tukiaseman ja kontrollerin välillä. LWAPP mahdollistaa nopeat handoff-ajat, mikäli laite toimii layer 2 tasossa, niin handoff luvataan ajaksi alle 14 ms ja layer 3 tasossa alle 30 ms. /15./

9.2.1 Tason 2 LWAPP

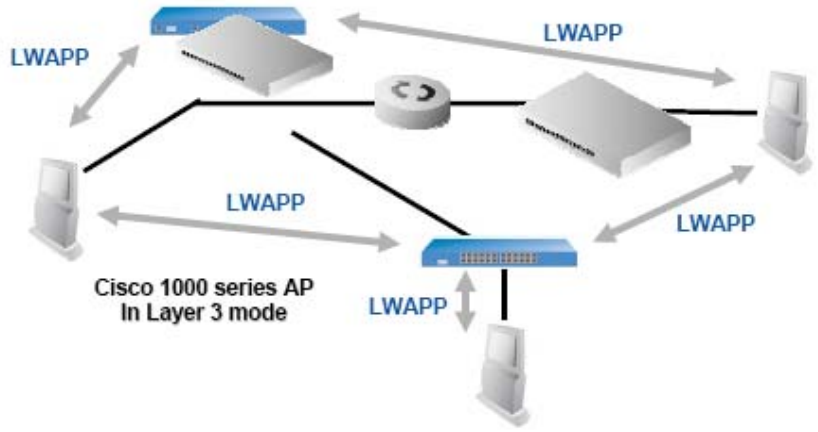
Tason 2 LWAPP (Kuva 15.) sijaitsee ethernet-kehyksessä. WLAN-kontrollerin ja tukiaseman tulee sijaita samassa aliverkossa tai olla suoraan kytkettynä.



Kuva 15. Tason 2 LWAPP:n toimintaperiaate /20/

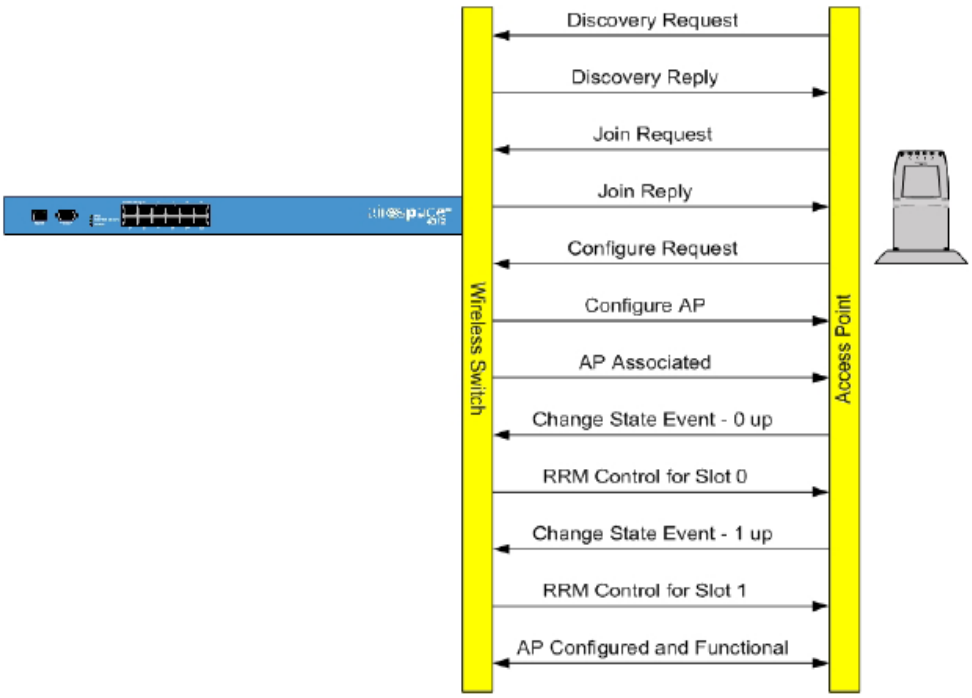
9.2.2 Tason 3 LWAPP

Tason 3 LWAPP (Kuva 16.) sijaitsee UDP/IP kehyksessä. WLAN kontrolleri ja tukiasema voivat olla joko suoraan kytkettynä toisiinsa, kytketty samaan aliverkkoon tai sitten kytketty eri aliverkkoihin. Tukiasema saa DHCP-palvelimelta IP-osoitteen jonka avulla se toimii myös tasolla 3.



Kuva 16. Tason 3 LWAPP:n toimintaperiaate /20/

Tukiaseman ja kontrollerin välillä tapahtuvaa liikennettä LWAPP:aa käyttäen voidaan esittää kuvalla 17.



Kuva 17. Tukiaseman ja kontrollerin välinen liikenne /20/

Ensimmäisenä tukiasema lähettää discovery requestin, joko broadcastina mikäli kyseessä on layer 2 tukiasema, tai sitten DHCP optiota 43, jolla se hakee informaation DHCP-palvelimelta, tai sitten DNS:aa käyttäen. Mahdollisuus discovery-paketin lähettämiseen on myös ilmatien kautta, mikäli se lä-

hettää sen toisen tukiaseman kautta. Tämän jälkeen tukiasema lähettää X509 julkisen sertifikaattinsa, jota kontrolleri käyttää salaamaan sen oman sertifikaatin. Tämän jälkeen kaikki kontrollidata tukiaseman ja kontrollerin välillä on kryptattu käyttäen AES-algoritmia. Tukiasema tarkistaa myös onko kontrollerilla uudempi ohjelmistoversio kuin sillä. Mikäli on, niin se lataa uudemman version itsellensä, asentaa sen ja käynnistää itsensä uudelleen. Mikäli versio on ajan tasalla oleva, niin tukiasema lähettää asetuspyynnön kontrollerille, johon kontrolleri vastaa lähettämällä tukiasemalle oikeat asetukset, mitkä tukiasema ottaa sitten käyttöön. Tässä vaiheessa tukiasema on täysin assosioitunut kontrolleriin. Seuraavaksi kontrolleri lähettää RRM tiedon slot 0:lle (802.11b/g) johon tukiasema kuittaa. Sitten se lähettää RRM infon koskien slot1:stä johon myös odotetaan kuittausta tukiasemalta. Tämän jälkeen tukiasema on täysin konfiguroitu ja toiminnassa. /20./

9.3 Laitteistot jotka hyödyntävät LWAPP-protokollaa

Seuraavassa esitellään laitteistoa, eli tukiasemia ja WLAN-kontrollereita jotka hyödyntävät Light Weight Access Point Protokollaa käytännössä.

9.3.1 Cisco 1000 sarjan Lightweight tukiasemat

Sarjan ominaisuudet

- Tukee 802.11a/b/g/h -standardeja
- Tukee LWAPP-protokollaa
- Tukee ns. “zero-touch”-konfigurointia ja keskitettyä hallintaa
- Tukee samanaikaista ilmatien tarkkailua sekä datapalvelua
- Reaaliaikainen RF-hallinta
- Kustannustehokas ja langaton IPS (Intrusion Prevention System)
- Sisäinen antenni, ulkoiselle antennille liitäntä
- Tukee uusia salausmenetelmiä WPA/802.11i WPA2
- Laadunvalvonta (QoS)

- Tason 2 ja 3 roaming
- IEEE 802.3af Power over Ethernet (PoE)

Mallikohtaiset ominaisuudet

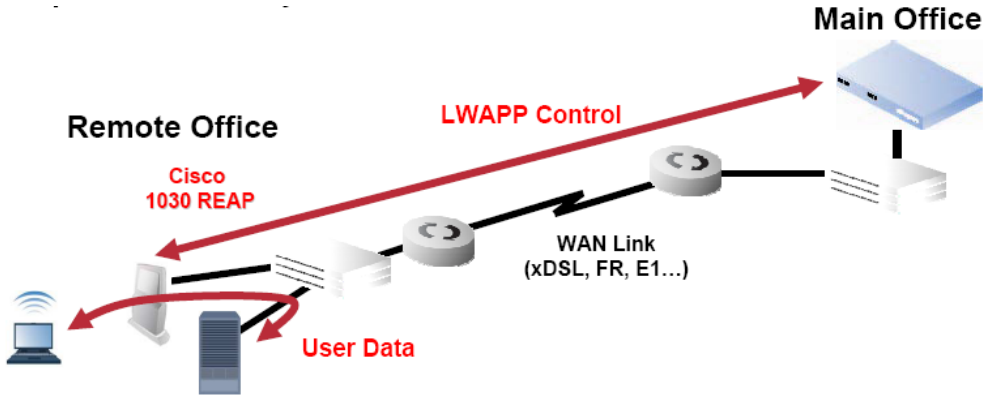
AIR-AP1010-E-K9 sisältää yhden 802.11b/g radiovastaanottimen/-lähettimen sekä yhden 802.11a radiovastaanottimen/-lähettimen. Se sisältää neljä ympärisäteilevää sisäistä antennia.

AIR-AP1020-E-K9 sisältää AP1010:n ominaisuuksien lisäksi yhden 5 GHz:n ja kaksi 2,4 GHz:n ulkoisia antenniadaptereita.

AIR-AP1030-E-K9 on tarkoitettu verkon reuna-alueilla toimivaksi tukiasemaksi. Se sisältää samat mallikohtaiset ominaisuudet kuin AP1020. Se on ns. REAP (Remote Edge Access Point)

REAP:n ominaisuudet

REAP (Kuva 18.) on suunniteltu tukemaan etätoimistoja muuttamalla LWAPP:n ajastimia. Kontrollointi data on edelleenkin kuitenkin LWAPP enkapsuloitu ja se lähetetään WLAN-kontrollerille. Asiakkaan dataa sen sijaa ei siirretä käyttäen LWAPP:aa vaan se on paikallisesti sillattu. REAP jatkaa paikallisen yhteyden tarjoamista vaikka WAN olisi alhaalla. /20./



Kuva 18. REAP:n toimintaperiaate /20/

9.3.2 Cisco Aironet 1130AG -tukiasema

- Voi toimia sekä tavallisena tukiasemana tai light weight -tukiasemana
- Toimii yhtäaikaisesti 2,4 GHz:n ja 5 GHz:n taajuuksilla
- Sisäiset 2,4 GHz ja 5 GHz ympärisäteilevät antennit
- Muotoilu suunniteltu erityisesti seinäkiinnitystä varten
- 4 tapaa virransyöttöön; 802.3af PoE, Cisco Legacy PoE, Cisco Power Injector tai paikallinen virtalähde
- Tietoturvaominaisuudet tukevat AES kryptausta ja 802.11i (WPA2) ominaisuuksia
- Mekaaninen lukollinen kiinnitys (kuva 19.)

Kuva 19. Cisco 1130AG-tukiasema

9.3.3 Cisco Aironet 1240AG -tukiasema

- Toimii yhtäaikaisesti 2,4 GHz:n ja 5 GHz:n taajuuksilla
- RP-TNC liittimet 2,4 GHz:n ja 5 GHz:n ulkoisille antenneille
- Tukee ulkoisia antenneja 10 dBi:n saakka 2,4 GHz:n taajuudella ja 9,5 dBi:n taajuudella 5 GHz:n saakka
- 4 tapaa virransyöttöön; 802.3af PoE, Cisco Legacy PoE, Cisco Power Injector tai paikallinen virtalähde
- Metallinen ulkokuori
- Toimii lämpötiloissa -20C - +55C

- Toimitetaan joko itsenäisesti toimivalla Cisco IOS ohjelmistolla tai LWAPP-ohjelmistolla (Kuva 20.)

Kuva 20. Cisco 1240AG -tukiasema

9.3.4 Cisco 2000 sarjan WLAN -kontrolleri

WLAN-kontrolleri on siis laite, joka hoitaa tukiasemien puolesta pääsynhallinnan, tietoturvahallinnan sekä palvelun laadun varmistuksen. Ciscolla on tarjolla tällä hetkellä kolme erilaista WLAN-kontrolleria, joihin tutustutaan seuraavassa. /20./ (Kuva 21. ja 22.)

- Tukee IEEE 802.11 a/b/g/d/h langattomia standardeja
- Tukee langallisista standardeista IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX ja IEEE 802.1Q VLAN-taggingia
- Tukee salaustekniikoita WPA ja 802.11i eli WPA2
- On hallittavissa joko web-pohjaisesti, HTTP/HTTPS:lla tai Telnetillä ja SSH-yhteydellä. Lisäksi laitteessa on sarjaportti suoraa hallintayhteyttä varten.
- Tukee maksimissaan kuutta Light Weight tukiasemaa
- Ei laajennusportteja
- Liitännät: sarjaportti RS-232 DTE-interface, neljä 10/100 Mbps RJ-45 ethernet BASE-T porttia, virtaliitäntä chuko

- Mitat: 241 x 152 x 41 mm, Paino 1,11 kg
- Toimii lämpötiloissa 0C – 40C
- Vuoden takuu /18./

Kuva 21. Cisco 2000 WLAN-kontrolleri /22/

9.3.5 Cisco 4402 ja 4404 WLAN -kontrollerit

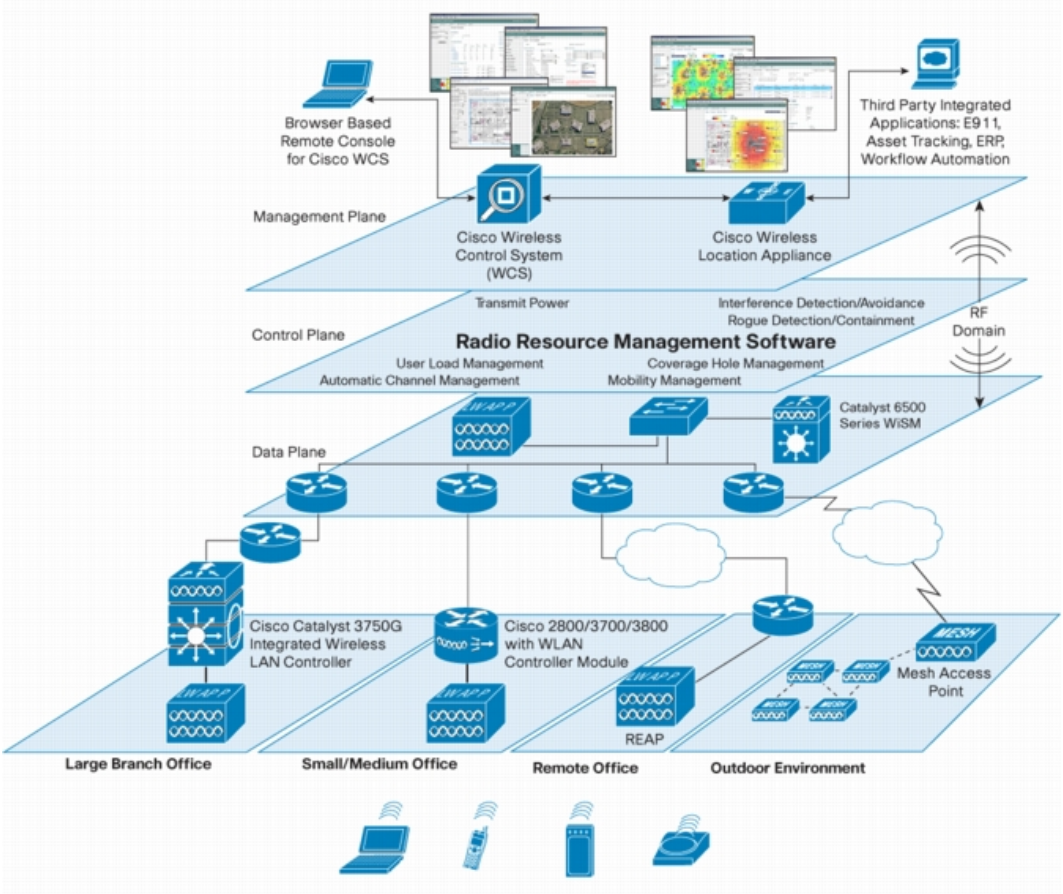
- Tukee IEEE 802.11 a/b/g/d/h -langattomia standardeja
- Tukee langallisista standardeista IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX ja IEEE 802.1Q VLAN taggingia
- Tukee salaustekniikoita WPA ja 802.11i eli WPA2
- On hallittavissa joko web-pohjaisesti, HTTP/HTTPS:lla tai Telnetillä ja SSH-yhteydellä. Lisäksi laitteessa on sarjaportti suoraa hallintayhteyttä varten.
- 4402 kontrolleri tukee joko 12, 25 tai 50:ä LW tukiasemaa 4404 kontrolleri tukee maksimissaan 100 LW tukiasemaa
- 4404:ssa kaksi ja 4402:ssa yksi laajennusportti
- Liitännät: sarjaportti RS-232 DTE-interface, 4402 sarjassa kaksi ja 4404:ssa neljä 1000 Mbps RJ-45 Base-X SFP porttia, utility-portti 10/100/1000 Mbps RJ-45 ethernet, virtaliitäntä chuko
- Tuki kahdelle redundantille virtalähteelle
- Mitat: 443 x 400 x 44,5 mm, Paino 6,95 kg
- Toimii lämpötiloissa 0C – 40C
- Vuoden takuu /18./

Kuva 22. Ciscon 4400 sarjan WLAN kontrollerit /20/

9.4 Ciscon langaton kontrollointijärjestelmä (WCS)

Ciscon kehittämä WCS (Wireless Control System) on täydellinen alusta järjestelmänlaajuiseen WLAN-hallintaan. Se tarjoaa reaaliaikaisen näkyvyyden ja koko ilmatilan hallinnan. Ominaisuutena siinä on muunneltavissa olevat diagrammit/mallit helppoon menettelytapojen (policy) luomiseen. Järjestelmä on suunniteltu toimimaan WLAN kontrollereiden kanssa ja sillä pystytään hallitsemaan kaikkea aina etätoimistoista isoihin kampusverkkoihin. Hallintajärjestelmä kannattaa ottaa käyttöön viimeistään siinä vaiheessa kun langaton verkko sisältää lukuisia kontrollereita ja tukiasemia. /20./

WCS toimii serverialustalla upotetussa tietokannassa. Tämä mahdollistaa satojen WLAN kontrollerien hallinnan, jotka taas tarjoavat mahdollisuuden hallita tuhansia tukiasemia: WLAN kontrollerit voivat sijaita joko samassa verkkosegmentissä kuin Cisco WCS, eri aliverkossa tai sitten jopa pidempien yhteyksien päässä. (Kuva 23.)



Kuva 23. Ciscon WCS:n toimintaperiaate

Cisco WCS auttaa toteuttamaan mm. seuraavat asiat helpommin langattomassa verkossa:

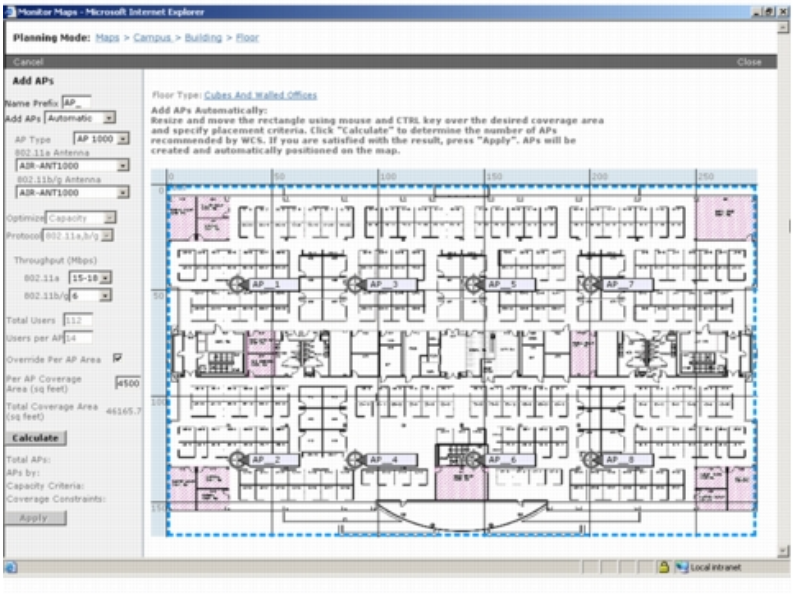
Langattoman verkon suunnittelu ja toteutus

WCS tarjoaa integroituna radiotaajuuksien ennustukseen käytetyn työkalun, jota voidaan käyttää yksityiskohtaiseen WLAN-tukiasemien sijainnin suunnitteluun, konfigurointiin ja tehon sekä peittoalueen arviointiin. Se mahdollistaa myös karttojen liittämisen siihen paremman suunnittelun takaamiseksi. /27./

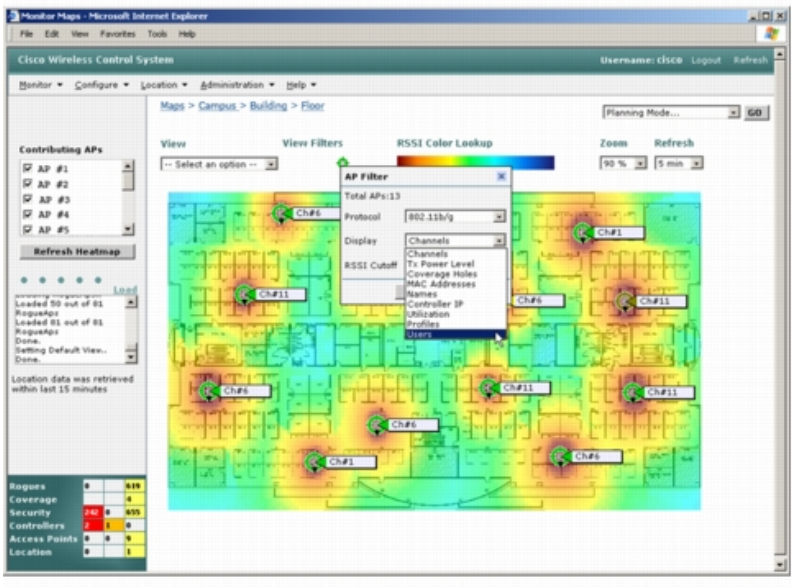
Verkonhallinta ja ongelmien kartoitus

WCS tarjoaa työkalut langattoman verkon visuaaliseen ja suorituskyvyn tarkkailemiseen (Kuva 24.). Tähän kuuluvat tarkat ”lämpökartat" (Kuva 25.), jotka ilmaisevat radiotaajuuksien käytön syötettyjen karttojen päällä. WCS tarjoaa myös reaaliaikaiset hallinnointimahdollisuudet WLAN-kontrollerien

käytön myötä, mukaan lukien kanavien määritykset sekä tukiasemien tehonsäädöt. Systeemistä saa selville yhdellä silmäyksellä verkon peittoalueen, hälytykset ja tärkeimmät statistiikat helpolle WLAN-hallinnalle. /27./



Kuva 24. Hallintatyökalu

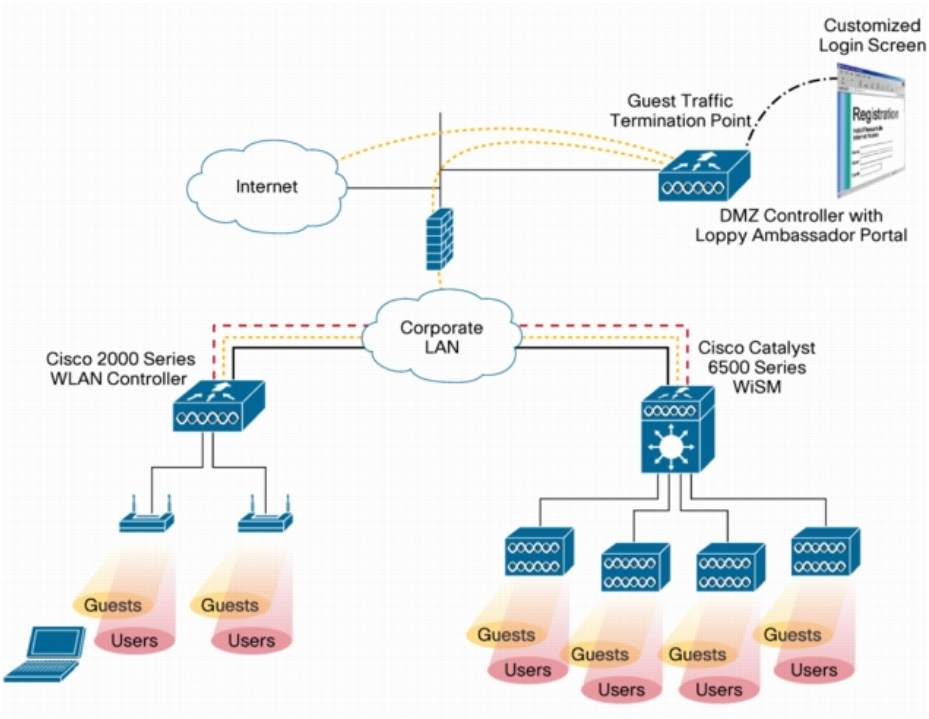


Kuva 25. Hallintatyökalun "lämpökartta"

Vierailijoiden ja henkilökunnan erottelu

Cisco WCS tarjoaa kustomoitavan suojatun vierailijoiden hallinnan, joka mahdollistaa yrityksen pitämään verkkonsa suojattuna, samalla kuin yrityksen ulkopuolisille, esim. vieraille tarjotaan rajoitettu pääsy verkkoon. Admin voi halutessaan myös ladata html-kuvan kontrollerille, joka korvaa normaalin sisäänkirjautumiskuvan

Yrityksellä on myös mahdollisuus käyttää WCS:n tarjoamaa ”Guest Access Lobby Ambassador” ominaisuutta WLAN kontrollerilla. Tämä ominaisuus mahdollistaa lokaalien käyttäjänimien ja salasanojen luomisen sekä lokaalin tai RADIUS-pohjaisen tunnistamisen vierailijoille. /27./ (Kuva 26.)



Kuva 26. WCS:n suojattu vierailijoiden pääsyn mahdollistaminen

Sisätiloissa tapahtuva seuranta

WCS tarjoaa keinon tehokkaasti seurata langattomia laitteita verkossa. Tämä käsittää Wi-Fi-kortilla varustetut tietokoneet, kämmentietokoneet sekä muut mobiililaitteet, jotka on varustettu Wi-Fi-lähettimellä. WCS:n perusver-

siolla on mahdollista selvittää minkä tukiaseman kanssa langaton laite on assosioitunut, antaen näin administraattorille mahdollisuuden seurata, minkä tukiaseman alueella käyttäjä on. Käyttöympäristöissä missä vaaditaan tarkempaa sijainnin määritystä, voidaan käyttää WCS:n versiota missä on paikannuspalvelu implementoituna (Cisco WCS with Location). Se käyttää Ciscon kehittämää ohjelmistoa, nimeltään ”RF sormenjälki” teknologiaa. Se vertaa reaaliaikaista RSSI (Received Signal Strength Indication) signaalia tunnettuihin rakennuksen yksityiskohtiin. Tämän seurauksena käyttäjän sijainti voidaan määrittää muutaman metrin tarkkuudella. /27./ (Kuva 27.)

Kuva 27. Seurantatyökalu

Langaton tietoturva Cisco WCS:ssa

WCS tarjoaa täyden valikoiman työkaluja tietoturvapolitiikan hallintaan langattomassa ympäristössä. RF-hyökkäyksen allekirjoituksella ja langattoman tunkeutumisen estolla WCS auttaa administraattoria luomaan hyökkääjälle räätälöitävissä olevia allekirjoituksia joita voidaan käyttää hyökkäyksen nopeaan tunnistamiseen, kuten DoS, Netstumbler ja väärät tukiasemat. Järjestelmä voidaan ohjelmoida hälyttämään automaattisesti, mikäli hyökkäys tunnistetaan.

WCS käyttää Ciscon patentoimaa menetelmää jatkuvaan laittomien tukiasemien ja ad-hoc-verkkojen monitoroimiseen. Jos laittomia laitteita ilmestyy, niin WCS pystyy määrittelemään niiden sijainnin ja uhkatason. Näin administraattori voi WCS:n avulla hoitaa rosvolaitteet.

WCS sisältää myös ns. ”service policy enginen” joka mahdollistaa virtuaali-LAN:ien, RF:n, QoS:n ja tietoturvakäytäntöjen helpon luomisen. Administrator voi luoda monia uniikkeja SSID:tä joissa kaikissa on erilaiset tietoturvaasetukset. Esimerkiksi vierailijoille oma SSID, joka voidaan varmistaa webbiautentikoinnilla, mobiileille äänilaitteille voi olla oma SSID ja yrityksen työntekijöille oma SSID jossa tietoturvana voidaan käyttää 802.11i:a tai IPSec:ia. /27./

User exclusion lists

Käyttäjien määrittelyn avulla IT-henkilöstö voi käyttää WCS:aa sulkeakseen ei-toivotut käyttäjät ulos langattomasta verkosta. Tämä voidaan toteuttaa myös määräajaksi. /27./

WLAN-järjestelmän hallinta

WCS tekee siis langattoman verkon konfiguroinnin, valvomisen ja hallinnan yhtä helpoksi kuin perinteisten verkkojen hallinnan. Se mahdollistaa adminin tekemään joko yhden mallin kaikille verkossa oleville WLAN-kontrollereille ja tukiasemille, tai sitten vaikka jokaiselle omansa. WCS yhdistää kaiken oleellisen ja tärkeän informaation verkosta, kuten signaalin häiriötasot, SNR-tason, signaalin vahvuuden ja verkon topologian yhteen paikkaan. Tämä mahdollistaa mahdollisien ongelmien helpon korjaamisen.

Mahdolliset ohjelmistopäivitykset kaikkiin järjestelmässä oleviin laitteisiin on mahdollista suorittaa yhdestä paikasta WCS:n avulla. Kuten aiemmin tuli ilmi, niin WCS mahdollistaa yksittäisen laitteen tarkan etsimisen langattomasta järjestelmästä. Tämä eliminoi tarpeen manuaaliseen tietokannan konfigurointiin ja ylläpitoon ja tarjoaa tarkan informaation mm. langattoman verkon kapasiteetin riittävyydestä.

Ciscon WCS pystyy myös tarjoamaan adminille lukuisia eri raportteja mm. verkon käyttöasteesta järjestelmätietoihin, sekä asiakastiedoista radioverkon käyttöasteeseen. /27./

10 WLAN-VERKON SUUNNITTELU AHLSTROM OYJ:LLE

10.1 Ahlstrom Oyj:n esittely

Ahlstrom on johtava korkealaatuisten kuitumateriaalien kehittäjä, valmistaja ja markkinoija. Yhtiön valmistamia kuitukankaita ja erikoispapereita käytetään monissa jokapäiväisissä tuotteissa, esim. suodattimissa, hygieniapyyhkeissä, lattiamateriaaleissa, etiketeissä ja teipeissä. Ahlstromin kuituosaaminen ja innovatiivisuus ovat luoneet yhtiölle vahvan markkina-aseman monilla liiketoiminta-alueilla. Yhtiön 5 600 työntekijää palvelevat asiakkaita tuotantolaitoksilla tai myyntitoimistoissa yli 20 maassa kuudessa maanosassa. Ahlstromin liikevaihto oli 1,55 mrd. euroa vuonna 2005. Ahlstromin osake on noteerattu Helsingin Pörssin päälistalla. Yhtiön internet-osoite on www.ahlstrom.com.

10.2 WLAN-verkon suunnittelu Ahlstrom Oyj:lle

10.2.1 Työn tavoite

Projektin ideana oli toteuttaa joustava langaton verkko yrityksen konttoreille ja tehtaille, jotka sijaitsevat eri puolilla maailmaa. Ahlstromin toimistojen koot vaihtelevat yhden tukiaseman vaativista toimistoista, aina 50 tukiasemaa vaativiin kokonaisuuksiin. Ideana oli saada aikaan konttoreihin kriittiset alueet kattava langaton lähiverkko, jota voisivat käyttää sekä yrityksen työntekijät että vierailijat. Tarkoitus ei ole korvata jo olemassa olevaa ethernet-verkkoa, vaan tukea sitä liikkuvuudella. Ulkopuolisille vierailijoille tarjotaan yhteys internetiin, mutta pääsy yrityksen intranetiin estetään. Pienemmissä konttoreissa, kuten Helsinki työntekijämäärältään on, ei käytetä LWAPP-protokollaa, vaan ratkaisu toteutetaan kustannustehokkaammin käyttäen Ciscon tukiasemien ohella Juniperin palomuuri/reititintä. Ainakin Windsor Locksiin tulee WLAN-kontrollerin avulla hallinnoitavat tukiasemat. Mikkeliin

tuotantotehtaalle on myös tulossa koko tehtaan kattava WLAN-verkko, joten kontrollerin sijoittaminen sinne on myös järkevää. Yhtenä vaihtoehtona on WLAN-kytkimen sijoittaminen eri paikkakunnalle kuin tukiasemat ovat. Tässä ongelmana on kuitenkin paikkakuntien välisen yhteyden rajoittuminen 512kbps:n ADSL-yhteyteen. Tästä johtuen ongelmana voisi olla yhteyden hidastuminen, mikäli langattoman verkon käyttäjiä olisi monta ja tukiasemien ja WLAN-kontrollerin välinen liikenne olisi suuri. Esplanadin toimistolle on kaavailtu tulevan neljä Ciscon 1131AG-tukiasemaa ja yksi Juniperin Netscreen 5GT -palomuuri.

10.2.2 Työn toteutus

Työn käytännön puoli toteutettiin Ahlstromin Helsingin Esplanadin konttorilla. Työssä käytettiin kahta Ciscon 1131AG-sarjan tukiasemaa ja Juniperin Netscreen 5GT -palomuuria.

Ciscon tukiasemat konfiguroitiin niin että niillä oli kolme SSID:tä. Ensimmäinen SSID, yrityksen työntekijöille, on toteutettu käyttäen WPA2-AES-salausta ja käyttäjien autentikointi verkkoon tapahtuu IEEE 802.1X-protokollalla RADIUS-palvelimen kautta. Tämä verkko on tarkoitettu yrityksen työntekijöille ja siinä ei ole sisä- tai ulkoverkon suhteen rajoituksia. Tässä on myös tärkeää huomioida, että Windows XP SP2 käyttöjärjestelmä ei tue WPA2-salausta ilman päivitystä. Päivityksen voi hakea Microsoftin sivuilta. On tärkeää muistaa, että päivitystä ei löydy Windows update-palvelun kautta.

Toinen SSID on vierailijoille tarkoitettu ja alkuperäisen suunnitelman mukaan siinä ei olisi lainkaan salausta. Harkinnan alla on vielä jonkinlaisen WEP-salauksen käyttö. Sen tarkoitus on tarjota Ahlstromin vierailijoille pääsy julkiseen internetiin, eli sisäverkko on suljettu palomuurilla.

Kolmas SSID on tarkoitettu korvaamaan yrityksen joissakin toimistoissa jo käytössä ollut vanhentunut ja suojaukseltaan heikkoa WEP-40bit-salausta käyttänyt SSID. Se käyttää siis WEP-salausta WPA-salauksen sijaan johtuen yhteensopivuusongelmista.

Tukiasemien ja Netscreenin palomuurin väliseen yhteyteen käytettiin virtuaali-LAN:ia ja tarkemmin protokollaa IEEE 802.1Q. Tukiasemat kiinnitettiin ethernet-kaapelilla palomuurin trusted-portteihin. Netscreen 5GT -palomuuri piti päivittää versioon 5.3.0r3.0, jotta tuki VLAN-tageille saatiin. Jokaiselle SSID:lle määritettiin tukiasemasta oma VLAN-tagi. Palomuurin asetuksiin määritettiin vastaaville tageille sub-interfacet ja omat verkkoavaruudet. Nyt palomuurilta voidaan määrittää jokaiselle VLAN:lle haluttu tietoturvapolitiikka. Palomuurin untrusted-portti kytkettiin yrityksen sisäverkkoon. Palomuurin ja tukiasemien konfigurointiesimerkit ovat liitteenä. (LIITE 1 ja LIITE 2)

10.2.3 Cisco 1131AG -tukiaseman konfigurointi Ahlstrom Oyj:n käyttöön

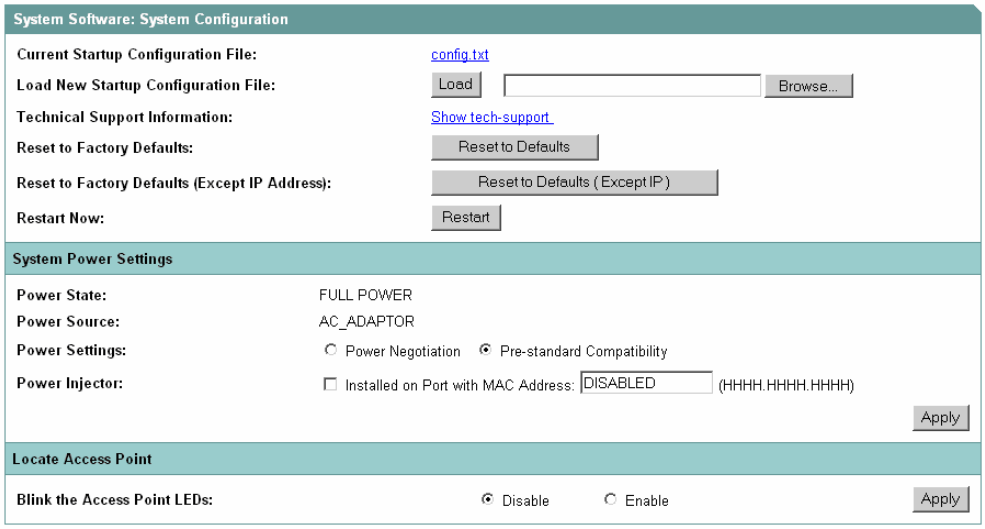
Ciscon tukiasema on tehdasasetuksilla sellaisessa tilassa, että sillä ei ole IP-osoitetta määritettynä, vaan se hakee sellaisen automaattisesti dhcp-serveriltä. Tästä syystä kun laite otetaan käyttöön, se kytketään verkkoon ja ilmoitetaan ylläpidolle tästä. Tämän jälkeen ylläpito ottaa etäyhteyden laitteeseen ja syöttää siihen oikean konfiguraation.

Config.txt-tiedoston valmisteleminen

Avataan valmis config.txt-tiedosto ja muutetaan siihen tukiaseman nimi, laitteen IP-osoite, sekä muut IP-osoitteet alueen mukaiseksi. Config.txt-tiedosto on liitteenä. Tallennetaan tiedosto.

Config.txt-tiedoston lataaminen laitteeseen

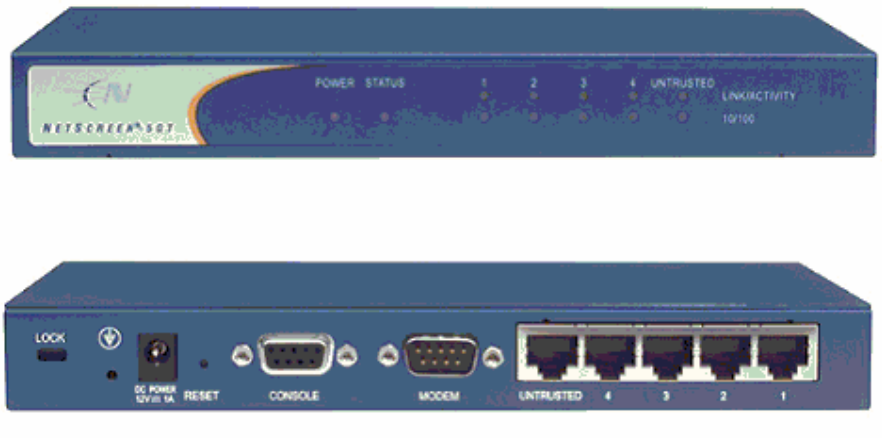
Tarkistetaan laitteen MAC-osoitteen perusteella minkä ip-osoitteen dhcp-palvelin on antanut sille. Ip-osoitteen selvittyä otetaan selainyhteys laitteeseen, oletuskäyttäjänimi on Cisco ja salasana Cisco. Oikealle avautuvasta valikosta valitaan kohta ”SYSTEM SOFTWARE” ja sen alavalikko ”System Configuration”. Avautuva näkymä on kuvan 28. mukainen.



Kuva 28. Cisco IOS system configuration

Kohtaan ”Load New Startup Configuration File:” valitaan Browse ja etsitään valmisteltu config.txt-tiedosto ja painetaan load. (HUOM! Pop-uppien tulee olla sallittuna, muuten päivitys ei onnistu!) Tämän jälkeen laite käynnistyy uudelleen ja uudet asetukset tulevat käyttöön.

10.2.4 Netscreen 5GT -palomuuri



Kuva 29. Netscreen 5GT -palomuuri edestä ja takaa

Netscreen palomuuri (Kuva 29.) on yritysluokan palomuuri jossa on yksi untrust 10/100 ethernet portti, neljä trust 10/100 -ethernet-porttia, konsoliportti ja modeemiportti. Se tukee uusimman päivityksen myötä tässä työssä tarvittua VLAN-taggingia ja siinä on sisäänrakennettu virusskanneri.

11 YHTEENVETO

Tässä insinöörityössä käsiteltiin langattomia lähiverkkoja tutustumalla ensin niiden rakenteeseen ja historiaan, sekä varsinkin niiden soveltuvuuteen yrityskäyttöön. WLAN-verkot ovat tulossa osaksi yrityksien tietoverkkoja ja ne ovat yleistymässä suurimmissa kaupungeissa tarjoten esimerkiksi kahviloiden asiakkaille ilmaisia internetyhteyksiä.

WLAN-verkkojen suurimmaksi huolenaiheeksi on muodostumassa niiden tietoturvallisuus. Nykypäivänä esimerkiksi Helsingissä on lukuisia avoimia verkkoja, joihin kuka tahansa voi kytkeytyä ja joita voi käyttää hyväkseen. Lehdistä on saanut lukea, kuinka varkaat ovat käyttäneen hyväkseen naapurin internet-yhteyttä omiin tarkoituksiinsa, kuten varojen siirtämiseen yrityksen tililtä omalleen. Tällaista tapahtumaa on hyvin vaikea jäljittää ja avoimen WLAN-verkon haltija voi helposti joutua syntipukiksi. Myös ensimmäisenä yleistynyt salausmenetelmä WEP eli wired equivalent privacy on erittäin haavoittuvainen murtoyrityksille, sillä se on hakkeroitavissa useilla internetistä löytyvillä ohjelmilla. Riittää vain että liikennettä kuuntelee tarpeeksi kauan. Uusin tekniikka tämän insinöörityön valmistuessa on WPA2 tai IEEE 802.11i, jossa salausalgoritmiksi on vaihtunut WEP:ssa ja WPA:ssa käytetyn RC4:n tilalle AES. Mikäli mahdollista, niin tätä suojausta kannattaisi aina käyttää, jotta riski tietomurroille pienenisi huomattavasti.

Työssä perehdyttiin myös LWAPP-protokollaan, joka on vahvasti ehdolla IETF:n tulevaksi CAPWAP-protokollaksi. Sitä tullaan käyttämään suurten WLAN-verkkojen hallinnoimiseen keskitetysti. On huomattavan paljon helpompaa, jos esimerkiksi 50:tä tukiasemaa voidaan päivittää ja konfiguroida uudelleen yhdestä paikasta, yhdellä kertaa verrattuna siihen että jokainen tukiasema tulisi erikseen päivittää. Tämä onnistuu WLAN-kontrollerien avulla. Langattomien tukiasemien ja kontrollerien välissä siis käytettäisiin LWAPP-protokollaa. Myös langaton kontrollointijärjestelmä WCS on tekemässä itseään tarpeelliseksi yrityksissä, jotka haluavat helposti monitoroida verkkoliikennettä ja varmistaa, että mahdolliset tunkeilijat havaitaan nopeasti ja heidän pääsynsä kriittisiin sovelluksiin estetään.

Seuraava uusi mullistus WLAN-markkinoilla tulee olemaan IEEE:n 802.11n-luonnos joka ratifioitaneen standardiksi vuonna 2007. Se tarjoaa käyttäjilleen

teoriassa jopa 600 Mbps:n nopeudet ja siinä on valmiiksi tuki monelle antennille. Käytännössä luonnoksen mukaan nopeuden tulisi olla vähintään 100 Mbps. Myös signaalin kantama tulee pitenemään standardin myötä.

VIITELUETTELO

/1/ Granlund, Kaj, *Langaton tiedonsiirto*. Docendo, 1. painos, Porvoo 2001

/2/ Reid, Neil – Seide, Ron, *802.11 (Wi-Fi) Networking handbook*. McGraw-Hill. Berkeley, California, USA 2003.

/3/ Juutilainen, Matti, *Langaton lähiverkko luentomateriaali*. Lappeenranta University of Technology. verkkodokumentti [Viitattu 14.3.2006]. Saatavissa: http://www.it.lut.fi/kurssit/03-04/010651000/luennot/wlan.pdf

/4/ Puska, Matti, *Langattomat lähiverkot*. Gummerus Oy, Jyväskylä 2005

/5/ Geier, Jim – Suom. Holttinen, Jarmo, *Langattomat verkot*. Edita, Helsinki 2005

/6/ Kurki, Jouko, *WLAN physical and MAC layer* (luentomateriaali). Helsingin AMK. verkkodokumentti [Viitattu 17.3.2006]. Saatavissa: http://opetus.stadia.fi/kurki/Courses/WirelessLAN/WLAN_course_2006/WL_6_WLAN_802_11_PHY_MAC_functions.pdf

/7/ Digitoday: *Naapurin WLAN-yhteyden luvaton käyttö ei ole välttämättä laitonta*, verkkodokumentti [viitattu 20.3.2006]. Saatavissa: http://www.digitoday.fi/showPage.php?page_id=14&news_id=47089

/8/ *Langattomat ratkaisut*, Daimler Oy, verkkodokumentti [viitattu 20.3.2006]. Saatavissa: http://www.daimler.fi/daimler/site.nsf/LookupUnikMainPages/DOMO-5ARD7D?OpenDocument

/9/ Wikipedia: *Langattoman lähiverkon tietoturva*, verkkodokumentti [viitattu 20.3.2006]. Saatavissa: http://fi.wikipedia.org/wiki/WLAN_tietoturva#WPA2_.28AES.29

/10/ WLAN-tietopankki, Dacco Oy, Verkkodokumentti [viitattu 20.3.2006]. Saatavissa: http://wlan.dacco.fi/sanasto.htm

/11/ Wi-Fi Alliance, WPA2 *Security Now Mandatory for Wi-Fi certified Products*, verkkodokumentti 13.3.2006 [viitattu 20.3.2006]. Saatavissa: http://www.wi-fi.org/opensection/news/pressrelease-031306-wpa2mandatory/

/12/ Niemi, Juha, *WLAN-turvallisuus*, 18.4.2003 Helsingin Yliopisto, Verkkodokumentti [viitattu 20.3.2006]. Saatavissa: http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf

/13/ Wikipedia: *HIPERLAN*, verkkodokumentti [viitattu 13.3.2006]. Saatavissa: http://en.wikipedia.org/wiki/HIPERLAN

/14/ Wikipedia: *Langaton Lähiverkko*, verkkodokumentti [viitattu 10.3.2006]. Saatavissa: http://fi.wikipedia.org/wiki/Langaton_verkko

/15/ Cisco systems white paper, *Understanding the lightweight access point protocol (LWAPP)*, verkkodokumentti [viitattu 8.3.2006]. Saatavissa: http://www.cisco.com/application/pdf/en/us/guest/products/ps6306/c1244/cdccont_0900aecd802c18ee.pdf

/16/ Suvanto, Ville, *WLAN-artikkeli Muropaketti*, verkkodokumentti [viitattu 15.3.2006]. Saatavissa: http://www.soneraplaza.fi/tietokoneet/artikkeli/0,2998,h-9093_a-142588,00.html

/17/ Digitoday*: D-Link siirtää älyä kytkimiin*, verkkodokumentti [viitattu 10.3.2006]. Saatavissa: http://www.digitoday.fi/showPage.php?page_id=9&news_id=29338

/18/ Cisco Systems data sheet, *Cisco wireless LAN controllers*, verkkodokumentti [viitattu 24.3.2006]. Saatavissa: http://www.cisco.com/en/US/products/ps6308/products_data_sheet0900aecd802570b0.html

/19/ Tietokone 18.1.2006, *EWC:stä tulee seuraava wlan-standardi*, verkkodokumentti [viitattu 10.3.2006]. Saatavissa: http://www.cisco.com/en/US/products/ps6308/products_data_sheet0900aecd802570b0.html

/20/ Järventie, Tomi, *Cisco Centralized WLAN solution*, PP-esitys Ahlstrom Oyj [viitattu 8.3.2006].

/21/ Cox, John, Network World, *Lightweight, standardized WLAN access*, verkkodokumentti [viitattu 21.3.2006]. Saatavissa: http://www.networkworld.com/weblogs/wireless/002679.html

/22/ Trapezenetworks IT-Glossary: *CAPWAP* verkkodokumentti [viitattu 3.5.2006]. Saatavissa: http://www.trapezenetworks.com/en/technology/glossary_1.asp

/23/ Marshall, Trevor, *Antennas enhance WLAN security*, verkkodokumentti [viitattu 28.3.2006]. Saatavissa: http://www.trevormarshall.com/byte_articles/byte1.htm

/24/ Mikro-PC, *D-Link älyttää wlan-kytkimiä*, verkkodokumentti 19.3.2004 [viitattu 28.3.2006]. Saatavissa: http://mikropc.net/uutiset/index.jsp?categoryId=atk&day=20040319

/25/ Unstrung verkkodokumentti: *LWAPP Pushed Through* 18.1.2006 [viitattu 3.5.2006] Saatavissa: http://www.unstrung.com/document.asp?doc_id=87103

/26/ IETF-verkkosivut, *Evaluation of Candidate CAPWAP Protocols*, Elokuu 2005, verkkodokumentti [viitattu 3.5.2006]. Saatavissa: http://www.ietf.org/internet-drafts/draft-ietf-capwap-eval-00.txt

/27/ Cisco Systems data sheet, *Cisco Wireless Control System*, verkkodokumentti [viitattu 24.7.2006] Saatavissa: http://www.cisco.com/en/US/products/ps6305/products_data_sheet0900aecd802570d0.html

Cisco Aironet 1130AG tukiaseman konfiguraatio

```
!
! Last configuration change at 13:21:56 GMT Mon Jul 31 2006 by Cisco
! NVRAM config last updated at 13:21:56 GMT Mon Jul 31 2006 by Cisco
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname xxxxxxxx
!
enable secret xxxxxxxxxxx
!
clock timezone GMT 3
ip subnet-zero
ip name-server xxx.xxx.xxx.xxx
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
 server xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
 server xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
 server xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
dot11 ssid ssid3
   vlan 4
   authentication open
!
dot11 ssid ssid1
   vlan 2
   authentication open eap eap_methods
   authentication key-management wpa
   guest-mode
!
dot11 ssid ssid2
```

```
   vlan 3
   authentication open
   mbssid guest-mode
!
power inline negotiation prestandard source
!
!
username Cisco password xxxxx
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 2 mode ciphers aes-ccm
 !
 encryption vlan 4 key 1 size 40bit xxxxx transmit-key
 encryption vlan 4 mode ciphers wep40
 !
 ssid ssid3
 !
 ssid ssid1
 !
 ssid ssid2
 !
 mbssid
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0
36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
!
interface Dot11Radio0.4
 encapsulation dot1Q 4
 no ip route-cache
```

```
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
 bridge-group 4 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption vlan 2 mode ciphers aes-ccm
 !
 encryption vlan 4 key 1 size 40bit xxxxxxxxxxxxx transmit-key
 encryption vlan 4 mode ciphers wep40
 !
 ssid ssid3
 !
 ssid ssid1
 !
 ssid ssid2
 !
 mbssid
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
 bridge-group 3 spanning-disabled
!
interface Dot11Radio1.4
 encapsulation dot1Q 4
 no ip route-cache
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding
 bridge-group 4 spanning-disabled
```

```
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface FastEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled
!
interface FastEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
 bridge-group 3 spanning-disabled
!
interface FastEthernet0.4
 encapsulation dot1Q 4
 no ip route-cache
 bridge-group 4
 no bridge-group 4 source-learning
 bridge-group 4 spanning-disabled
!
interface BVI1
 ip address xxx.xxx.xxx.xxx 255.255.255.0
 no ip route-cache
!
ip default-gateway xxx.xxx.xxx.xxx
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646 key
xxxxxxxxxxxxxxxx
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
!
sntp server 192.43.244.18
sntp broadcast client
end
```

Juniper Netscreen 5GT palomuurin konfiguraatio

```
set clock timezone 2
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "trust" zone "Trust"
set interface "trust.2" tag 2 zone "Trust"
set interface "trust.3" tag 3 zone "Trust"
set interface "trust.4" tag 4 zone "Trust"
set interface "untrust" zone "Untrust"
unset interface vlan1 ip
set interface trust ip xxx.xxx.xxx.xxx/xx
set interface trust nat
```

```
set interface trust.2 ip xxx.xxx.xxx.xxx/xx
set interface trust.2 nat
set interface trust.3 ip xxx.xxx.xxx.xxx/xx
set interface trust.3 nat
set interface trust.4 ip xxx.xxx.xxx.xxx/xx
set interface trust.4 nat
set interface untrust ip xxx.xxx.xxx.xxx/xx
set interface untrust route
set interface untrust gateway xxx.xxx.xxx.xxx/xx
set interface trust.2 mtu 1500
set interface trust.3 mtu 1500
set interface trust.4 mtu 1500
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface trust ip manageable
set interface trust.2 ip manageable
set interface trust.3 ip manageable
set interface trust.4 ip manageable
set interface untrust ip manageable
unset interface trust.2 manage ssh
unset interface trust.2 manage snmp
unset interface trust.2 manage ssl
set interface trust.2 manage ident-reset
unset interface trust.3 manage telnet
unset interface trust.3 manage snmp
unset interface trust.3 manage ssl
unset interface trust.4 manage ping
unset interface trust.4 manage ssh
unset interface trust.4 manage telnet
unset interface trust.4 manage snmp
unset interface trust.4 manage ssl
unset interface trust.4 manage web
set interface untrust manage ping
set interface trust dhcp server service
set interface trust.2 dhcp server service
set interface trust.3 dhcp server service
set interface trust.4 dhcp server service
set interface trust dhcp server enable
set interface trust.2 dhcp server enable
set interface trust.3 dhcp server enable
set interface trust.4 dhcp server enable
set interface trust dhcp server option lease 1440000
set interface trust dhcp server option gateway xxx.xxx.xxx.xxx/xx
set interface trust dhcp server option netmask xxx.xxx.xxx.xxx
set interface trust dhcp server option dns1 xxx.xxx.xxx.xxx
set interface trust.2 dhcp server option lease 1440000
set interface trust.2 dhcp server option gateway xxx.xxx.xxx.xxx
set interface trust.2 dhcp server option netmask xxx.xxx.xxx.xxx
set interface trust.2 dhcp server option dns1 xxx.xxx.xxx.xxx
set interface trust.3 dhcp server option lease 1440000
```

```
set interface trust.3 dhcp server option dns1 xxx.xxx.xxx.xxx
set interface trust.4 dhcp server option lease 1440000
set interface trust.4 dhcp server option dns1 xxx.xxx.xxx.xxx
set interface trust dhcp server ip xxx.xxx.xxx.xxx to xxx.xxx.xxx.xxx
set interface trust.2 dhcp server ip xxx.xxx.xxx.xxx to xxx.xxx.xxx.xxx
set interface trust.3 dhcp server ip xxx.xxx.xxx.xxx to xxx.xxx.xxx.xxx
set interface trust.4 dhcp server ip xxx.xxx.xxx.xxx to xxx.xxx.xxx.xxx
set flow tcp-mss
unset flow tcp-syn-check
set hostname ns5gt

set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set dns host dns1 xxx.xxx.xxx.xxx
set dns host dns2 0.0.0.0
set address Trust " xxx.xxx.xxx.xxx/xx" xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
set address Trust " xxx.xxx.xxx.xxx/xx" xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
set address Trust " xxx.xxx.xxx.xxx/xx" xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
set address Untrust " xxx.xxx.xxx.xxx/xx" xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set url protocol sc-cpa
exit
set policy id 3 from "Trust" to "Untrust"  " xxx.xxx.xxx.xxx/xx" "Any" "ANY" deny log
set policy id 3
exit
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit log
set policy id 1
exit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit log
set policy id 2 disable
set policy id 2
exit
set policy id 4 from "Trust" to "Trust"  " xxx.xxx.xxx.xxx/xx" "Any" "ANY" deny log
set policy id 4
exit
set global-pro policy-manager primary outgoing-interface untrust
set global-pro policy-manager secondary outgoing-interface untrust
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
set ntp server "0.0.0.0"
```

```
set ntp server backup1 "0.0.0.0"
set ntp server backup2 "0.0.0.0"
set modem speed 115200
set modem retry 3
set modem interval 10
set modem idle-time 10
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Punaisella merkityt kohdat ovat muutettu tietoturvan takia