

Vesa Lähdetkorpi

WLAN-suunnitelman laatiminen yritykselle

Opinnäytetyö

Kevät 2012

Tekniikan yksikkö

Tietojenkäsittely

Sovellustuotanto



SEINÄJOEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖN TIIVISTELMÄ

Koulutusyksikkö: Tekniikan yksikkö
Koulutusohjelma: Tietojenkäsittely
Suuntautumisvaihtoehto: Sovellustuotanto

Tekijä: Vesa Lähdetkorpi

Työn nimi: WLAN-suunnitelman laatiminen yritykselle

Ohjaaja: Erkki Koponen

Vuosi: 2012

Sivumäärä: 31

Liitteiden lukumäärä: 0

Langattoman verkon tehtävänä on yksinkertaisuudessaan tarjota tiedonsiirto käyttäjän ja lähteen välillä. Yhä kehittyvien mobiililaitteiden ja muiden kannettavien koneiden perusedellytyksenä on toimiva ja tehokas tiedonsiirto, jolloin internetin ja yritys- tai kotiverkon palvelut tulevat hyödynnettyä tehokkaasti.

Tämän opinnäytetyön tavoitteena on laatia WLAN-suunnitelma pk-yritykselle. Suunnitelma kattaa laitteet, asennuksen, tietoliikenteen sekä tietoturvan.

Menetelmänä on perehtyä langattoman verkon käsitteisiin, laitteisiin, standardeihin sekä tietoturvaan kirjallisuuden avulla. Tämän jälkeen laaditaan teoretiedon perusteella WLAN-suunnitelma pk-yritykselle.

Suunnitelman valmistelu aloitetaan hankintaperiaatteiden listauksella, jonka jälkeen esitetään kuvalla esimerkkiyrityksen pohjapiirustus. Kuvan avulla selitetään tarvittava laitteisto ja niiden asennuspaikat. Lopuksi kerrotaan laitteiden asennuksesta ja konfiguroinnista.

Suunnitelman tuloksena saatiin valmis WLAN-suunnitelma, jonka pk-yritys voi toteuttaa ohjeita hyväksi käyttäen haluamanaan aikana.

Asiasanat: WLAN, langattomat lähiverkot, standardit, tietoturva

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology
Degree programme: Business Information Technology
Specialisation: Application Production

Author: Vesa Lähdetkorpi

Title of the thesis: WLAN plan for a small and medium-sized enterprise

Supervisor: Erkki Koponen

Year: 2012

Number of pages: 31

Number of appendices: 0

The objective of this thesis was to create a WLAN-plan for a small business. The plan needed to cover the equipment, installation, communications and information security.

First, wireless networking concepts, devices, standards and information security were studied. Then, based on the theoretical information a WLAN plan was formed.

The plan started with listing the acquisition principles, which was followed by a picture of the example company's floor plan. The required wireless devices and computers were presented in this picture. Finally, installation and configuration of the hardware were explained.

The outcome of the plan was a complete WLAN-design which can be used by a small or medium-sized enterprise using the instructions in any given time.

Keywords: WLAN, wireless local area network, standards, security

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

SISÄLLYS

KÄYTETYT TERMIT JA LYHENTEET

KUVA- JA TAULUKKOLUETTELO

1 JOHDANTO	9
2 WLAN-MÄÄRITTELY JA TOIMINTAPERIAATE	11
2.1 Määrittely ja käsitteitä.....	11
2.2 Toimintaperiaate	12
3 WLAN-LAITTEET JA -STANDARDIT	14
3.1 Laitteet	14
3.2 Standardit.....	17
4 WLAN-TIETOTURVA JA SUOJAUS	20
4.1 Riskit	20
4.2 Tietoturva ja suojausmenetelmät	21
4.2.1 WEP.....	21
4.2.2 WPA.....	22
4.2.3 WPA2.....	22
5 WLAN-SUUNNITELMA YRITYKSELLE	23
5.1 Projektin aloitus.....	23
5.2 Suunnittelu ja asennus.....	23
5.2.1 Suunnittelu	24
5.2.2 Asennus	25
JOHTOPÄÄTÖKSET	30
LÄHTEET	31

KÄYTETYT TERMIT JA LYHENTEET

AES	Advanced Encryption Standard, salausmenetelmä.
Bluetooth	Lyhyen kantaman radioteknologia tiedonsiirtoon.
DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla, jakaa IP-osoitteet verkkoon kytketyille laitteille.
DSL	Digital Subscriber Line, tietoliikenneyhteys nopeaan tiedonsiirtoon.
DSSS	Direct Sequence Spread Spectrum, suorasekvenssitekniikka, hajaspektritekniikka.
EAP	Extensible Authentication Protocol, käyttäjän ja laitteen tunnistusprotokolla
FHSS	Frequency Hopping Spread Spectrum, taajuushypelytekniikka, hajaspektritekniikka.
IEEE	Institute of Electrical and Electronics Engineers, standardointijärjestö.
MAC	Medium Access Control, verkkolaitteen fyysinen osoite.
MIMO	Multiple Input and Multiple Output, monilähetintekniikka, useamman rinnakkaisen lähettimen ja vastaanottimen käyttö.

OFDM	Orthogonal frequency division multiplexing, monikan- toaaltomodulointi.
PCI	Peripheral Component Interconnect, pöytäkoneen laajen- nuskorttipaikka.
SSID	Service set identifier, langattoman lähiverkon tunnus.
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla.
WAN	Wide Area Network, tiedonsiirtoverkko, internet.
WDS	Wireless Distribution System, tekniikka usean tukiaseman yhdistämiseksi.
WEP	Wired Equivalent Privacy, ensimmäinen 802.11- standardin suojausmenetelmä.
Wi-Fi	Wireless Fidelity, langaton lähiverkko.
WLAN	Wireless Local Area Network, langaton lähiverkko.
WPA	Wi-Fi Protected Access, Wi-Fi Alliancen luoma suojaus- menetelmä.
WPA2	Tietoturvastandardi, tunnetaan myös nimellä 802.11i.

(Puska 2005; Granlund 2007.)

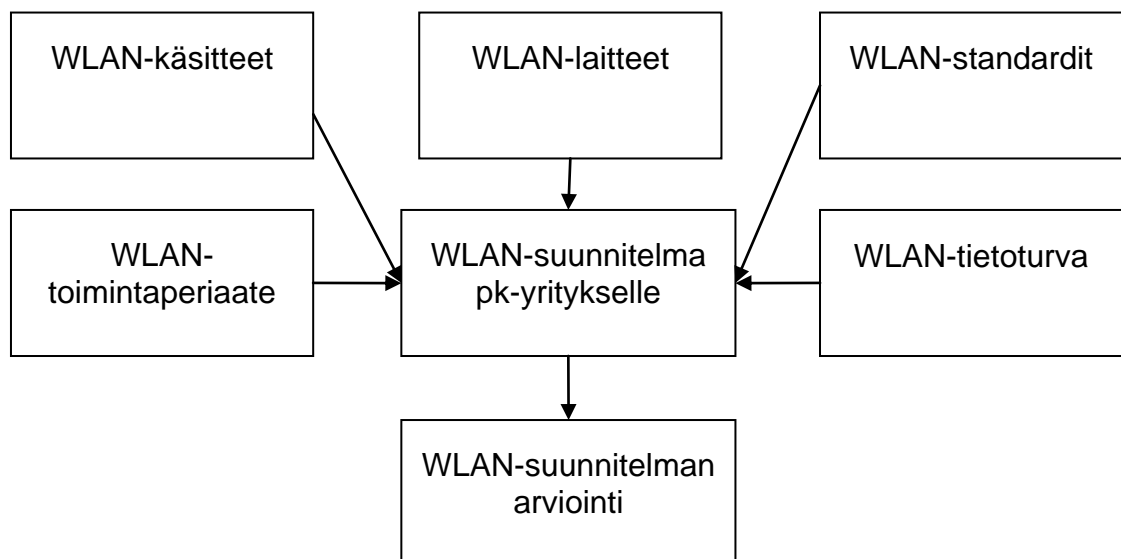
KUVA- JA TAULUKKOLUETTELO

Kuva 1. Opinnäytetyön eteneminen.	9
Kuva 2. Yksinkertainen kotiverkko. (Wi-Fi a 2012.).....	13
Kuva 3. TP-Link langaton tukiasema. (TP-Link 2012.).....	14
Kuva 4. Langattoman tukiaseman asetussivu. (Port forward 2012.).....	15
Kuva 5. ZyXEL langaton sovitin. (ZyXel 2012.).....	16
Kuva 6. Pohjapiirustus esimerkkiyrityksen tiloista.	24
Kuva 7. Tukiaseman internet-yhteyden määrittäminen.	26
Kuva 8. Tukiaseman IP-määrittäminen.	26
Kuva 9. Tukiaseman kanava-asetukset.	27
Kuva 10. Tukiaseman WDS-asetukset.	28
Taulukko 1. IEEE 802.11-sukupolvet. (Wi-Fi b. 2012.)	17

1 JOHDANTO

WLAN (Wireless Local Area Network) eli langaton lähiverkko on viime vuosina yleistynyt niin yrityksissä, kotitalouksissa kuin julkisissa rakennuksissa. Sitä käytetään paljon tiloissa, joissa halutaan tarjota langaton yhteys, kuten lentokentät ja rautatieasemat. Näissä langallinen yhteys olisi mahdoton tarjota suurelle nopeasti vaihtuvalle ihmisjoukolle. Yhä kehittyvien mobiililaitteiden myötä langattomuudesta on tullut välttämätön tiedonsiirtotie.

Tämän opinnäytetyön tavoitteena on laatia WLAN-suunnitelma pk-yritykselle. Suunnitelma kattaa laitteen, asennuksen sekä tietoturvan suunnittelun esimerkiksi yritykselle. Suunnitelman käyttöönoton toteutus jätetään kunkin pk-yrityksen itsensä toteutettavaksi.



Kuva 1. Opinnäytetyön eteneminen.

Menetelmänä opinnäytetyössä on ensin perehtyä teoriaan ja WLAN-käsitteisiin, -laitteisiin sekä -standardeihin ja kuvata WLAN-toimintaperiaate (kuva 1). Lisäksi käsitellään WLAN-tietoturvan ja suojauksen periaatteita. Teoriatiedon perusteella laaditaan pk-yritykselle WLAN-toteutussuunnitelma, joka kattaa WLAN-laitteet, -standardit, -tietoliikenteen sekä -tietoturvan.

Luvussa 2 määritellään WLAN ja kuvataan sen toimintaperiaate. Luku 3 käsittelee verkon pysyttämiseen sekä siihen yhdistämiseen tarvittavia laitteita, luvussa käydään läpi myös WLAN-standardit. Luku 4 keskittyy kuvaamaan WLAN-tietoturvaa, siihen kohdistuvia riskejä sekä käytössä olevia suojausvaihtoehtoja. Luvussa 5 laaditaan pk-yritykselle WLAN-suunnitelma. Luvussa 6 arvioidaan laadittua suunnitelmaa ja annetaan suosituksia suunnitelman toteuttamiselle.

2 WLAN-MÄÄRITTELY JA TOIMINTAPERIAATE

Tässä luvussa käydään läpi langattoman lähiverkon määritelmä, mitä sillä tarkoitetaan, kuinka se toimii ja mitä hyötyä siitä on ihmisille jokapäiväisessä elämässä.

2.1 Määrittely ja käsitteitä

Langaton lähiverkko tarkoittaa tiedon siirtämistä radioteitse eli langattomasti. Laitteet voivat yhdistää toisiinsa lähes missä tahansa ilman fyysisiä rajoituksia, ainoa kaapelointia tarvitseva laite on tukiasema, joka lähettää signaalin vastaanottaville työasemille. (Flyktman 2012.)

Langattomuuden avulla internetiä ja muita viestintäsovelluksia voidaan käyttää missä tahansa ilman fyysisiä rajoituksia. Tämä mahdollistaa liikkumisen vapauden rakennuksen eri huoneissa ja ulkona signaalin vahvuuden sen salliessa. Esimerkiksi kotonaan työhuoneessa työskentelevä ihminen voi vapaasti siirtyä laitteiston kanssa huoneesta toiseen, vaikkapa televisiota katsomaan. Suurin etu langattomassa verkossa on sen luoma liikkumisen vapaus ja kiinteistä pisteistä eroon pääsy. (Geier 2004, 3.)

Kustannuksiltaan langaton lähiverkko on edullinen tapa liittää useita erilaisia laitteita kodin tai yrityksen verkkoon ja sen kautta internetin tarjoamiin palveluihin (Hakala & Vainio 2005, 152).

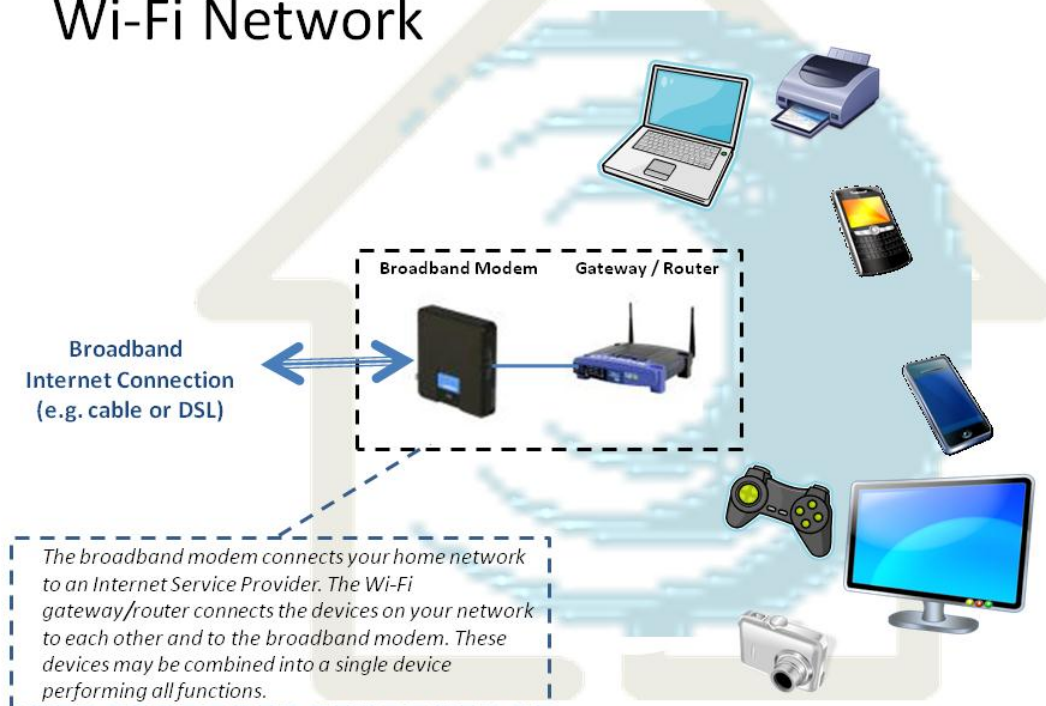
Kaapelointiin perustuvaan langalliseen lähiverkkoon verrattuna langaton ratkaisu on yleensä helpompi, nopeampi sekä halvempi niin koti- kuin yrityskäyttäjällekin. Monissa yrityksissä yleiskaapelointi on olemassa, mutta omakotitaloissa ja kerrostalohuoneistoissa on harvoin rakennusvaiheessa verkkokaapelointia mietitty. Tällöin langattomuus on oivallinen ratkaisu, kun verkko on jaettava usealle käyttäjälle. (Puska 2005, 19.)

2.2 Toimintaperiaate

Langattoman verkon liikennöinti tapahtuu ilmateitse mikroaaltoalueella, näitä samoja taajuuksia käyttävät esimerkiksi puhelimet sekä Bluetooth-laitteet. Bluetooth on lyhyen kantaman langaton verkkotekniikka, joka on kehitetty erityisesti puhelimien ja muiden pienten lisälaitteiden liittämiseen kannettavaan tietokoneeseen. Jotkin mikroaaltoja hyödyntävät laitteet, kuten mikroaaltouunit ja tutkat, saattavat aiheuttaa häiriöitä toimiessaan samoilla aallonpituuksilla. (Hakala & Vainio 2005, 153, 172.)

Verkon signaalia voivat heikentää monet fyysiset esteet sekä luonnonilmiöt. Tiheä lumi- tai vesisade saattaa laskea verkon kantamaa jopa puoleen normaalista. Kiinteistä esteistä rakennukset ovat tavallisesti signaalin esteenä, mutta myös puut sekä mäkinen maasto voivat huonontaa tai jopa estää verkon toiminnan. Kyseisten seikkojen vuoksi verkon suunnitteluvaiheessa on tärkeää kiinnittää huomiota mahdollisiin esteisiin ja sijoittaa verkon tukiasemat niiden mukaan. (Geier 2004, 38.)

Simple Wi-Fi Network



Kuva 2. Yksinkertainen kotiverkko. (Wi-Fi a 2012.)

Kuvassa 2 esitellään tyypillinen langaton kotiverkko. Langaton tukiasema yhdistää kaikki WLAN-sovittimella varustetut laitteet samaan lähiverkkoon ja laajakaistamodeemiin. Modeemi kytkee tukiaseman internetiin. Nämä kaksi laitetta voidaan myös yhdistää, jolloin yksi laite hoitaa sekä modeemin, että tukiaseman tehtäviä. (Wi-Fi a. 2012.)

Kuvan 2 kotiverkon toimintaperiaate on laajennettuna siirrettävissä myös pk-yrityksen tarpeisiin. Pienissä yrityksissä kuvan mukainen ratkaisu on täysin toimiva. Laajemmissa käyttöympäristöissä voidaan ottaa käyttöön useampia tukiasemia, jolloin saadaan laajennettua verkon peittoaluetta ja esimerkiksi yhdistettyä eri rakennusten tiedonsiirto.

Wi-Fi (Wireless Fidelity) tarkoittaa langatonta lähiverkkoa ja on Wi-Fi Alliance yhteisön tuotemerkki WLAN-tuotteille. Yhteisö jakaa sertifikaatteja lähiverkkotuotteille, jotka läpäisevät tietyt minimivaatimukset. Näin varmistetaan myös tuotteiden yhteensopivuus toistensa kanssa. (Granlund 2007, 293.)

3 WLAN-LAITTEET JA -STANDARDIT

Seuraavissa alaluvuissa kuvataan tarkemmin langattoman lähiverkon asentamiseen tarvittavia laitteita ja niiden toimintaa sekä WLAN-standardeja.

3.1 Laitteet

WLAN-tiedonsiirrossa välttämättömiä laitteita ovat langaton tukiasema sekä erilaiset päätelaitteet. Muita mahdollisesti tarvittavia välineitä ovat laajakaistamodeemi sekä erilaiset tukiaseman signaalin voimakkuutta lisäävät antennit.



Kuva 3. TP-Link langaton tukiasema. (TP-Link 2012.)

Langaton tukiasema (kuva 3) lähettää verkkosignaalin verkossa oleville tietokoneille sekä mobiililaitteille. Se yhdistää päätelaitteet lähiverkkoon sekä internetiin

laajakaistamodeemin kautta. Tukiasema on yksi langattoman lähiverkon tärkeimmistä laitteista. Aseman tukema WLAN-standardi on merkittävin valintaperuste koska siihen kytkeytyvien päätelaitteiden on tuettava samaa teknologiaa. (Hakala & Vainio 2005, 158.)

Tukiasemassa voi olla myös sisäänrakennettu laajakaistamodeemi, jolloin erillistä modeemia ei tarvita, sekä kytkin joka mahdollistaa tietokoneiden kytkemisen fyysisesti verkkokaapelilla. Laitteen sijoituspaikka kannattaa valita huolella mahdollisten esteiden välttämiseksi tukiaseman ja päätelaitteiden välillä. Tiedonsiirtonopeus saattaa heikentyä, jos laitteiden välissä on pitkä välimatka tai seiniä aiheuttamassa häiriötä. (Flyktman 2012.)

Product Page: DIR-635 Hardware Version: A1 Firmware Version: 1.07

D-Link

DIR-635 // SETUP ADVANCED TOOLS STATUS SUPPORT

INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS

WIRELESS

Wireless Network Settings

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless :

Wireless Network Name : (Also called the SSID)

Enable Auto Channel Scan :

Wireless Channel :

802.11 Mode :

Channel Width :

Transmission Rate : (Mbit/s)

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

Setting Visibility Status to Invisible is another way to secure your network. With visibility disabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

If you have enabled Wireless Security, make sure you write down the Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Kuva 4. Langattoman tukiaseman asetussivu. (Port forward 2012.)

Langatonta tukiasemaa hallitaan usein web-pohjaisella konfiguraatio sivulla, (kuva 4) josta löytyy kaikki laitteen hallintaan tarvittavat asetukset. Sivulle pääsee tu-

kiaseman ohjekirjassa kerrotusta osoitteesta ja sille kirjaututaan valmistajan määrittämällä pääkäyttäjän tunnuksesta sekä salasanalla. (Hakala & Vainio 2005, 159.)



Kuva 5. ZyXel langaton sovitin. (ZyXel 2012.)

Langattomaan lähiverkkoon yhdistämiseksi päätelaitteessa on oltava WLAN-sovitin vastaanottamassa tukiaseman lähettämää signaalia. Sovittimen koosta riippuen laite sisältää radio-osan, liittimet sekä mahdollisesti erillisen antennin signaalin vahvistamiseksi. Kannettavissa tietokoneissa sekä mobiililaitteissa WLAN-sovitin on sisäänrakennettu, mutta pöytäkoneita varten tarvitaan usein erillinen PCI-paikkaan asennettava kortti (kuva 5). (Puska 2005, 156.)

Sovittimen radio-osa sisältää lähetys- ja vastaanottoelektronikan, joka tukee kortista riippuen useampia eri WLAN-standardeja (802.11). Jotta yhteys tukiaseman ja langattoman verkkokortin välillä olisi mahdollinen, molempien laitteiden on tuettava samaa WLAN-tekniikkaa.

3.2 Standardit

Langaton lähiverkkotekniikka määritellään IEEE 802.11 -standardilla eri teknologiasukupolviin. Wi-Fi Alliance, joka koostuu keskeisistä laitevalmistajista, suunnittelee uudet tuotteet ja esittelee ne IEEE-järjestölle, joka hyväksyy uuden teknologian. Langattomat tekniikat määritellään 802.11-numerosarjalla ja eri sukupolvet erotetaan lopusta löytyvällä kirjaimella, esimerkiksi 802.11g. Kaistanleveys, suorituskyky ja taajuus ovat ominaisuuksia, jotka on määritelty verkon standardissa. Näiden toimintojen lisäksi tietoturvaa kehitetään aina eteenpäin uuden sukupolven ilmestyessä. Valmistajat saattavat myös lisätä muita ominaisuuksia standardiin, jos näkevät sen tarpeelliseksi. (Wi-Fi b 2012.)

Verrattuna lankaverkkoihin langattoman lähiverkkotekniikan kehitys on ollut erittäin nopeaa ja Wi-Fi Alliance on jatkuvasti kehittämässä nopeampia ja vikasietoisempia ratkaisuja. Laitteiden yhteensopivuus on turvattu yhdellä kaikkien laitevalmistajien käyttämällä verkkostandardilla.

Taulukko 1. IEEE 802.11-sukupolvet. (Wi-Fi b. 2012.)

Standardi	Julkaistu	Taajuusalue	Modulointi	Kapasiteetti
802.11	1997	2,4 GHz	FHSS ja DSSS	2 Mb/s
802.11a	1999	5 GHz	OFDM	54 Mb/s
802.11b	1999	2,4 GHz	DSSS	11 Mb/s
802.11g	2003	2,4 GHz	DSSS ja OFDM	54 Mb/s
802.11n	2009	5 ja 2,4 GHz	OFDM	250 + Mb/s

Taulukossa 1 on esitetty 802.11-standardien taajuusalueet, modulointitekniikka sekä teoreettinen maksimikapasiteetti. Ensimmäinen ja vanhin julkaistu standardi

oli 802.11. Se toimi 2,4 GHz:n taajuusalueella ja kapasiteetiltaan pystyi siirtämään 2 Mb/s. Modulointitekniikkana toimi FHSS (taajuushyppelyhajaspektri) ja DSSS (suorasekvenssihajaspektri). Uuden laajennuksen kehitystyö alkoi 1997 ja vuonna 1999 julkaistiin 802.11a. Se nosti teoreettisen tiedonsiirtonopeuden jopa 54 Mb/s ja toimi 5 GHz:n taajuusalueella. Laajennus toimi OFDM-modulaatiotekniikalla (Orthogonal frequency division multiplexing). Toinen vuonna 1999 julkaistuista standardeista oli 802.11b, jonka käyttämä taajuus 2,4 GHz tarkoittaa sitä, ettei se ole yhteensopiva samana vuonna julkaistun 802.11a:n kanssa. 802.11b:n maksimikapasiteetti on 11 Mb/s ja modulaatiotekniikkana toimii DSSS. (Granlund 2007, 301, 303.)

Modulaatio tarkoittaa tietokoneen digitaalisen datan muuntamista analogiseksi radiosignaaliksi, jonka jälkeen se voidaan lähettää ilmateitse. Taajuushyppely on hajaspektritekniikka, joka on alun perin kehitetty sotilaskäytössä oleviin langattomiin järjestelmiin. Taajuushyppelytekniikan etuina on mahdollisuus hyppiä nopeasti eri radiokanavilla mahdollisten häiriöiden sekä salakuuntelun välttämiseksi. Suorasekvenssitekniikassa radiosignaalin teho levitetään laajalle taajuusalueelle kertomalla lähetettävä signaali hajautusavaimella. Hajautusavain koostuu mikrosirusta, jolla on oma radiotaajuus. Tämän taajuuden ja lähetettävän datan taajuuden kertomalla saadaan voimakkaampi ja suuremmalle alueelle yltävä signaali. (Granlund 2007, 116, 117.)

Nopeille langattomille lähiverkoille soveltuu OFDM-modulaatiotekniikka sen häiriösietokyvyn sekä tehokkuuden ansiosta. OFDM-tekniikkaa kutsutaan monikaistatekniikaksi sen moduloidessa lähetettävän signaalin useisiin alikanaviin. Langattomien laitteiden yhdistämisvaiheessa yhteyden osapuolet erittelevät mahdolliset häiriöt käytettävissä olevista alikanavista, ja ongelman huomattessaan hylkäävät sen. Jäljelle jäävistä alikanavista saadaan tämän jälkeen muodostettua toimiva datayhteys. (Granlund 2007, 112.)

Vuonna 2003 julkaistiin 802.11g, joka on 802.11a:n ja 802.11b:n risteytys. Tekniikan taajuusalueena toimi 2,4 GHz, joten se on yhteensopiva vanhemman 802.11b:n kanssa. Uuden tekniikan avulla yhteensopivuus vanhemman version kanssa saatiin turvattua samalla nostaten siirtonopeuden 54 Mb/s. Toimiessaan

vanhemman version kanssa modulaatiotekniikkana käytetään DSSS-tekniikkaa, muuten käytössä on OFDM. (Granlund 2007, 305.)

Uusin standardeista ja lähes kaikissa nykyisin myytävistä laitteista löytyvä tekniikka on 802.11n. Vuonna 2009 julkaistu tekniikka lupaa keskimäärin 250 Mb/s tiedonsiirtonopeuden ja enimmillään 540 Mb/s. Nopeuden lisäksi verkon kantamaa laajennettiin huomattavasti edelliseen versioon verrattuna. 802.11n tukee 2,4 GHz:n ja 5 GHz:n taajuuksia ja on siten yhteensopiva edellisten versioiden kanssa. Standardi perustuu MIMO-antennitekniikkaan (MultipleInput and MultipleOutput) ja OFDM-monikaistatekniikkaan. Uuden antennitekniikan avulla lähetin ja vastaanotin voivat käyttää useampaa eri antennia, jolloin lähetysteho ja nopeus saadaan suuremmaksi. (Granlund 2007, 305.)

Suurimmat eroavaisuudet eri sukupolvissa tulevat modulointi- ja koodaustekniikoista. Keskenään eri tekniikat eivät ole yhteensopivia, mutta laitevalmistajat ovat varustaneet WLAN-tuotteita, jotka tukevat useampaa eri standardia ja ovat siten yhteensopivia vanhemmissakin verkoissa. (Hakala & Vainio 2005, 155.)

4 WLAN-TIETOTURVA JA SUOJAUS

Langaton lähiverkko ilman hyvää tietoturvaa ja suojausta on turvallisuusriski verkon omistajalle. Seuraavissa alaluvuissa käsitellään WLAN-riskejä sekä tietoturvan varmistamista.

4.1 Riskit

Perinteisen langallisen verkon tapaan langattomien lähiverkkojen uhat ovat ensisijaisesti samanlaisia, mutta langattomuus luo uusia mahdollisia riskejä ilman fyysistä rajoitusta. Passiiviseksi uhkiksi luetaan verkon salakuuntelu, jonka tarkoituksena on kerätä tietoa mahdollista tunkeutumista varten. Liikenteen kuuntelua ja tiedon keräämistä on vaikea estää ja mahdotonta havaita, koska tekijä voi olla pitkänkin matkan päässä. Verkon liikenteen tutkimiseen ja kuunteluun on saatavissa valmiita laitteita ja ohjelmia, joiden avulla voidaan selvittää lähiverkon turvamenettelyitä ja salauksia. (Puska 2005, 69.)

Verkkoon yrittävän tunkeutujan lähettäessä dataa tai signaalia on kyseessä aktiivinen uhka. Aktiiviseksi uhiksi luetaan verkossa liikkuvan datan häirintä tai muokaus sekä järjestelmään tunkeutuminen. Langattoman verkon tukiaseman ja muiden laitteiden ylikuormittaminen turhilla liittymis- ja palvelupyynnöillä häiritsee verkon toimintaa ja siinä toimivien laitteiden yhteyksiä. Rajoittamalla palvelupyyntöjen määrää sekä eristämällä verkko ulkopuolisilta häiriöiltä, voidaan varautua tahattomiin sekä tahallisiin uhkiin ja häiriöihin. (Puska 2005, 69.)

Langattoman verkon käyttäjän ja tukiaseman välissä kulkevan tiedon vääristyessä, eli korruptoituaessa tahattomasti, laitteet tarkastavat kyseisen datan tarkistussumman ja virheen huomattessaan hylkäävät sen. Tahallisessa tiedon muokkauksessa ja siihen käsiksi pääsyssä on kyseessä jokin ulkopuolinen taho, joka yrittää päästä

tunkeutumaan tukiaseman ja käyttäjän väliin. Sopivilla järjestelyillä ja varotoimenpiteillä mahdolliset väärinkäytökset voidaan havaita ja estää. (Puska 2005, 69.)

Passiivisia ja aktiivisia menetelmiä hyödyntäen tunkeutujan lopullinen päämäärä saattaa olla langattomaan järjestelmään hyökkääminen. Langattoman verkon ollessa yhteydessä palvelimiin ja työasemiin voi murtautujalla olla mahdollisuus päästä käsiksi näihin laitteisiin. Ulkopuolisen käsiksi pääseminen tiedostoihin ja sen huomaaminen riippuu palvelimen tietoturvasta ja suojauksesta. (Puska 2005, 69.)

4.2 Tietoturva ja suojausmenetelmät

Langattoman tukiaseman lähettämää signaalia ei voida rajoittaa vain halutulle alueelle, vaan sen sisältämä tieto on saatavissa myös rakennusten ja rajojen ulkopuolella verkon vahvuuden sen mahdollistaessa. Tästä syystä onkin suositeltavaa salata lähetettävä signaali jollain saatavissa olevista menetelmistä. Seuraavissa alaluvuissa käydään läpi mahdollisia suojausmenettelyitä, joiden käyttö mahdollistaa turvallisen WLAN-verkon.

4.2.1 WEP

IEEE 802.11 -standardi sisältää WEP-salauksen (Wired Equivalent Privacy), jolla pyritään luomaan tietoturvaltaan tehokas suojaus langattomaan verkkoon, sekä samanlaiset olosuhteet kuin perinteisessä kiinteässä lankaverkossa. Salaus tosin huomattiin pian riittämättömäksi sen heikkouden ja vanhanaikaisuuden vuoksi. (Granlund 2007, 317.)

WEP-tunnistus perustuu tukiasemiin ja päätelaitteisiin jaettuihin salausavaimiin. Salausavaimia on kahta eri pituutta, 64- ja 128-bittia. Suojausmenetelmässä ei ole automaattisesti vaihtuvia avaimia mikä edesauttaa lyhyen salausavaimen kanssa WEP-suojauksen murtamista. (Hakala & Vainio 2005, 168.)

4.2.2 WPA

WPA (Wi-Fi Protected Access) on Wi-Fi Alliancen luoma salausprotokolla, joka on luotu korvaamaan WEP:n puutteita. Suojaus kehitettiin sellaiseksi, että sen käyttöönotto onnistuu ohjelmistopäivityksellä vanhoihin WEP-laitteisiin. Suojauksessa salausavain vaihtuu automaattisesti 10 000 paketin välein, tähän käytetään TKIP-protokollaa (Temporal Key Integrity Protocol), joka parantaa tietoturvaa ja se korvaa myös monia muita WEP:n puutteita. Käyttäjien tunnistuksesta huolehtii EAP (Extensible Authentication Protocol), joka varmistaa informaation kulun oikealle käyttäjälle. (Hakala & Vainio 2005, 169.)

Tukiaseman ja päätelaitteen yhdistäessä laitteille jaetaan väliaikainen 128-bittinen salausavain. TKIP yhdistää väliaikaisen avaimen päätelaitteen MAC-osoitteen (Medium Access Control) kanssa, jonka avulla saadaan datan suojaukseen käytettävä salausavain. (Geier 2004, 183.)

4.2.3 WPA2

Viimeisin salausmenetelmä on WPA2, joka tunnetaan myös nimellä IEEE 802.11i. Siirtyminen WEP:stä WPA:han onnistui pelkällä ohjelmistopäivityksellä, mutta WPA2 toi uusia tietoturvamenetelmiä. Uusi tekniikka vaatii rautatason muutoksia elektroniikkaan, täten vanhat laitteet eivät voi toimia uudella suojauksella. Verkon liikenteen salauksesta huolehtii vuonna 2002 julkaistu AES (Advanced Encryption Standard). Nykyisin Wi-Fi Alliancen sertifioiduissa laitteissa WPA2-suojaus on pakollinen. (Granlund 2007, 321.)

WPA2:ssa käytetään AES-salausta, joka tarjoaa erittäin vahvan suojauksen langattomaan lähiverkkoon. Korkeintaan 256-bittinen salausavain on tietoturvasiantuntijoiden mukaan mahdoton murtaa ja WPA2 AES-salausta käytetäänkin monissa valtion langattomissa verkkojärjestelmissä. (Geier 2004, 184.)

5 WLAN-SUUNNITELMA YRITYKSELLE

Tässä luvussa tutustutaan esimerkkiyrityksen toimitiloihin ja suunnitellaan toimiva langaton lähiverkko, joka palvelee organisaatiota mahdollisimman hyvin edistäen liiketoimintaa.

5.1 Projektin aloitus

Yrityskäyttöön rakennettu langaton lähiverkko tehostaa käyttäjäorganisaation liiketoimintaa ja kilpailuetua. Perusvaatimukset verkon suunnitteluun tulevat yrityksen liiketoiminnasta ja käyttötarpeista. Tarpeelliset tietotekniikkapalvelut ja -sovellukset tuodaan liiketoiminnan ja käyttäjien vaatimuksista. Verkon käyttäjien, käyttötapojen, päätelaitteiden ja palveluiden perusteella saadaan muotoiltua tekniset vaatimukset langattomalle lähiverkolle samalla huomioiden ratkaisujen joustavuus, muunnettavuus ja laajennusmahdollisuudet. (Puska 220.)

Verkkosuunnitelman lisäksi ennen asennuksen aloitusta on syytä tehdä WLAN-katselmus jos asennuskohde sisältää runsaasti fyysisiä esteitä tai sijoittuu laajalle alueelle. Radioaaltojen tarkkaa kulkua on haastava ennakoida suunnitteluvaiheessa, jolloin verkon peittoalueen sekä antennien sijoituspaikkojen ja ulkoisten häiriötekijöiden kartoittaminen on tarpeen. (Puska 219.)

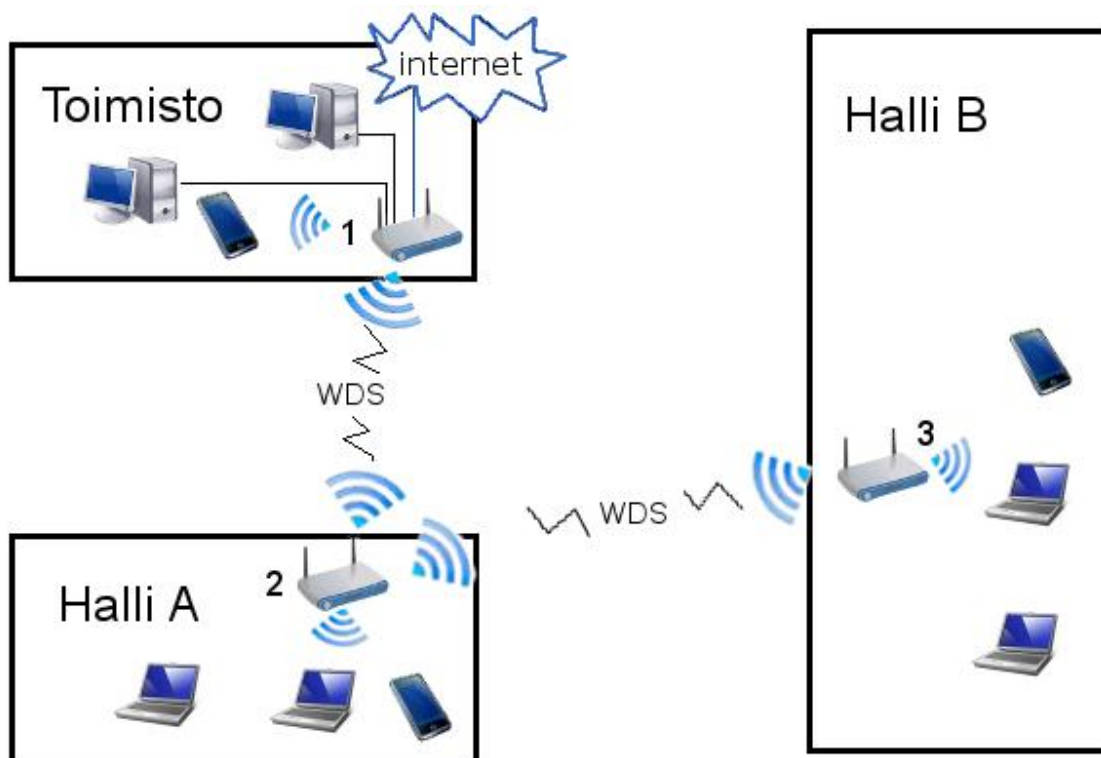
Tämän opinnäytetyön tavoitteena on muotoilla ja suunnitella tekniset vaatimukset sekä asennusohjeet langattomalle lähiverkolle pk-yrityskäyttöön.

5.2 Suunnittelu ja asennus

Seuraavissa alaluvuissa luodaan konkreettinen suunnitelma esimerkkiyrityksen langattoman lähiverkon toiminnan järjestämiseen sekä asennukseen.

5.2.1 Suunnittelu

Esimerkkiyrityksen tilanne on seuraavanlainen (kuva 6). Toimistorakennukseen tulee internetyhteys, joka on jaettu langallisesti tilassa sijaitseviin tietokoneisiin. Pihapiirissä on toimiston lisäksi kaksi muuta rakennusta, joihin olisi tarve saada langaton lähiverkko ja internetyhteys.



Kuva 6. Pohjapiirustus esimerkkiyrityksen tiloista.

Kuvassa 6 on pohjapiirustus yrityksen toimistorakennuksesta sekä kahdesta tuotantohallista. Toimistossa sijaitsevaan langattomaan tukiasemaan on liitetty verkko-kaapelilla pöytä-tietokoneita ja tukiasema on liitetty laajakaistamodeemiin. Suunnitelman mukaan tukiasema 1 jakaa langattoman verkon WDS-tekniikalla tuotantohallissa A sijaitsevaan tukiasema 2:een, jonka kautta verkko jaetaan vielä halli B:ssä sijaitsevaan tukiasema 3:een. Tuotantohalleissa käytettävät päätelaitteet voivat tämän avulla yhdistää verkkoon läheisimmästä yhdyspisteestä.

WDS-tekniikalla voidaan jatkaa langatonta verkkoa käyttämällä tukiasemia siltana tai toistimena, jolloin verkkoa voidaan laajentaa hyvinkin suurelle alueelle sekä

useisiin rakennuksiin. Verkon jatkaminen tapahtuu langattomasti, joten fyysistä kaapelointia tukiasemien välille ei tarvita. Tukiasema kommunikoi vain toisten yhteyspisteiden kanssa jos toimitilaksi on asetettu siltaavaan tilaan. WDS-verkossa olevien tukiasemien toimiessa toistimina voi niihin ottaa yhteyttä myös muut verkon alueella olevat langattomat päätelaitteet. WDS-tekniikkaa käyttävät ratkaisut ovat usein valmistajien omia kehitelmiä eivätkä siten kuulu IEEE 802.11-standardien piiriin. WDS-verkossa langattomat tukiasemat keskustelevat keskenään MAC-osoitteita käyttäen. Ennen verkon pystyttämistä on kaikkien verkkoon liitettävien tukiasemien fyysiset MAC-osoitteet selvitettävä laitteiden ohjekirjasta tai esimerkiksi tukiaseman pohjassa sijaitsevasta tarrasta. WDS-tekniikalla toteutetun verkon haittapuolina on liikenteen nopeuden lasku, joka johtuu verkkoliikenteen kierrättämisestä usean tukiaseman kautta. (Punkari 2009.)

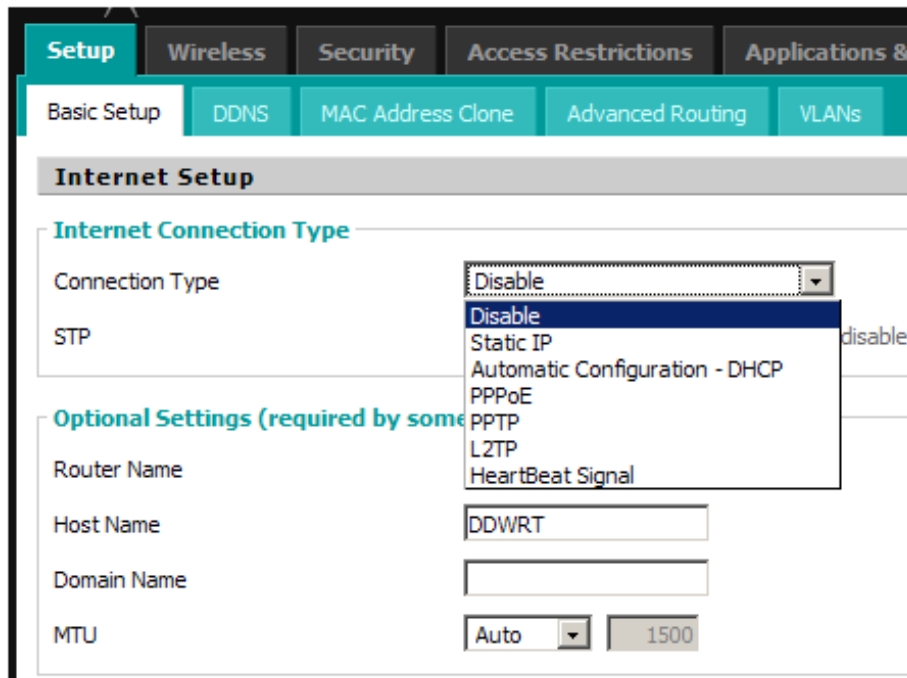
Esimerkkiyrityksen suunnitelmassa (kuva 6) hankitaan kolme saman merkkistä ja mallista tukiasemaa jotka asennetaan yrityksen eri rakennuksiin. Toimistorakennuksessa sijaitseva tukiasema toimii perinteisesti jakaen internetyhteyden tilassa sijaitseviin tietokoneisiin ja mobiililaitteisiin (kuva 2). Tähän laitteeseen konfiguroidaan tarvittavat asetukset, joiden avulla tukiaseman kommunikointi tuotantohalleissa sijaitsevien tukiasemien kanssa onnistuu. Vastaavasti halli A:ssa ja B:ssä olevat tukiasemat viritetään asianmukaisesti, jolloin ne osaavat ottaa vastaan ja lähettää dataa toimistossa sijaitsevalle tukiasemalle samalla jakaen verkon eteenpäin. Tukiasemiin kiinnitetyt antennit tarjoavat rajallisen verkon kantavuuden, joten kahden rakennuksen välisen välimatkan ollessa useita kymmeniä metrejä saataan tarvita ulkoisia antennia tehostamaan kantomatkaa. Fyysinen kaapelointi on tarpeellista vain toimistorakennuksessa, jossa tukiasema täytyy liittää internetyhteyttä jakavaan laajakaistamodeemiin.

5.2.2 Asennus

WDS ei ole standardoitu tekniikka ja jokaisella langattomia tuotteita valmistavalla yrityksellä on omat ratkaisunsa käytössä, joten käytän asennusohjeiden luomisessa avoimeen lähdekoodiin perustuvaa DD-WRT -laiteohjelmistoa. DD-WRT on vaihtoehtoinen Linux-pohjainen avoimen lähdekoodin ohjelmisto WLAN-

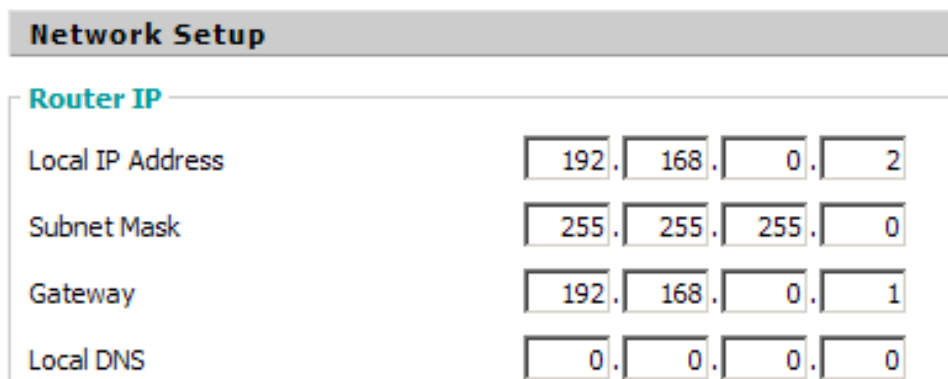
tukiasemille ja se toimii mm. Linksys, D-link ja Buffalo merkkisten laitevalmistajien tuotteissa (Dd-wrt 2012).

Tukiaseman konfigurointi alkaa kirjautumalla internet-selaimella laitteen hallintasivulle, jonka osoite löytyy aseman ohjekirjasta. Tietokoneen täytyy olla kytkettynä verkkokaapelilla tukiasemaan, jotta sivulle pääseminen olisi mahdollista.



Kuva 7. Tukiaseman internet-yhteyden määrittäminen. (Weiss 2006.)

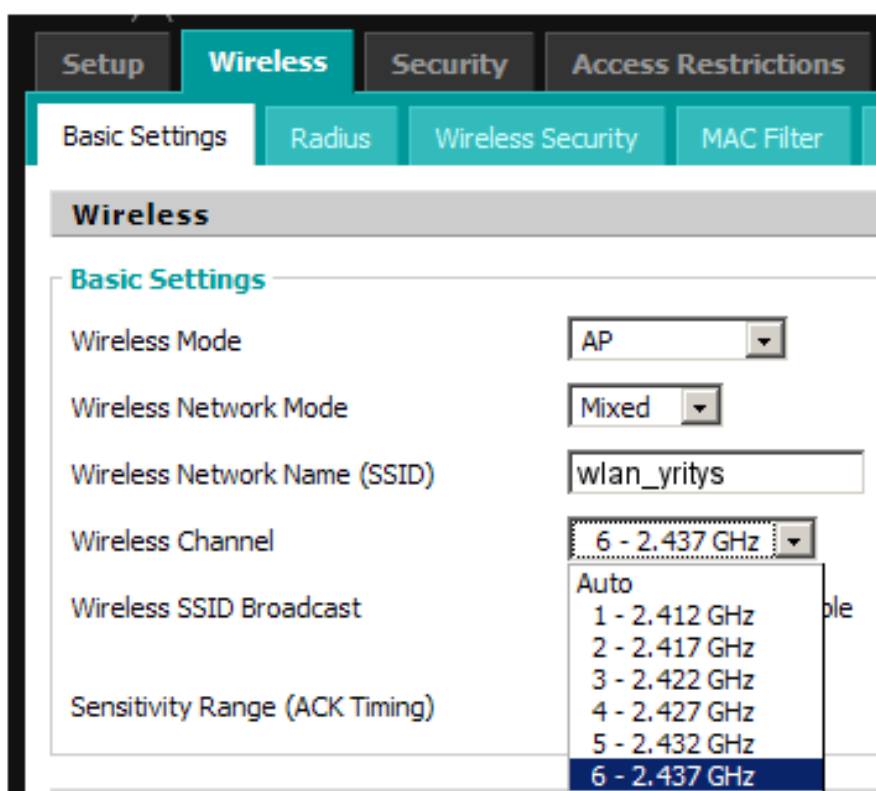
Toimistorakennuksessa (kuva 6) tukiasema 1 toimii päälaitteena jolloin se saa internet-yhteyden laajakaistamodeemilta, tukiasemien 2 ja 3 WAN-yhteydet (Wide Area Network) valitaan suljetuksi (kuva 7).



Kuva 8. Tukiaseman IP-määrittäminen. (Weiss 2006.)

Toimiakseen yhdessä tukiasemien on oltava samassa aliverkossa. Tukiasema 1:n paikallinen IP-osoite on 192.168.0.1 joten vastaavasti tukiasema 2:n osoitteeksi on asetettava 192.168.0.2 (kuva 8) ja tukiasema 3:n 192.168.0.3. Gateway-osoitteeksi tukiasema 2:een ja 3:een määritetään ensimmäisen tukiaseman paikallinen IP-osoite. Samalta asetussivulta löytyy myös DHCP-palvelimen (Dynamic Host Configuration Protocol) asetukset, joka kytketään pois 2:n ja 3:n laitteen käytöstä, jolloin ne saavat päätelaitteille tukiasema 1:n jakamat IP-osoitteet.

Seuraavaksi tukiasemat 2 ja 3 asetetaan reitittävään tilaan valitsemalla advanced setup -valikosta operating mode ja alavalikosta router. Tietoturva-asetuksista sammutetaan molempien tukiasemien palomuurit, koska se on tukiasema 1:ssä päällä ja asemat 2 ja 3 vain välittävät tiedon eteenpäin. Aina asetusten muutosten jälkeen tallennetaan tiedot sivun alalaidasta löytyvällä save-painikkeella.

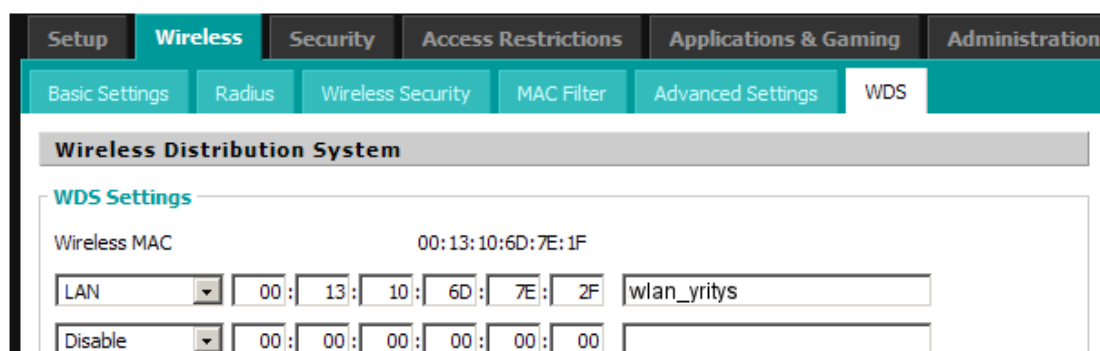


Kuva 9. Tukiaseman kanava-asetukset. (Weiss 2006.)

Kaikkien WDS-verkkoon liitettävien tukiasemien on toimittava samalla langattomalla kanavalla (kuva 9). Wireless-valikosta asetetaan jokaisen aseman langattomaksi tilaksi AP ja kanavaksi 6. Mikäli yhteyden läheisyydessä on muita langattomia

verkkoja, on suositeltavaa valita mahdollisten häiriöiden ja päällekkäisyyksien välttämiseksi eri taajuusalue. SSID (Service set identifier) eli langattoman verkon nimi määritetään kaikkiin tukiasemiin sama tunnus ja nopean yhteyden varmistamiseksi wireless network -alavalikosta valitaan N tai NG-mixed. Langattoman verkon toimiessa N-tilassa saadaan myös käyttöön tehokas WPA2-suojaus.

Ennen asemien WDS-asetuksien määrittämistä sammutetaan konfiguroinnin ajaksi laitteiden langattoman verkon suojaus, jolloin pystytään varmistamaan laitteiden toimivuus ilman häiriöitä. Tukiasema 1:stä myös kytketään pois MAC-filteröinti.



Kuva 10. Tukiaseman WDS-asetukset. (Weiss 2006.)

WDS-asetusten (kuva 10) määrittämiseen tarvitaan jokaisen tukiaseman MAC-osoite, joka yleensä löytyy laitteen pohjasta tai WDS-asetussivulta. Tukiasema 1:en WDS-sivulta valitaan pudotusvalikosta LAN sekä syötetään tukiasema 2:sen MAC-osoite ja verkkotunnus. Tukiasema 2:n WDS-asetuksiin syötetään sekä aseman 1 ja 3 MAC-osoitteet ja vastaavasti kolmanteen tukiasemaan määritellään toisen aseman tiedot.

Asetusten määrittämisen jälkeen tiedot tallennetaan ja laitteet käynnistetään uudelleen, jonka jälkeen tukiaseman WDS-taulukossa näkyy kaikki verkkoon kytketyt yhdyspisteet ja niiden välillä siirretyt datapaketit. Kun yhteyden toimivuus laitteiden välillä on varmistettu, otetaan jokaisen tukiaseman suojaus ja tietoturva käyttöön. Kaikkiin asemiin määritellään WPA2-salaus ja yhteyden varmistamisen jälkeen tukiasemat siirretään niille varattuihin kohteisiin.

Tukiasemien paikoilleen asettamisen jälkeen tarkistetaan yhteys laitteiston välillä ja onnistuneen yhteydenmuodostuksen jälkeen langaton lähiverkko on käyttövalmis. Tuotantohalleissa sijaitsevat kannettavat tietokoneet sekä mobiililaitteet voivat nyt yhdistää langattoman verkon avulla internetiin sekä samaan lähiverkkoon kuin toimistorakennuksessa olevat pöytätietokoneet.

JOHTOPÄÄTÖKSET

Opinnäytetyön tuloksena saatiin valmis langattoman lähiverkon suunnitelma pk-yrityksen käyttöön. Tavallinen kodin ja pienen alueen langaton lähiverkko laajennettiin yrityskäyttöön soveltuvaksi ja siinä toimivaksi. Verrattuna perinteiseen langalliseen vaihtoehtoon langattomasta saadaan yhtä luotettava ja turvallinen mutta paljon kustannustehokkaampi ratkaisu ilman kaapelien asennusta. Langattomuus mahdollistaa työntekijöiden vapaan liikkumisen ja sen myötä tehostuneen tuotannon ja työnteon. Mahdollisia ongelmatilanteita saattaa ilmetä mm. laiterikkojen myötä, mutta verkko on suunniteltu siten, että siinä olevat laitteistot on helppo korvata uusilla ja toimivilla välineillä.

Suunnitelma luotiin esimerkkiyritykselle ja näkisin sen olevan toteutettavissa monessa pk-yrityksessä, jolla on tarvetta langattomaan verkon laajentamiseen rakennusten välille. Projektin käyttöönotto on mahdollista myös kotioloissa, koska tarvittavat välineet ja ominaisuudet löytyvät myös kuluttajaluokan laitteistoista.

Asennusvaiheessa on syytä tarkastaa mahdolliset esteet ja häiriöt jotka voivat häiritä verkon signaalin kulkua. Ennen tukiasemien asennusta paikoilleen on syytä konfiguroida ne samassa paikassa yhteyden varmistamiseksi sekä turhan laitteiden välisen kulkemisen välttämiseksi. Tiheään asutulla alueella saattaa ongelmaiksi nousta vapaan langattoman taajuuden löytäminen ja ruuhkautuminen.

WLAN-suunnitelmasta muodostui pitkälle saman luontoinen, jota olin ennen opinnäytetyön aloittamista hahmotellut. Tukiasemien yhdistämisessä käytetty WDS-tekniikka oli pääpiirteittäin tiedossani ennen työn aloitusta ja sen yksityiskohdat selkenivät opinnäytetyön edetessä.

LÄHTEET

Dd-wrt. 2012. About DD-WRT. [Verkkosivu]. [Viitattu 28.5.2012]. Saatavissa: <http://www.dd-wrt.com/site/content/about>

Flyktman, R. 2012. Langaton verkko. [Verkkosivu]. [Viitattu 24.4.2012]. Saatavissa: http://laitetekniikka.com/tietokone/langaton_verkko.html

Geier, J. 2004. Langattomat verkot. Holttinen, J. Helsinki: IT Press.

Granlund, K. 2007. Tietoliikenne. Jyväskylä: Docendo.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Port forward. 2012. Langattoman tukiaseman asetussivu. [Verkkosivu]. [Viitattu 7.5.2012]. Saatavissa: http://screenshots.portforward.com/Dlink/DIR-635/Wireless_Settings.htm

Punkari, V. 2009. Verkon laajennus WLAN tekniikalla. [Verkkosivu]. [Viitattu 24.5.2012]. Saatavissa: http://www.wpk.tpu.fi/Tutkinto/seminaariin/Seminaari_Vesa_Punkari.pdf

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Talentum media Oy.

TP-Link. 2012. Langaton tukiasema. [Verkkosivu]. [Viitattu 7.5.2012]. Saatavissa: <http://uk.tp-link.com/products/details/?categoryid=238&model=TL-WR1043ND>

Weiss, A. 2006. DD-WRT. [Verkkosivu]. [Viitattu 28.5.2012]. Saatavissa: <http://www.wi-fiplanet.com/tutorials/article.php/3628576/>

Wi-Fi a. 2012. Simple home network. [Verkkosivu]. [Viitattu 17.4.2012]. Saatavissa: <http://www.wi-fi.org/discover-and-learn/simple-home-network>

Wi-Fi b. 2012. Discover and Learn. [Verkkosivu]. [Viitattu 17.4.2012]. Saatavissa: <http://www.wi-fi.org/discover-and-learn>

ZyXel. 2012. Langaton sovitin. [Verkkosivu]. [Viitattu 5.5.2012]. Saatavissa: http://www.zyxel.com/fi/fi/products_services/nwd310n.shtml?t=p

