VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Lauri Karhu

Langattoman lähiverkon suunnittelu ja toteutus

Case päiväkoti Punahilkka

Liiketalous ja matkailu
2011

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Lauri Karhu
Opinnäytetyön nimi	Langattoman lähiverkon suunnittelu ja toteutus
Vuosi	2011
Kieli	suomi
Sivumäärä	35
Ohjaaja	Antti Mäkitalo

Tämän työn tarkoituksena oli suunnitella ja toteuttaa langaton lähiverkko sekä tutustua sen eri osa-alueisiin ja tekniikkaan. Työ tehtiin Vaasan kaupungin atk-osaston toimeksiantona vaasalaiseen päiväkoti Punahilkkaan.

Langattomat lähiverkot ovat nykyään suosittuja ratkaisuja, sillä ne tarjoavat käyttäjille mahdollisuuden joustavaan ja liikuteltavaan työskentelyyn. Työvälineet kehittyvät koko ajan langattomampaan suuntaan, jolloin langattoman lähiverkon tarve kasvaa.

Tutkimus aloitettiin tutustumalla langattomien lähiverkkojen historiaan, keskeisimpiin standardeihin sekä tietoturvaan. Langattoman lähiverkon turvallisen käyttämisen mahdollistamiseksi tietoturvaan on syytä kiinnittää erityistä huomiota.

Lisäksi työssä käydään läpi langattomien lähiverkkojen tekniikkaa ja tutustutaan yhteen tapaan toteuttaa langaton lähiverkko. Työssä esitellään eri vaihtoehtoja, miten suunnitella langattoman lähiverkon toteutus.

Työssä suunniteltiin ja toteutettiin langaton lähiverkko, joka mahdollistaa usean eri verkon käyttämisen. Usean eri verkon käyttäminen mahdollistaa hallinto-, opetus- sekä vierailijaverkon käytön.

Avainsanat langaton, lähiverkko, tietoturva, suunnittelu

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Lauri Karhu
Title	Designing and Creating a Wireless Local Area Network
Year	2011
Language	Finnish
Pages	35
Name of Supervisor	Antti Mäkitalo

The aim of this thesis was to design and create a wireless local area network (WLAN) and become acquainted with the different parts and techniques of WLAN.

WLAN is currently a popular solution because it enables flexible and transferable working. WLANs are needed more and more at workplaces as the development of the computing devices has become wireless.

The research was started by exploring the history, standards and data security of WLAN. To make sure that the use of the WLAN is safe data security must be well planned and selected.

In this thesis techniques of the WLAN were reviewed. Also, one way to create WLAN was explored. Thesis also shows different options to design it. The WLAN was designed and created in this thesis for broadcasting various networks with different features such as educational, guest and intra networks.

Keywords Wireless, Local Area Network, Data Security, Designing

SISÄLLYS

KÄSITELUETTELO

AES	Advanced Encryption Standard, lohkosalausmenetelmä
BSS	Basic Service Set, yhden tukiaseman verkkoinfrastruktuuri
DHCP	Dynamic Host Configuration Protocol, protokolla, joka jakaa verkossa IP-osoitteita
DoS	Denial of Service, palvelunestohyökkäys
DSSS	Direct Sequence Spread Spectrum, suorasekvenssihajaspektri
EAP	Extensible Authentication Protocol, tunnistusprotokolla
ESS	Extended Service Set, verkkoinfrastruktuuri, joka muodostuu useasta BSS-verkosta
ICV	Integrity Check Value, WEP-salauksessa käytettävä eheystarkiste
IEEE	The Institute of Electrical and Electronics Engineers, kansainvälinen sähköinsinööriliitto
LWAPP	Light Weight Access Point Protocol, tukiasemien ja tukiasemaohjaimen eli kontrollerin välillä käytettävä protokolla
OFDM	Orthogonal Frequency Division Multiplexing, ortogonaalinen taajuusjakomultipleksointi
PoE	Power over Ethernet, Ethernet-kaapeloinnin kautta tapahtuva virransyöttö
RC4	Rivest Cipher 4, WEP-salauksessa käytettävä salausalgoritmi
RF	Radio Frequency, radiotie
TKIP	Temporal Key Integrity Protocol, WLAN-salaustekniikka
WLAN	Wireless Local Area Network, langaton lähiverkko

1 JOHDANTO

Langattomilla lähiverkoilla on tärkeä rooli useissa työorganisaatioissa. Langattomat verkot ovat yleistyneet vauhdilla viime vuosina, sillä kehitys kulkee jatkuvasti mobilisoituvaan suuntaan. Langaton lähiverkko tarjoaa kiinteän verkon rinnalle jaettavuudeltaan joustavamman vaihtoehdon. Langattoman verkon etuja ovat jaettavuuden lisäksi langallisiin verkkoihin nähden kustannustehokkuus ja helppokäyttöisyys.

Tekniikka on kehittynyt aina vain langattomampaan suuntaan. Kannettavat tietokoneet sekä erilaiset mobiililaitteet, kuten älypuhelimet ja taulutietokoneet, ovat nykyisin keskeisimpiä työvälineitä. Nämä laitteet antavat mahdollisuuden liikkuvuuteen ja luovat tarpeen langattomalle verkolle.

Tässä työssä keskityn langattoman lähiverkon suunnitteluun ja toteutukseen. Työssä käyn läpi langattoman verkon suunnittelua ja toteutusta niin teorian kuin käytännön osalta. Teoriaosuuden kautta esittelen langattoman lähiverkon syntyä, tekniikkaa, yleisimpiä standardeja sekä sen tietoturvaa. Langattoman lähiverkon turvallisuus on nykyään yksi tärkeimmistä asioista käyttöönotossa.

Työ toteutetaan Vaasan kaupungin ATK-osaston toimeksiantona vaasalaiseen päiväkotiin, jossa langattoman lähiverkon tarve on huomattu. Langaton lähiverkko tukee olemassa olevaa Ethernet-verkkoa ja mahdollistaa mobilisoituvien työvälineiden käytön. Lisäksi langaton lähiverkko antaa mahdollisuuden joustavampaan työntekoon. Työssä käytän Vaasan kaupungin käytössä olevaa tekniikkaa ja noudatan kaupungin yleisiä laitestandardeja sekä toimintatapoja.

Tutkimuksen ongelmana on, miten ratkaista laajan organisaation keskitetty langattomien lähiverkkojen hallinta. Ongelman ratkaisemiseksi esittelen kontrolleripohjaisen toteutuksen. Hallittavuutta parannetaan etähallintajärjestelmällä ja LWAPP-protokollaan perustuvilla tukiasemilla. Työ esittelee yhden lähestymistavan suunnitella ja toteuttaa langattomia lähiverkkoja.

2 LANGATON LÄHIVERKKO

2.1 Historiaa

Langattoman lähiverkon eli WLAN (Wireless Local Area Network) tekniikan synnyn mahdollisti Motorolan valmistama Altair 1980-luvun puolivälissä. Tuolloin käytössä olleet tekniikat olivat pääsääntöisesti valmistajakohtaisia. IEEE (Institute of Electrical and Electronics Engineering) aloitti vuonna 1990 WLAN-standardikehityksen ja ensimmäinen standardi julkaistiin vuonna 1997. Tämä standardi tunnetaan nimellä 802.11-standardi. Nykyisin suosituimmat standardit ovat 802.11b, 802.11g, 802.11n. (Puska 15–16)

2.2 Langattoman lähiverkon tekniikka

Langattoman verkon suurin ero perinteiseen Ethernet-verkkoon on käytössä oleva siirtotie. Langallisissa Ethernet-verkoissa tieto siirtyy kaapeloinnin vuoksi sähköjännitteen avulla. WLAN-verkoissa tiedon siirtämiseen käytetään joko radiotaajuksia eli RF-signaaleja tai valosignaaleja, jolloin tieto siirtyy ilmatiessä näkymättömästi (Geier 69).

RF-signaali on ilmateitse käytetty sähkömagneettinen aalto, jonka avulla tieto saadaan siirrettyä laitteesta toiseen. Radiotaajuus on maailmassa yleisin käytössä oleva tapa kuljettaa tietoa langattomasti. (Geier 70)

Valosignaali on harvemmin käytetty tapa langattomissa verkoissa. Valosignaalia käytetään langattomissa verkoissa yleensä lyhyillä matkoilla tai esimerkiksi rakennusten välisissä yhteyksissä. (Geier 76)

Kummatkin tiedon siirtämisessä olevat signaalit ovat alttiita häiriölle eli niin sanotulle interferenssille. Interferenssilähteitä on monia, mutta tyypillisimpiä ovat mikroaaltouunit sekä langattomat puhelimet, jotka voivat aiheuttaa häiriötä signaaliin. Interferenssi on yksi tärkeimpiä syitä suunnitella langaton lähiverkko huolellisesti. (Geier 87)

2.3 Langattoman lähiverkon keskeisimmät standardit

Standardien tärkein tavoite on mahdollistaa eri valmistajien laitteiden toimiminen yhdessä. Langattomat lähiverkot perustuvat 802.11 standardiperheeseen, joka sai alkunsa 1997. Tällöin julkaistiin ensimmäinen 802.11-standardi (Geier 118).

Vuonna 1997 julkaistu 802.11-standardi tarjosi enimmäisnopeudekseen 2 Mbps. 802.11-standardi sai vuonna 1999 jatkoa 802.11b-standardista, joka oli tullessaan suurempinopeuksinen laajennus olemassa olleelle 802.11-standardille. 802.11b:ssä enimmäisnopeus on teoreettisesti 11 Mbps. 802.11b-standardi on edistänyt ominaisuuksillaan langattoman lähiverkon kysyntää ja kasvua. Käytössä oleva taajusalue on täysin sama kuin 802.11b:n edeltäjässä eli 2.4 GHz. 802.11b-tukiasemia sekä verkkokortteja on ollut markkinoilla vuodesta 1999, tästä syystä useimmat nykyisin käytössä olevat langattomat verkot tukevat kyseessä olevaa standardia (Geier 126).

802.11b-standardi sai jatkoa vuonna 2003, kun IEEE julkaisi uuden 802.11g-standardin. 802.11g on täysin yhteensopiva edeltäjänsä kanssa. Tämän standardin teoreettiseksi nopeudeksi saatiin 54 Mbps. (Geier 127) 802.11g toimii samaisella 2.4 GHz:n taajudella, mutta 802.11b:n käyttämän DSSS:n (suorasekvenssihajaspektri) sijaan 802.11g käyttää OFDM:ää (Orthogonal Frequency Division Multiplexing). OFDM-tekniikka perustuu alasignaaleihin, jotka kulkevat rinnakkain. Jaetut signaalit siirretään samanaikaisesti eri taajuuksilla. (Puska 40–41) 802.11g-standardin edut ovat yhteensopivuus 802.11b:n kanssa, eli mikäli käytössä on ollut 802.11b yhteensopivia laitteita onnistuu niiden päivittäminen 802.11g-laitteisiin vaivatta (Geier 127).

802.11n-laajennuksen tarkoituksena on tarjota entistä parempi suorituskyky aiempiin standardeihin verrattuna. IEEE julkaisi 802.11n-standardin vuonna 2009. Tämä laajennus on täysin yhteensopiva 802.11b:n ja 802.11 g:n kanssa, mutta yhteensopivuustilassa käytössä oleva nopeus on vanhemman standardin määräämä. Standardin teoreettiseksi nopeudeksi luvataan 250 Mbps, joten käytännössä nopeus on 100 Mbps, eli sama kuin perinteisellä Ethernetillä (Wikipedia 2011).

Tärkeä standardi WLAN:in historiassa on myös vuonna 2004 julkaistu 802.11i, tietoturvastandardi, joka, tarjoaa paremmat tietoturvamahdollisuudet vanhojen standardien sijaan. Standardi, joka tunnetaan nimellä WPA2, jonka ominaisuuksia käydään tarkemmin läpi luvussa kolme. 802.11i-standardi parantaa aikaisempia tietoturvaominaisuuksia ja ne on määritelty standardiksi. Standardin käyttöönotosta saattaa aiheutua lisäkustannuksia, sillä toimiakseen oikein se edellyttää yhteensopivia laitteita (Granlund 317).

2.4 Langattoman lähiverkon kanavat

Langattoman verkon tukiasemat voivat käyttää Euroopassa 13 eri kanavaa, joilla on eri taajuudet. Kanavat jakautuvat taajuuksien mukaan eli jokaisella kanavalla on käytössä tietty taajuus. Tukiasemissa Wifi-sertifikaatti vastaa kanavien yhteensopivuudesta. Kun yksi kanava ruuhkautuu usean tukiaseman langattomassa ratkaisussa, vaihdetaan tukiasemaan, joka käyttää toista kanavaa. Alla oleva taulukko osoittaa eri kanavat ja niiden käyttämät taajuudet (Puska 45–46).

Tukiasemat voidaan määritellä käyttämään yhtä tiettyä kanavaa, jolloin jokaisella sarjassa olevalla tukiasemalla on oma kanava. Kontrolleripohjaisessa ratkaisussa tukiasemat voivat käyttää automaattista kanavan hakua, jolloin kontrolleri määrittää kanavat. Kontrolleripohjaisuudesta kerron lisää kappaleessa neljä.

Kanava	Taajuusalue
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

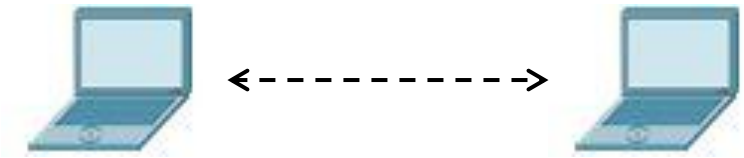
Taulukko 1. Kanavat ja taajuusalueet

2.5 Langattoman lähiverkon topologiat

Topologialla tarkoitetaan tapaa, jolla eri laitteet on kytketty toisiinsa (Granlund 77).

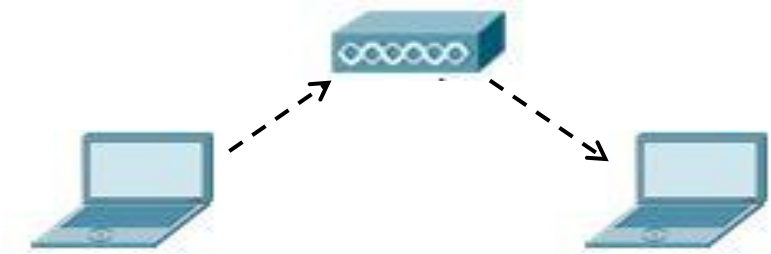
Langattomat verkot mahdollistavat kolme erilaista variaatiota siitä, miten laitteet kytkeytyvät toisiinsa. Perusarkkitehtuuri tunnetaan nimellä BSS (Basic Service Set), joka koostuu joukosta laitteita. Nämä laitteet kykenevät kommunikoimaan keskenään BSS:n suositusten mukaisesti (Granlund 294).

IBSS (Independet Basic Service Set) on eri laitteiden muodostama verkko, joka ei kytkeydy lainkaan kiinteään verkkoon. IBSS-verkosta käytetään tunnetummin nimitystä Ad-Hoc-Network. IBSS-verkko on yleensä rakennettu tilapäiseksi vaihtoehdoksi tiettyä tarvetta varten, esimerkiksi toiseen tietokoneeseen liitettyyn tulostimeen halutaan tulostaa toiselta tietokoneelta. Tässä tapauksessa laitteet kommunikoivat keskenään ilman kiinteätä verkkoa, esimerkiksi langatonta lähiverkkoa. Ad-Hoc -verkossa ei käytetä lainkaan tukiasemaa, kuten kuvio 1. osoittaa. Laitteet liikennöivät toistensa kanssa suoraan muodostaen vertaisverkon (Geier 117).



Kuva 1. Ad-Hoc -verkko

Kun käytössä ovat kiinteä tukiasema ja siihen liitetyt muut laitteet, kuten kannettavat tietokoneet, kyseessä on BSS eli Basic Service Set -verkko. Laitteiden välinen kommunikointi tapahtuu tukiaseman kautta. Tukiaseman kautta tapahtuva kommunikointi on esitetty kuviossa 2. (Granlund 295)



Kuva 2. BSS-verkko

ESS (Extended Service Set) on BSS-verkosta laajennettu kokonaisuus, joka muodostuu useista runkoverkkoon kytketyistä tukiasemista. ESS on hyvin yleinen käytäntö luoda langattomia verkkoja, jotka kattavat esimerkiksi koko rakennuksen, jolloin käyttäjät voivat liikkua laitteineen vapaasti huomaamatta tukiasemavaihdoksia. ESS-verkko on esitetty kuviossa 3. (Granlund 296)

Kuva 3. ESS-verkko

2.6 LWAPP

LWAPP eli Lightweight Access Point Protocol -tukiasemia ohjataan yleisesti kontrolleripohjaisesti. Kontrolleri on verkon aktiivilaite, minkä tehtävänä on yksinkertaistaa langattomien verkkojen ylläpitoa ja käyttöä. Kontrolleripohjaisen ratkaisun avulla verkkoa voidaan hallita keskitetysti. Kontrolleripohjainen ratkaisu mahdollistaa LWAPP-protokollaan pohjautuvien LAP eli Lightweight Accespoint tukiasemien käytön, jolloin tukiasemat rekisteröityvät kontrolleriin ja siirtä-

vät hallintansa kontrollerille, joka puolestaan siirtää tietoliikennepaketit langallisen ja langattoman verkon välillä (Cisco 2011).

LWAPP on protokolla, jonka tärkein tehtävä on tukiaseman ja tukiasemakontrollerin välisen kommunikaation määritteleminen. LWAPP-protokolla on IETF:n-RCF 5412 sertifioitu protokolla. LWAPP-tukiasemat saavat asetuksena suoraan kontrollerilta. LWAPP-protokolla on nykyään Cisco Systems:n kehityksenalainen (Gråsten 18).

Protokollan tärkein ominaisuus on useiden tukiasemien yhtäaikainen hallittavuus. Käytössä olevia tukiasemia ei tarvitse konfiguroida, vaan asetuksista vastaa kontrolleri. Kyseisen tekniikan avulla verkon valvonta ja vianetsintä on paljon vaivattomampaa ja nopeampaa. Kontrollerin kanssa toimiakseen tukiasemien täytyy tukea LAP (Lightweight Access Point) ominaisuutta, että kontrolleri osaa antaa oikeat asetukset verkon tukiasemille (Gråsten 19).

Rekisteröityäkseen oikein kontrolleriin LAP-tukiasema käyttää LWAPP-protokollaa. Tukiasemien ja kontrollerin välinen kommunikointi tapahtuu OSI-mallin toisella ja kolmannella kerroksella. Liityttyään kontrolleriin tukiasema saa Firmware-ohjelmiston, joka on kontrolleripohjainen. Kontrolleri määrää käytettävän Firmware-version LWAPP-pohjaisissa ratkaisuissa. LWAPP-protokolla käyttää liikenteen varmistamiseksi Secure Key Distribution -menetelmää (Cisco 2011).

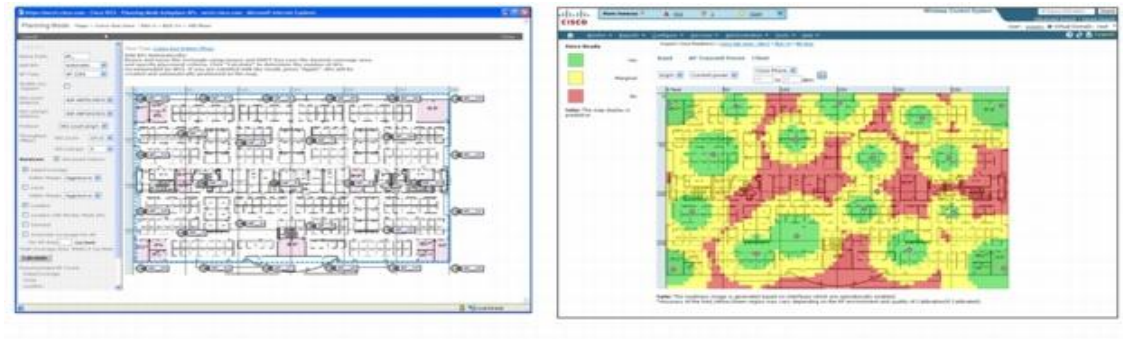
2.7 Cisco WCS -etähallintajärjestelmä

WCS eli Wireless Control System on Cisco Systems:in kehittämä ratkaisu langattomien lähiverkkojen hallintaan. Järjestelmän avulla verkon hallinta varsinkin isoissa organisaatioissa helpottuu huomattavasti. WCS-etähallintajärjestelmä on suunniteltu toimimaan kontrollereiden kanssa, jolloin etähallintajärjestelmällä hallitaan kontrollereita jotka hallitsevat tukiasemia (Cisco 2011). Alla olevassa kuvassa esitetään WCS-järjestelmän hallintasivu ja suunnittelussa käytettävä lämpökartta.

Kuva 4. WCS-hallintasivu ja lämpökartta (Cisco 2011)

WCS on palvelinalustainen upotettu tietokanta. WCS:n avulla voidan hallita useita eri langattoman lähiverkon kontrollereita. WLAN kontrollerit mahdollistavat puolestaan useiden tukiasemien hallittavuuden (Cisco 2011).

WCS-etähallintajärjestelmä auttaa myös langattomien verkkojen suunnittelussa ja toteutuksessa. Langattoman lähiverkon suunnittelemisen helpottamiseksi järjestelmään voidaan liittää omia karttapohjia. Järjestelmän avulla voidaan suunnitteluvaiheessa myös optimoida peittoalueita siirtelemällä tukiasemia haluttutuihin paikkoihin. WCS:n avulla jokainen kontrolleriin liittynyt tukiasema voidaan konfiguroida juuri halutulla tavalla (Cisco 2011). Alla olevassa kuvassa on esitetty WCS-järjestelmän suunnittelusivusto, jonne voidaan ladata haluttu karttapohja ja sijoittaa siihen tukiasemia. Sivusto helpottaa löytämään mahdolliset peittoalueet.



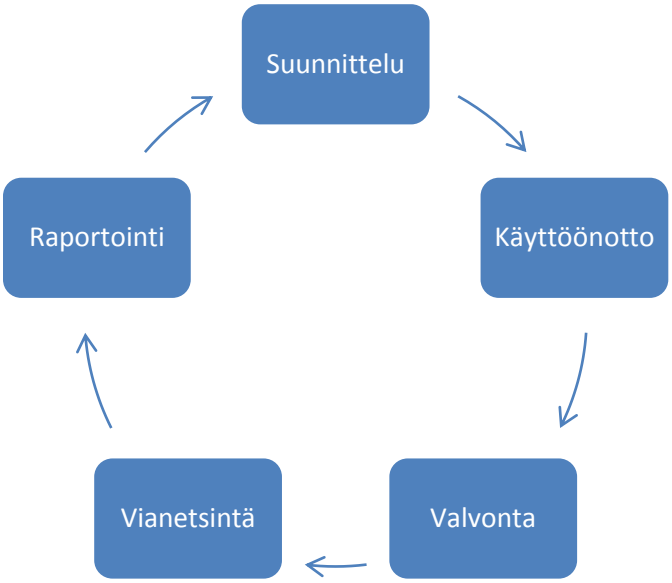
Kuva 5. WCS-suunnittelusivu (Cisco 2011)

Lisäksi järjestelmän avulla vianetsintä ja ongelmien kartoittaminen on vaivattomampaa, sillä järjestelmän avulla voidaan seurata kaikkia verkon tukiasemia. Järjestelmän avulla yksittäiset hälytykset ja muut tärkeät verkkoon liittyvät asiat on helppo havaita. WCS-hallintajärjestelmän avulla langattomien verkkojen valvonta on pyritty tekemään mahdollisimman vaivattomaksi. Langattoman verkon hallinta ja konfigurointi voidaan suorittaa samasta paikasta. Hallintaa helpottavat myös erilaisten raporttien tekeminen ja ongelmatilanteissa reaaliaikaiset hälytykset. WCS:n avulla voidaan myös rajata ei-haluttuja käyttäjiä ulos verkosta. Tämä tapahtuu käyttämällä User Exclusion List -ominaisuutta, jolloin käyttäjän kirjautumistietoja käyttäen, hänet on mahdollista sulkea ulkopuolelle langattomasta verkosta. (Cisco 2011).

WCS-järjestelmän avulla pystytään hallita myös vieralijaverkkoa, jolloin organisaation ulkopuoliset henkilöt voidaan rajata pois henkilökunnalle tarkoitetusta verkosta. Vierailijaverkon avulla organisaation oma verkko voidaan pitää suojattuna, jolloin vierailijoilla on mahdollisuus käyttää rajoitettua verkkoa (Cisco 2011).

Koko Wlan-järjestelmän hallinta on pyritty tekemään vaivattomaksi verkon ylläpitäjille. Järjestelmänvalvoja voi halutessaan tehdä jokaiselle kontrollerille oman käyttömallinsa tai sitten jokaisen käyttämään samaa mallia. WCS-järjestelmän avulla järjestelmänvalvoja voi saada lukuisia raportteja langattoman verkon tilasta.

Raportteja ovat muun muassa verkon käyttöasteet, joita voi halutessaan raportoida päivien, viikkojen tai kuukausien ajalta (Cisco 2011). Alla oleva kuva esittää langattoman lähiverkon elinkaaren, jonka eri vaiheisiin WCS tarjoaa tehokkaan ratkaisun.

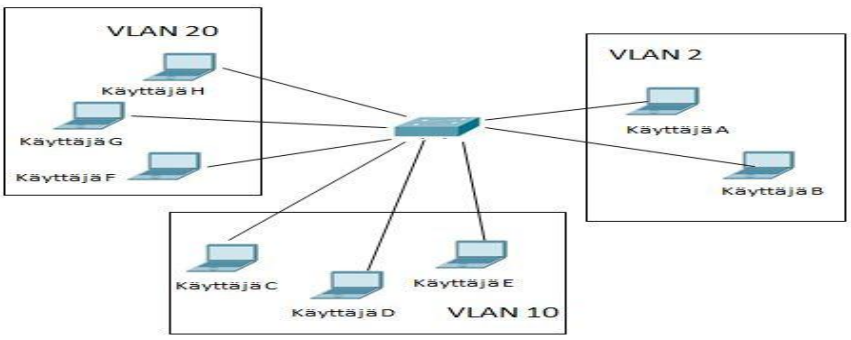


Kuva 6. Langattoman lähiverkon elinkaari

2.8 Langaton lähiverkko ja VLAN

VLAN eli Virtual Lan on virtuaalilähiverkko, jolla voidaan jakaa organisaation tietoliikenneverkko pienempiin ja loogisiin osiin. Virtuaalilähiverkkoja käytetään kytkinpohjaisessa ratkaisussa, joissa eri VLAN:n väliset yhteydet reititetään reitittimellä. VLAN-tekniikan avulla tietoverkko jaetaan hallittaviin osiin, esimerkiksi niin, että eri osastoilla on käytössä oma VLAN (Javvin 2011).

Alla oleva kuva esittää verkon jakamista pienimpiin osiin VLAN -tekniikan avulla.



Kuva 7. VLAN-verkkokaavio

Langaton lähiverkko voidaan jakaa virtuaalilähiverkon avulla omaksi verkoksi. Tällöin langaton lähiverkko toimii tietyllä IP-alueella, jolloin tukiasemat saavat toimiakseen verkossa oikeat IP-osoitteet. Langattomaan lähiverkkoon liittyneet asiakkaat käyttävät myös VLAN:n määräämää IP-osoitealuetta. Langattoman lähiverkon jakaminen omaksi loogiseksi verkoksi helpottaa verkon ylläpitoa ja hallittavuutta (Javvin 2011).

3 LANGATTOMAN LÄHIVERKON TIETOTURVA

Langattomissa lähiverkoissa viestisignaalit kulkevat ilmateitse, joten ne ovat kenen tahansa tavoitettavissa täysin avoimesti. Vapaasti liikkuvat signaalit asettavat tietoturvan erittäin tärkeään asemaan. (Geier 171) 802.11-suositusten mukaisesti standardin asettamilla tavoitteilla pyritään samankaltaiseen suojaustasoon kuin kiinteällä lankaverkolla (Granlund 317). Langattoman lähiverkon tietoturvaa voidaan parantaa erilaisten todennusten ja suojausten avulla.

3.1 Langattoman lähiverkon tietoturvauhat

Langattomaan lähiverkkoon liittyy erilaisia tietoturvauhkia. Tyypillisimpiä uhkia ovat liikenteen tarkkailu, palvelunesto tai luvaton pääsy.

Liikenteen tarkkailuun on olemassa monenlaisia niin kutsuttuja hakkerointityökaluja, joiden avulla liikenteen tarkkailu on mahdollista. Työkalujen avulla hakkeri voi saada selville langattomassa lähiverkossa kulkevan datan sisällön. Luvaton liikenteen tarkkailu saadaan estettyä käyttämällä tukiaseman ja siihen liittyneen laitteen välisessä kommunikaatiossa liikenteen salaamista. Salauksen avulla data säilyy yksityisenä, sillä liikenteen data salataan salausavaimella (Geier 172).

Langatonta lähiverkkoa uhkaa myös luvaton pääsy, mikäli langattoman verkon tietoturva-asetukset eivät ole kunnossa. Nykyään langattoman lähiverkon tietoturvaan kiinnitetään entistä enemmän huomiota, mutta valitettavasti langaton lähiverkko voidaan toteuttaa liian vajavaisin asetuksin. Luvatonta pääsyä varten langattomaan verkkoon tulisi konfiguroida tukiaseman ja siihen liittyneen laitteen välinen kaksisuuntainen sekä yhtenäinen todennus. Todennuksen avulla joko käyttäjä tai käytössä oleva laite on tunnistettavissa (Geier 176).

Palvelunesto- eli DoS-hyökkäys (Denial of Service) on uhka, jolla saadaan aikaan langattomalle verkolle joko toimintaa haittaavia vaikutuksia tai koko verkon kaatuminen. Palvelunestohyökkäyksillä voidaan aiheuttaa mittavia taloudellisia menetyksiä. Palvelunestohyökkäyksiä on monenlaisia, mutta tyypillisimpiä niistä ovat väsytyshyökkäys sekä voimakkaan radiosignaalin käyttö. Väsytyshyökkäyk-

sessä verkkoa kuormitetaan liikenteen tulvalla, joka täyttää verkon resurssit ja näin ollen saa verkon kaatumaan. Voimakkaan radiosignaalin käyttö perustuu tehokkaaseen lähettimeen, joka saa aikaan tukiasemien ja verkkokorttien käyttökelvottomuuden. Voimakkaan radiosignaalin käyttäminen on käyttäjälle hyvin riskialtista, sillä vahvan lähettimen täytyy olla mahdollisimman lähellä itse verkkoa (Geier 176–177).

3.2 WEP

WEP (Wired Equivalent Privacy) on 802.11-standardin alkuperäinen salausmetodi. Nykyään WEP-salaus on vanhentunut ja sen on todettu olevan altis erilaisille verkkohyökkäyksille. WEP-salaus muodostuu erilaisista komponenteista (Granlund 318).

Todentamisessa eli autentikoinnissa käytetään kahta eri menetelmää, joko kaikille avointa pääsyä verkkoon tai salausavaimeen perustuvaa autentikointia. Salausvain on kaikille yhteinen, mikä perustuu haaste-vastaustekniikkaan. Haaste-vastaustekniikassa tukiasema lähettää asiakaslaitteelle joko luku- tai kirjainyhdistelmän. Asiakaslaitteen täytyy kyetä salakirjoittamaan yhdistelmä käyttäen verkon WEP-salausavainta, jonka asiakaslaite palauttaa takaisin tukiasemalle. Tukiaseman tehtävänä on tarkistaa, onko asiakaslaite osannut salakirjoittaa yhdistelmän oikein, jos on, asiakaslaite tuntee salausavaimen. (Granlund 318)

WEP-suojauksessa luottamuksellisuus hoidetaan RC4-jonosalaajalla. RC4-jonosalaajan alustusvektori siirtyy sanoman mukana, jolloin siirtyy myös käytössä olleen WEP-salausavaimen tieto. (Granlund 318)

WEP-salauksen eheystarkistus varmistetaan ICV-tarkisteella (Integrity Check Value), joka liitetään sanomaan. (Granlund 318) Eheystarkistuksen tarkiste on tarkistuksesta saatu summa, jonka vastaanottavana toimiva asema laskee uudestaan ja vertaa tätä tulosta lähettävältä asemalta saamaan tarkisteeseen. Mikäli vastaanottavan aseman tarkiste ei vastaa kehyksen tarkistetta, käyttäjälle ilmoitetaan tai kehys hylätään. (Geier 181)

3.3 WPA

WPA (WiFi Protected Access) on salausmetodi, joka on päivitys WEP-salaukselle, sillä WEP on ominaisuuksiltaan liian heikko. WPA:n parannuksiin lukeutuvat kaksisuuntainen todennus sekä dynaaminen avaimen salaus. WPA-salausta käyttävillä asiakkailla on mahdollisuus vaihteleviin salausavaimiin, minkä ansioista salausta on vaikea murtaa. (Geier 184)

WPA-salauksen myötä voidaan käyttää EAP TLS (Extensible Authentication Protocol Transport Layer Security) -autentikointitapaa, joka mahdollistaa autentikointipalvelimen, esimerkiksi RADIUS:n (Remote Authentication Dial In User Service) käytön. Ulkopuolisen autentikointipalvelimen ollessa käytössä autentikointiprosessin edetessä käsiteltävä tieto siirtyy palvelimelle suojatusti tukiaseman kautta. Tällöin palvelin todentaa käyttäjän joko käyttäjä- tai konetilin avulla. Langattomien lähiverkkojen autentikointipalvelimina voidaan käyttää langattomien verkkojen kontrollereita eli ohjaimia tai muita vastaavia yhdysliikennelaitteita. (Granlund 320)

Mikäli autentikointipalvelinta ei ole mahdollista käyttää, WPA tarjoaa kevyemmän tavan autentikoida. Tässä tavassa autentikointi hoidetaan PSK (Pre Shared Key) -menetelmällä. Menetelmässä tukiasema sekä asiakaslaite todentavat itsensä käyttämällä haaste-vastaustekniikkaa, jossa molemmat autentikoituvat nelivaiheisesti toisilleen. (Granlund 320)

Salauksessa käytetään lyhytikäistä TK eli Temporal Key -salausavainta. Salausavain luodaan TKIP-protokollalla eli Temporal Key Interchange Protocol. TKIP-protokolla osaa muuntaa käytettäviä salausavaimia älykkäästi, jolloin samoja avaimia on käytössä todella harvoin (Granlund 321).

3.4 WPA2

WPA2 eli Wifi Protected Access 2 tunnetaan myös 802.11i-standardina. WPA2 tarjoaa samat ominaisuudet kuten WPA. WPA2 eroaa kuitenkin edeltäjästään AES (Advanced Encryption Standard) -salauksen ansioista. WPA2-suojaus on nykyisin pakollinen WiFi-sertifikaatin saaneissa laitteissa (Granlund 321).

3.5 802.1x

IEEE:n 802.1x -standardin käyttäminen mahdollistaa tehokkaan tavan käyttäjän todennukseen ja valvontaan täysin automaattisesti. 802.1x on porttikohtainen todentaminen, jonka avulla voidaan estää luvattomien laitteiden liittyminen verkkoon. Langattomissa verkoissa standardin liittymispiste on tukiasema. Standardi tarjoaa dynaamisen salausavaimen muuttamisen ja se yhdistää EAP-protokollaa niin langattomissa kuin langallisissa siirtoteissä. 802.11x-standardi tukee myös useita muita todennustapoja, esimerkiksi Kerberosta, Token Card -tunnistusta ja varmenteita. (Geier 188)

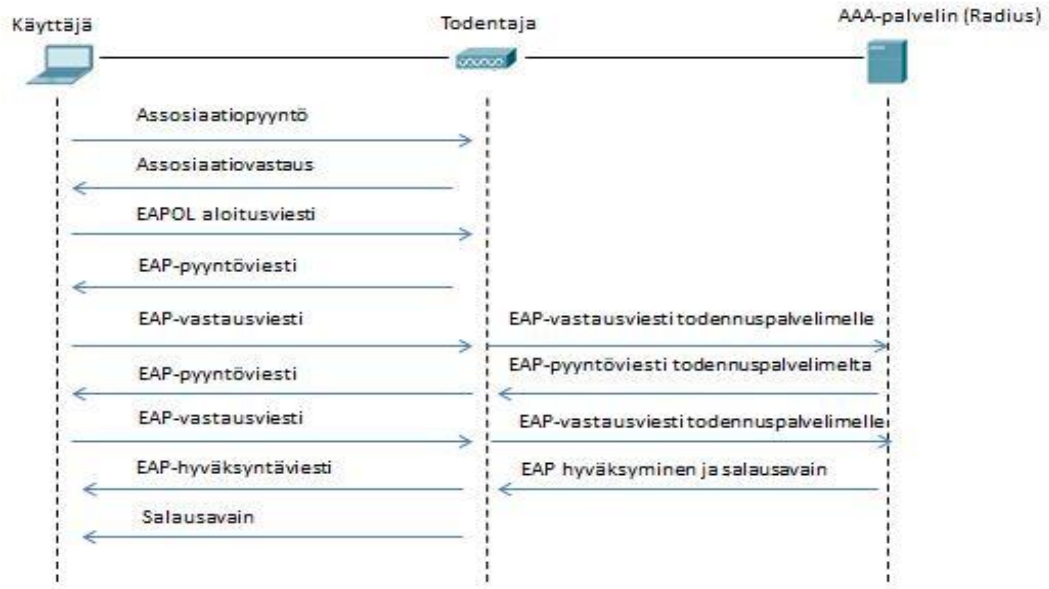
Kun tukiasemaan luodaan yhteys, tukiasema aukaisee portin, joka sallii ainoastaan EAP-paketit sisäverkossa toimivalle todennuspalvelimelle. Tukiasema estää muiden protokollien, kuten DHCP:n (Dynamic Host Configuration Protocol), paketit ennen kuin asiakas on varmistettu todennuspalvelimella. (Granlund 323)

Standardin toiminta-ajatus perustuu kahden portin luomiseen autentikoituvalle asiakkaalle. portit ovat auktorisoitu ja auktorisoimaton portti laitteessa, joka tarjoaa pääsyn verkkoon. Esimerkkinä tällaisesta laitteesta on langattoman lähiverkon tukiasema. Aluksi asiakas käyttää ainoastaan auktorisoimatonta porttia, jolloin asiakas ohjautuu todennuspalvelimelle, jossa autentikointi tapahtuu. Auktorisoimattoman portin kautta kulkevat vain EAP-paketit eli autentikointiviestit. EAP-paketit kulkeutuvat EAPOL eli Extensible Authentication Protocol Over LAN paketointitekniikalla autentikoijalta todennuspalvelimelle. Todennuspalvelimella tehdään varmennus asiakkaan tiedoista ja, mikäli ne löytyvät todennuspalvelimen käyttämästä tietokannasta, voidaan asiakas ohjata käyttämään auktorisoitua porttia, jolloin hänellä on pääsy verkkoon ja sen palveluihin (Snyder 2010).

802.1x -standardin yksi tärkeimmistä piirteistä on, että sen avulla voidaan sulkea luvattomat ja vieraat laitteet ulkopuolelle organisaation sisäverkosta. Lisäksi standardi tarjoaa järkevän tavan autentikoida asiakas verkon reunalla. Verkon reunalla tapahtuva autentikointi tarkoittaa liityntäpisteessä tapahtuvaa autentikoimista eli esimerkiksi langattomissa lähiverkoissa asiakas autentikoituu tukiasemassa (Snyder 2010).

Standardi ei itsessään tarjoa todennusmekanismeja eli sitä käytettäessä on valittava jokin EAP-tyyppi. Eri tyyppejä tukevat sovellukset sijaitsevat joko todennuspalvelimella tai laitteiden sovelluksissa. (Geier 190)

Alla olevassa kuvassa esitetään 802.1x-standardin autentikointiprosessi.



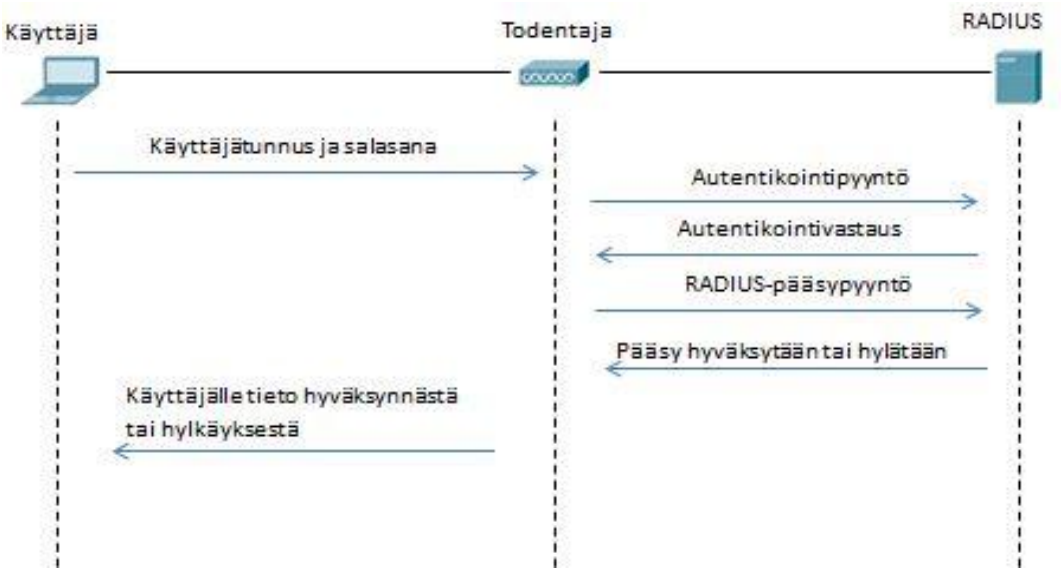
Kuva 8. 802.1x-autentikointiprosessi

3.6 RADIUS

RADIUS eli Remote Authentication Dial In User Service on todennuspalvelin, joka vastaa verkon pääsynvalvonnasta.

Mikäli langattomassa lähiverkossa halutaan käyttää AAA (Authentication, Authorization and Accounting) -palvelua, täytyy käytössä olla RADIUS-protokollaan pohjautuva palvelin. RADIUS toimii todennuspalvelimella, joka toimii pääsynvalvojana. Todennuspalvelin käyttää pääsynvalvonnassa olemassa olevia käyttäjätietoja, kuten Active Directory, jossa hallitaan organisaation käyttäjätilejä tai palvelimelle voi luoda oman tietokannan, jota käytetään todentamiseen (Puska 259-261).

Asiakkaan liittyessä langattomaan verkkoon RADIUS-palvelin käy läpi prosessin, jonka aikana käyttäjän tiedot tarkistetaan. Mikäli käyttäjän tiedot ovat oikein, asiakkaalle annetaan pääsy verkkoon. Mikäli tiedot eivät ole oikein, asiakas jätetään verkon ulkopuolelle (Puska 76–77). Alla oleva kuva selventää asiakkaan, tukiaseman ja RADIUS-palvelimen välisen kättelyvaiheen, jonka aikana käyttäjän tiedot tarkistetaan.



Kuva 9. RADIUS-palvelin ja käyttäjän todennus

4 TIETOLIIKENNETEKNIIKKA

Tämän työn tarkoituksena oli suunnitella ja luoda langaton verkko vaasalaiseen päiväkoti Punahilkkaan. Työ oli toimeksianto Vaasan kaupungin ATK-osastolta. Suunnitteluvaiheessa otin huomioon ATK-osaston käyttämät laitteet sekä standardit, joten päätin rakentaa langattoman verkon olemassa olevalla tekniikalla.

4.1 Kiinteän verkon G.SHDSL-tekniikka

Vaasan kaupungilla on kuituyhteydet moneen eri kaupunginosaan laajalla säteellä. Päiväkoti Punahilkkaan saakka ei kuituyhteyttä ollut saatavilla, joten verkko on rakennettu G.SHDSL-tekniikalla.

G.SHDSL on tekniikka, joka perustuu SHDSL (Single-pair High-speed Digital Subscriber Line) -tekniikkaan. G.SHDSL on nykyään yleinen nimitys SHDSL-tekniikalle. G-SHDSL on ITU-T (International Telecommunications Union) luoma standardi G.991.2. Standardin tarkoituksena on ollut helpottaa eri tekniikoiden käyttämistä, joten niistä luotiin G.991.2-standardi (Granlund 383-386).

G.SHDSL on tekniikaltaan symmetrinen tiedonsiirtotapa eli yhteyden nopeus on molempiin suuntiin täysin sama. Päiväkotiin tuleva yhteys on mahdollistettu käyttäen kahta kupariparia, jolloin yhteyden nopeudeksi saadaan enintään 11,4Mbps. Päiväkoti Punahilkkaan SHDSL-linja on luotu käyttämällä DCombus:n valmistamia IRIS20 SHDSL-modeemilaitteita. Yhteyden keskus sijaitsee lähellä olevassa koulussa, jossa IRIS20-laite muuttaa linjan dataliikenteeksi. Päiväkodissa yhteyden ottaa vastaan toinen IRIS20 -laite, joka siirtää linjan tietoliikennelaitteille. Iris20 käyttää kahta kierrettyä paria mahdollistaen 11,4Mbps:n nopeuden linjalle. (DCombus 2011)

4.2 Kiinteä verkko rakennuksessa

SHDSL-linja siirtyy IRIS20-modeemilaitteesta tietoliikennetilassa olevalle pääkytkimelle, jonka kautta linkki välittyy muille talokytkimille. Päiväkodissa on kolme ristikytkentä- eli tietoliikennetilaa, joista verkkoa jaetaan eri puolille ra-

kennusta. Tietoliikennetilat sijaitsevat lukituissa tiloissa eivätkä asiaankuulumattomat henkilöt pääse niihin.

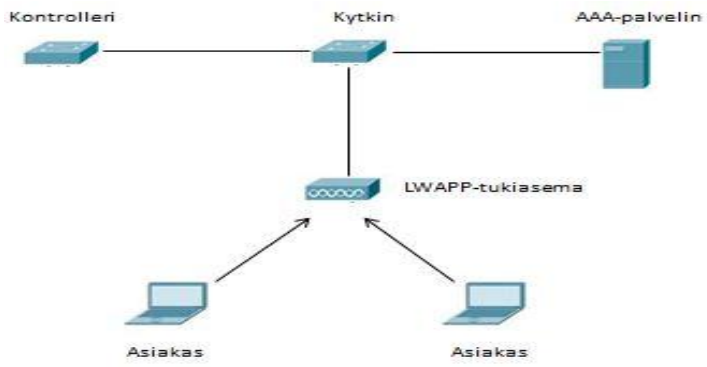
Tietoliikennelaitteina käytetään Cisco Systems:in valmistamia 2960-sarjan PoE eli Power over Ethernet -kytkimiä. Power over Ethernet -tekniikka mahdollistaa virransyötön suoraan lähiverkkokaapeloinnin kautta.

802.3af on IEEE:n standardi, jossa PoE -tekniikka on määritelty. Tekniikan avulla voidaan syöttää verkkokaapelilla virtaa eri laitteille, kuten langattoman lähiverkon tukiasemille ja IP-puhelimille. PoE-kytkimen virransyöttö on 48 V tasajännite, joka siirtyy kytkimeltä ristikytkentään ja sitä kautta laitteelle. (Puska 199)

Power over Ethernet -tekniikka helpotti tukiasemien sijoittelun suunnittelua, sillä PoE:n avulla ulkopuolisia virtalähteitä ei tarvittu.

4.3 Langattoman lähiverkon tekniikka

Langattomia tukiasemia ohjaa WLAN-kontrolleri, joita kaupungilla oli käytössä kaksi. WLAN-kontrollerit olivat Cisco Systems:n 4404 kontrollereita. WLAN-kontrolleri on laite, jonka avulla voidaan varmistaa laatu, pääsynhallinta sekä tietoturva tukiasemien puolesta. Kontrollerit mahdollistavat langattoman lähiverkon keskitetyn hallinnan. Alla olevassa kuvassa on esitetty yksinkertaistettu kontrolleriratkaisu havainnollistamaan ratkaisua.



Kuva 10. Kontrolleriratkaisuesimerkki

WLAN-kontrollereiden rinnalla käytössäni oli Cisco Systems:n kehittämä WCS (Wireless Control System) -hallintajärjestelmä, joka mahdollistaa järjestelmänlaajuisen langattoman lähiverkkohallinnan. Hallintajärjestelmän avulla langattomien lähiverkkojen sekä tukiasemien ylläpito ja valvominen ovat helpompaa, sillä WCS:n avulla verkkoa voidaan valvoa reaaliaikaisesti. WCS-hallintajärjestelmän avulla hallitaan käytössä olevia kontrollereita, jotka puolestaan hallitsevat tukiasemia. Kontrollereille voidaan antaa kaikki tarvittava tieto, esimerkiksi eri langattomien verkkojen tiedot, salausmenetelmät sekä muut asetukset, joita tukiasemat tarvitsevat.

Tukiasemina käytin Cisco Systems:n 1100 laitteita. Tukiasemat toimivat verkossa niin kutsuttuina LWAPP (Light-Weight Access Point) -laitteina, joita kontrollerit ohjaavat. Tukiasemat saavat siis kaiken tiedon, kuten langattomat verkot, tietoturvan sekä muut ominaisuudet kontrollerin kautta. Tukiasemat toimivat vastaanottavina, kun käyttäjä liittyy langattomasti verkkoon.

Tukiasemat pystyvät jakamaan eri verkkoja, sillä useassa eri toimessa tarvitaan useampaa kuin yhtä verkkoa. Kaupungin organisaatiossa tukiasemat jakavat hallinnon-, opetus- sekä vierasverkkoja. Tukiasemien jakamat verkot on määritelty kontrollereilla, jotka hallinnoivat tukiasemia. Jokaisella verkolla on toimintatarkoitus. Hallinnonverkkoa käyttävät pääasiallisesti organisaation työntekijät. Opetusverkkoa käytetään asianmukaisesti opetukseen ja vierailijaverkkoon voivat liittyä ulkopuoliset kuten eri organisaatioiden kouluttajat, joille vierailijatunnukset luodaan asiakohtaisesti.

Langattomien tukiasemien IP-osoitealue on toteutettu virtuaalilähiverkon eli VLAN:n (Virtual LAN) avulla. Tällöin kytkimen portteihin, joihin tukiasema tullaan liittämään, konfiguroidaan kyseessä oleva portti käyttämään langattomalle tukiaemalle tarkoitettua VLAN:a. Tämän tekniikan avulla verkko voidaan jakaa loogisiin osiin, jolloin verkonhallinta ja ylläpito helpottuvat.

4.4 Tietoturvamenetelmät

Kartoitettuani käytössä olleen tekniikan tutustuin käytössä oleviin tietoturvatapoihin. Käytössäni oli aiemmin hyväksi todetut ratkaisut, joten en nähnyt tarpeelliseksi alkaa muuttaa niitä.

Langattomissa lähiverkoissa todennuspalvelimena toimii RADIUS (Remote Authentication Dial-In User Service) -protokollaa hyödykseen käyttävä ACS (Cisco Secure Access Control Server) -palvelin. ACS-palvelin käyttää niin kutsuttua AAA-palvelua (Authentication, Authorization, Accounting) eli suomeksi autentikointi, valtuutus ja tilastointi. Palvelin käyttää hyväkseen organisaation käytössä olevaa AD (Active Directory) -hakemistoa, joka sisältää organisaatiossa työskentelevien käyttäjätiedot kuin myös käytössä olevien laitteiden konetilit.

ACS-palvelimella on tietokantayhteys AD-hakemistoon, jonka avulla todennuspalvelin tarkistaa asiakkaan tiedot ja antaa näin ollen pääsyn liittymään verkkoon. Mikäli käyttäjän tiedot löytyvät ja ovat oikein, todennuspalvelin antaa asiakkaalle valtuutuksen liittyä verkkoon. Autentikoinnissa voidaan käyttää joko käyttäjätietoihin tai konetiliin perustuvaa todennusta.

5 LANGATTOMAN LÄHIVERKON SUUNNITTELU

Tutustuttuani aluksi olemassa olevaan tekniikkaan oli minun helpompi alkaa suunnitella itse langatonta lähiverkkoa.

5.1 Langattoman lähiverkon suunnittelu ja katselmus

Tietotekniikkaprojektien, kuten langattoman lähiverkon toteuttamisen ja sen onnistumisen kannalta tärkein ja kriittisen vaihe on vaatimusmäärittely. Toteutuksen haluava organisaatio antaa perusvaatimukset langattomalle lähiverkolle. Käytössä olevien laitteiden sekä palveluiden mukaan määritetään langattomalle verkolle tekniset vaatimukset. Suunnittelussa on hyvä muistaa myös tehdyn ratkaisun laajennettavuus, joustavuus sekä muunneltavuus (Puska 220).

Langattoman lähiverkon suunnittelemisessa teknisen toteutuksen vaatimusten tulee sisältää peittoalueiden- ja päätelaitteiden tiedot, verkon suorituskyky sekä käyttäjien määrä. Langattoman verkon verkkosuunnitelman tulee sisältää myös tukiasemien alustavat sijoituspaikat sekä tukiasemien käyttämät kanavat. Langattomassa verkossa signaalin etenemistä ja käyttäytymistä on hyvin vaikea arvioida etukäteen, joten verkon toiminnan kannalta on suoritettava katselmus eli Site Survey. Katselmuksen avulla pyritään varmistamaan langattoman lähiverkon luotettava toiminta (Puska 220–221).

5.2 Langattoman lähiverkon katselmukset

Ensimmäiseksi päätin tutustua kiinteistöön, jonne langaton verkko rakennettaisiin eli tässä tapauksessa päiväkoti Punahilkkaan. Tämän lisäksi keräsin myös tiedusteluja henkilökunnalta, mitä vaatimuksia heillä on langattomalle lähiverkolle. Saamani informaation perusteella pystyin hahmottelemaan tukiasemille sijoituspaikat sekä päättämään tukiasemien määrän. Tämän ensimmäisen katselmuksen jälkeen minun oli helppo luoda suunnitelma langattoman verkon toteuttamiseen. Tämän katselmuksen yhteenvetona tulin siihen tulokseen, että käyttäisin kiinteistössä neljää tukiasemaa, sillä kiinteistössä on kaksi kerrosta. Tällöin kolme tukiasemaa sijaitsisi alakerrassa ja yksi tukiasema riittäisi yläkertaan.

Ensimmäisen katselmuksen tein tarkoituksella ilman tukiasemia, sillä ensin halusin tutustua kiinteistöön sekä kerätä tietoa työntekijöiltä verkon vaatimuksista. Tämän jälkeen päätin suorittaa toisen katselmuksen, jolloin liittäisin kiinteistöön yhden tukiaseman varmistuakseni langattoman signaalin kuuluvuudesta.

Tukiasemana käytin Ciscon AIR-LAP 1142N-K9 laitetta, joka toimii verkossa niin sanottuna LWAPP-asemana. Katselmuksen aikana vaihtelin tukiaseman paikkaa niille sijoille, mihin olin suunnitelmissani päätynyt. Tällä tavoin pystyin varmistumaan signaalin kuuluvuudesta juuri niillä alueilla, missä langattoman verkon toivottiin erityisesti kuuluvan. Kun tukiasema oli liitetty verkkoon, piirsin suunnittelun tueksi lämpökartan EKAHAU:n HeatMapper -ohjelmalla. Lämpökartta ilmaisee signaalin voimakkuuden eri alueilla. Lämpökartan luominen on hyvin yleinen tapa suunniteltaessa langattomia lähiverkkoja. Lämpökartan tekemisessä käytin apuna kiinteistön pohjakarttaa. Turvallisuussyistä en saanut lupaa lisätä kiinteistön pohjakuvaa opinnäytetyön raporttiin.

En luottanut ainoastaan lämpökartan antamaan tulokseen, vaan käytin sen tueksi Ping-komentoa, joka on TCP/IP-protokollan työkalu. Ping-komento lähettää Echo request -paketin, johon etälaite vastaa Echo reply -paketilla. Lähetin Ping-komennon kannettavalta tietokoneelta, joka oli kytkeytynyt langattomasti verkkoon samassa verkossa olevalle pääpalvelimelle. Ping-kyselyn aikana liikuin rakennuksen sisällä ja tarkkailin signaalin kuuluvuutta ja kyselyn vasteaikojen tuloksia. Tällä tavalla on mahdollista saada lämpökarttoja varmempi tulos signaalin käyttäytymisestä, sillä lämpökartta tehdään pohjakuvan perusteella, jossa rakenteelliset ominaisuudet eivät välttämättä tule esiin.

Lämpökartoista ja ping-testistä saatu tulos oli paljon luotettavampi kuin mitä ensimmäinen katselmus osoitti. Tämän toisen katselmuksen jälkeen päätin jatkaa langattoman verkon toteuttamista kolmella tukiasemalla eli kaksi tukiasemaa alakertaan ja yksi yläkertaan. Tähän tulokseen päädyin siksi, että kahdella tukiasemalla päästiin tulokseen, joka mahdollisti langattoman lähiverkon käytön haluttuihin paikkoihin. Toisen katselmuksen aikana päätin myös tukiasemille lopulliset sijoituspaikat. Tukiasemat tulisi sijoittaa paikkoihin, joihin asiaankuulumattomilla

henkilöillä ei ole suoraa pääsyä, näin ollen yleisissä tiloissa päädyin valitsemaan tukiasemille paikat kattolistojen yläpuolelta sekä lukollisista tietoliikennetiloista.

Katselmuksista saadut tulokset kokosin yhteen dokumenttiin, josta tein varsinaisen suunnitelman tukemaan langattoman verkon toteutusta. Yritin tehdä suunnitelmasta mahdollisen kattavan, että itse toteutusvaiheessa säästyttäisiin isommilta ongelmilta. Katselmuksia tehdessäni tulin tulokseen, että yhtä ainoata oikeaa tapaa ei ole olemassa, vaan jokainen suunnitelman tekijä käyttää apunaan niitä työkaluja, mitkä tuntuvat itselle parhaimmilta. Itse päädyin lämpökarttoihin ja konkreettiseen verkon testaamiseen.

6 LANGATTOMAN LÄHIVERKON TOTEUTUS

Langattoman lähiverkon suunnittelemisen huolellinen toteutus on tärkein tapa välttää virheet itse verkon toteuttamisvaiheessa. Toteutuksen ja käyttöönoton jälkeen on hyvä tehdä viimeinen katselmus ja varmistua langattoman lähiverkon moitteettomasta toiminnasta (Puska 227).

Toteutuksen ensimmäinen vaihe oli sijoittaa tukiasemat omille paikoilleen. Sijoittelupaikkojen kriteereinä oli tukiasemien turvallisuus eli paikkojen täytyi sijaita joko lukituissa tiloissa tai ulkopuolisten pääsemättömissä, tässä tapauksessa kattolistojen yläpuolella. Lisäksi toteutuksessa täytyi ottaa huomioon rakennuksen arkkitehtuurilliset ja visuaaliset rajoitukset, sillä kiinteistön seinille ei haluttu mitään ylimääräistä. Yleisissä tiloissa tukiasemat tulivat kattolistojen päälle ja kaapelit sijoitettiin kaapelikouruihin. Tietoliikennetilassa oleva tukiasema sijoitettiin niin että se ei häiritse pääsyä tietoliikennelaitteille.

Sijoittelun valmistuttua oli aika ristikytkeä tukiasema kytkimeen. Kytkinportti täytyi määrittää tiettyyn virtuaalilähiverkkoon eli VLAN:in, että tukiasema toimisi sille varatussa verkossa.

Tukiasemien liityttyä verkkoon tein viimeisen katselmuksen, jolla varmistuin siitä, että langaton lähiverkko toimii. Päädyin käyttämään tukiasemien asetuksissa automaattista kanavan hakua, jolloin kontrolleri määrää asemalle sopivan kanavan yhden ruuhkauduttua. Automaattinen kanavan valinta toimii tässä tapauksessa parhaiten, koska tukiasemat saavat hallintansa kontrollerin kautta.

Viimeinen katselmus osoitti verkon toimivan halutulla tavalla, minkä jälkeen päädyin luomaan ylläpitoa varten WCS-järjestelmään pohjakuvan rakennuksesta, mistä selviää tukiasemien paikat ja kuuluvuusalueet. WCS-järjestelmä mahdollistaa samaisten lämpökarttojen piirtämisen kuin mitä tein suunnitteluvaiheessa. Ylläpitoa tukee pohjakuva rakennuksesta, josta voi nähdä tukiasemien paikat rakennuksen sisällä. Ylläpidon helpottamiseksi tukiasemat nimettiin tarkasti paikkojen mukaan järjestelmään.

Suunnitelmassa ja toteutuksessa jätettiin varaa langattoman lähiverkon muunneltavuudelle ja joustavuudelle. Verkkoa voidaan tarvittaessa laajentaa, mikäli tulevaisuudessa niin halutaan. Toteutuksen lopputulos oli toivotunlainen. Langaton lähiverkko toimi luotettavasti ja tukiasemien sijoittelulla mahdollistettiin langattoman verkon kuuluvuus juuri niihin paikkoihin, missä langattomalle verkolle oli suurin tarve.

Lopputuloksena sain aikaan toimivan langattoman lähiverkon, joka kattaa jokaisen paikan, missä sen toivottiin toimivan. Langattoman lähiverkon tietoturvasta vastaa ACS-palvelin, joka toimii todennuspalvelimena. Kun käyttäjä kirjautuu langattomaan verkkoon, hän ottaa yhteyden todennuspalvelimeen, mikäli käyttäjän tiedot ovat oikeat, hänet autentikoidaan lähiverkkoon. Langattoman lähiverkon tietoliikenne on salattu WPA2-salauksella.

7 YHTEENVETO

Tämän opinnäytetyön tarkoitus oli suunnitella ja toteuttaa langaton lähiverkko ja tutustua langattomaan tekniikkaan, historiaan sekä käytössä olleeseen laitteistoon.

Työtä aloittaessani minulla oli käsitys langattomasta tekniikasta sekä sen kehityksestä. Entuudestaan tuttua oli myös langattoman lähiverkon tietoturva sekä autentikointimenetelmät. Itse verkon suunnitteleminen oli minulle täysin uutta ja siihen jouduinkin tutustumaan hyvin laajasti. Hyvin suunniteltu langaton lähiverkko toimii luotettavasti ja sen ylläpitäminen on huomattavasti helpompaa kuin vajavaisesti suunnitellun. Suunnitteluvaiheessa jouduin etsimään tietoa kirjallisuudesta, kollegoilta sekä laitevalmistajilta. Usea langattomia verkkoja käsittelevä teos esittelee myös vaihtoehtoja langattomien verkkojen suunnitteluun.

Vaikkakin langattomuus ja sen eri tekniikat olivat entuudestaan tuttuja, ongelmilta en välttynyt. Suunnittelin langattoman lähiverkon ison organisaation toimeksiantona, joten minun täytyi ottaa huomioon Vaasan kaupungin yleiset sopimukset niin laitteiden kuin työtapojen suhteen. Tietoliikennelaitteet olivat hyväksi havaittuja, joten en nähnyt syytä muuttaa niitä.

Kontrolleripohjainen ratkaisu ei ollut minulle aiemmin tuttu, joten jouduin etsimään tietoa itse laitteista ja niiden toiminnasta. Kontrolleripohjainen ratkaisu on mielestäni erittäin toimiva isossa organisaatiossa, sillä silloin tukiasemia voi hallita keskitetysti. Kontrolleritekniikan myötä opettelin myös käyttämään WCS-etähallintajärjestelmää, joka parantaa keskitettyä hallintaa.

Työn suunnitteluun ja toteutukseen olen tyytyväinen. Käytin runsaasti aikaa suunnitelman hahmottamiseen, jotta toteutusvaihe olisi mahdollisimman vaivaton. Suunnittelussa käytin apuna tämän päivän tarjoamaa tekniikkaa piirtämällä lämpökarttoja kiinteistön pohjakuvasta. Suunnittelun toteutuksena sain aikaan toimivan ja luotettavan langattoman lähiverkon. Verkkoa on tulevaisuudessa tarpeen mukaan helppo laajentaa, mikäli tarvetta tällaiselle on.

Langattomat lähiverkot tulevat olemaan tulevaisuudessa entistä tärkeämpiä jokaisella työpaikalla, sillä markkinoille tulevat työvälineet mobilisoituvat koko ajan. Mobilisoituva tekniikka mahdollistaa joustavuuden ja liikkuvuuden, joten langaton verkko tulee aina vain tarpeellisemmaksi. Tulevaisuus näyttää, syrjäyttääkö langaton lähiverkko kiinteän, kaapeloidun verkon kokonaan.

LÄHTEET

Kirjat

Geier, Jim – Suom. Holttinen, Jarmo 2004, Langattomat verkot. Helsinki. Edita.

Granlund, Kaj 2007. Tietoliikenne 1.painos. Jyväskylä. WSOYpro/Docendo

Puska, Matti 2005. Langattomat lähiverkot. Jyväskylä. Gummerus

Elektroniset julkaisut

Cisco Systems. 2011. Cisco Wireless Control System (WCS). Viitattu 11.11.2011. http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

Cisco System 2011. LWAPP Traffic Study. Viitattu 18.11.2011. http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a0080901caa.shtml

Design Combus. 2007. Designs Combuksen verkkosivut. Viitattu 26.10.2011. http://www.dcombus.com/upload/public/iris10-20/DCombus_Iris20_Esite.pdf

Gråsten, Ville. 2011. Keskitetty verkonhallinta Cisco WLAN-kontrollerilla ja WCS:llä. Opinnäytetyö. Mikkelin ammattikorkeakoulu. PDF-dokumentti. Viitattu 12.11.2011.
https://publications.theseus.fi/bitstream/handle/10024/29951/Grasten_Ville.pdf?sequence=1

Javvin Company 2011. VLAN: Virtual Local Area Network and IEEE 802.1Q. Viitattu 19.11.2011.
http://www.javvin.com/protocolVLAN.html

Snyder, Joel 2010. What is 802.1X?. Viitattu 29.11.2011. http://www.networkworld.com/news/2010/0506whatisit.html

Wikipedia. 2011. IEEE 802.11. Viitattu 24.10.2011. http://fi.wikipedia.org/wiki/IEEE_802.11