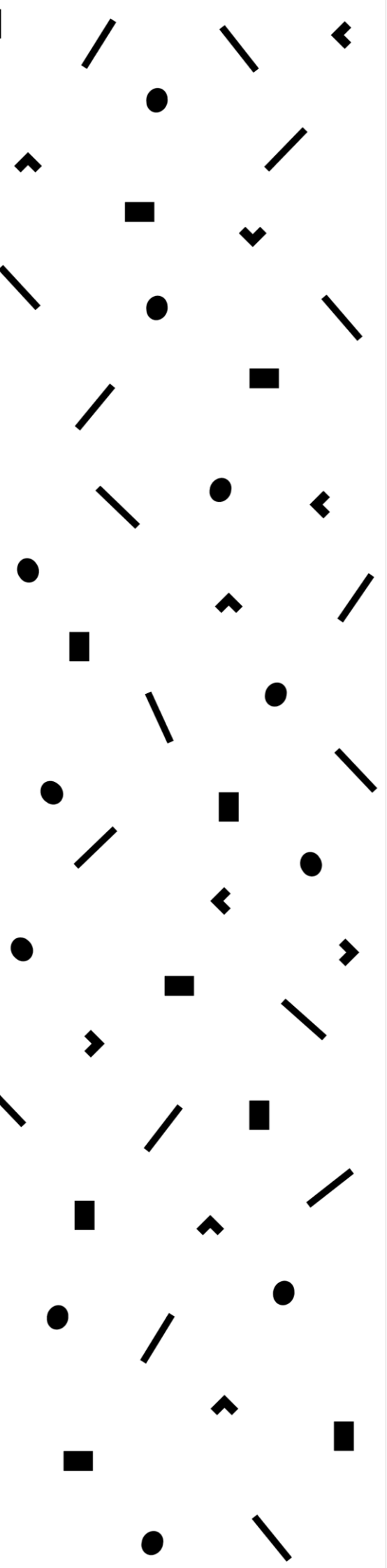


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

LANGATTOMAN LÄHIVERKON UUDISTUS LAHTELAISELLE YRITYKSELLE

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Tekijän Antti Holopainen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HOLOPAINEN, ANTTI:

Langattoman lähiverkon uudistus
Lahtelaiselle yritykselle

Tietoliikennetekniikan opinnäytetyö, 47 sivua

Kevät 2015

TIIVISTELMÄ

Opinnäytetyön tavoite oli suorittaa langattoman lähiverkon toteutus ja lähiverkon laitteiden uudistus ruoka-alan yrityksen kylmävarastoon sekä toimistotiloihin. Työn toimeksiantajana oli ITsPro Oy. Lähiverkkojen teoriaosuudessa selvitetään ensin OSI-viitemallin tärkeys lähiverkkojen tekniikkaa käsittelevissä töissä ja käydään läpi yleisimmät lähiverkon laitteet: hubi, silta, kytkin ja reititin. Lähiverkon laitteista edetään langattomiin lähiverkkoihin ja langattomien lähiverkkojen yleisimpiin standardeihin, joista nykyisin yleisimmässä adoptoitu standardi on 802.11n. Langattomien lähiverkkojen keskitetyn hallinnan teoriaosuudessa tarkastellaan kahta käytössä olevaan protokollaa, LWAPP:aa ja CAPWAP:aa. LWAPP on Cisco Systemsin omistama standardi, johon CAPWAP perustuu.

Tutkimustehtävänä oli vertailla eri valmistajien tarjoamia laitteita ja etsiä valikoimista sopiva kontrollipohjainen ratkaisu yrityksen langattoman verkon tarpeisiin. Vertailussa oli mukana Ciscon, ZyXELin ja D-Linkin saman hintaluokan laitteita, joista kuitenkaan D-Link ei tarjonnut sopivaa tukiasemaa pakastetiloissa vallitsevaan matalaan lämpötilaan. Parhaaksi ratkaisuksi valittiin ZyXELin NWA-tuoteperheen laitteet niiden ominaisuuksien ja hinnan perusteella.

Työn toteutus aloitettiin yrityksen verkkosuunnitelman tekemisestä, josta edettiin testiympäristön rakentamiseen ja laitteiston testaamiseen. Testaamisen jälkeen laitteet asennettiin paikalleen kahden työpäivän kuluessa käyttäen saksinosturia. Tätä ennen sähköasennusalan yritys oli käynyt tekemässä tukiasemien arviotujen sijaintien perusteella johtovedot ja verkkopistokkeet kylmähalliin. Työn tuloksena oli lähes koko rakennuksen kattava, nopea langaton lähiverkko. Langattoman lähiverkon avulla varastotyöntekijät pystyvät päivittämään varastosaldoja suoraan mobiililaitteilla, vähentäen näin turhan kävelyn määrää pöytäkoneille.

Asiasanat: WLAN, wifi, kontrolleri, tukiasema

Lahti University of Applied Sciences
Degree Programme in Information Technology

HOLOPAINEN, ANTTI: Modernization of a local wireless network for a company based in Lahti

Bachelor's Thesis in telecommunications, 47 pages

Spring 2015

ABSTRACT

The objective of this thesis was to build a wireless LAN (Local Area Network), modernize the devices of the existing LAN for a commercial building containing cold storage and office space. The work was commissioned by ITsPro Oy. LAN theory is explained with the OSI (Open Systems Interconnection) reference model along with the most common LAN equipment: hub, bridge, switch and router. The basic function of WLAN (Wireless Local Area Network) is explained, along with common standards in WLANs, of which the most commonly adopted is 802.11n. The theory section on the centralized management of WLANs explains the function of two common protocols, the LWAPP and CAPWAP. LWAPP is a proprietary Cisco Systems standard, which CAPWAP is based on.

Comparison of different manufacturers' equipment was necessary for finding a suitable selection of control-based solutions for the needs of corporate wireless networks. The comparison included devices from the same price range: Cisco, ZyXEL, D-Link. D-Link, however, did not provide appropriate support for the access point of the frozen food area. The ZyXEL NWA family of devices was chosen as the best solution because of their characteristics and price.

The execution of the work started with network topology planning, after which the hardware was built and tested in a test environment. After testing, the equipment was installed within two working days using a scissor jack. Prior to this, the electrical installation company had been doing the installation work for the network cable and outlets in cold storage spaces. The result was a comprehensive, high-speed wireless local area network which covers almost the entire building. With the wireless LAN, warehouse workers will be able to update stock balances directly from mobile devices, thus reducing the need to walk to a desktop computer.

Key words: WLAN, wifi, controller, access point

SISÄLLYS

LYHENNELUOTTELO

CAPWAP	Control and Provisioning of Wireless Access Points. Tukiasemien ja WLAN-kontrollereiden välisiin yhteyksiin käytettävä protokolla.
DHCP	Dynamic Host Configuration Protocol. Protokolla, jonka avulla asiakaslaite saa verkon IP-osoitteen automaattisesti.
DMZ	DeMilitarized Zone. Palomuurin vyöhyke, joka on yleensä avoin internetiin päin.
DoS	Denial of Service. Palvelunestohyökkäys.
HTTP	Hypertext Transfer Protocol. Käytetään siirtämään verkkosivuja tiedonsiirtoprotokolla.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
LAN	Local Area Network. Rajoitetulla maantieteellisellä alueella sijaitseva lähiverkko.
LWAPP	Lightweight Access Point Protocol. Tukiasemien ja WLAN-kontrollereiden väliseen liikennöintiin käytettävä protokolla.
MAC	Medium Access Control layer. OSI-mallin tiedonsiirtokerroksen osakerros. Laitteen MAC-osoite.
MAN	Metropolitan Area Network. Yksi tai useampi LAN-verkko kaupunkialueella.
Mbps	Tiedonsiirtonopeus megabittiä sekunnissa.
MIMO	Multiple Input Multiple Output. Lähettämiseen ja vastaanottamiseen käytetään useaa antennia.
OFDM	Orthogonal Frequency Division Multiplexing. Monikantoaaltomodulointitekniikka, joka perustuu tiedon jakamiseen usealle alikantoaallolle.

VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
WEP	Wired Equivalent Privacy. Langattomien lähiverkkojen salausmenetelmä.
WiFi	Wireless Fidelty. Tavaramerkki, jota käytetään laatutason symbolina.
WLAN	Wireless Local Area Network. Langaton lähiverkko, jossa verkkolaitteet yhdistyy langattomasti.
WPA	Wi-Fi Protected Access. Langattomien lähiverkkojen tietoturvaprotokolla.
WPA2	Wi-Fi Protected Access 2. WPA:n korvaava tietoturvaprotokolla.

1 JOHDANTO

Opinnäytetyön tarkoituksena oli toteuttaa keskitetysti hallittu langaton lähiverkko keskisuureen, noin 2000 m^2:n kylmävarastohalliin sekä samassa rakennuksessa oleviin toimistotiloihin. Osa varastotiloista on ympäri vuorokauden lämpötilaltaan pakkasen puolella, mikä vaati käytettävän laitteiston osalta tutkimustyötä. Langaton lähiverkko sallii tulevaisuudessa varastotyöntekijöiden käyttää varaston hallintaan liittyviä sovelluksia suoraan mobiliilaitteista.

Käytännön työhön kuului kytkimien, langatottomien tukiasemien sekä tukiasemakontrollerin konfigurointi ja asennus. Langattoman lähiverkon toteutuksiin sisällytettiin myös vierailijaverkon toteutus.

2 LÄHIVERKOISTA YLEISESTI

Lähiverkot muodostuvat verkkoliikenteen ohjauslaitteista sekä niihin kytketyistä oheislaitteista, kuten tietokoneista ja tulostinlaitteista. Lähiverkot on suunniteltu toimimaan rajatulla maantieteellisellä alueella ja tarjoamaan käyttäjille nopean ja turvallisen yhteyden paikallisiin resursseihin. (Cisco verkkoakatemia 2002, 31.)

Jotta voidaan ymmärtää lähiverkoissa tapahtuvaa liikennettä ja lähiverkkojen suunnittelua, on hyvä tarkastella ensin tietoliikenteen yleistä viitemallia. Viitemalleja on useita, mutta tässä opinnäytetyössä viitataan International Organization for Standardizationin (ISO) luomaan Open Systems Interconnection (OSI) -viitemalliin. Viime vuosituhannella tietoverkkojen määrä kasvoi valtavasti. Tietoverkkojen kasvu toi mukanaan toistensa kanssa yhteensopimattomia verkkolaitteita ja verkkototeutuksia. Vuonna 1984 ISO julkisti OSI-viitemallin, joka toimii tänä päivänäkin verkkojen suunnittelun, rakentamisen ja vikaselvityksen pohjana. (Cisco verkkoakatemia 2002, 45.)

OSI-viitemallissa on seitsemän kerrosta, joista jokainen vastaa tiettyä osaa verkon toiminnasta. OSI-malli on kuvattu graafisesti kuviossa 1. Kaikki kerrokset, lukuunottamatta sovelluskerrosta, tarjoavat palveluitaan ylemmälle kerrokselle. Kerrostaminen on mahdollistanut verkon komponenttien standardisoimisen ja edelleen erityyppisten verkkolaitteiden ja ohjelmistojen yhteistoiminnan. (Cisco verkkoakatemia 2002, 54.)

OSI-viitemallin seitsemän kerrosta ovat seuraavat:

1. Kerros: sovelluskerros (application layer).
2. Kerros: esitystapakerros (presentetion layer).
3. Kerros: istuntokerros (session layer).
4. Kerros: kuljetuskerros (transport layer).
5. Kerros: verkkokerros (network data layer).
6. Kerros: siirtoyhteyskerros (data link layer).
7. Kerros: fyysinen kerros (physical data layer).

OSI-viitemallin kolme ylintä kerrosta, sovellus-, esitystapa- ja istuntokerros, vastaavat käyttöliittymästä, datan formatoinnista ja sovelluksiin pääsystä.

Sovelluskerros on kerroksista lähinnä käyttäjää ja tarjoaa käyttäjän sovelluksille pääsyn verkkopalveluihin, esimerkiksi verkkotulostukseen tai yrityksen ftp-tiedostopalvelimeen. Esitystapakerros varmistaa, että sovelluskerroksen lähettämä data on toisen järjestelmän sovelluskerroksen luettavissa. Esityskerros huolehtii myös tiivistämisestä ja salauksesta. Istuntokerros pitää huolen, että eri sovellusten data pysyy erillään. (Cisco verkkoakatemia 2002, 56.)

Neljä alempaa kerrosta, kuljetus-, verkko-, siirtoyhteys- ja fyysinen kerros, määrittelevät, kuinka dataa siirretään johdon kautta, verkkolaitteiden läpi kohdelaitteeseen. Kuljetuskerros tarjoaa datan kuljetuspalvelun, mikä tarkoittaa että ylempien kerroksien ei tarvitse huolehtia kuljetuksen käytännön toteutuksiin liittyvistä yksityiskohdista. Kuljetuskerros huolehtii myös palvelun luotettavuudesta käyttämällä virheentunnistusta, virheenkorjausta sekä vuonohausta. Verkkokerros tarjoaa loogisen osoitteistuksen, jota reitittimet käyttävät polun päättelemiseen. Siirtoyhteyskerros tarjoaa datan siirron fyysisen linkin yli. Fyysinen kerros määrittelee sähköiset, mekaaniset, proseduraaliset ja toinimmalliset spesifikaatiot päätejärjestelmien välisen fyysisen yhteyden aktivointiin. (Cisco verkkoakatemia 2002, 58.)

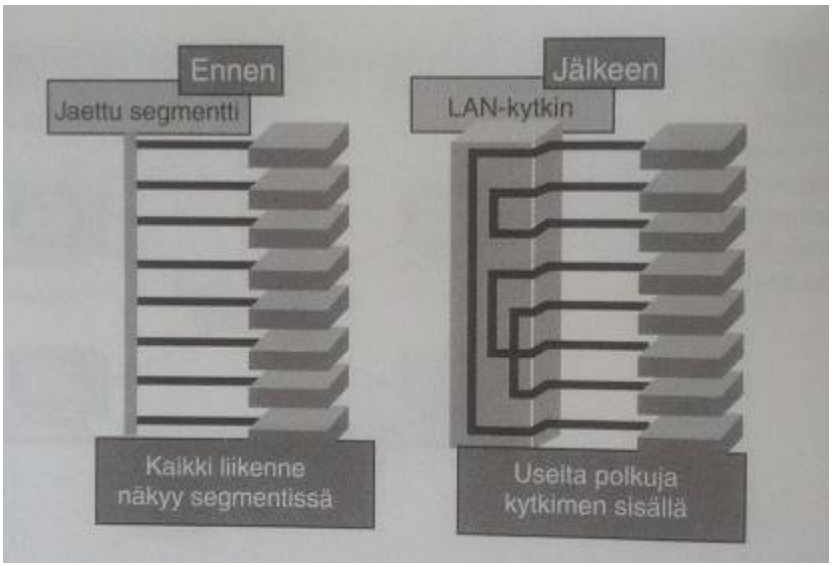
KUVIO 1. OSI-malli (Wikipedia, 2015c)

OSI-mallin kuvaa tarkasteltaessa voidaan havainnoida, että käyttäjän lähettäessä tietoja verkosta tapahtumakulku on OSI-mallissa ylhäältä alaspäin, kun taas käyttäjän vastaanottaessa tietoja tapahtumakulku on alhaalta ylöspäin.

Tyypillisiä lähiverkkojen laitteita ovat verkkokortit, sillat, kytkimet ja reitittimet. Verkkokortti (network interface card, NIC) on 2-kerroksen laite, joka löytyy tyypillisesti loppukäyttäjän päätelaitteesta. Verkkokortti, joka voi olla verkkopiuhan päähän kytkettävän laitteen lisäksi myös langaton adapteri, kommukoi verkon kanssa sarjamuotoisesti ja tietokoneen kanssa rinnakkaismuotoisesti. Verkkokortti muodostaa tietokoneen ja verkon välisen fyysisen yhteyden. (Cisco Verkkoakatemia 2002, 259.)

Silta on 2-kerroksen yksinkertainen laite, joka analysoi sisään tulevat kehykset ja tekee edelleenlähetyspäätöksiä perustuen kehysten sisältämään informaatioon. Silloilla voidaan muodostaa suurista verkkosegmenteistä pienempiä segmenttejä. Verkon segmentöinnin taustalla voi olla yritys parantaa verkon suorituskykyä eliminoimalla siinä esiintyvä tarpeeton liikenne ja minimoimalla törmäysten mahdollisuus. Suodatus tapahtuu MAC-osoitteen perusteella. (Cisco verkkoakatemia 2002, 260.)

Kytkimet edustavat siltojen lailla lähiverkon segmentöintiä ruuhkautumisen ja törmäysten estämiseksi. Kytkimen ja sillan ero kuvataan kuviossa 2. Kytkin yhdistää lähiverkkosegmenttejä käyttäen MAC-osoitetaulua päätelläkseen, mihin segmenttiin kehys kuuluisi lähettää. Kytkimet saavuttavat erittäin alhaisen viivetason, sillä kehys voidaan lähettää vastaanottajalla jo ennen kuin kehys on kokonaisuudessaan saapunut kytkimeen. Tämä tarkoittaa, että kyseessä on 2-kerroksen laite, mutta kytkimet voivat toimia myös 3-kerroksen kytkennällä, eli Internet Protocal- tai IP-kytkennällä. Tällöin kytkin on lähiverkkokytkimen ja reitittimen risteytys. Kytkimet tukevat myös monia toimintoja, joita silloista ei löydy, kuten virtuaalilähiverkkoja. Käytännössä käyttäjät voivat kytkimen avulla kommunikoida verkossa keskenään rinnakkain ilman törmäyksiä. (Cisco verkkoakatemia 2002, 263.)

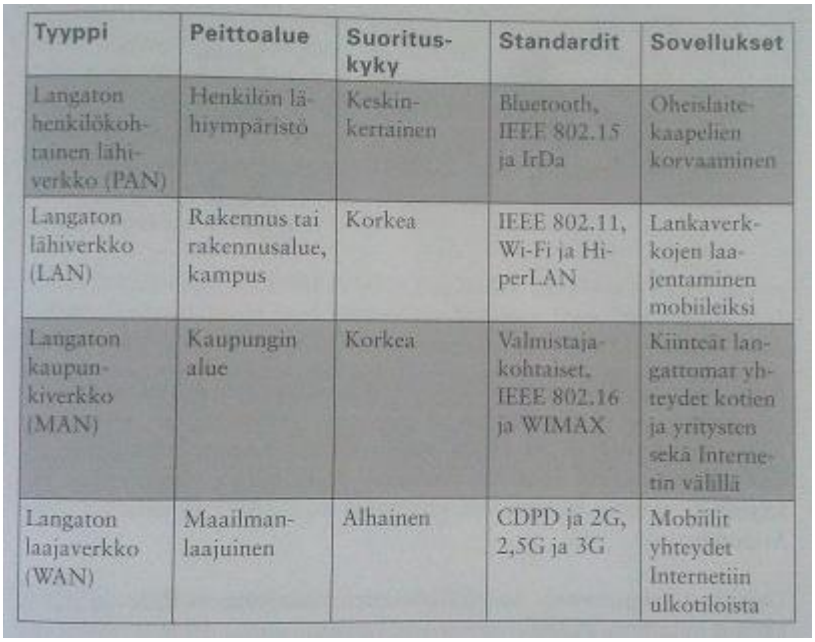


KUVIO 2. Kytkimen ja sillan ero (Cisco verkkoakatemia 2002, 264)

Reitittimet ovat lähiverkon liikenteen ohjauksessa kehittyneimpiä laitteita. Reititin toimii verkkokerroksessa perustaen kaikki lähetyspäätöksensä 3-kerroksen protokollaosoitteisiin. Reitittimin segmentointi on mahdollista suoritta ylimmällä mahdollisella tasolla. Reititin tutkii paketit yksityiskohtaisesti päätelläkseen niille parhaan mahdollisen polun. Tämä prosessi aikansaa jonkin verran viivettä. (Cisco verkkoakatemia 2002, 268.)

3 LANGATTOMAT LÄHIVERKOT

Langattoman lähiverkon avulla työntekijät voivat käyttää kaikkia lähiverkon resursseja tehokkaasti hyödykseen, mutta ilman varsinaista fyysistä yhteyttä lähiverkkoon. Tämä sallii liikkumisen vapauden toimisto- ja tehdasympäristöissä, ilman että palvelut tai sovellukset lakkaisivat toimimasta käyttäjien päätelaitteilla. Työntekijät voivat siis työskennellä myös muuallakin kuin työpöytiensä ääressä. Langaton lähiverkko omaa tyypillisesti korkean suorituskyvyn, jossa tiedonsiirron nopeus on 54 Mbps luokkaa. Langattomien lähiverkkojen lisäksi on olemassa muita langattomia verkkotyyppejä, joilla on eri standardit ja käytännön sovellukset. Verkkotyypit kuvattuna kuviossa. (Geier 2005, 5.)



Tyyppi	Peittoalue	Suoritus-kyky	Standardit	Sovellukset
Langaton henkilökohtainen lähiverkko (PAN)	Henkilön lähiympäristö	Keskinkertainen	Bluetooth, IEEE 802.15 ja IrDa	Oheislaitekaapelien korvaaminen
Langaton lähiverkko (LAN)	Rakennus tai rakennusalue, kampus	Korkea	IEEE 802.11, Wi-Fi ja HiperLAN	Lankaverkkojen laajentaminen mobiileiksi
Langaton kaupunkiverkko (MAN)	Kaupungin alue	Korkea	Valmistajakohtaiset, IEEE 802.16 ja WIMAX	Kiinteät langattomat yhteydet kotien ja yritysten sekä Internetin välillä
Langaton laajaverkko (WAN)	Maailmanlaajuinen	Alhainen	CDPD ja 2G, 2,5G ja 3G	Mobiilit yhteydet Internetiin ulkotiloista

KUVIO 3. Langattomia verkkotyyppejä (Geier 2005, 5)

Siinä missä lähiverkoissa siirtotienä toimii kupari- tai kuitukaapeli, langattomien lähiverkkojen siirtotienä toimii ilma, mutta signaali kulkee myös tyhjiössä. Lähetyksen laatu riippuu lähetyslaitteen lähetystehosta, antennien tyypistä ja sijainnista sekä ympäristössä olevista esteistä. Tyypillisiä esteitä yritysympäristöissä ovat rakennusten väliseinät, jotka heikentävät signaalia seinämateriaalin tyypistä ja paksuudesta riippuen. (Geier 2005, 37.)

Langattomien lähiverkkojen rakenneosana toimii ensisijaisesti tukiasema, joka yhdistää ilmatiessä kulkevat langattomat signaalit lankaverkkoon. Mikäli

yrityksen rakennuksessa on enemmän kuin yksi tukiasema, voidaan tukiasemien välillä toteuttaa liikkuvaa käyttöä eli roamingia. Käyttäjän päätelaite yhdistää silloin aina ympäristössä olevaan vahvimpaan tukiasemaan ja vaihtaa tukiasemaa aina tarpeen vaatiessa. (Geier 2005, 38.)

4 LANGATTOMAN LÄHIVERKON STANDARDIT

Langattomien lähiverkkojen vallitsevin standardi on 802.11, jonka yleisesti käytössä olevat versiot toimivat 2,4 GHz:n ja 5 GHz:n taajusalueilla. Standardin 802.11 ja siitä edelleen jatkokehiteltyjen parannusten suorituskyky ja toimintataajuus on esitetty taulukossa 1. Alkuperäisen standardin ongelmana oli laitteistojen yhteensopimattomuus, mikäli langattomien päätelaitteiden välillä oli käytössä standardin eri versio. (Geier 2005, 9.)

Wi-Fi Alliance -valmistajayhteenliittymä sisällytti 802.11-standardiin toimintoja, jotka nimettiin Wireless Fidelityksi, eli Wi-Fi:ksi. Mikäli langattomasta päätelaitteesta löytyy Wi-Fi-merkintä, laite on taattu toimimaan yhdessä muiden Wi-Fi-merkittyjen laitteiden kanssa. (Geier 2005, 9.)

TAULUKKO 1. Tärkeimmät standardit nopeusjärjestyksessä (Wikipedia 2015a)

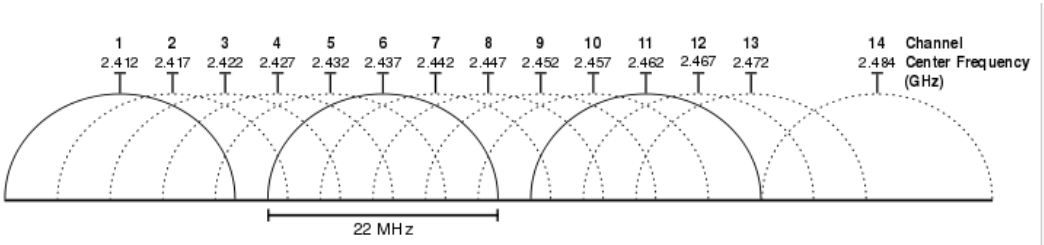
Standardi	Taajuus (GHz)	Maksiminopeus (Mbps)	MIMO-vuot
802.11	2,4	2	0
802.11a	5	54	0
802.11b	2,4	11	0
802.11g	2,4	54	0
802.11n	2,4/5	72,2	4
802.11ac	5	866,7	8

Alkuperäinen versio IEEE 802.11 -standardista ratifioitiin vuonna 1997, mutta 802.11 -standardi on nykyisin vanhentunut. 802.11-standardi sisältää taajuushyppelyhajaspaktrin (FHSS) ja suorasekvenssihajaspektrin (DSSS) 2,4 GHz:n taajuuskaistalla ja 2 Mbps enimmäisnopeudella. FHSS-tukiasemat voidaan määrittää 15:lle eri hyppelykuoviolle, sallien näin 15 FHSS-tukiaseman

toimimisen samalla alueella. Käytännössä laitevalmistajat eivät tarjoa laitteita alkuperäisellä 802.11-standardilla, sillä 802.11-siirtonopeus on erittäin alhainen ja FHSS ei toimi yhdessä muiden 802.11-standardien kanssa. (Geier 2005, 124.)

IEEE julkaisi 802.11a-standardin vuoden 1999 lopulla. Standardi määrittelee Orthogonal Frequency Division Multiplexing -tekniikan käytön, joka sallii 54 Mbps enimmäisnopeuden 5 GHz:n kaistalla. Signaalin kantama voi olla 30 metriä, riippuen tiedonsiirron nopeudesta. Verrattuna alkuperäiseen 802.11-standardiin, 802.11a tarjoaa suuremman kapasiteetin. Lisäksi 5 GHz:n kaistanleveydessä ei ole niin paljon häiriöitä aiheuttavia laitteita, kuten mikroaaltouuneja tai langattomia puhelimia, jotka toimivat 2,4 GHz:n kaistalla. Suurimman ongelman 802.11a-standardissa muodostaa melko lyhyt kantama, joten tukiasemia tarvitaan enemmän kuin alkuperäisessä 802.11 standardissa saman peittoalueen kattamiseksi. Myöskään 802.11a ja 802.11b/g eivät päätelaitteiden osalta suoraan yhteensopivia. (Geier 2005, 125.)

Samanaikaisesti 802.11a-standardin kanssa julkaistiin myös 802.11b-standardi, joka on alkuperäisen 2,4 GHz:n kaistalla toimivan standardin laajennus. 802.11b-standardi tarjoaa 11 Mbps enimmäisnopeuden. 802.11b-standardin omaavan laitteen kantama voi olla sisätiloissa jopa 100 metriä. Tämä johtaa suoraan kustannussäästöihin langattoman sisäverkon toteuttamisessa, sillä tukiasemia ei tarvitse asettaa niin tiheään kuin aikaisemmin. Standardin suurin ongelma on, että siitä löytyy vain kolme kanavaa, jotka eivät mene toistensa kanssa päällekkäin. Kanavien leveydet on kuvattuna kuviossa 4. Tyypillinen ratkaisu langattoman verkon toteuttamisessa 802.11b-standardilla on käyttää pelkästään 1, 6 ja 11 kanavia. Standardissa määritellään kanavat yhdestä neljääntoista asti, mutta esimerkiksi Yhdysvalloissa käytössä on ainoastaan kanavat 1 - 11. 802.11b-standardiin pätee samat häiriötekijät kuten alkuperäisessä 802.11-standardissa, sillä 802.11b käyttää samaa 2,4 GHz:n kaistaa. (Geier 2005, 126.)



KUVIO 4. 2,4 GHz kaistan käytettävissä olevat kanavat (Wikipedia 2015b)

Kolmas modulointistandardi ratifioitiin vuonna 2003, nimeltä 802.11g. 802.11g tarjoaa 54 Mbps siirtonopeuden 2,4 GHz:n kaistalla, käyttäen OFDM:ää kuten 802.11a. 802.11g on takaisinpäin yhteensopiva 802.11b-laitteiden kanssa mikä tarkoittaa, että yrityksen 802.11b-tukiasemat on mahdollista muuttaa 802.11g yhteensopiviksi laitteiston ohjelmiston päivityksellä. Standardi näki nopeaa adoptointia kuluttajilta jo ennen ratifiointia, mikä johtui standardin tarjoamasta suuresta nopeudesta ja pitkästä kantamasta. Useimmat markkinoilla olleet tuotteet tukivat tuolloin jo dual-band- tai tri-mode- ominaisuutta, mikä tarkoittaa että laite tukee a- ja b/g-standardeja yhdessä radiopiirissä. (Geier 2005, 127.)

802.11n-standardi ratifioitiin vuonna 2009. 802.11n:n päämäränä oli parantaa standardia lisäämällä siihen multiple-input multiple-output (MIMO)-antennit, joiden avulla tiedon lähetykseen ja vastaanottamiseen voidaan käyttää useampaa antennia samanaikaisesti. Tämä voi lisätä joko tiedonsiirron nopeutta tai vakautta. 802.11n operoi sekä 2,4 GHz:n että 5 GHz:n kaistalla, joista jälkimmäinen on optionaalinen. Tiedonsiirron maksiminopeus on 72,2 Mbps tai 150 Mbps (yhdellä MIMO vuolla), riippuen onko kaistanleveys 20 MHz vai 40 MHz. (Wikipedia 2015b.)

802.11ac toi edelleen parannuksia 802.11-standardiin. 802.11ac ratifioitiin vuonna 2013. Suurimpia muutoksia standardissa ovat leveämpi kaistanleveys 5 GHz:n kaistalla (80 MHz ja 160 MHz, verrattuna edellisen standardin 20 MHz ja 40 MHz kaistanleveyteen), korkeampi modulaatio (256-QAM vs. 64-QAM) ja Multi-user MIMO (MU-MIMO). Tämä johtaa osaltaan suurempiin tiedonsiirtonopeuksiin, jopa 866Mbps (yhdellä MIMO vuolla) käyttämällä suurinta kaistanleveyttä. (Wikipedia 2015b.)

IEEE 802.11ah on vielä toistaiseksi julkaisematon standardi, jonka on arvioitu tulevan ratifioiduksi vuonna 2016. Standardi määrittelee kaistanleveydeksi alle 1 GHz, joka mahdollistaa alhaisen taajuuden omaavan signaalin propagaation ominaisuuksien vuoksi entistä paremman kantavuuden ja läpäisyn. (Wikipedia 2015b.)

IEEE 802.11ax tulee olemaan tulevaisuudessa korvaaja 802.11ac standardille. IEEE 802.11ax arvioitu julkaisemispäivä on vuonna 2019. Standardin on tarkoitus mahdollistaa nelinkertainen siirtonopeus verrattuna 802.11ac standardiin. (Wikipedia 2015b.)

5 LANGATTOMAN VERKON KESKITETTY HALLINTA

Ensimmäisen sukupolven langattomat lähiverkot käyttivät itsenäisiä tukiasemia. Paljon on muuttunut sen jälkeen, kun ensimmäiset langattomat verkot on omaksuttu käyttöön. Tämän päivän langattomissa verkoissa pelkkä itsenäinen tukiasema harvoin riittää. (Cisco Systems 2015e.)

Yritykset tarvitsevat langattoman kattavuuden kokonaisille rakennuksille. Näiden langattomien verkkojen on tuettava palveluita, kuten ääni, vieras-yhteys, sijainti ja tunkeutumisenhallinta (Wireless Intrusion Prevention Systems, WIPS), mutta samalla tarjota myös yksinkertaistettu käyttöönotto, hallinta ja skaalautuvuus. (Cisco Systems 2015e.)

5.1 Keskitetyn hallinnan tavoitteet

Nykypäivän yritykset tarvitsevat langattomia lähiverkkoja, jotka täyttävät kaikki taulukossa 2 esitetyt vaatimukset. Jos vaatimuksen kohdalla käytettäisiin itsenäistä tukiasemaratkaisua kontrolleripohjaisen ratkaisun sijasta, langattoman verkon toteutus olisi joko hankalampi tai mahdoton.

TAULUKKO 2. Keskitetyn hallinnan tavoitteet (Cisco Systems 2015e)

Vaatimus	Selitys	Itsenäinen tukiasemaratkaisu
Kerroksen 2 nopea verkkovierailu	Saumaton asiakasverkkovierailu eri tukiasemien ja virtuaalisten lähiverkkojen yli	Lisää langattomien domain palveluiden (Wireless Domain Services, WDS) laite (tukiasema tai kytkin-moduuli)
Kerroksen 3 nopea verkkovierailu	Saumaton asiakasverkkovierailu eri tukiasemaien ja virtuaalisten lähiverkkojen yli	Ei saatavilla itsenäisessä ratkaisussa

(jatkuu)

TAULUKKO 2. (jatkuu)

Laitteiston päivityskustannukset	Aika, joka kuluu ottaessa käyttöön ylimääräisiä hallintaominaisuuksia ja työntäessä uusia konfiguraatiota tukiasemiin	Ota käyttöön keskitetyn hallinnan valvonta-asema, tai käytä hallinta skriptejä
Tunketujien esto (IDS)	Kyky tunnistaa tukiaseman matkimista, hyökkäyksiä, ja luvattomaa käyttöä	Käytä WDS-pohjaista IDS-järjestelmää
Paikannuspalvelut	Visualisointi vastaanotetun signaalin voimakkuus-ilmaisimen muutoksista (RSSI) ja langattomien laitteiden sijainnin näyttäminen	Käytä erillistä alueen kartoitus- ratkaisua
Dynaaminen RF	Välitön, dynaaminen sopeutuminen RF ympäristöön	Käytä Simple Network Management Protocol (SNMP); RF tietoa on saatavilla manuaaliseen tarkasteluun ja toimintaan
Kuormituksen tasaaminen	Automaattinen kuormituksen tasaaminen vierekkäisten tukiasemien välillä	Yksittäiset tukiasemat mainostavat kuormaa, mutta kuormitus ei automaattisesti jakaudu eri tukiasemien välillä
Verkkovierailijat	Kyky tarjota asiakkaiden, toimittajien ja kumppaneiden pääsy	Toteuta erikoistunut runko VLAN (trunk VLAN) kuhunkin tukiasemaan ja

(jatkuu)

TAULUKKO 2. (jatkuu)

	langattomaan verkkoon, pitäen verkon turvallisena	levittää niitä koko yrityksessä
Ääni WLANin kautta	Kustannustehokas, reaaliaikainen puhepalvelu käyttämällä olemassa olevaa langatonta infrastruktuuria	Toteuta tukiasemaan perustuvan Call Admission Control (CAC); ohjaus on per-tukiasema perusteella eikä koordinoitu useiden tukiasemien välillä
Hallinta	Kustannustehokas, yksinkertaistettu WLAN hallinta ja käyttöönotto	Toteuta skriptejä tai SNMP ratkaisu määrittämään WLAN hallinta ja konfiguroi jokainen tukiasema erikseen

5.2 Keskitetyn hallinnan protokollat

5.2.1 LWAPP

LWAPP (LightWeight AccessPoint Protocol) on Cisco Systemsin kehittämä protokolla, joka yhtenäistää kommunikaatioprotokollaa kevyiden tukiasemien ja WLAN laitteiden välillä, kuten kontrollerit, kytkimet ja reitittimet. LWAPP protokollan tavoitteita ovat seuraavat:

- Vähentää prosessointia tukiasemissa, mikä vapauttaa tukiaseman resursseja keskittyä yksinomaan langattomaan verkon saatavuuteen, suodatussääntöjen ja politiikan täytäntöönpanojen sijasta.
- Sallia keskitetty liikenteen käsittely, autentikointi, salaus, ja politiikan täytäntöönpanoa koko WLAN-järjestelmässä.
- Tarjoata geneerinen kapselointi ja siirtomekanismi erilaisten toimittajien tukiasemien välillä, käyttäen joko kerroksen 2 infrastruktuuria tai IP-reititettyä verkkoa.

(P. Calhoun 2010, 9.)

5.2.2 CAPWAP

CAPWAP protokolla perustuu perustuu LWAPP protokollaan. CAPWAP protokolla mahdollistaa langattoman verkon Access Controllerin (AC) hallita useita langattomia terminaatiopisteitä (Wireless Termination Point, WTP) langattomassa verkossa. CAPWAP protokolla on määritelty olemaan itsenäinen kerroksen 2 (Layer 2) teknologiasta. (P. Calhoun 2009, 8)

CAPWAP protokolla tarjoaa kaksi operointotilaa: Split ja Local Medium Access Control. Split- tilassa kaikki kerroksen 2 langaton tiedonsiirto ja hallintakehykset kapseloidaan CAPWAP protokollan kautta ja AC ja WTP vaihtavat niitä keskenään. (P. Calhoun 2009, 8.)

Local MAC- toimintatapa mahdollistaa datakehyksien olla joko paikallisesti sillattuna, tai tunneloituna 802.3 kehyksinä. Tunnelointi edellyttää, että WTP suorittaa 802.11 integraatiotoiminnan. Kummassakin tapauksessa, kerroksen 2 langattoman tiedonsiirron hallinnan kehykset käsitellään paikallisesti. CAPWAP protokollan tavoitteita ovat seuraavat:

- Keskittää todennuksen ja menettelytapojen valvontatehtävät yhteen sijaintiin langattomassa verkossa. Keskitetty hallinta voi pitää sisällään myös muita tietoja, kuten tukiasemien siltaus-, salaus- ja käyttäjien datan siirtoon liittyviä asetuksia. Näiden toimintojen keskittäminen yhteen sijaintiin tarjoaa kustannussäästöjä ja lisää tehokkuutta, kun jokaista tukiasemaa ei tarvitse valvoa tai konfiguroida erikseen.
- Sallia korkeamman tason protokollien prosessoinnin siirtämisen langattomilta terminaatiopisteiltä. Tämä jättää WTP:n resurssit verkon kannalta ajaltaan kriittisten sovellusten käyttöön, käyttäen yleensä teholtaan hyvin rajallisten WTP laitteden prosessointitehot tehokkaasti hyödyksi.
- Tarjota laajennettavissa oleva protokolla, joka ei ole siduttu mihinkään tiettyyn langattomaan teknologiaan. Laajennettavuus on tarjottu geneerisen kapseloinnin ja siirtomekanismin kautta, jonka avulla CAPWAP protokollaa voidaan soveltaa moniin tukiasematyyppeihin tulevaisuudessa.

(P. Calhoun 2009, 8.)

6 LANGATTOMAN LÄHIVERKON TIETOTURVA

Koska langattoman verkon signaalit ovat vapaasti kaikkien nähtävissä, on tärkeää taata että yrityksen langattoman sisäverkon liikenne on suojattu asianomaisesti ulkopuolisten katseilta. Langattomaan lähiverkkoon voi kohdistua monenlaisia tietoturvauhkia, kuten passiivinen tarkkailu, luvaton pääsy ja palvelunesto (DOS). (Geier 2005, 172.)

Suojaamattomassa verkossa hakkeri tai satunnainen nuuskija voi tarkkailla langattomia datapakettaja vapaasti saatavilla olevilla työkaluilla, ja noukkia liikenteen joukosta mitä tahansa siellä esiintyvää tietoa, kuten salasanoja ja käyttäjätunnuksia. Ratkaisu on suojata langattoman asiakaslaitteen ja tukiaseman välinen liikenne muuntamalla databitit salaisen avaimen avulla. (Geier 2005, 172.)

Vaikka langattoman lähiverkon ympäristössä olisikin otettu huomioon tietoturvasuojakset, voi riskin muodostaa silti rosvotukiasema, joka saattaa olla ajattelemattoman työntekijän asentama suojaamaton tukiasema tai hakkerin työkalu yrityksen työntekijöiden tietojen urkkimiseen. Monet kontrolleripohjaiset wlan-ratkaisut tarjoavat ratkaisun rosvotukiasemien löytämiseen. Kun wlan-kontrollerilla on tiedossa kaikki yrityksen lailliset tukiasemat, on yksinkertaista skannata verkkoa ja etsiä sieltä asiaankuulumattomia tukiasemia. (Geier 2005, 172.)

Palvelunestohyökkästä vastaan taas on lähes mahdotonta täysin puolustautua, ellei oteta huomioon ulkopuolisten signaalien eristämistä rakennuksesta. Tämä on kuitenkin kallista ja epäkäytännöllistä, ja uhan mahdollisuus on harvinainen sekä helposti paikannettavissa. Palvelunestoa suunnitteleva hakkeri pystyy esimerkiksi täyttämään ilmatien voimakkaalla signaalilla estäen asiaankuuluvan liikenteen täysin. (Geier 2005, 172.)

Salaus muuntaa datapaketin bitit sellaiseen muotoon, että salakuuntelija ei enää pysty lukemaan niitä selkokielisenä. Salauksen purkaminen voidaan suorittaa ainoastaan oikealla avaimella.

WEP on 802.11 optionaalinen todennus- ja salausstandardi, joka käyttää RC4 vuosalausta. WEP toimii MAC-kerroksessa ja määrittelee datan salaukseen ja purkamiseen jaetun salaisen avaimen. Salausprosessissa WEP valmistelee 24-bittisen alustusvektorin, joka perustuu jaettuun salaiseen avaimeen. Vastaanottajan on käytettävä samaa avainta, joten jokainen tukiasema ja verkkokortti on määritettävä käyttämään samaa salausvainta. WEP tarkistaa, onko lähetettyä dataa muutettu siirron aikana, jossa käytetään hyväksi kehyksen eheystarkistetta. Mikäli eheystarkiste ei vastaa odotuksia, niin WEP hylkää kehyksen. WEP on kuitenkin haavoittuva, koska avaimet ovat kiinteitä ja alustusvektorit ovat lyhyitä. Koska WEP on vain 24-bittinen, ruuhkaisessa verkossa sama alustusvektori voi toistua alle tunnissa. Jos hakkeri kerää tällöin riittävästi samaan alustusvektoriin perustuvia kehyksiä, voi hän määritellä kehysten perusteella salaisen avaimen sisällön. Lopputulos on, että kaikki WEP-salattu liikenne on täysin hakkerin luettavissa. (Geier 2005, 182.)

Temporal Key Integrity Protocol (TKIP) on parannus langattomien lähiverkkon tietoturvaan, jota kutsuttiin alkujaan myös WEP2 nimellä. TKIP korjaa WEP-salauksessa esintyneen ongelman, jossa avainta käytettiin jatkuvasti uudelleen, jolloin WEP salauksessa käytetty avain oli myös hakkerin selvitettävissä. TKIP-prosessi alkaa, kun päätelaitteen ja tukiaseman välillä jaetaan 128-bittinen väliaikainen avain. Väliaikainen avain yhdistetään päätelaitteen MAC-osoitteen kanssa ja siihen lisätään 16 oktetin alustusvektori. Näin varmistetaan, että jokainen asema käyttää salauksessa eri avainta. Parannuksiin kuuluu myös vahvempi salausprotokolla, Advanced Encryption Standard. AES käyttää Rine Dale –salausalgoritmia, joka on asiantuntijoiden mielestä murtamaton. (Geier 2005, 184.)

Wi-Fi Protected Access on Wi-Fi Alliancen WEP päivitys, joka mahdollistaa avaimen salaamisen dynaamisesti ja kaksisuuntaisen todennuksen. Käytännössä päivitys sisältää TKIP protokollan ja viestin eheyden tarkistuksen. WPA2 korvasi alkuperäisen WPA:n ja toi mukanaan tuen Counter Mode with CBC-MAC protokollalle, joka korvaa aikaisemman TKIP protokollan. (Geier 2005, 186.)

7 LAITTEISTOVAIHTOEHDOT WLAN-TOTEUTUKSEEN

Langattoman verkon toteutuksen päämäränä on mahdollistaa työntekijöiden ylläpitää varastosaldoja mobiililaitteilta, kuten tableteilta, perinteisten työasemien sijasta. Tämä helpottaa työntekoa, sillä varastotyöntekijät voivat tehdä varastosaldojen muutokset tai tarkistukset suoraan hyllypaikalla, eikä heidän tarvitse kävellä työpisteelle ja odottaa sen vapautumista. Lisäksi langattoman verkon on tarkoitus tuoda vierailijaverkko koko rakennukseen. Rakennus pitää sisällään 2-kerroksiset toimisto-, ruokailu- ja neuvottelutilat sekä lämpötilojen mukaan osioidun varastohallin, jossa on korkeat varastohyllyt. Varastotilassa on varastoitavien elintarvikkeiden mukaisesti vaihteleva lämpötila. Pakastetuotteet ovat huonelämpötilaltaan noin -15 celsiusasteen tilassa, kun taas muut tuotteet ovat huonelämpötilaltaan muutaman asteen pakkasen puolella. Tämä tarkoittaa, että valittavien laitteiden, erityisesti tukiasemien, on siedettävä kovaa pakkasta, ja niiden suunnitelussa täytyy olla huomioitu mahdollinen kondensio laitteen sisällä, johtuen laitteen omasta lämmöntuotosta ja laitteen ulkopuolella vallitsevasta suuresta lämpötilaerosta. Näihin tiloihin valitaan siis pääosin ulkokäyttöön suunniteltuja tukiasemia. Toimistotiloissa taas vallitsee normaali sisälämpötila, joten siellä voidaan käyttää tavanomaisia sisäkäyttöön tarkoitettuja tukiasemia.

Käytettävien kytkimien on oltava vierailijaverkon toteutusta varten hallittavia, jotta kytkimissä voidaan määrittää, missä porteissa kuljetetaan mitäkin VLAN liikennettä. Vierailijaverkon ja sisäverkon liikenne eristetään näin toisistaan. Kontrollerilta ei vaadita mitään erityisiä ominaisuuksia, lukuunottamatta kykyä hallita vähintään 9:ää tukiasemaa, joka on toteutuksen minimimäärä tukiasemia täyden kattavuuden saavuttamiseksi. Tukiasemien lukumäärän määritys käydään läpi seuraavassa luvussa. Kaikkien tukiasemien tulisi olla PoE-ominaisuudella varustettuja, eli niiden tulisi saada virta suoraan verkkopiuhasta.

7.1 ZyXEL

ZyXelin NWA tuoteperhe tarjoaa NWA3160-N tukiaseman, joka voidaan tarvittaessa muuttaa myös kontrolleriksi. NWA3160-N kontrollerimoodissa olevan tukiaseman kanssa yhteensopivat tukiasemat ovat NWA3560-N sisäkäyttöön tarkoitettu tukiasema ja NWA3550-N ulkokäyttöön tarkoitettu

tukiasema. NWA3160-N kontrollerimoodissa tukee korkeintaan 24 hallittua tukiasemaa.

Kaikki laitteet ovat PoE-tuettuja, joten niiden asentamisessa ei tarvita erikseen verkkovirtapistokkeita. Koska ZyXel oli pintapuolisessa vertailussa olleista tuotteista edullisin, käytettiin niitä mittapuuna muita tuotteita vertailtaessa. Tarkemmassa tarkastelussa ZyXelin tuoteperhe täytti kaikki ympäristön ensisijaiset vaatimukset eikä niissä ollut ylimääräisiä ominaisuuksia, jotka olisivat jääneet toteutuksessa käyttämättä. Ulkotilojen tukiasemien kustannuksia suunniteltaessa tuli ottaa huomioon, että ulkotilan tukiaseman mukana ei tullut antenneja, vaan ne oli tilattava erikseen. Valitun NWA-tuoteperheen spesifikaatiot on kuvattu kuviossa 5.

Model		NWA3160-N	NWA3560-N	NWA3550-N
Product name		802.11 a/b/g/n Unified Pro Access Point 	802.11 a/b/g/n Dual-Radio Unified Pro Access Point 	802.11 a/b/g/n Dual-Radio Outdoor Unified Pro Access Point 
Main Design				
Wireless frequency		2.4 GHz or 5 GHz	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz
Radio		1	2	2
Antenna		2 external dipole	4 external dipole	4 N-type connectors*
Supported data rates		802.11 a/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps 802.11n: up to 300 Mbps in MCS15 (40 MHz; GI = 400 ns)		
RF Specifications				
Frequency band	2.4 GHz (11 g/n)	USA: 2.412 to 2.462 GHz		
		ETSI: 2.412 to 2.472 GHz		
	5 GHz (11 a/n)	USA: 5.150 to 5.250 GHz; 5.725 to 5.850 GHz		
		ETSI: 5.15 to 5.35 GHz; 5.470 to 5.725 GHz		
Typical Transmit Output Power (Conducted)				
FCC	11 b/g	24 dBm	24 dBm	24 dBm
	11 g/n	21 dBm	21 dBm	21 dBm
	11a	21 dBm	21 dBm	21 dBm
	11 a/n	21 dBm	21 dBm	21 dBm
EU	11 b/g	17 dBm	17 dBm	17 dBm
	11 g/n	17 dBm	17 dBm	17 dBm
	11a	21 dBm	21 dBm	21 dBm
	11 a/n	21 dBm	21 dBm	21 dBm
LAN				
Number of 10/100/1000 Mbps LAN ports		1	1	1
PoE		Yes	Yes	Yes
PoE power draw		11 W	14 W	28 W
WLAN Features				
Maximum throughput		Up to 120 Mbps	Up to 140 Mbps	Up to 140 Mbps
WMM (Wi-Fi certified)		Yes	Yes	Yes
WEP		Yes	Yes	Yes
WPA/WPA2-PSK		Yes	Yes	Yes
WPA2 (Wi-Fi certified)		Yes	Yes	Yes
WPA/WPA2-Enterprise		Yes	Yes	Yes
EAP-TLS, TTLS, PEAP, SIM		Yes	Yes	Yes
Network				
VLANs		Yes	Yes	Yes
DHCP client		Yes	Yes	Yes
Security				
IEEE 802.1X		Yes	Yes	Yes
MAC filtering		Yes	Yes	Yes
RADIUS authentication		Yes	Yes	Yes
Embedded RADIUS server		Yes	Yes	Yes
EAP-type		EAP-TLS, EAP-TTLS, PEAP, SIM, FAST, AKA		
Rogue AP detection		Yes	Yes	Yes
Rogue AP containment		Yes	Yes	Yes
WLAN Management				
Controller mode		Yes	Yes	Yes
Standalone AP mode		Yes	Yes	Yes
Managed AP mode		Yes	Yes	Yes
CLI with SSH		Yes	Yes	Yes
Web UI with SSL		Yes	Yes	Yes
SNMP		Yes	Yes	Yes

KUVIO 5. ZyXel laitteiden yhteenveto (ZyXel 2015a)

7.2 D-Link

D-Linkin tuoteperheestä valittiin kontrolleriksi entry-tason kontrolleri, DWC-1000 (kuvio 6). Oletuksena kontrolleri tukee kuutta tukiasemaa, mutta määrää on mahdollista nostaa 24:n tukiasemaan ostamalla DWC-1000-6AP-LIC lisenssejä. Kyseinen kontrolleri tukee DWL-8600AP, DWL-6600AP ja DWL-3600AP tukiasemia (kuvio 7).

KUVIO 6. D-Link kontrolleri DWC-1000 (D-Link 2015a)

Access Point Management	
Compatible Managed APs	• DWL-8600AP • DWL-6600AP • DWL-3600AP
AP Discovery & Control	• Layer-2 • Layer-3
AP Monitoring	• Managed AP • Rogue AP • Authentication Fail AP • Standalone AP
Client Monitoring	• Authenticated Client • Rogue Client • Authentication Fail Client • Ad-hoc Client
Centralised RF/Security Policy Management	• Supported

KUVIO 7. DWC-1000 tuetut tukiasemat ovat rajalliset (D-Link 2015b)

Kontrollerin tuetuet tukiasemamallit ovat kaikki lämpötilan sietokyvyltään sisäkäyttöön tarkoitettuja tukiasemia, joiden operointilämpötila saa olla 0-40 °C. Tämä tarkoittaa, että D-Linkin tuoteperheestä ei löydy tässä hintaryhmässä lainkaan ulkokäyttöön sopivia tukiasemia, joita voitaisiin hallita DWC-1000 kontrollerin kautta. Sisäkäyttöön sopivista tukiasemista järkevin valinta näytti olevan DWL8600-AP, josta löytyy neljä säädettävää ulkoista antennia. DWL8600-AP tukiaseman spesifikaatiot on esitetty kuviossa 8.

Wireless Unified 802.11n Access Point

Wireless Frequency Range	▪ 802.11a: 5.15GHz to 5.35GHz and 5.725GHz to 5.825GHz ▪ 802.11b/g: 2.4GHz to 2.4835GHz ▪ 802.11n: 2.4 GHz-2.497 GHz and 4.9 GHz – 5.85 GHz			
Radio and Modulation Type	▪ For 802.11b (DSSS): DBPSK @ 1Mbps, DQPSK @ 2Mbps, CCK @ 5.5 and 11Mbps ▪ For 802.11a/g (OFDM): BPSK @ 6 and 9Mbps, QPSK @ 12 and 18Mbps, 16QAM @ 24 and 36Mbps, 64QAM @ 48, 54Mbps ▪ For 802.11a/g (DSSS): DBPSK @ 1Mbps, DQPSK @ 2Mbps, CCK @ 5.5 and 11Mbps ▪ For 802.11n: PSK/CCK, DQPSK, DBPSK, OFDM			
RF Channels	5GHz	12 Non-Overlapping Channels for US and Canada, 8 Non-Overlapping Channels for Japan, 19 Non-Overlapping Channels for EU, 5 Non-Overlapping Channels for China		
	2.4GHz	11 Channels for US, 13 Channels for EU, 13 Channels for Japan		
Transmit Output Power[4] (Typical at Each Throughput Rate)	802.11a	17dBm at 6/9/12/18Mbps, 15dBm at 24/36Mbps, 14dBm at 48Mbps, 13dBm at 54Mbps		
	802.11b	17dBm at 1/2/5.5/11Mbps		
	802.11g	17dBm at 6/9/12/18Mbps, 16dBm at 24/36Mbps, 15dBm at 48Mbps, 14dBm at 54Mbps		
	802.11n	5GHz Band/HT-20	5GHz Band/HT-40	2.4GHz Band/HT-20	2.4GHz Band/HT-40
		17 dBm at MCS0/8 17 dBm at MCS1/9 17 dBm at MCS2/10 15 dBm at MCS3/11 15 dBm at MCS4/12 14 dBm at MCS5/13 13 dBm at MCS6/14 12 dBm at MCS7/15	16 dBm at MCS0/8 16 dBm at MCS1/9 16 dBm at MCS2/10 14 dBm at MCS3/11 14 dBm at MCS4/12 13 dBm at MCS5/13 12 dBm at MCS6/14 11 dBm at MCS7/15	17 dBm at MCS0/8 17 dBm at MCS1/9 17 dBm at MCS2/10 16 dBm at MCS3/11 16 dBm at MCS4/12 15 dBm at MCS5/13 14 dBm at MCS6/14 13 dBm at MCS7/15	16 dBm at MCS0/8 16 dBm at MCS1/9 16 dBm at MCS2/10 15 dBm at MCS3/11 15 dBm at MCS4/12 14 dBm at MCS5/13 13 dBm at MCS6/14 12 dBm at MCS7/15
Receiver Sensitivity	802.11a	-87dBm at 6Mbps, -86dBm at 9Mbps, -84dBm at 12Mbps, -81dBm at 18Mbps, -77dBm at 24Mbps, -75dBm at 36Mbps, -68dBm at 48Mbps, -67dBm at 54Mbps		
	802.11b	-92dBm at 1Mbps, -90dBm at 2Mbps, -88dBm at 5.5Mbps, -84dBm at 11Mbps		
	802.11g	-87dBm at 6Mbps, -87dBm at 9Mbps, -85dBm at 12Mbps, -82dBm at 18Mbps, -79dBm at 24Mbps, -76dBm at 36Mbps, -71dBm at 48Mbps, -70dBm at 64Mbps		
	802.11n	5GHz Band/HT-20	5GHz Band/HT-40	2.4GHz Band/HT-20	2.4GHz Band/HT-40
		–82 dBm at MCS0/8 –79 dBm at MCS1/9 –77 dBm at MCS2/10 –74 dBm at MCS3/11 –70 dBm at MCS4/12 –66 dBm at MCS5/13 –65 dBm at MCS6/14 –64 dBm at MCS7/15	–79 dBm at MCS0/8 –76 dBm at MCS1/9 –74 dBm at MCS2/10 –71 dBm at MCS3/11 –67 dBm at MCS4/12 –63 dBm at MCS5/13 –62 dBm at MCS6/14 –61 dBm at MCS7/15	-85 dBm at MCS0/8 -82 dBm at MCS1/9 -80 dBm at MCS2/10 -77 dBm at MCS3/11 -74 dBm at MCS4/12 -69 dBm at MCS5/13 -68 dBm at MCS6/14 -67 dBm at MCS7/15	-82 dBm at MCS0/8 -79 dBm at MCS1/9 -77 dBm at MCS2/10 -74 dBm at MCS3/11 -71 dBm at MCS4/12 -66 dBm at MCS5/13 -65 dBm at MCS6/14 -63 dBm at MCS7/15
Antennas	▪ 4 Dualband detachable omnidirectional antennas with reverse SMA connectors ▪ Antenna Gain: 6dBi for 5GHz frequency band, 4dBi for 2.4GHz frequency band			
Ethernet Interface	10/100/1000BASE-T Port With 802.3af PoE			
Configurable Operation Mode	▪ Access Point only ▪ Access Point with Wireless Distribution System ▪ Wireless Distribution System			

KUVIO 8. D-Link DWL-8600AP tukiaseman ominaisuudet, tukiasema vastaa ZyXelin NWA3560-N tukiaseman ominaisuuksia (D-Link 2015c)

7.3 Cisco

Kontrolleriksi Ciscon tuotevalikoimasta valittiin 2500-sarjan laite, joka on Ciscon entry-tason kontrolleri (kuvio 10). Ciscon 2500-sarjan kontrolleri tukee enintään 75 tukiasemaa, ja käyttää CAPWAP-protokollaa tukiasemien hallitsemiseen. Sisätilojen tukiasemaksi valittiin Cisco Aironet 802.11n G2-sarjan 2600-malli, joka on suunniteltu pienyrityksille, varastohalleille sekä toimistotiloille. Ulkotilojen tukiasemaksi valittiin 1532E-sarjan tukiasema (kuvio 12). Laitteiden ominaisuudet ovat ympäristön vaatimusten kannalta samat kuin ZyXelin

laitteissa, lukuunottamatta että Cisco Aironet 2600-sarjan tukiasema kykenee jopa 450Mbps nopeuteen, käyttämällä 40Mhz kanavan leveyttä 5Ghz:n taajuusaluella. Cisco Aironet 2600-sarjan tukiaseman spesifikaatio on kuvattu kuviossa 11. (Cisco Systems 2015d)

Ciscon tuoteperheestä löytyy monia Ciscon kehittämiä ominaisuuksia kuten Cisco CleanAir Technology ja Cisco OfficeExtend Solution, jotka eivät ole toteutettavassa ympäristössä oleellisia. Cisco CleanAir teknologia havaitsee ja yrittää mitigoida RF-häirintää, ja yrittää näin turvata langattoman verkon suorituskykyä. Rakennus sijaitsee kuitenkin niin syrjässä muusta asutuksesta, että RF-häirintä ei ole aiheellinen huolenaihe. Cisco OfficeExtend tarjoaa hyödyllisiä ominaisuuksia etätyöntekijöille, mutta kaikki yrityksen työntekijät tekevät töitä pääosin paikan päällä. (Cisco Systems 2015d.)

KUVIO 9. Cisco 2500 Series Wireless Controller (Cisco Systems 2015b)

Feature	Benefits
Scalability	• Supports up to 75 access points • Supports up to 1000 clients
Ease of Deployment	• For quick and easy deployment Access Points can be connected directly to 2504 Wireless LAN Controller via two PoE (Power over Ethernet) ports
High Performance	• Wired-network speed and nonblocking performance for 802.11n and 802.11ac networks. Supports up to 1 Gbps throughput
RF Management	• Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwideCisco CleanAir® technology integration
Comprehensive End-to-End Security	• Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
End-to-end Voice	• SupportsUnified Communications for improved collaboration through messaging, presence, and conferencing • Supports allCisco Unified Wireless IP Phones for cost-effective, real-time voice services
High-Performance Video	• Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
PCI Integration	• Part of Payment Card Industry (PCI) certified architecture, and are well-suited for retail customers who deploy transactional data applications such as scanners and kiosks
OfficeExtend	• Supports corporate wireless service for mobile and remote workers with secure wired tunnels to the Cisco Aironet® 600, 1130, 1140 or 3500 Series Access Points • Extends the corporate network to remote locations with minimal setup and maintenance requirements • Improves productivity and collaboration at remote site locations • Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access • Reduced carbon dioxide emissions from a decrease in commuting • Higher employee job satisfaction from ability to work at home • Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Enterprise Wireless Mesh	• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network • Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing
Environmentally Responsible	• Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours
Mobility, Security and Management for IPv6 & Dual-Stack Clients	• Secure, reliable wireless connectivity and consistent end-user experience • Increased network availability by proactive blocking of known threats • Equips administrators for IPv6 troubleshooting, planning, client traceability from a common wired and wireless management system
Guest Anchor and Wired Guest Access	• Supports up to 15 guest anchor Ethernet over IP (EoIP) tunnels forpath isolation of guest traffic from enterprise data traffic • Extends the guest access services to the wired clients on par with other WLAN Controllers

KUVIO 10. Cisco 2500-sarjan kontrollerin avainominaisuudet (Cisco Systems 2015a)

802.11n Version 2.0 (and Related) Capabilities	• 3x4 multiple-input multiple-output (MIMO) with three spatial streams • Maximal ratio combining (MRC) • 802.11n and 802.11a/g beamforming • 20- and 40-MHz channels • PHY data rates up to 450 Mbps (40-MHz with 5 GHz) • Packet aggregation: Aggregated MAC Protocol Data Unit (A-MPDU) (Tx/Rx), Aggregated MAC Protocol Service Unit (A-MSDU) (Tx/Rx) • 802.11 dynamic frequency selection (DFS) • Cyclic shift diversity (CSD) support			
Data Rates Supported	**802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps**			
	802.11bg: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps			
	802.11n data rates (2.4 GHz[1] and 5 GHz):			
	MCS Index[2]	**GI[3] = 800ns**		**GI = 400ns**
		20-MHz Rate (Mbps)	**40-MHz Rate (Mbps)**	**20-MHz Rate (Mbps)**	**40-MHz Rate (Mbps)**
	0	6.5	13.5	7.2	15
	1	13	27	14.4	30
	2	19.5	40.5	21.7	45
	3	26	54	28.9	60
	4	39	81	43.3	90
	5	52	108	57.8	120
	6	58.5	121.5	65	135
	7	65	135	72.2	150
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270

KUVIO 11. Cisco Aironet 2600-sarjan tukiaseman ominaisuudet (Cisco Systems 2015c)

Item	Specification			
802.11n and Related Capabilities	• 1530I: 3x3 MIMO with 3 spatial streams (2.4 GHz) and 2x3 MIMO with 2 spatial streams (5 GHz) • 1530E: 2x2 MIMO with 2 spatial streams (2.4 GHz) and 2x2 MIMO with 2 spatial streams (5 GHz) • 20-MHz (2.4 and 5 GHz) and 40-MHz (5 GHz only) channels • PHY data rates up to 300 Mbps • Packet aggregation: A-MPDU (Tx/Rx) • 802.11 dynamic frequency selection (DFS) • Cyclic shift diversity (CSD) support			
Data Rates Supported	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps			
	802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps			
	802.11n data rates (2.4 and 5 GHz):			
	MCS Index[1]	**GI[2] = 800 ns**		**GI = 400 ns**
		20-MHz Rate (Mbps)	**40-MHz Rate (Mbps)**	**20-MHz Rate (Mbps)**	**40-MHz Rate (Mbps)**
	0	6.5	13.5	7.2	15
	1	13	27	14.4	30
	2	19.5	40.5	21.7	45
	3	26	54	28.9	60
	4	39	81	43.3	90
	5	52	108	57.8	120
	6	58.5	121.5	65	135
	7	65	135	72.2	150
	8	13	27	14.4	30
	9	26	54	28.9	60
	10	39	81	43.3	90
	11	52	108	57.8	120
	12	78	162	86.7	180
	13	104	216	115.6	240
	14	117	243	130	270
	15	130	270	144.4	300
	16	19.5		21.7	
	17	39		43.3	
	18	58.5		65	
	19	78		86.7	
	20	117		130	
	21	156		173.3	
	22	175.5		195	
	23	195		216.7	
	MCS 16-23 available on 1530I on 2.4 GHz only.			

KUVIO 12. Cisco 1532e-sarjan ulkokäyttöön tarkoitetun tukiaseman ominaisuudet (Cisco Systems 2015f)

7.4 Laitteistojen vertailu

Laitteiston vertailu suoritettiin arvioimalla seuraavia kriteereitä edellisestä luvusta:

- kontrollerin sallittu määrä tukiasemia.
- lähetysteho.
- ulkoiset, suunnattavat antennit.

- pakkasensieto.
- PoE, mahdollisuus kytkeä virta laitteeseen verkkojohdon kautta.

TAULUKKO 3. Laitteistovalmistajien kontrollerien vertailu

	ZyXel NWA3160-N	D-Link DWC-1000	Cisco 2500 Series Wireless Controller
Enimmäismäärä tukiasemia	24	24	75
PoE sisään	Kyllä	Ei	Ei
Sisäänrakennettu kytkin	Ei	Kyllä	Kyllä

TAULUKKO 4. Laitteistovalmistajien sisäkäyttöön tarkoitettujen tukiasemian vertailu

	ZyXel NWA3560-N	D-Link DWL8600-AP	Cisco Aironet 2600
Tuetut standardit	802.11a 802.11b/g 802.11a/n 802.11g/n	802.11a 802.11b/g 802.11n	802.11a 802.11b/g 802.11n
Enimmäis-lähetysteho	24 dBm	17 dBm	23 dBm
Ulkoiset antennit	4	4	4
PoE sisään	Kyllä	Kyllä	Kyllä

Mainostettu suorituskyky	140 Mbps	600 Mbps	450 Mbps
Vähimmäis-operointilämpötila	0°C	0°C	0°C

TAULUKKO 5. Ulkokäyttöön tarkoitettujen tukiasemien vertailu

	ZyXel NWA3550-N	D-Link (ei saatavilla)	Cisco 1532e
Tuetut standardit	802.11a 802.11b/g 802.11a/n 802.11g/n	-	802.11a 802.11b/g 802.11n
Enimmäis-lähetysteho	24 dBm	-	29dBm
Ulkoiset antennit	4	-	4
PoE sisään	Kyllä	-	Kyllä
Mainostettu suorituskyky	140 Mbps	-	300 Mbps
Vähimmäis-operointilämpötila	-40°C	-	-30°C

Kontrollerin vertailu on kuvattuna taulukossa 3. Ympäristön tarpeisiin riittää ZyXelin tuote, sillä tukiasemien määrä jää kokonaisuudessaan alle 24, ja laitteessa ei ole tarvetta sisäänrakennetulle kytkimelle.

Sisäkäyttöön tarkoitetuista tukiasemista ZyXel jäi teoreettisesti hitaimmaksi. Ympäristössä ei kuitenkaan ole suurta kaistaa vieviä sovelluksia, ja mainostettu 140 Mbps suorituskyky riittää yrityksen tarpeisiin. ZyXelin laitteesta löytyi suurin lähetysteho, mutta Ciscon Aironet 2600-sarjan tukiasema häviää sille ainoastaan yhdellä dBm:llä. Kaikista tukiasemista löytyy 4 suunnattavaa antennia, ja niihin voidaan syöttää virta verkkokaapelin kautta. Sisäkäyttöön tarkoitettujen tukiasemien vertailu on kuvattuna taulukossa 4.

Ulkokäyttöön tarkoitetuissa tukiasemissa teknisesti parempi laite on Ciscon 1532e, jossa on sekä parempi lähetysteho että suorituskyky. ZyXelin NWA3550-N ilmoittama 24 dBm lähetysteho ja 140 Mbps suorituskyky riittävät kuitenkin yrityksen tarpeisiin. Sekä Ciscon että ZyXelin tukiasemat kestävät pakkasta -30°C asti, joten ne täyttävät vaatimukset operointilämpötilan osalta. Ulkokäyttöön tarkoitettuja tukiasemia ei löytynyt D-Linkin valikoimista vertailussa olleelle kontrollerille. Ulkokäyttöön tarkoitettujen tukiasemien vertailu on kuvattuna taulukossa 5. Koska D-Link ei tukenut kontrollerimallissaan ulkokäyttöön tarkoitettuja tukiasemia, ja Ciscon tuotteet olivat kalliimpia kuin ZyXELin tuotteet, valittiin ympäristön laiteratkaisuksi ZyXELin NWA tuoteperhe.

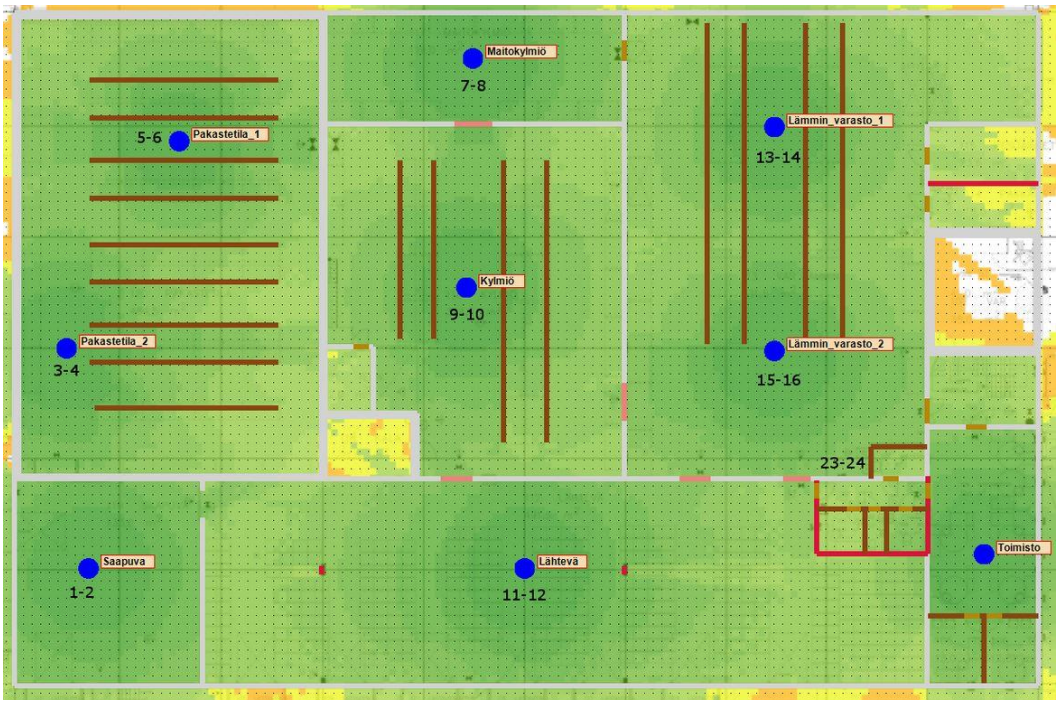
8 SUUNNITTELU

Ennen muun työn aloittamista, kartoitettiin ensin ympäristön nykyinen verkkotopologia. Vanhan topologian perusteella toteutettiin verkkosuunnitelma uudesta ympäristöstä, johon kuvattiin mitä virtuaalilähiverkkoja kuljetettiin minkäkin laitteen välillä.

Ympäristön palomuurilaite ei tukenut VLAN liikennettä, mutta esimerkiksi vierailijaverkon VLAN2 liikenne oli mahdollista purkaa kytkimellä, ja kuljettaa vierailijaverkon liikenne sisäverkosta eristetyssä verkkojohdossa palomuurille lähiverkosta eristettyyn porttiin.

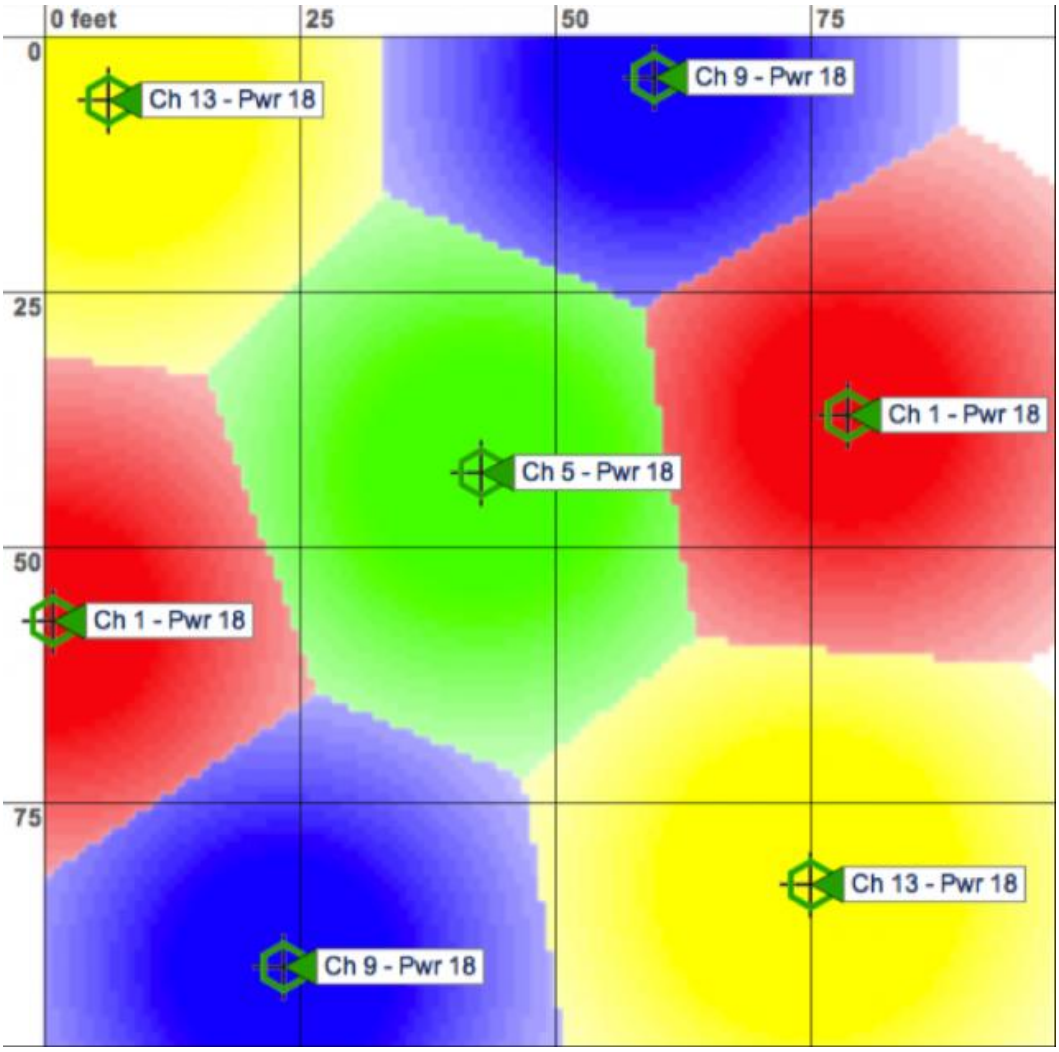
8.1 Tarvittavien tukiasemien määrä

Tarvittavien tukiasemien määrä määritettiin wlan-suunnitteluohjelmalla (kuvio 13), johon piirretään kaikki rakennuksen seinät oikeassa mittakaavassa, sekä määritetään niihin oikea seinämateriaali. Seinämateriaalin vaimennus määritettiin paikan päällä suorittamalla mittaus, jossa laskettiin paljonko seinän takaa tuleva signaali heikentyi. Lisäksi kuvaan piirrettiin muut tekijät, kuten ovet ja varastohyllyt. Kun pohjakuva oli valmis, sijoitettiin kuvaan tukiasemia valmistajan antamilla lähetystehon arvoilla, sekä määritettiin tukiasemian korkeus lattiasta sekä antennien sijanti. Tämän jälkeen tukiasemia lisättiin niin paljon, että koko varastohalliin saatiin kattava kuuluvuus. Käytetty suunnitteluohjelma oli Aerohive WiFi Planner.



KUVIO 13. Tukiasemien määrä ja summittainen sijanti määritettiin WLAN-suunnitteluohjelman avulla, joka kertoo tukiasemien signaalien vahvuudet erilaisten seinämateriaalien läpi

Kanavien suunnitteluun käytettiin myöskin visuaalista työkalua (kuvio 14). Tämä auttoi varmistamaan, että mitkään tukiasemien kanavat eivät menneet päällekkäin, ja näin aiheuttaneet mahdollisesti häiriötä palvelun laatuun. Tukiasemien kanaviksi valittiin 1, 6 ja 11.



KUVIO 14. Kanavien määrittely suunniteluohjelmalla (Aerohive 2015)

8.2 Langattoman sisäverkon tietoturva

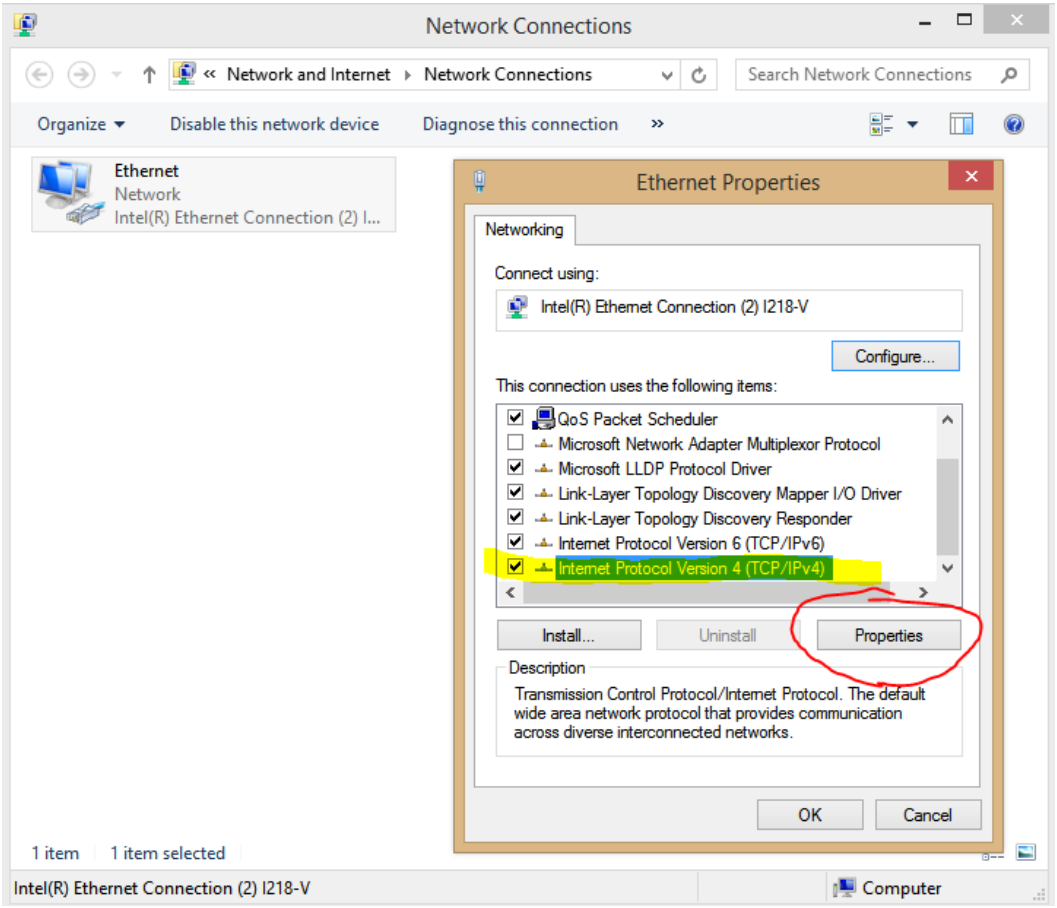
Langattoman sisäverkon tietoturvaksi valittiin WPA2-PSK (AES). Tämä tarkoittaa, että jotkut vanhemmat asiakaslaitteet eivät välttämättä saa yhteyttä sisäverkkoon, mutta tietoturvan taso on korkein, mitä laitteisiin oli asennushetkellä saatavilla.

Vieralijaverkko toteutettiin eristämällä vierailijaverkko sisäverkosta omaan virtuaaliverkkoonsa. Kyseinen virtuaaliverkko kuljetettiin palomuurille, josta edelleen liikenne ohjattiin internetiin, ja estettiin kaikki muu liikenne palomuurisäännöin.

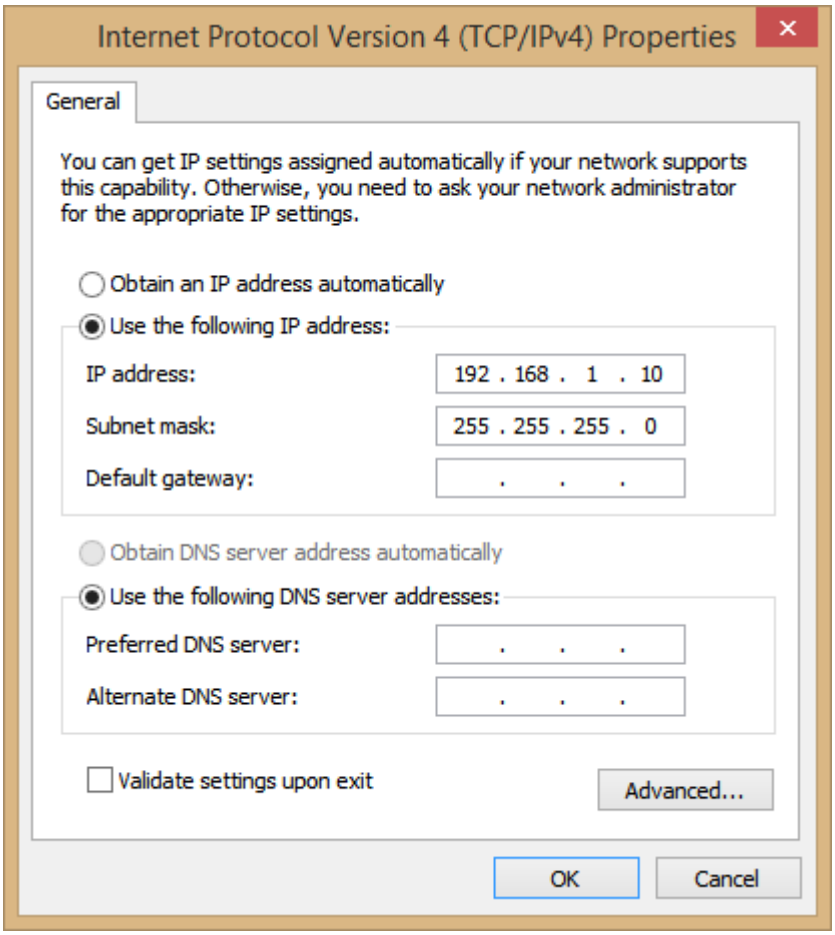
9 ZYXEL-JÄRJESTELMÄN KÄYTTÖÖNOTTO

Tukiasemien asennusta varten varastohalliin täytyi ensin suorittaa verkkojohtojen veto ja verkkopistokkeiden asennus. Tämän työn hoiti sähköasennuksiin erikoistuva yritys. Itse tietoverkon laitteistojen asentamiseen käytössä täytyi olla saksinosturi, jolla pääsi noin 5m:n korkeuteen.

Jotta laitteita päästään konfiguroimaan, täytyy ensin kytkettävän laitteen verkkokortin IP-asetuksia säätää niin, että laite on samassa osoiteavaruudessa tukiaseman kanssa (kuvio 15, 16). Oletuksena laitteiden hallinta-osoite on muotoa http://192.168.1.2, riippuen minkä tyyppinen laite on kyseessä. Windows-työasemalla verkkokortin IP-asetuksiin päästään ohjauspaneelin kautta.



KUVIO 15. Verkkokortin asetukset



KUVIO 16. Verkkokortin asettaminen samaan osoiteavaruuteen, kuin konfiguroitava tukiasema

9.1 Kytkinten konfigurointi

Tukiasemilta tuleva vierasverkon liikenne ohjattiin palomuurin DMZ-porttiin omassa VLAN-verkossa ja sisäverkosta eristetystä ip-avaruudessa. Tätä varten kytkimiin täytyi määrittää, mitkä portit kuljettavat mitäkin VLAN liikennettä. Pääkytkimen virtuaalilähiverkot konfiguroitiin taulukon 4 mukaisesti.

VLAN1: sisäverkko VLAN2: vierailijaverkko

TAULUKKO 6. Pääkytkimen VLAN konfiguraatio

Portti	VLAN1	VLAN2	Selitys
1-42	untagged	blocked	Päätelaitteet
43-44	untagged	tagged	Tukiasemat
45-46	tagged	tagged	↓DOWNLINK↓ Varastoon + 1 extra
47	blocked	untagged	↑UPLINK↑ DMZ
48	untagged	blocked	↑UPLINK↑ LAN

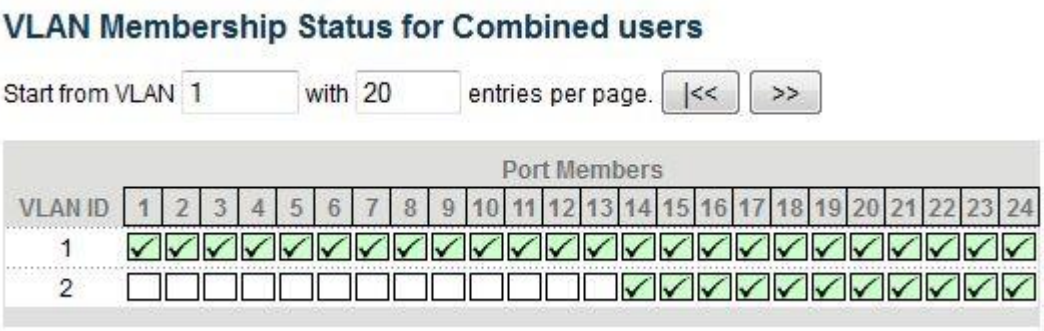
Pääkytkimen konfigurointilogiikka ajateltiin seuraavasti:

- Portit 1-42 ovat sisäverkon päätelaitteita varten, vlan1 untagged, vlan2 estetty.
- Portit 43-44 ovat tukiasemia varten, vlan1 untagged tukiasemien hallintaliikennettä varten, vlan2 tagged vierailijaverkon kuljetusta varten.
- Portit 45-45 ovat johtavat varaston kytkimelle, plus yksi ylimääräinen portti laajennusta varten.
- Portti 47 johtaa VLAN2 vierailijaverkon internetiin.
- Portti 48 johtaa VLAN1 sisäverkon palomuurille.

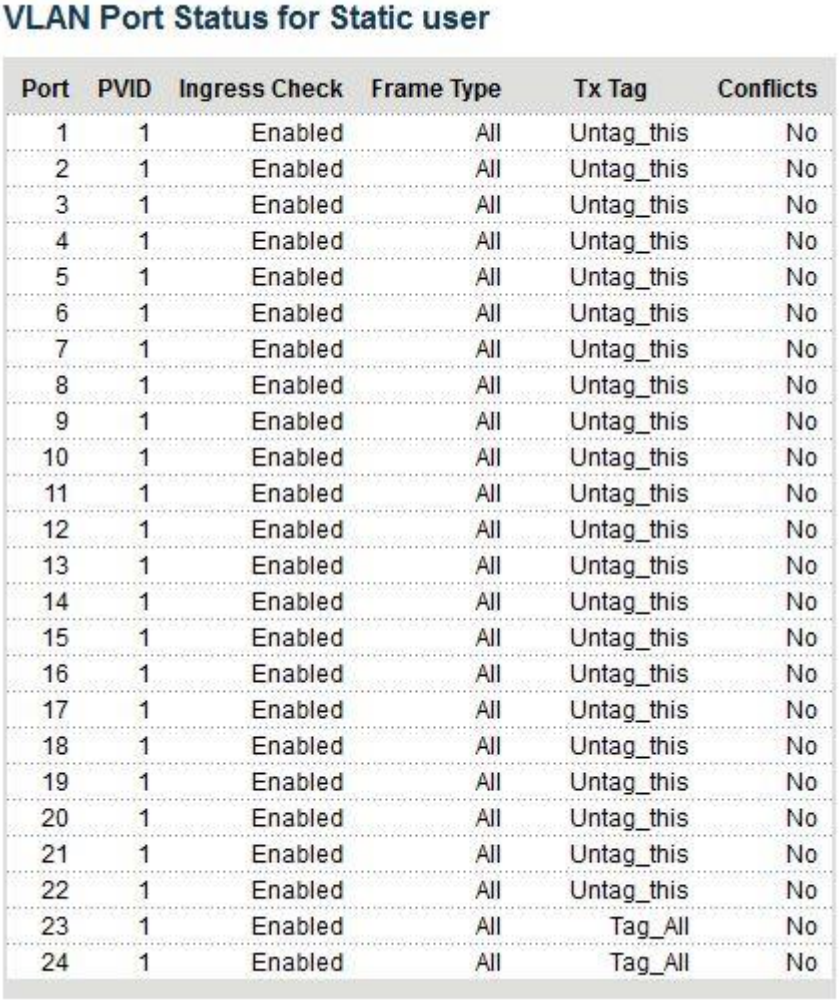
Varaston kytkimen virtuaalilähiverkot konfiguroitiin taulukon 4 mukaisesti. Varsinainen konfiguraatiotyö tehtiin graafisesta käyttöliittymästä, kuvattuna kuvioissa 17 ja 18.

TAULUKKO 7. Varaston kytkimen VLAN konfiguraatio

Portti	VLAN1	VLAN2	Selitys
1-13	untagged	blocked	Päätelaitteet
14-22	untagged	tagged	Tukiasemat
23-24	tagged	tagged	↑UPLINK↑ Pääkytkin + 1 extra



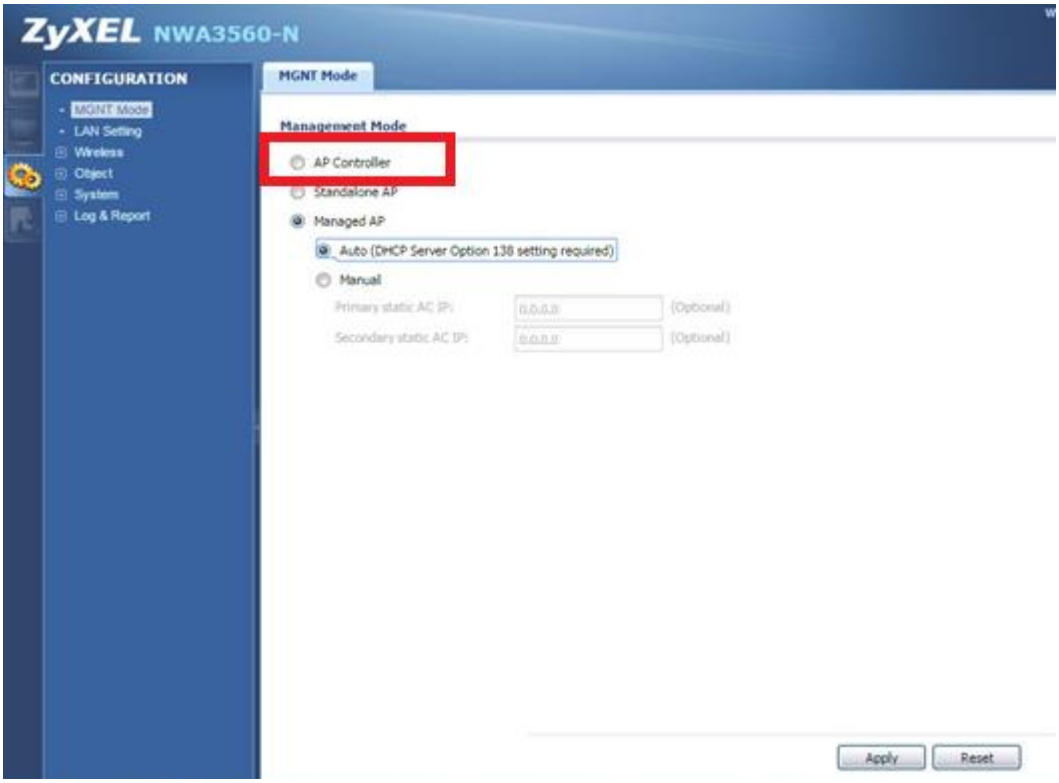
KUVIO 17. Kytkimen VLAN konfiguraation graafinen näkymä 1/2



KUVIO 18. Kytkimen VLAN konfiguraation graafinen näkymä 2/2

9.2 Kontrollerin konfigurointi

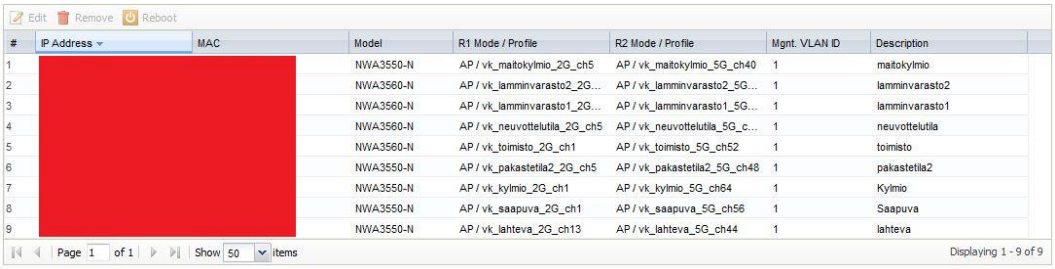
Tukiaseman ja kontrollerin konfigurointi tapahtuu osoittamalla internet-selain tukiaseman hallintaosoitteeseen, josta päästään kuvion 19 mukaiseen näkymään.



KUVIO 19. Tukiaseman saa muutettua kontrolleriksi valitsemalla Management Modesta AP Controller

Kun tukiasema on asetettu AP Controller- tilaan, tukiasema lataa laitteen oletuskonfiguraation ja käynnistyy uudestaan tyhjentäen tukiaseman kaikista siihen tähän mennessä tehdyistä muutoksista. Tämän jälkeen laitetta voidaan käyttää kontrollerina. Ensimmäiseksi kontrolleriin luodaan verkossa käytettävät SSID- ja salausasetukset, minkä jälkeen jokaiselle tukiasemalle luodaan oma radioprofiili. Profiiliin kytketään SSID- ja salausasetukset, joita käsitellään kontrollerissa objektina. Tämä tarkoittaa, että esimerkiksi verkon SSID arvoa voidaan muuttaa objektista, ja muutos näkyy kaikissa profiileissa, jotka käyttävät kyseistä objektia. Tukiaseman profiilin määritellään myös käytettävät 2,4 GHz:n ja 5 GHz:n kanavat. Kun profiili on valmis, liitetään se oikeaan tukiasemaan. Tukiasemat voidaan tunnistaa kontrollerissa MAC-osoitteen perusteella, jos ne on

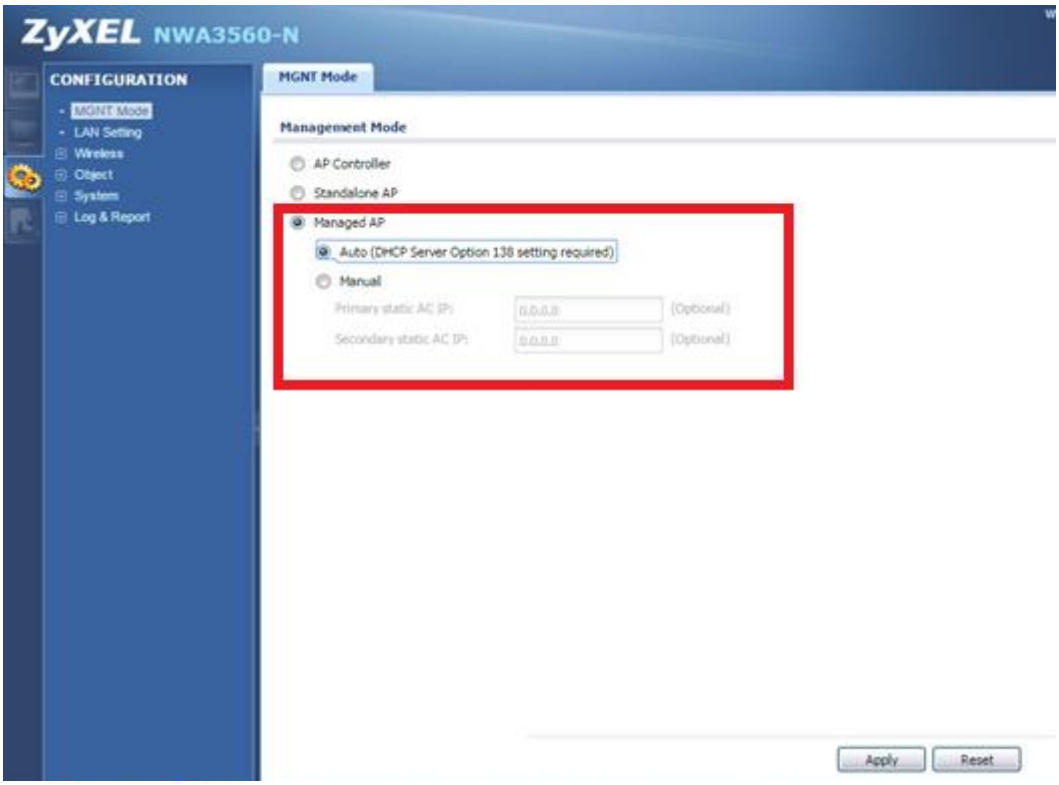
otettu ennen varsinaista asennusvaihetta laitteista talteen. Valmis kontrolleri, johon on määritelty kaikki tukiasemien profiilit, on kuvattu kuviossa 20.



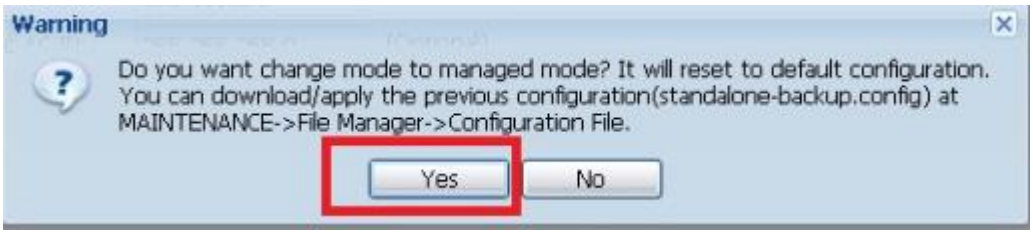
KUVIO 20. Kontrollerin konfigurointiin sisältyy kaikkien tukiasemien profiilien luominen, jossa kerrotaan mm. mitä kanavaa tukiaseman tulee käyttää

9.3 Tukiasemien konfigurointi

Tukiaseman alustava konfigurointi ei vaadi muuta kuin tukiaseman asettamisen hallittuun tilaan. Laite voidaan tässä vaiheessa konfiguroida hakemaan oman IP-osoitteensa automaattisesti DHCP-palvelimelta tai asettaa IP-asetukset manuaalisesti. Tukiaseman muuttaminen hallittuun tilaan on kuvattu kuviossa 21.



KUVIO 21. Suoraan tukiasemalla tehtävä konfigurointi ei vaadi muuta, kuin tukiaseman asettamisen Managed- tilaan



KUVIO 22. Apply- napin painamisen jälkeen laite lataa oletuskonfiguraation, ja poistaa siten kaikki laitteeseen tähän mennessä tehdyt muutokset

Kun tukiasema on muutettu managed-tilaan, voidaan sille määrittää kontrollerista oikea profiili, jolloin kontrolleri lataa tukiasemaan kaikki profiilissa määritellyt asetukset, kuten SSID-, salaus-, kanava- ja käyttöoikeusasetukset. Kontrolleri, johon on lisätty kaikki tukiasemat, on kuvattuna kuviossa 19.

9.4 Langattoman verkon toiminta

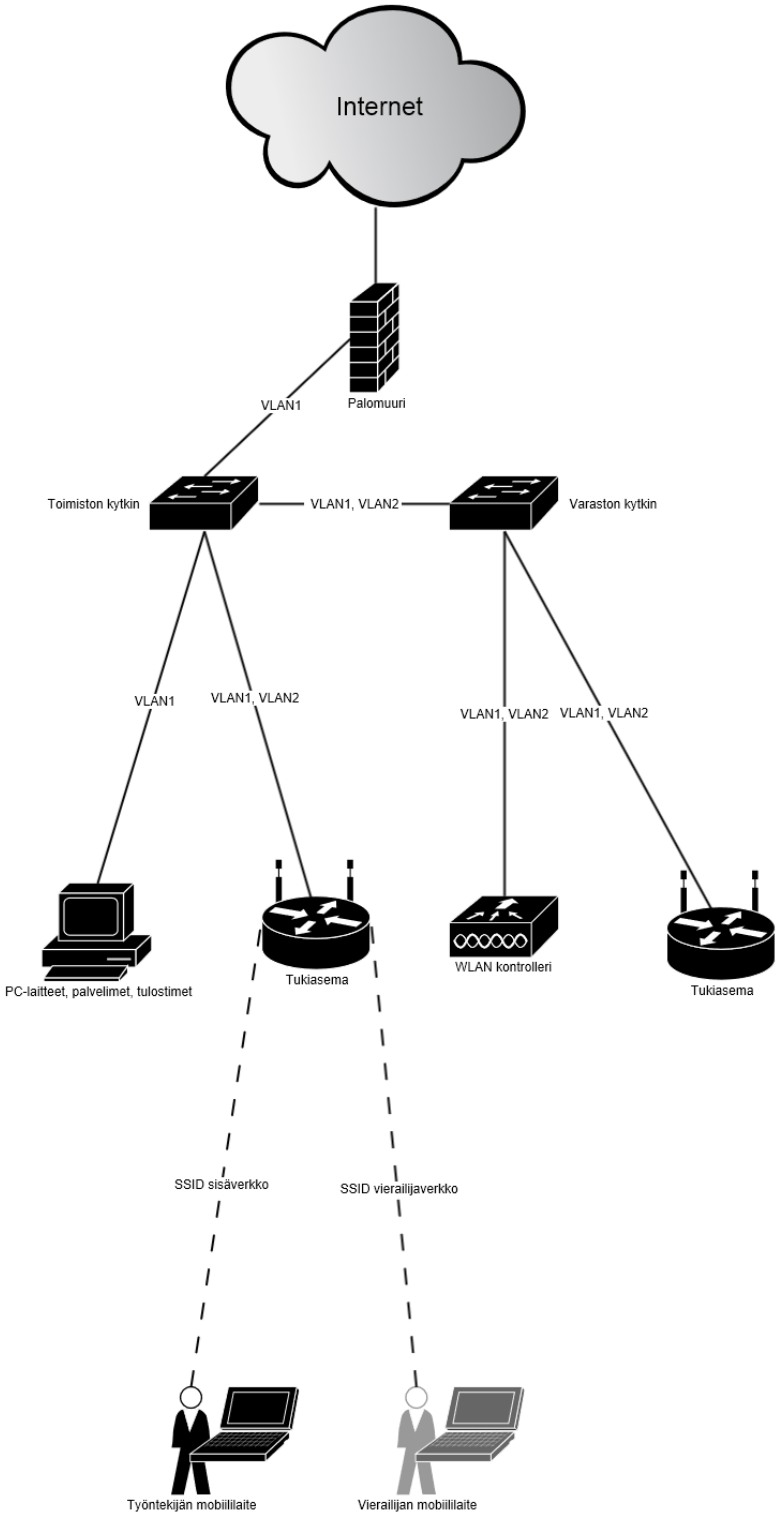
Toteutuneen verkkoympäristön kuvaan viitataan kuviossa 23. Ympäristöön lisättiin uuden WLAN-verkon toiminnan mahdollistamiseksi kaksi kytkintä, jotka

korvasivat ympäristön vanhat, ei-hallittavat kytkimet. Uusi pääkytkin oli ZyXELin hallittava 48-porttinen gigabitin kytkin, jossa ei ollut PoE-tukea. Pääkytkimeen ei ollut tarve tarjota PoE tukea jokaiselle portille, vaan ainoastaan muutamalle siihen kytketylle tukiasemalle. Tätä PoE-tuen puuttumista paikkaamaan pääkytkimen rinnalle asennettiin PoE-injektoreita, joiden avulla toimiston tukiasemat saatiin asennettua ilman AC-adaptereita. Varaston kytkin oli ZyXELin hallittava 24-porttinen kytkin PoE tuella, joka salli kaikkien varaston tukiasemien asentamisen ilman AC-adaptereita. PoE:n käyttö tukiasemien tapauksessa sallii myös tukiaseman uudelleen käynnistyksen pelkästään verkkojohdon irrotuksella, mikäli tukiasema on jostain syystä mennyt jumiin eikä se vastaa enää hallintakutsuihin. Kytkimiin määritettiin kaksi virtuaaliverkkoa, joista VLAN1 toimi sekä kontrollerilin hallintaverkkona että sisäverkon verkkona. VLAN2 määritettiin vierailijaverkoksi, joka eristettiin täysin sisäverkosta.

Tukiaseman liittyminen kontrolleriin tapahtuu ensin liittämällä tukiasema kytkimen portiin, jossa on joko suoraan PoE tuki, tai porttiin, johon tulee virta PoE-injektorin kautta. Lisäksi kyseisessä kytkimen portissa täytyy olla VLAN1 tilassa untagged ja VLAN2 tilassa tagged, jotta tukiasemien konfiguraatioliikennettä, sisäverkon liikennettä ja vierailijaverkon liikennettä voidaan kuljettaa eteenpäin. Kun tukiasema käynnistyy, se hake ensin IP-osoitteen verkon DHCP-palvelimelta. Tämän jälkeen kontrolleri havaitsee tukiaseman CAPWAP protokollan avulla tasolla 3, VLAN1 verkossa. Kun kontrolleri on havainnut tukiaseman, se pitää manuaalisesti hyväksyä kontrollerin käyttöliittymästä, mikäli kyseessä oli täysin uusi tukiasema. Jos tukiasema oli ollut verkossa jo ennestään kiinni, laite tunnistaa sen MAC-osoitteen perusteella. Mikäli tukiasemien konfigurointia tarvitsee muuttaa, siihen liittyvä konfigurointiliikenne tapahtuu CAPWAP protokollalla, kuljetettuna VLAN1 verkossa.

Langattoman verkon standardina käytettiin 802.11n standardia, joka tarjoaa käyttöön sekä 2,4 GHz:n ja 5 GHz:n taajuusalueet. 2,4 GHz:n taajusalueella käytettiin kanavia 1, 6 ja 11, jotta mikään kanava ei aiheuttaisi häiriötä toiselle. 5 GHz:n taajuusalueella käytössä on enemmän kanavia, ja useimmalle tukiasemalle

pystyttiin näin määrittämään täysin oma kanava. Yksi tukiasema mainosti kahta SSID:tä (sisäverkko ja vierailijaverkko) samanaikaisesti yhdellä radiopiirillä. Sisäverkkoon liittyneet käyttäjät ohjattiin VLAN1 virtuaaliverkkoon, kun taas vierailijaverkkoon liittyneet olivat virtuaaliverkossa VLAN2. Molemmissa verkoissa liikenteen salaukseen käytettiin WPA2 protokollaa, esijaetulla avaimella (PSK) ja AES salausalgoritmilla.



KUVIO 23. Toteutuneen verkon kuva

10 YHTEENVETO JA JOHTOPÄÄTÖKSET

Keskitetysti hallittavat wlan-järjestelmät ovat osa tehokkaasti ylläpidettävää nykypäivän IT-ympäristöä. Yksittäisten tukiasemian hallita on jäänyt historiaan kaikissa paitsi aivan pienimissä ympäristöissä. Esimerkiksi langattoman verkon salasanan vaihtaminen saattaisi viedä suuremmassa wlan-ympäristössä tuntikausia, jos salasana täytyisi vaihtaa jokaiseen tukiasemaan erikseen, puhumattakaan mistään muista ylläpitotoimenpiteistä. Langattomassa sisäverkossa tuo mukanaan muitakin hyötyjä, sillä monella työntekijällä on nykypäivänä mukanaan monenlaisia verkkoyhteyden vaativia laitteita. Matkapuhelin, tabletti ja kannettava ovat kaikki yleisiä työvälineitä, joilla on tarve päästä käsiksi nopeaan internet-yhteyteen tai sisäverkon resursseihin. Langaton sisäverkko vähentää myös tarvittavien johtojen määrää työpisteiden tietokoneita kytkettäessä ja sallii työntekijöiden liikkua työpisteiltä toisaalle ilman yhteyden menettämistä yrityksen sisäverkon sovelluksiin.

Eri järjestelmiä vertailtaessa Cisco vaikutti laadukkaimmalta, mutta myös hinnaltaan kalleimmalta. Lisäksi Ciscon tuotteissa oli joitakin ominaisuuksia, joista ei ollut ympäristössä käyttöä. D-Linkin tuoteperhe tarjosi pelkästään sisäkäyttöön sopivia tukiasemia, joten ne eivät soveltuneet ainakaan pakastetiloissa käytettäviksi. ZyXelin tuotteet tarjosivat kaikki avainominaisuudet, kylmien lämpötilojen keston sekä sopivan määrän kontrolloitavia tukiasemia, ilman ylimääräisiä kustannuksia. Yksinkertaisuuden ja tuotetuen vuoksi kaikki tuotteet valittiin ZyXeliltä.

Laitepäätöksen tekemisen jälkeen suoritettiin ensin pienen testiympäristön toteuttaminen kytkimillä, tukiasemilla ja kontrollerilla ennen varsinaista asennustyön tekemistä. Tällä varmistettiin, että laitteet varmasti toimivat ennen paikalleen asennusta, sillä asennuspaikka oli monessa kohtaa noin viiden metrin korkeudessa, eikä laitteita saa vaihdettua ilman saksinosturia. Tämä osoittautuikin kannattavaksi, sillä yksi ulkotilojen tukiasemista kieltäytyi toimimasta huoneenlämmössä ja pysyi päällä ainoastaan kun lämpötila oli pysyvästi pakkasen puolella. Kyseinen laite toimitettiin ZyXelille vaihdettavaksi.

Laitteiden asennus kesti kokonaisuudessaan kaksi työpäivää ja oli osin haastavaa, sillä pakastetilojen lämpötila oli noin -20 celsiusastetta ja vaati kuitenkin sormiketteryyttä tukiasemien kiinnitysruuveja pyöriteltäessä. Lisäksi pakastehallien kylmäpuhaltimet olivat muutamien metrin päässä asennuspaikoista, mikä lisäsi osaltaan kylmän viiman määrää.

Laitteistojen asennuksen jälkeen suoritettiin kaikkien tukiasemien testaus, jossa mitattiin signaalin vahvuutta ja roaming-ominaisuuden nopeutta. Näissä ei nähty puutteita, ja järjestelmä nähtiin valmiiksi käyttöön otettavaksi. Työn tuloksena oli nopea langaton sisäverkko varastotyöntekijöille, jotka pystyvät ylläpitämään varastosaldoja suoraan mobiililaitteilta perinteisen pöytäkoneen sijasta. Tämä vähentää edestakaisessa kävelyssä kulunutta aikaa ja pienentää virheiden määrää, sillä varastosaldoja pystyy muuttamaan suoraan hyllypaikkaa tarkastellessa. Toimistotyöntekijät voivat helposti liittää kannettaviaan yrityksen sisäverkkoon ilman ylimääräisiä verkkojohtoja. Vierailijoilla on pääsy internetiin langattomasti vierailijaverkon kautta, mikä on hyödyllistä, sillä kylmävarastohalli vaimentaa puhelinverkon signaalia merkittävästi estäen signaalin paikoittain kokonaan.

LÄHTEET

Aerohive. 2015. figure_6_w640.png [viitattu 13.4.2015]. Saatavissa: http://cdn2.content.compendiumblog.com/uploads/user/353b2039-a79a-484d-95f4-d4af4fc7eeda/99964814-45e7-4c4d-a0f6-b90b76e41c61/Image/204e185cd83163da161856436ba6fb85/figure_6_w640.png

Cisco Verkkoakatemia. 2002. Ensimmäinen vuosi. Helsinki: Edita Prima Oy

Cisco Systems 2015e. The Benefits of Centralization in Wireless LANs. [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd8040f7b2.html

Cisco Systems. 2015d. DWL-8600 Datasheet [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/dam/en/us/products/collateral/enterprise-networks/officeextend-solution/at_a_glance_c45-652411.pdf

Cisco Systems. 2015b. 2500-series-wireless-controllers [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/wireless/2500-series-wireless-controllers/index.html#

Cisco Systems. 2015a. 2500-series-wireless-controllers [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.pdf

Cisco Systems. 2015c aironet-2600 Datasheet [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2600-series/data_sheet_c78-709514.pdf

Cisco Systems. 2015f aironet-1530 Datasheet [viitattu 13.4.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data_sheet_c78-728356.html

D-Link. 2015a. DWC1000 [viitattu 13.4.2015]. Saatavissa: http://www.dlink.com/uk/en/business-solutions/wireless/unified-wireless/wireless-controllers/dwc-1000-d-link-wireless-controller

D-Link. 2015b. DWC1000 Datasheet [viitattu 13.4.2015]. Saatavissa: http://www.dlink.com/-/media/Business_Products/DWC/DWC%201000/Datasheet/DWC_1000_Datasheet_EN_UKI_2.pdf

D-Link. 2015c. DWL-8600 Datasheet [viitattu 13.4.2015]. Saatavissa: ftp://ftp.dlinkla.com/pub/DWL-8600AP/DWL-8600AP_A1_Datasheet_01(W).pdf

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

P. Calhoun, M. Montemurro, D. Stanley. 2009. RFC 5415. CAPWAP Protocol Specification. [viitattu 13.4.2015]. Saatavissa: https://tools.ietf.org/html/rfc5415#section-1.1

P. Calhoun, R. Suri, N. Cam-Winget, M. Williams, S. Hares, B. O'Hara, S.Kelly. 2010. RFC 5412. Lightweight Access Point Protocol. [viitattu 13.4.2015]. Saatavissa: https://tools.ietf.org/html/rfc5412#section-2

Wikipedia. 2015a. IEEE 802.11. [viitattu 13.4.2015]. Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11

Wikipedia. 2015b. List of WLAN channels. [viitattu 13.4.2015]. Saatavissa: http://en.wikipedia.org/wiki/List_of_WLAN_channels

Wikipedia. 2015c. OSI-mallin kerrokset. [viitattu 13.4.2015]. Saatavissa: http://fi.wikipedia.org/wiki/OSI-malli#/media/File:OSI-malli.jpg

ZyXel. 2015a. NWA3160-N Datasheet [viitattu 13.4.2015]. Saatavissa: ftp://ftp2.zyxel.com/NWA3160-N/datasheet/NWA3160-N_5.pdf