Metropolia

TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

LANGATTOMAT LÄHIVERKOT 100–300 KÄYTTÄJÄN YRITYKSISSÄ

Työn tekijä: Samuli Rantala
Työn valvoja: Jukka Louhelainen
Työn ohjaajat: Jouko Näätänen

Työ hyväksytty: ___. ___. 2010

Jukka Louhelainen
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin Appelsiini Finland Oy:lle osana Metropolia Ammattikorkeakoulun insinööriopintojani. Työn aihe selvisi helposti, mutta insinöörityön varsinainen tekeminen päivätyön ohella vaati oman aikansa.

Kiitän projektissa mukana olleita henkilöitä, erityisesti Appelsiinin puolelta Thomas Jaatista, Marko Johanssonia ja Jouko Näätästä. Iso kiitos kuuluu myös perheelleni tukemisesta ja jaksamisesta tämän työn aikana.

Helsingissä 14.2.2010

Samuli Rantala

TIIVISTELMÄ

Työn tekijä: Samuli Rantala

Työn nimi: Langattomat lähiverkot 100-300 käyttäjän yrityksissä

Päivämäärä: 14.2.2010 **Sivumäärä:** 53 s.

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: lehtori Jukka Louhelainen

Työn ohjaaja: Jouko Näätänen

Tässä työssä perehdytään WLAN-verkkoihin 100–300 käyttäjien yrityksissä. Työ tehtiin yhteistyössä Appelsiini Finland Oy:n kanssa.

WLAN-verkot mahdollistavat verkkoyhteyden toimittamisen yrityksissä sellaisiin tiloihin, joissa normaalia kiinteää verkkoa ei ole tarjolla tai sen käyttö on hankalaa. Langattomalla verkolla on myös helppo tarjota verkkoyhteys neuvottelutiloihin, niin yrityksen työtekijöille kuin vierailijoillekin.

Yrityskäytössä langattomien verkkojen tietoturva korostuu huomattavasti kotikäyttöä enemmän. Työssä painotettiin verkkoja tutkiessa erityisesti näkökantaa verkon turvallisuuden osalta yrityskäytössä.

Työssä käydään aluksi läpi WLAN-verkkojen yleisiä määritelmiä. Tämän jälkeen tutustutaan langattomien verkkojen vaatimuksiin yrityskäytössä, erityisesti suojauksen ja fyysisen rakenteen osalta.

Työtä tehdessä haastateltiin kolmen eri yrityksen langattoman verkon ylläpitäjiä. Ylläpitäjiltä selvitettiin tietoa verkkojen rakenteista, tekniikoista ja syistä, miksi verkoissa oli päädytty käytettyihin ratkaisuihin.

Tutkituista yrityksistä tehtiin yhteenvedot ja lopuksi määriteltiin suositukset langattomien verkkojen tekniikoille tutkittujen yritysten kokoisissa yrityksissä.

Työn lopuksi luotiin vielä lyhyt katsaus tulevaisuuden tekniikoihin ja näkymiin yrityskäytössä.

Avainsanat: WLAN, langaton lähiverkko, yrityskäyttö, tietoturva

Metropolia

ABSTRACT

Name: Samuli Rantala

Title: Wireless networks in 100-300 user companies

Date: 14.2.2010 **Number of pages:** 53

Department: **Study Programme:**

Information Technology Telecommuniactions

Instructor: Jukka Louhelainen, lecturer

Supervisor: Jouko Näätänen

The purpose of this study was to learn about wireless networks in 100 to 300 user companies. The study was assigned by Appelsiini Finland corporation.

WLAN networks enable network connections to places where normal wired networks are not avaible or would not be convenient to use. Wireless networks also enable network access for convention rooms, where it can be used by the company staff or visitors.

Wireless networks in business use require significantly more security than private use. This work was done especially in the wireless security at the business point of view.

The thesis starts by introducing general principles of wireless networks. Following that the study concentrates in business requirements of wireless networks, especially in network security and physical structure of the network.

This study was done by interviewing network administrator of three different companies. The purpose of the interviews was to find out what kind of wireless networks there were in the companies and why the used technologies were chosen.

Based on the interviews, summary and recommendations were made about wireless networks in companies size of those that were studied.

A brief look into the future of wireless networks was made at the end of the thesis.

Keywords: WLAN, wireless networks, business use, security

SISÄLLYS

1 JOHDANTO

Tässä työssä on tarkoituksena perehtyä kolmeen erilaiseen langattomaan verkkoon yrityskäytössä: kohteena on kolme 100–300 käyttäjän yritystä. Yritykset on nimetty tietoturvan takia Yritys A:ksi, Yritys B:ksi ja Yritys C:ksi. Tarkoituksena on tutkia, mitä kyseiset yritykset halusivat langattomalta sisäverkolta ja miksi se haluttiin rakentaa.

Valittujen yritysten langattomiin verkkoihin perehdyttiin haastattelemalla kyseisten yritysten verkkojen ylläpitäjiä. Ylläpitäjiltä selvitettiin tietoja verkon rakenteesta, käytetyistä tekniikoista, syitä käytettyjen tekniikoiden valinnoille ja haasteista verkkojen käytössä.

Tarkoituksena on myös selvittää, miten hyvin kyseiset verkot ovat toimineet käytössä, voidaanko jotain ratkaisuista suositella jatkossa muille asiakkaille ja jos ei, niin selvittää, mikä olisi nykyaikainen ja toimiva ratkaisu langattoman verkon rakentamiseen kohdeyritysten kaltaisissa yrityksissä.

Työssä keskitytään nimenomaan langattomien verkkojen käyttöön yrityskäytössä, joten yksityiskäyttöön tarkoitettuja tekniikoita tai menetelmiä ei käsitellä kovinkaan tarkasti.

Työn alussa käsitellään, mitä langattomat verkot ovat ja mitä erityistarpeita yrityskäytöllä on verkoille, esimerkiksi verkon rakenteen tai verkkoon tunnistautumisen osalta. Tämän jälkeen tutustutaan tutkittaviin yrityksiin ja tehdään niiden pohjalta loppupäätelmät, mikä ratkaisuista on paras tai mahdollisesti tutkitaan, onko markkinoilla olemassa parempia ratkaisuja.

Lopuksi luodaan lyhyesti katsaus, mitä tulossa olevat langattomat tekniikat merkitsevät kohteena olevien yritysten kokoisille yrityksille.

2 MITÄ LANGATTOMAT LÄHIVERKOT OVAT?

Langattomilla lähiverkoilla tarkoitetaan tekniikkaa, jolla tietokoneet tai muut laitteet voivat muodostaa verkkoyhteyden toisiinsa tai olemassa olevaan kiinteään verkkoon langattomasti. [1.]

Kiinteä verkko voi tässä yhteydessä olla suora yhteys internetiin tai sitten lähiverkko kotona tai yrityksessä. Yrityskäytössä langatonta verkkoa yleensä

käytetään kannettavan tietokoneen kytkemistä langattomasti yrityksen kiinteään lähiverkkoon ja sitä kautta tarvittaessa internetiin. Langattoman lähiverkon ei siis ole yrityskäytössä tarkoitus korvata kiinteää verkkoa, vaan se toimii sen langattomana jatkeena.

Yleisesti langattomista lähiverkoista puhuttaessa käytetään termiä WLAN, eli Wireless Local Area Network. Langattomat lähiverkot ovat nykypäivänä käytännössä kaikki IEEE 802.11 –standardiin perustuvia [2]. IEEE, eli *Institute of Electrical and Electronics Engineers* on kansainvälinen järjestö, joka ylläpitää ja suunnittelee erilaisia tekniikan alan standardeja. Ensimmäinen 802.11 -standardi muodostettiin vuonna 1997 ja sitä tarkennettiin vuonna 1999. [3.]

802.11-standardi kehittyy tasaisin väliajoin tuoden mukanaan uusia ominaisuuksia langattomiin verkkoihin. Suurimmat uudistukset koskevat yleensä uusia taajuusalueita, nopeampia nopeuksia, parempaa liikenteen salausta ja parempaa laitteiston suojausta tunkeutujia vastaan. [3.]

2.1 Verkon rakenne

Langattoman lähiverkon voi muodostaa suoraan kahden päätelaitteen, esimerkiksi kahden kannettava tietokoneen, välille (kuva 1) tai sitten langattoman tukiaseman avulla päätelaitteen ja kiinteän verkon välille (kuva 2).

2.1.1 AD-HOC-verkko

Suoraan laitteiden välisiä yhteyksiä harvemmin käytetään, vaan suurin osa yhteyksistä on langattomasta päätelaitteesta kiinteään verkkoon. Näistä päätelaitteiden välisistä yhteyksistä käytetään myös termiä AD-HOC-verkko.

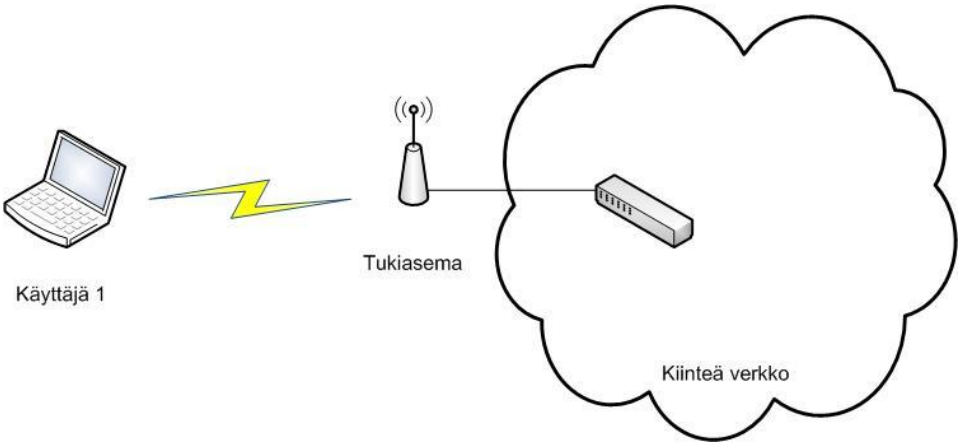
Suoran yhteyden käytön vähyys johtuu pääosin tämänhetkisen standardin mukaisten AD-HOC-verkkojen toiminnan vaatimasta korkeasta laskentatehosta ja sitä kautta suuresta virrankulutuksesta. Nykytekniikalla toteutettujen AD-HOC-verkkojen muodostaminen on myös käyttäjille turhan vaikeaa. [1.]

Kuva 1. Yhteys päätelaitteiden välillä

2.1.2 Tukiasemapohjainen verkko

Kiinteään verkkoon yhdistettäessä verkon reunalle tarvitaan langaton tukiasema, joka toimii siltana kiinteään verkkoon (kuva 2). Päätelaite muodostaa langattomasti yhteyden tukiasemaan, joka ohjaa liikenteen eteenpäin kiinteään verkkoon.

Eri langattomat verkot tukiasemissa erotellaan langattomien verkkojen tunnisteilla (SSID), joita voi yritystason tukiasemissa olla määriteltynä useampia. Yleisesti verkkojen tunnisteista puhuttaessa niitä kutsutaan yksinkertaisesti verkkojen nimiksi. Lisäksi yksittäiset verkot eritellään erillisillä kanavilla, joita on valittavissa Euroopassa 13 eri kanavaa ja Yhdysvalloissa 11 kappaletta. Kanaviin jaottelu mahdollistaa häiriöiden välttämisen, mikäli samalla alueella on useampi langaton verkko. [1.]



Kuva 2. Yhteys tukiaseman kautta

2.2 Taajuudet

WLAN-tekniikka perustuu OFDM-modulointiin, joka tarkoittaa, että tietoa voidaan siirtää samanaikaisesti usealla taajuudella niiden sekoittamatta toisiaan. Tätä hyödynnetään WLAN-verkoissa siten, että verkkoja voi olla sa-

malla maantieteellisellä alueella ilman, että ne häiritsevät merkittävästi toistensa toimintaa. Koska taajuuskaista on rajallinen, hidastavat samalla taajuudella olevat verkot toisiaan.

Tällä hetkellä WLAN-tekniikan käyttämä 2,4 GHz:n alue on vielä jaettu kanaviin, jotka nykyisissä 802.11g-luokan laitteissa ovat leveydeltään 20 MHz. Mikäli samalla alueella on käytössä runsaasti verkkoja, saattavat tyhjät tai vähemmän käytössä olevat kanavat loppua kesken ja verkot alkavat hidastaa toisiaan huomattavasti.

Ongelma korostuu erityisesti käytettäessä uusimman standardin 802.11n mukaisia laitteita. 802.11n-standardin mukaisten kanavien leveys on 40 MHz, jolloin ne varaavat kaksi vierekkäistä 802.11g-standardin kanavaa. Mikäli häiriöttömiä 40 MHz kanavia ei ole tarjolla, siirtyvät n-standardin laitteet käyttämään 20 MHz:n kanavaa, joka välittömästi puolittaa nopeuden siitä, mitä 40 MHz:n kanavaleveyttä käytettäessä.

Euroopassa käytössä olevat WLAN-verkkojen taajuudet ovat yleisesti 2,4 GHz ja Amerikassa käytössä oleva 5 GHz:n alue. Lisäksi uusin 802.11n-standardi käyttää haluttaessa 5 GHz:n aluetta myös muualla maailmassa. 5 GHz:n alue on vähemmän ruuhkainen kuin 2,4 GHz:n alue, joten sitä käytettäessä pyritään välttämään häiriöitä muiden samalla taajuusalueella liikennöivien verkkojen tai tekniikoiden kanssa. Näin pyritään myös saavuttamaan standardin mukainen 40 MHz:n kaistanleveys ja sitä kautta täysi nopeushyöty uudesta standardista. [3.]

2.3 Nopeudet

WLAN-verkkojen nopeudet ovat parantuneet jatkuvasti uusien standardien mukaan. Uusimpien tekniikoiden ansiosta langattoman verkon kautta pystytään nykyään tarvittaessa siirtämään sujuvasti jo erittäin paljon tiedonsiirtokapasiteettia vaativia sovelluksia, kuten esimerkiksi teräväpiirtovideota.

Aikajärjestyksessä standardien nopeudet ovat seuraavat:

- 802.11, nopeudeltaan 1 tai 2 Mbit/s, nykypäivänä korvattu uudemmilla tekniikoilla.
- 802.11a, nopeudeltaan 54 Mbit/s, käyttää 5 MHz aluetta ja käytössä ainoastaan Amerikassa.

- 802.11b, nopeudeltaan 11 Mbit/s, vanhentunut tekniikka, mutta käytössä vielä joissakin ympäristöissä ja yhteensopivuuden takia nykyiset tukiasemat vielä tukevat kyseistä standardia.

- 802.11g, nopeudeltaan 54 Mbit/s, yleisin tällä hetkellä käytössä oleva tekniikka.

- 802.11n, nopeudeltaan 600 Mbit/s, uusin virallistettu standardi, joka todennäköisesti alkaa korvata 802.11g-standardia uusien laitteiden saapuessa markkinoille.

Kyseiset nopeudet ovat vain standardin maksiminopeuksia. Todellinen käytettävissä oleva tiedonsiirtonopeus on huomattavasti matalampi. Pieni osa tiedonsiirtokapasiteetista kuluu verkon kontrolliviesteihin, mutta suurin hävikki syntyy signaalin häiriöistä.

Langattomien verkkojen tiedonsiirtonopeus on erittäin riippuvainen signaalin laadusta. Useimmiten ilman suoraa näköyhteyttä päätelaitteesta tukiaseman antenniin, ei siirtokapasiteettia voida saavuttaa läheskään täydellisesti. On myös huomioitava, että yhden tukiaseman alueella maksiminopeus on jaettu kaikkien tukiasemaa käyttävien käyttäjien kesken. [3.]

2.4 Tunnistautuminen ja salaus

Tunnistautumisella tarkoitetaan hallintaa siitä, kuka verkkoon pääsee. Yksinkertaisimmillaan tunnistautumisella rajataan ei-toivotut tahot verkon ulkopuolelle. Salauksella taas tarkoitetaan liikenteen salaamista, jolloin ulkopuolinen taho ei voi kaapata verkon liikennettä ja lukea sitä selkokielisesti. [4.]

Suurin ongelma langattomissa verkoissa on alusta lähtien ollut verkkoon tunnistautuminen, liikenteen salaus ja näihin liittyvät tietoturvariskit. Kiinteässä verkossa riski sille, että joku ulkopuolinen pääsisi kytkeytymään verkkoon ja kuuntelemaan liikennettä, on huomattavasti pienempi kuin langattomia verkkoja käytettäessä.

Langaton verkko jatkuu yritysten tilojen ulkopuolelle, mahdollisesti pitkänkin matkaa, jos esimerkiksi antennit on sijoiteltu huolimattomasti. Helpommillaan ulkopuolinen taho voi tulla päätelaitteen kanssa yrityksen lähelle ja pyrkiä tunkeutumaan yrityksen langattomaan verkkoon kaukaa rakennuksen ulkopuolelta. [1; 2.]

Samaan langattoman verkon heikkouteen perustuu niin sanottu *Man in the middle -hyökkäys*. Kyseisessä hyökkäyksessä ulkopuolinen taho hankkiutuu mahdollisimman lähelle hyökättävää verkkoa, esimerkiksi rakennuksen ulkopuolelle. Hyökkääjä käynnistää tämän jälkeen oman tukiasemansa, joka asetetaan mainostamaan samaa verkon nimeä kuin yrityksessä käytössä oleva verkko. Jos hyökkääjän tukiaseman teho on paikallisesti suurempi kuin yrityksen oikean verkon, yhdistävät käyttäjien päätelaitteet siihen ja yrittävät tunnistautua yrityksen tunnuksilla hyökkääjän verkkoon. Tästä hyökkääjä saa käyttöönsä tarvittavat tiedot, jotta yrityksen verkkoon voidaan murtautua.

Salaukseen onkin kiinnitetty erityisesti huomiota, kun tekniikkaa on kehitetty. Tällä hetkellä WLAN-tekniikan voimakkain salaus on vahvuudeltaan riittävän hyvä, että sitä voidaan käyttää yritystasolla turvallisesti.

Mikäli tukiasemalle ei ole määritelty mitään tunnistautumistekniikkaa tai salausta, kulkee kaikki liikenne verkossa selkokielisenä ja ulkopuoliset voivat myös helposti päästä kirjautumaan verkkoon ja sitä kautta käsiksi kaikkiin verkon resursseihin. Tällaiseen verkkoon muodostetaan yhteys yksinkertaisimmillaan hakemalla päätelaitteen avulla lähistöllä olevien verkkojen nimet ja sen jälkeen yhdistämällä haluttuun verkkoon omalla päätelaitteella.

Koska useimmiten liikenne kuitenkin halutaan suojata, on langaton verkko mahdollista salata ja suojella erilaisilla tekniikoilla. [1; 2.]

2.4.1 Verkon nimen piilottaminen ja MAC-suodatus

Yksinkertaisimmillaan pääsy verkkoon voidaan yrittää estää piilottamalla langattoman verkon nimi, jolloin verkkoon pystyy yhdistämään vain tietämällä verkon nimi etukäteen. Tähän voidaan yhdistää vielä tukiasemalle tarkistus, joka vertaa yhteyttä ottavan laitteen verkkokortin tunnusta, eli MAC-osoitetta, ennalta määriteltyihin ja estää pääsyn, mikäli tunnus ei löydy listalta. MAC-osoite on laitevalmistajan määrittelemä, ainutlaatuinen tunniste verkkokortille. Tätä osoitetta käytetään tunnistamaan yksittäinen laite verkossa.

Kyseiset tekniikat eivät kuitenkaan salaa liikennettä millään tekniikalla, ja ne ovat myös nykytekniikalla helposti kierrettävissä yleisessä jakelussa olevilla ohjelmistoilla. Näiden hyökkäysohjelmistojen toiminta perustuu siihen, että kuunnellaan haluttua verkkoa omalla laitteistolla ja kaapataan siinä liikkuvia

paketteja. Tämän jälkeen salaamattomat paketit puretaan ja niistä on helposti luettavissa verkon nimi ja lisäksi verkon eri laitteiden MAC-osoitteita. Yleisesti saatavilla olevilla ohjelmistoilla hyökkääjä voi helposti vaihtaa oman verkkolaitteensa MAC-osoiteen vastaamaan verkossa jo olevaa laitetta, jolloin pääsy verkkoon onnistuu, jos muita suojauksia ei ole. [1; 2.]

2.4.2 WEP

WEP eli *Wired Equivalent Privacy* oli ensimmäinen tekniikka, jolla hallittiin tunnistautumista tukiasemalle ja sitä kautta verkkoon sekä pyrittiin salaamaan tukiasemien ja langattomien päätelaitteiden välinen liikenne. Tekniikan tarkoituksena on salata kaikki langattomassa verkossa liikkuva liikenne sekä sitä kautta estää ulkopuolisten pääsy tukiasemalle.

Tekniikasta on olemassa eri versioita, mutta yleisimmät perustuvat 64-bittiseen tai 128-bittiseen salaiseen avaimeen. Tekniikkana WEP on nykypäivänä täysin vanhentunut ja siitä on löytynyt vakavia tietoturvaheikkouksia. WEP-salaus on nykyään purettavissa jopa muutamassa minuutissa yleisesti saatavilla olevilla ohjelmistoilla. [4.]

Suurin heikkous WEP:ssä on se, että langattomassa verkossa liikkuvissa tietoliikennepaketeissa on pieniä osia verkon avaimesta sekä se, että kaikki liikenne salataan vaihtumattomalla avaimella. Halutessaan tunkeutuja voi kuunnella verkkoa ja kaapata salattuja paketteja. Kun paketteja on kaapattu tarpeeksi, voidaan ne analysoida ja tiedon perusteella saada haltuun verkon kokonainen salausavain. Tämän jälkeen tunkeutujalla on täysi pääsy verkkoon ja kaikkeen siellä liikkuvaan liikenteeseen. Lisäksi jo ennen salauksen täydellistä purkamista hyökkääjä voi lähettää verkkoon väärennettyjä paketteja ja näihin saatujen vastausten avulla yrittää selvittää salausavainta.

Heikkouksistaan huolimatta WEP-tekniikan käyttäminen on suositeltavampaa kuin käyttää täysin suojaamatonta verkkoa. Tekniikalla saadaan estettyä tahattomat ulkopuoliset yhteydet verkkoon ja salattua edes heikosti verkon liikenne.

2.4.3 WPA

WPA eli *Wi-fi Protected Access* kehitettiin korjaamaan WEP:n pahimmat ongelmat. WPA:n ensimmäinen versio sisältää lähes kaikki IEEE:n 802.11i-

standardin vaatimuksista. Kyseinen standardi pitää sisällään vaatimukset WLAN-verkkojen tunnistautumiselle ja salaukselle.

WPA ei siis ole standardi, vaan *Wi-Fi Alliance* –järjestön määrittelemä sertifikaattiluokitus. Wi-Fi Alliance on kansainvälinen järjestö, joka määrittelee tiettyjä vaatimuksia langattoman verkon laitteille, jotta ne saavat käyttää *Wi-Fi Certified* –nimeä. Mikäli käytettävä langaton laite tukee tiettyjä vaatimuksia verkon turvallisuuden osalta, se saa käyttää WPA- tai WPA2-luokitusta.

Ensimmäinen versio WPA:sta käyttää salaukseen TKIP eli *Temporal Key Integrity Protocol* –tekniikkaa. Kyseinen protokolla on pohjimmiltaan parannettu versio WEP-tekniikasta yrittäen kuitenkin korjata sen pahimmat heikkoudet. TKIP vaihtaa liikenteen salausavainta tasaisin väliajoin ja lisää paketteihin eheyden tarkistusmahdollisuuden. Salausavaimen vaihdolla pyritään hankaloittamaan liikenteen purkua ja verkkoon tunkeutumista. Pakettien eheystarkistuksen avulla voidaan varmistaa, ettei verkossa liiku muokattuja, mahdollisesti haitallisia paketteja.

TKIP:stä on kuitenkin löydetty tiettyjä haavoittuvuuksia, joista vakavimmat mahdollistavat salauksen murtamisen jopa muutamissa minuuteissa. Kyseinen heikkous toimii siten, että hyökkääjä kaappaa verkon liikennettä, kunnes saadaan kaapattua salattu *ARP* eli *Address Resolution Protocol* -paketti. Kyseisiä paketteja käytetään verkossa liikennöitäessä jatkuvasti verkon osoitteiden selvittämiseen. ARP-paketit ovat erittäin lyhyitä, joten ne on hyvin helppo tunnistaa ja sitä kautta murtaa verkon salaus.

Muiden heikkouksien lisäksi WPA on altis palvelunestohyökkäyksille, koska tukiasemaa voidaan pommittaa väärillä yhteysyrityksillä niin raskaasti, etteivät verkon hyväksytyt laitteet pääse kirjautumaan tukiasemalle. [1; 2; 5]

2.4.4 WPA2

Löydettyjen heikkouksien takia WPA:sta kehitettiin uusi versio, *WPA2*. WPA2 pitää sisällään kaikki 802.11i-standardin vaatimukset ja tekniikka on tietoturvaltaan tällä hetkellä riittävä yrityskäyttöön. WPA2 salaa liikenteen *AES (Advanced Encryption Standard)* -menetelmällä, jonka vahvinta versiota ei pystytä murtamaan nykyisillä laitteilla, eikä siitä ole löytynyt murtamista mahdollistavia heikkouksia.

AES on yleisesti käytössä oleva salausstandardi, joka perustuu salattavan tiedon salaamiseen useaan päällekkäiseen kertaan, jotta saadaan aikaan erittäin vahva salaus. Vahvin tällä hetkellä käytössä oleva versio AES-tekniikasta on 256-tavuinen versio, jossa tieto on salattu 14 päällekkäistä kertaa.

Kuten kaikki salausmenetelmät, myös AES vaatii käytettävältä laitteistolta laskentatehoa salauksen muodostamiseen ja purkuun. Koska AES on tarkasti määritelty standardi, on se nykyään tuettuna käytännössä kaikissa langattoman verkon laitteissa laitteistotasolla, jolloin sen käyttö ei lisää verkon viivettä merkittävästi.

WPA2-tekniikkaan on myös lisätty palvelunestohyökkäyksen tunnistus, jolloin tukiasema lakkaa vastaamasta hyökkääjälle, jos virheellisiä kirjautumisyrityksiä on tullut tietty määrä lyhyessä ajassa.

Tunnistautuminen WPA2-salattuun verkkoon tapahtuu joko ennakkoon jaetulla avaimella (*Pre Shaded Key, PSK*) tai useimmiten yrityskäytössä erillisen tunnistajan ja varmennuspalvelimen (esimerkiksi *Radius*) kautta. Ennakkoon jaetulla avaimella toimivaa tunnistautumista kutsutaan termillä *WPA2 Personal*, ja se on suunnattu enimmäkseen kotikäyttöön tai rajoitetusti hyvin kevyeen yrityskäyttöön. Jaettu avain syötetään, kun verkkoyhteyttä muodostetaan ja päätelaite saa muodostettua yhteyden tukiasemaan.

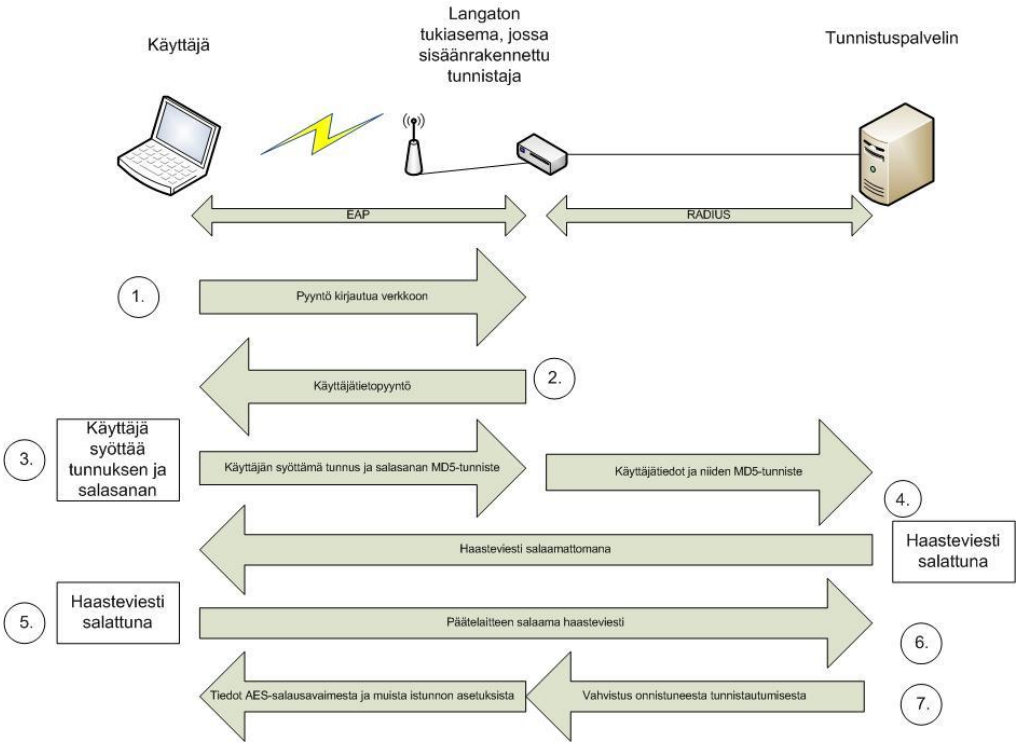
Ennakkoon jaetun avaimen heikkoutena on se, että avaimen muuttuessa se pitää tiedottaa erikseen jokaiselle langattoman verkon käyttäjälle. Tästä syystä avainta ei yrityskäytössä voi muuttaa kovin usein, mikä vaarantaa tietoturvan, jos avain vuotaa ulkopuolisten tietoon. Yritysluokan laitteistolla varmempi menetelmä onkin käyttää tunnistautumiseen erillistä tunnistuspalvelinta. Erillistä palvelinta käyttävää tunnistautumismenetelmää kutsutaan termillä *WPA Enterprise*. Kyseinen menetelmä on standardoitu nimellä 802.11X. [1; 3; 5.]

2.4.5 802.11X ja RADIUS

Tunnistuspalvelinta käytettäessä yhteys muodostetaan erilliseen laitteeseen, tunnistajaan, joka toimii päätelaitteen ja varmennuspalvelimen välissä vahvasti salatulla protokollalla (*Extensible Authentication Protocol*, EAP). Liikenne tunnistajalta tunnistuspalvelimelle taas käyttää nykyään lähes aina

RADIUS (*Remote Authentication Dial In User Service*) -protokollaa. Tunnistaja voi olla erillinen laite, tai se voi olla integroitu langattomaan tukiasemaan.

Tunnistautuminen RADIUS-palvelimen avulla voidaan jakaa seitsemään vaiheeseen (kuva 3). [1; 3.]



Kuva 3. Tunnistautuminen RADIUS-palvelimelle

1. Käyttäjän päätelaite yrittää yhdistää tukiasemaan käyttäen tunnistautumisessa omaa MAC-osoitettaan. Ainoa liikenne, mikä päätelaitteen ja tukiaseman välillä liikkuu, on EAP-liikenne.

2. Päätelaite pyytää tunnistajalta verkkoon tunnistautumisen aloitusta ja tunnistaja vastaa kysymällä tunnusta ja salasanaa.

3. Päätelaite kysyy käyttäjältä tunnusta ja salasanaa. Salasanaa ei lähetetä tunnistajalle, vaan ainoastaan salasanasta laskettu *MD5-tarkiste*. Tunnistaja tarkastaa tässä vaiheessa onko käyttäjän syöttämä tunnus olemassa järjestelmässä. Tunnistaja lisää käyttäjätietoihin vielä uuden MD5-tarkisteen, muuttaa tiedot RADIUS-sanomaksi ja lähettää ne eteenpäin tunnistuspalvelimelle.

4. Tunnistuspalvelin vastaa viestillä, joka pitää sisällään satunnaisen merkkijonon ja salaisella avaimella salatun MD5-tunnisteen. Tätä viestiä kutsutaan haasteeksi. Tunnistaja muuttaa viestin EAP-pyynnöksi ja lähettää sen päätelaitteelle. Tunnistuspalvelin myös salaa haasteen kyseisen käyttäjän salaisella avaimella ja tallentaa sen paikallisesti.

5. Päätelaite salakirjoittaa saapuneen haasteviestin salaisella avaimella ja lähettää salatun viestin tunnistajalle, joka muuttaa viestin RADIUS-muotoon ja välittää sen tunnistuspalvelimelle.

6. Tunnistuspalvelin vertaa saapunutta, salattua haasteviestiä paikallisesti tallennettuun, salattuun haasteviestiin. Mikäli ne vastaavat toisiaan, on käyttäjä tunnistautunut onnistuneesti.

7. Tunnistuspalvelin lähettää viestin tunnistautumisen onnistumisesta ja antaa tukiasemalle luvan toimittaa istunnon salausavaimen. Nykyään käytettävä salausmenetelmä on useimmiten WPA2-AES. Avain on joka yhteyskerralla erilainen, joten pelkkä liikenteen kaappaaminen ei mahdollista avaimen selvittämistä.

Yrityksissä kirjautuminen salattuun verkkoon hoidetaan usein valmiilla asetuksilla ja tunnistuspalvelimella. Yleensä suurempien yritysten tietokoneet ovat vakioituja ja niihin pystytään määrittelemään keskitetysti asetuksia. Tämä mahdollistaa sen, että yrityksen sisäisen langattoman verkon tarvittavat tiedot on tallennettu koneelle jo etukäteen. Käyttäjän ei tarvitse tehdä muita toimenpiteitä kuin kytkeä langaton verkkokortti päälle, ja yhteys muodostuu yrityksen verkkoon automaattisesti, joka haluttaessa kysyy vain salasanaa RADIUS-palvelimelle. [1; 2; 3.]

Usein tunnistautumista vahvennetaan vielä erillisellä sertifikaatilla, joka on päätelaitteelle asennetussa tiedostossa tai kytkettynä päätelaitteeseen ulkoista kautta kuten USB-liitännällä. Kyseistä sertifikaattia käytetään todentamaan, että kyseessä on luvallinen laite yhteyden muodostamiseen.

Sähköiset sertifikaatit ovat aina jonkin tahon allekirjoittamia. Turvallisin vaihtoehto on niin sanottu ulkoinen sertifikaatti, jolloin sertifikaatin myöntää erillinen yritys. Ulkoinen yritys takaa omalla allekirjoituksellaan, että kyseinen

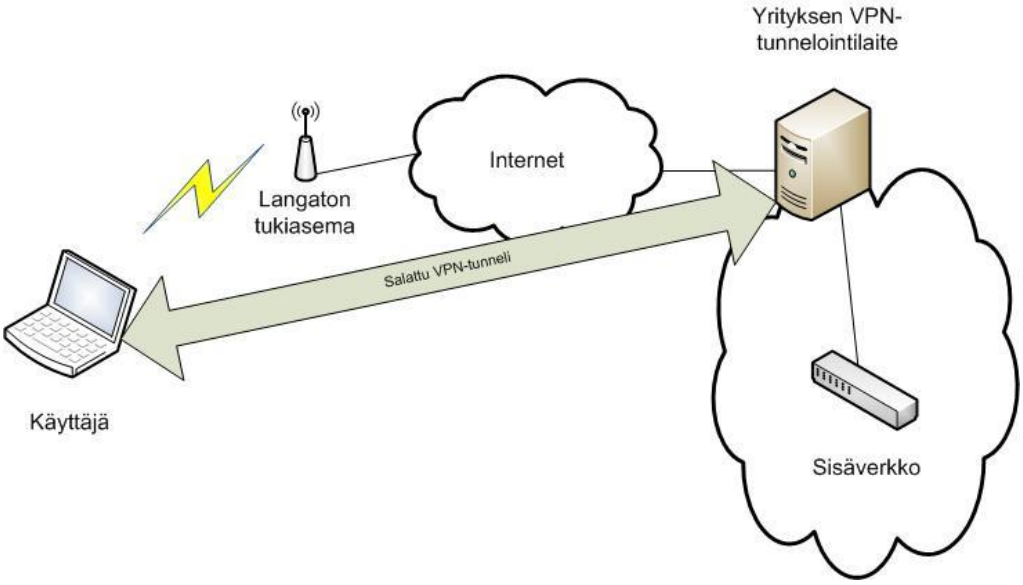
sertifikaatti kuuluu oikealle käyttäjälle. Ulkoisten sertifikaattien luotettavuus perustuu niitä myöntävien yritysten maineeseen ja luotettavuuteen.

Teknisesti ulkoisen sertifikaatin luonti tapahtuu siten, että ulkoisen yrityksen allekirjoittamia sertifikaatteja käyttävällä yrityksellä on sopimus, tunnukset ja tekninen laitteisto, millä sertifikaatit luodaan ulkoisen yrityksen kautta. Luodut sertifikaatit voidaan sitten tallentaa käyttäjien koneille tai muille tietovälineille kuten erilliselle sirukortille. Kun RADIUS-palvelin sitten suorittaa käyttäjän tunnistusta, se tutkii myös, että käyttäjän sertifikaatti on voimassa ja että se on oikean tahon myöntämä. Ulkoista sertifikaattia voidaan usein käyttää myös esimerkiksi VPN-yhteyksien tunnistautumisen vahvistamiseen tai muuhun tunnistautumiseen ulkoisten tahojen kanssa. VPN-yhteyksiä käsitellään lisää myöhemmin.

Toinen mahdollisuus yrityksillä sertifikaatin käytössä on allekirjoittaa sertifikaatti itse. Kyseisen tekniikan etuna on se, ettei yritys ole riippuvainen ulkoisesta tahosta sertifikaattien allekirjoituksessa. Haittapuolena taas on, että itse allekirjoitettu sertifikaatti ei ole pätevä muuhun kuin yrityksen sisäisiin toimiin. Lisäksi yrityksen sisäisesti allekirjoitettu sertifikaatti on, ainakin teoriassa, helppo väärentää. [4.]

2.4.6 VPN-tunnelointi

VPN-tunnelointi ei ole varsinaisesti langattomien verkkojen tekniikkaa, mutta sitä käyttämällä, muun liikenteen salauksen lisäksi, saadaan yhteyden tietoturvaa lisättyä huomattavasti. VPN on lyhenne sanoista *Virtual Private Network* ja sillä tarkoitetaan virtuaalista lähiverkkoyhteyttä, joka on luotu julkisen verkon yli kohdeverkkoon (kuva 4). [4.]



Kuva 4. VPN-tunnelointi

Langattomia verkkoja käytettäessä VPN-tunnelointi toteutetaan avaamalla vielä verkkoyhteyden muodostamisen jälkeen uusi salattu yhteys langattoman verkon yli. Usein VPN-verkkoja käytetään yrityksissä erityisesti etäyhteyksien muodostamiseen internetin yli yrityksen sisäverkkoon. Tekniikkaa voidaan kuitenkin käyttää hyödyksi myös yrityksen omaa langatonta verkkoa käytettäessä sen tuoman lisäturvan takia. Tällä hetkellä suurin osa VPN-liikenteestä on salattu käyttäen *IPsec* eli *Internet Protocol Security* –protokollaa.

IPsec-protokolla salaa liikenteen verkon alemmalla tasolla, joten sitä voidaan käyttää salaamaan kaikki päätelaitteen ja kohdelaitteen välinen liikenne mukaan lukien verkon hallintaviestit ja muu kontrolliliikenne. Muita suosittuja salausprotokollia VPN-käyttöön ovat *SSL* eli *Secure Sockets Layer*, *TLS* eli *Transport Layer Security* ja *SSH* eli *Secure Shell*. Kyseiset protokollat salaavat liikenteen ohjelmatasolla, joten ne ovat kevyempiä kuin IPsec, mutta vaativat käytettäviltä ohjelmilta tuen salaukselle.

VPN on ainoa mainituista salaustekniikoista, jolla jokainen verkossa liikkuva tietoliikennepaketti on salattu aina päätelaitteesta kohteena olevaan verkkoon asti. Käytettäessä VPN-salausta mahdollisen hyökkääjän on erittäin vaikeaa saada liikenteestä mitään haitallista selvitettyä. Vaikka langattoman verkon liikenteen salaus saataisiinkin purettua, liikkuu liikenne VPN-tunnelin

sisällä salattuna, joten hyökkääjä joutuu tietojen selvittämiseksi purkamaan toisen salauksen.

Haittana VPN-tunnelissa on, että se hidastaa liikennettä jonkin verran, koska kaikki liikkuva liikenne salataan. VPN-yhteys vaatii aina tuen joko päätelaitteen käyttöjärjestelmältä tai erilliseltä VPN-asiakasohjelmalta päätelaitteessa.

Yhteys pitää myös jokaisella yhteyskerralla erikseen avata, ja jos yhteydessä on katkoksia, joudutaan jokaisen katkoksen jälkeen tunnistautumaan uudestaan. Lisäksi kaikki VPN-liikenne kulkee yrityksen verkon kautta, joten jos yrityksen VPN-tunnelointilaite ei ole oikein mitoitettu yrityksen käyttöön, saattaa liikenteeseen tulla haitallista viivettä. [1; 2; 4.]

3 ERITYISVAATIMUKSET YRITYSYMPÄRISTÖISSÄ

Yrityksissä langattomilta verkoilta vaaditaan huomattavasti suurempaa suorituskykyä, hallittavuutta, toimintavarmuutta ja tietoturvaa kuin kotikäytössä. Suuremmat vaatimukset koskevat yrityskäytössä lähinnä langattoman verkon tukiasemia ja kiinteän verkon puolella olevia laitteita. Varsinaiset päätelaitteet ovat nykyaikana teknisesti samantasoisia niin kuluttaja- kuin yrityslaitteistoissa.

Kyseiset vaatimukset on tärkeää ottaa huomioon langattomia verkkoja rakennettaessa isoihin yrityksiin. Pienyritykset voivat tulla toimeen kuluttajatason laitteilla, mutta käyttäjämääriltään keskisuuret ja suuret yritykset tarvitsevat erityisesti raskaampaan käyttöön suunniteltua laitteistoa.

Yrityksissä on lähes aina olemassa oleva oma sisäverkko, jonka jatkeeksi langaton verkko yleensä halutaan. Tämä asettaa myös verkon muulle laitteistolle ja yrityksen verkon rakenteelle omat vaatimuksensa. [1.]

3.1 Verkon rakenne

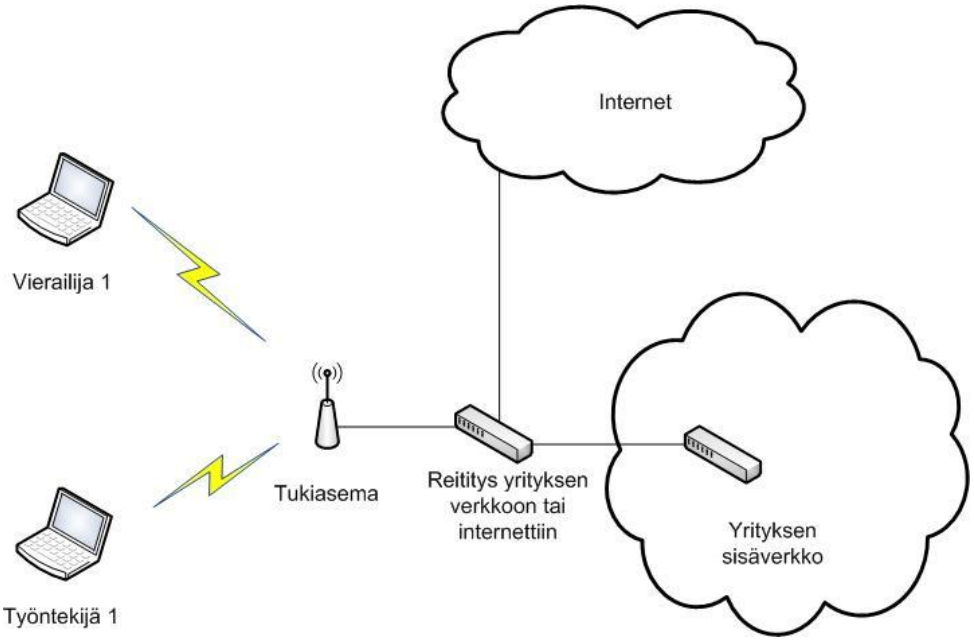
Tällä hetkellä lähes kaikissa yrityksissä käytetään Windows-pohjaisia sisäverkkoja. Näissä verkoissa on käytännössä aina käytössä *Active Directory* – eli aktiivihakemisto-rakenne. Kyseisessä rakenteessa verkossa on yksi palvelin joka, pitää sisällään käyttäjien tunnustiedot. Verkkoon kirjauduttaessa tämä kyseinen palvelin tarkastaa, onko käyttäjällä oikeus kirjautua verkkoon.

Langattomat verkot voivat käyttää hyödyksi aktiivihakemiston ominaisuuksia käyttäjien tunnistautumisessa verkkoon. RADIUS-palvelimen tunnistaja voi tarkastaa käyttäjän suoraan kiinteän verkon palvelimelta, eikä erillistä langattoman verkon käyttäjähallintaa tarvita. Active Directoryn avulla voidaan lisäksi jakaa käyttäjien koneisiin valmiiksi asetukset ja sertifikaatit, joita sitten käytetään langattomaan verkkoon yhdistettäessä ja tunnistautumisessa.

Asetusten jakelu tapahtuu *Group Policy* eli ryhmäkäytäntöjen avulla. Tällöin verkkoon voidaan määritellä erilliset asetukset esimerkiksi kiinteille tietokoneille ja kannettaville. Näin vältetään turhien asetusten määrittelemisestä sellaisiin laitteisiin, joissa ne ovat tarpeettomia. [1.]

3.1.1 Vierailijaverkko ja sisäverkko

Jos langaton verkko on yrityksessä tarkoitettu työntekijöiden käyttöön, on se usein yhdistetty suoraan sisäverkkoon, jolloin kaikki verkon normaalit palvelut ovat käytettävissä. Yleensä myös vierailijoille on rakennettu oma verkko, josta on pääsy ainoastaan julkiseen verkkoon eli käytännössä internetiin (kuva 5).



Kuva 5. Vierailijaverkko ja verkon rakenne

Vierailijaverkko on yleensä yhteensopivuuden takia täysin suojaamaton eikä vaadi yhteyden muodostamiseen salasanoja tai käytä minkäänlaista liikenteen salausta. Usein yritykset kuitenkin haluavat estää täysin ulkopuolisilta

verkon luvattoman käytön määrittelemällä verkolle aloitussivun, johon vierailija pakotetusti siirtyy yhteyttä muodostettaessa (kuva 6). Tästä pakotetusta aloitussivusta käytetään yleensä termiä *landing page*. Sivulla usein kysytään tunnuksia, ja ennen oikeiden tunnusten syöttämistä mikään muu kuin tunnistautumiseen vaadittava liikenne ei ole verkkoon sallittua. Kun tunnukset on syötetty, sallitaan verkon kautta kaikki normaali verkkoliikenne ja normaali internetin käyttö.

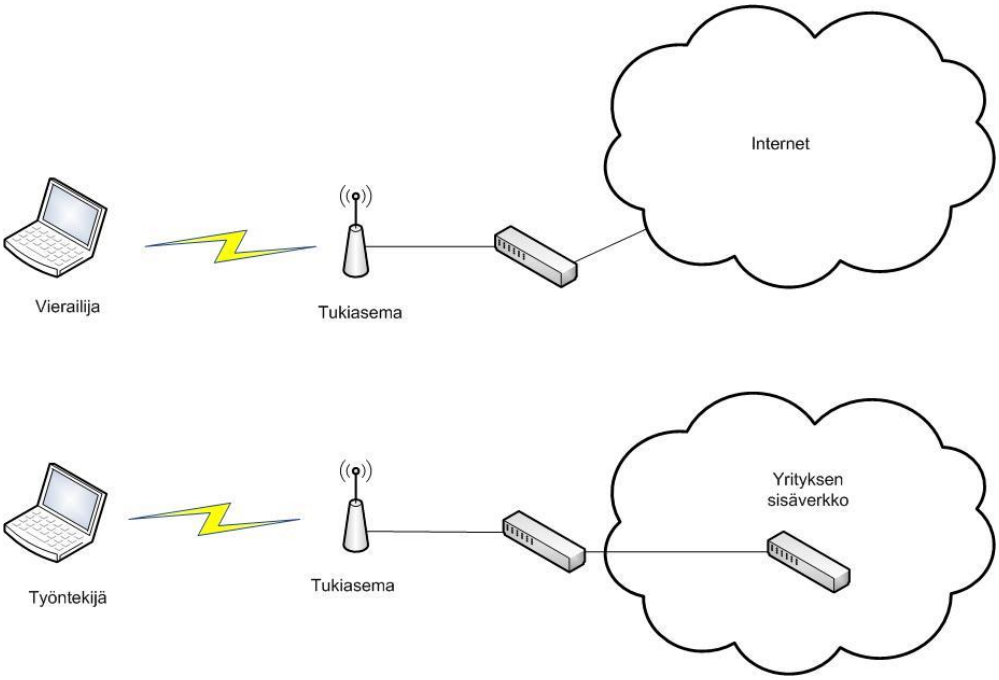
Kuva 6. Esimerkki sisäänkirjautumissivusta

Useimmiten verkkojen jako vierailijaverkkoon ja sisäverkkoon on toteutettu siten, että tukiasemalla on kaksi erinimistä langatonta verkkoa ja niiden perusteella määritellään, mihin liikenne ohjataan. Kyseisellä ratkaisulla saadaan vierailijoiden laitteet rajattua pois yrityksen sisäverkosta käyttäen kuitenkin samoja laitteita ja kiinteää verkotusta kuin sisäverkonkin liikenteessä.

Verkkojen jako laitteissa tapahtuu siten, että kytkimissä määritellään erilliset VLAN (*Virtual Local Area Network*) -verkot. VLAN-verkot ovat ohjelmistolla luotuja virtuaalisia lähiverkkoja, jotka käyttäytyvät samoin kuin kiinteät erilliset verkot, mutta käyttävät samoja laitteita liikennöintiin. Kaikkiin nykyaikaisiin kytkimiin voi luoda useampia VLAN-verkkoja ja määrittää tietyt kytkimen portit kuulumaan tiettyihin verkkoihin. Näin saadaan helposti esimerkiksi langattoman verkon antennit eristettyä omaan verkkoonsa kytkinten oikein asetettujen porttien avulla.

Mikäli mahdolliset riskit vierailijaverkon ja yrityksen sisäverkon välillä halutaan minimoida, voidaan vierailijaverkko rakentaa fyysisesti kokonaan

omaksi verkokseen. Tällaisesta ratkaisusta käytetään termiä *airgap*, joka tarkoittaa että kahden verkon välillä ei ole minkäänlaista fyysistä yhteyttä (kuva 7). Tällöin vierailijaverkolla on omat antennit, omat tukiasemat, omat kaapeloinnit ja oma yhteys ulkoverkkoon, eli internetiin. [1; 2.]



Kuva 7. Fyysisesti erotellut verkot

Kun verkot on fyysisesti erotettu toisistaan, ei ole riskiä, että vierailijaverkkoon päässyt tunkeutuja pääsisi murtautumaan yrityksen järjestelmiin ohjelmistollisesti tai edes laitteiston heikkouksien kautta. Erillisillä verkoilla myös estetään vahingossa tapahtuneet tietoturvariskit kuten virheellisesti määritetyt kytkimen asetukset. Virheellisinä asetuksina voidaan mainita esimerkiksi liikenteen reititys vahingossa internetiin yrityksen sisäverkon kautta.

Haittapuolena fyysisesti erotellussa verkossa on sen korkeat rakennuskustannukset ja hankala ylläpito, hallinnointi sekä valvonta. Kaikkia vierailijaverkkoa varten tehtäviä toimenpiteitä varten on kytkeydyttävä verkkoon erillisellä työasemalla, joka tietoturvan takia ei saisi olla mikään laite mitä käytetään normaalisti yrityksen sisäverkossa. Edellä mainituista syistä rakenteeltaan fyysisesti eroteltuja verkkoja ei yleensä normaaliin yrityskäyttöön rakenneta.

3.1.2 Antennien sijoittelu ja suorituskyky

Useimmissa yrityksissä yhden antennin alueella on mahdollista olla samaan aikaan kymmeniä käyttäjiä, joista osa on mahdollisesti yrityksen työntekijöitä ja osa vierailijoita. Kun käyttäjiä on suuri määrä samalla alueella, myös verkon suorituskyky saattaa muodostua ongelmaksi ja on huomioitava verkkoa rakennettaessa.

Yrityksille langattoman verkon on useimmiten tarkoitus kattaa mahdollisimman hyvin koko yrityksen tila. Tavallisilla kuluttajatason laitteilla tämä ei usein onnistu, joten nykyään yritysverkoissa on käytössä useampia erillisiä, hallintaa vaativia tukiasemia ja yksi niin sanottu kontrolleri, joka pitää sisällään kaiken tarvittavan laitteiston verkon toimintaan. Koska erilliset tukiasemat toimivat kontrollerin kiinteän verkon kytkentäporttien jatkeena, kutsutaan niitä yleensä radioporteiksi.

Koska radioporttien hallinta tapahtuu kontrollerilla, pystytään liikennettä ohjaamaan helposti uudestaan eri antennien välillä keskitetysti. Tämä mahdollistaa päätelaitteen liikkumisen eri radioporttien peittoalueilta toiselle, ilman että yhteys katkeaa. Kyseinen tilanne voisi muodostua esimerkiksi siirryttäessä kannettavan tietokoneen kanssa neuvottelutilasta takaisin omalle työpisteelle.

Erillisillä radioporteilla saavutetaan parempi kattavuus yrityksen tiloissa, kun niitä voidaan lisätä alueille, joissa kuuluvuus on huonompi. Koska kaikki yhteen radioporttiin yhdistäneet laitteet jakavat kyseisen radioportin tarjoaman nopeuden, voidaan radioportteja myös helposti lisätä alueelle, jossa yksittäisen radioportin tarjoama kaista alkaa loppua kesken.

Radioportit yhdistetään kontrolleriin normaalin kaapeloidun ethernet-verkon avulla ja usein radioportit myös saavat virtansa tätä kautta, niin kutsutun *Power over Ethernet* (PoE)-tekniikan avulla. Tällöin radioportteja varten ei tarvitse rakentaa kuin verkkoyhteys, mikä helpottaa niiden sijoittelua yrityksen tiloissa.

PoE-tekniikka vaatii tuen kytkimeltä johon ne kytketään, mutta on olemassa myös PoE-välikappaleita kytkimen ja radioportin väliin. Näillä välikappaleilla saadaan toimitettua virtaa radioportille kytkimeltä, joka ei tue PoE tekniikkaa. Mikäli ei ole mahdollista käyttää välikappaletta tai radioportissa ei ole PoE-

ominaisuutta, voidaan radioporteille yleensä järjestää sähkö erillisen muuntajan avulla tavallisesta sähköpistokkeesta, läheltä itse radioporttia. [1.]

3.2 Tietoturva yrityksissä

Koska yrityskäytössä verkon tietoturvan tärkeys korostuu yksityiskäyttöä enemmän, on erittäin tärkeää, että langatonta verkkoa voidaan käyttää mahdollisimman turvallisesti. Täysin murtamattomaksi ei mitään verkkoa pystytä rakentamaan, mutta yhdistelemällä tarkan tietoturvapolitiikan, hyvän verkon fyysisen rakenteen, oikeat laitteet ja oikeat asetukset, voidaan tietoturvariskit minimoida.

Hyvä tietoturva perustuu aina siihen, että käyttäjät ovat tietoisia yrityksen tietoturvapolitiikasta ja ovat velvollisia noudattamaan sitä. Hyvään tietoturvapolitiikkaan kuuluukin, että käyttäjät eivät saa asentaa verkkoon omia laitteitaan ilman lupaa tai asentaa koneilleen mitään ohjelmia, joita yritys ei ole hyväksynyt. Näin saadaan minimoitua riski tahattomista rikkeistä tietoturvassa. [4.]

Langattoman, ja myös kiinteän, verkon liikenteen salaus ja tunnistautuminen verkkoon perustuu aina siihen, että käytetyt menetelmät luovat liikenteeseen mahdollisimman paljon satunnaisuutta. Suuri satunnaisuus tekee liikenteen kaappaamisen ja analysoimisen ulkopuolisen tahon toimesta lähes mahdottomaksi. Mikäli suojaus saadaan kuitenkin purettua, on se niin aikaa vievää, ettei siitä ole hyötyä hyökkääjälle.

Vahvoista salauksista ei ole apua, jos käyttäjien tunnukset ja salasanat ovat liimalapulla kannettavan tietokoneen pohjassa tai jos yritys ei ole määritellyt salasanoihin mitään vaatimuksia salasanan vahvuudelle. Matemaattisesti murtamaton järjestelmä saadaan haavoittuvaiseksi helposti, jos käyttäjät saavat valita salasanakseen esimerkiksi sanan, joka on viisi merkkiä pitkä ja kirjoitettu pelkillä pienillä kirjaimilla. Kyseisen kaltaisen salasanan murtaminen nykylaitteistolla ei kestä kuin muutamia minuutteja. [1; 2; 4.]

Verkon fyysinen rakenne tulee suunnitella niin, että se rajoittuu mielellään vain yrityksen tilojen sisäpuolelle. Langaton signaali kuitenkin kantaa hyvin rakenteiden läpi, joten täysin fyysisesti rajattua langatonta verkkoa on mahdoton rakentaa, mikäli samaan aikaan tulisi käyttäjille saada mahdollisimman kattavat yhteydet. Usein laajemmissa yritysverkoissa on myös tästä

syystä erilliset antennit, jolloin niiden sijoittelulla ja suuntaamisella voidaan vaikuttaa merkittävästi verkon kuuluvuuteen tarvittavilla ja tarpeettomilla alueilla.

Toinen tärkeä asia on huolehtia, että langattoman verkon salaus on ajan tasalla ja ettei käytetystä tekniikasta ole löytynyt haavoittuvuuksia, jotka vaatisivat kenties salausmenetelmän uusimista. On myös tärkeää tarkkailla, ettei verkkoon pääse laitteita, jotka saattavat vaarantaa sen tietoturvan. Hyvä tapa onkin estää pääsy verkkoon laitteilta, joiden ei tiedetä olevan varmasti turvallisia. Tähän voidaan hyvin soveltaa esimerkiksi MAC-suodatusta ja keskitettyä laitehallintaa verkon laitteille ja sitä kautta rajata pääsy vain yrityksen omille laitteille.

Esimerkkinä vakavasta tietoturvariskistä, joka on estettävissä MAC-suodatuksella ja verkon laitteiden tarkalla hallinnalla, on, jos käyttäjä kytkee kiinteään verkkoon, tahallisesti tai tahattomasti, oman salaamattoman, langattoman tukiaseman. Salaamattoman tukiaseman johdosta koko yrityksen verkko on haavoittuvainen tunkeutujien hyökkäyksille. Valvonnan avulla verkon ylläpitäjä havaitsisi tuntemattoman laitteen verkossa jo ennen kuin tuntematon laite saa pääsyn verkon resursseihin. [2; 4.]

Lisäksi kuten kiinteänkin verkon yhteydessä yrityksen tulee tietenkin huolehtia, että kaikissa yrityksen tietokoneissa on tietoturvaohjelmistot ja laitteiston ajurit ajan tasalla. On myös tärkeää käydä läpi laitteiden verkkoasetukset, koska osa oletuksina laitteissa olevista verkon jakoasetukista on vaarallisia ja ne saattavat tahattomasti jakaa käyttäjien työasemien kaikki tiedostot verkkoon. [1.]

4 TUTKITUT YRITYKSET

Tutkitut yritykset ovat eri toimialoilta, mutta tekevät normaalia toimistotyötä. Suurin osa verkon liikenteestä on sähköposti- sekä internet-liikennettä. Kaikissa yrityksissä on käytössä sekä kiinteitä työasemia että kannettavia tietokoneita.

Kaikki yritykset myös perustuvat Windows-pohjaisiin verkkoihin ja käyttävät verkoissaan ethernet-pohjaista verkkoa.

4.1 Yritys A

Yritys A sijaitsee yhdessä rakennuksessa ja käyttäjiä on noin 250. Rakennuksessa on 9 kerrosta, joissa jokaisessa on työhuoneiden lisäksi muutama neuvottelutila. Käytännössä kaikki aiempi verkkoliikenne talossa kulki ethernet-kaapelointia pitkin, koska suurin osa työasemista on kiinteitä ja käytössä olevat kannettavat tietokoneetkin käyttävät pääosin kiinteää verkkoa telakointiasemien kautta.

Tarve langattomalle sisäverkolle olikin ensisijaisesti saada verkkoyhteydet joustavasti neuvottelutiloihin ilman ylimääräisiä johtoja sekä internetyhteyden tarjoaminen langattomasti vierailijoille talossa. Alun perin tarkoitus oli kattaa vain neuvottelutilat, mutta myöhemmin suunnitelma laajennettiin koskemaan koko taloa.

Syy verkon laajentamiseen oli se, että langattoman verkon haluttiin kattavan neuvottelutilat myös jatkossa, jos niitä rakennetaan rakennukseen lisää. Lisäksi katsottiin, että langattoman verkon rakentamisen kokonaiskustannukset eivät nousseet ylimääräisistä radioporteista johtuen merkittävästi.

Suorituskyvyltään verkolta vaadittiin normaaleja toimistosovelluksia kuten sähköpostin ja internetin selaus. Videopuheluille tai muille runsaasti kaistaa vaativille sovelluksille ei verkkoa nähty tarpeelliseksi mitoittaa.

Ennen verkon pystytystä tila käytiin läpi mittalaitteilla, jotta saatiin tutkittua kattava peitto verkolle. Lisäksi samalla varmistettiin antenneille asennuspaikoiksi sellaiset kohdat, joihin vikatilanteissa on helppo päästä käsiksi.

4.1.1 Laitteisto

Koska rakennuksen olemassa oleva verkko oli toteutettu HP:n ProCurve-laitteilla, haluttiin myös langattoman verkon laitteisto samalta valmistajalta. Rakennuksen suuresta koosta johtuen päädyttiin hankkimaan yksi tehokas kontrolleri, johon kytkettiin ethernet-verkon yli useita radioportteja.

HP tarjosi valikoimissaan langattoman verkon kontrolleria, joka voitiin sijoittaa runkokytkimen laajennuspaikkaan. Koska verkossa oli valmiina jo tarvitunlainen runkokytkin, kontrolleriksi valittiin malli ”HP ProCurve Wireless Edge Services XL” (kuva 8), joka sijoitettiin yhteen ”HP ProCurve Switch

5308xl” –mallisista runkokytkimistä (kuva 9). Radioporteiksi valittiin kontrollerin kanssa yhteensopivat ”HP ProCurve Radio Port 230” (kuva 10). [6 ; 7; 8.]

Etuna kytkimen laajennuspaikkaan sijoitettavasta kontrollerista on se, että kytkin hoitaa kaiken verkkoliikenteen, jolloin kontrollerin hoidettavaksi jää vain langattoman liikenteen ohjaaminen. Tämä näkyy selvästi kontrollerin pienemmissä hankintakustannuksissa ja huomattavasti erillistä laitetta pienemmissä tilavaatimuksissa. Kyseinen kontrolleri olisi ollut mahdollista kahdentaa varalaitteella vikatilanteiden varalle, mutta langatonta verkkoa ei nähty niin kriittiseksi palveluksi, että kahdennettuja laitteita olisi tarvittu.

HP ProCurve Wireless Edge Services XL [6]

- Kytkimen laajennusosa. Kontrolleri on aina kytkettävä 5308xl-malliseen tai vastaavan kytkimen laajennuspaikkaan.

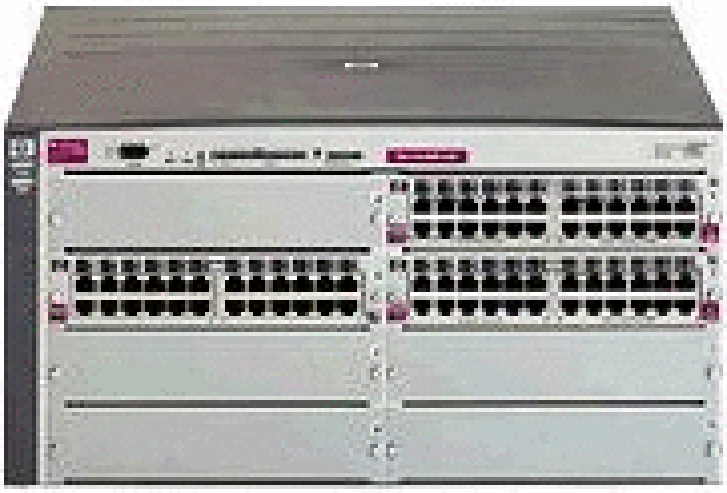
- Radioportteja saa kytkettyä yhteen kontrolleriin enintään 48 kappaletta. Yhteen 5308xl-kytkimeen voidaan kuitenkin kytkeä samanaikaisesti kaksi kontrolleria, jolloin radioporttien enimmäismäärä on 96 kappaletta [7].

- Tukee RADIUS-tunnistautumista, tukien EAP-TLS, EAP-MD5. EAP-TTLS ja PEAP protokollia.

- Siinä on sisäänrakennettu vierailijaverkon tunnushallinta ja tunnistautuminen.

- Se tunnistaa automaattisesti kiinteään verkkoon kytketyt radioportit [6].

Kuva 8. HP ProCurve Wireless Edge Services XL [6]



Kuva 9. HP ProCurve Switch 5308xl-kytkimen laajennuspaikat, joihin on asennettu ethernet-verkon laajennuskortteja [7.]

HP ProCurve Radio Port 230 [8]

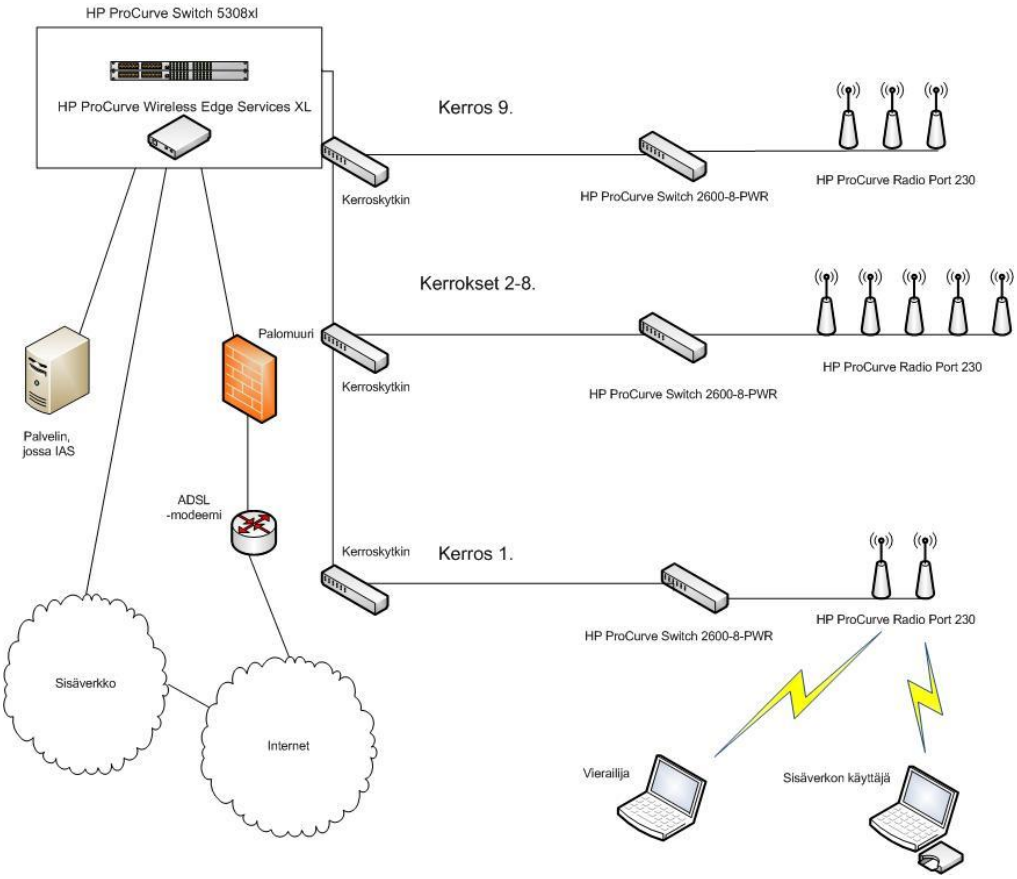
- Pelkkä radioportti, joka vaatii kontrollerin toimiakseen.
- Virransyöttö vain Ethernet-verkon yli PoE-tekniikalla.
- Tukee 802.11a- ja 802.11b/g -verkkoja.
- Sisäänrakennetut antennit, joten ei ole mahdollisuutta kytkeä lisäantenneja.
- Automaattinen tehonsäätö, jolla vältetään viereisten radioporttien häiritseminen liialla teholla. Tehonsäädöllä pyritään myös korvaamaan automaattisesti rikkoutunut tukiasema verkossa.

Kuva 10. HP ProCurve Radio Port 230 [8]

4.1.2 Verkon rakenne

Yrityksen A verkko on Windows-pohjainen, joten käytössä on Active Directory aktiivihakemisto käyttäjätietojen hallintaan sekä Group Policy -ryhmäkäytännöt asetusten jakeluun työasemille.

Rakennuksen kerroksissa 2-8 on jokaisessa 5 radioporttia. Alimmassa kerroksessa on henkilöstöravintolan tilojen takia vain kaksi porttia ja 9. kerros saatiin laajojen neuvottelutilojen takia katettua kolmella radioportilla (kuva 11).



Kuva 11. Verkon rakenne yrityksessä A

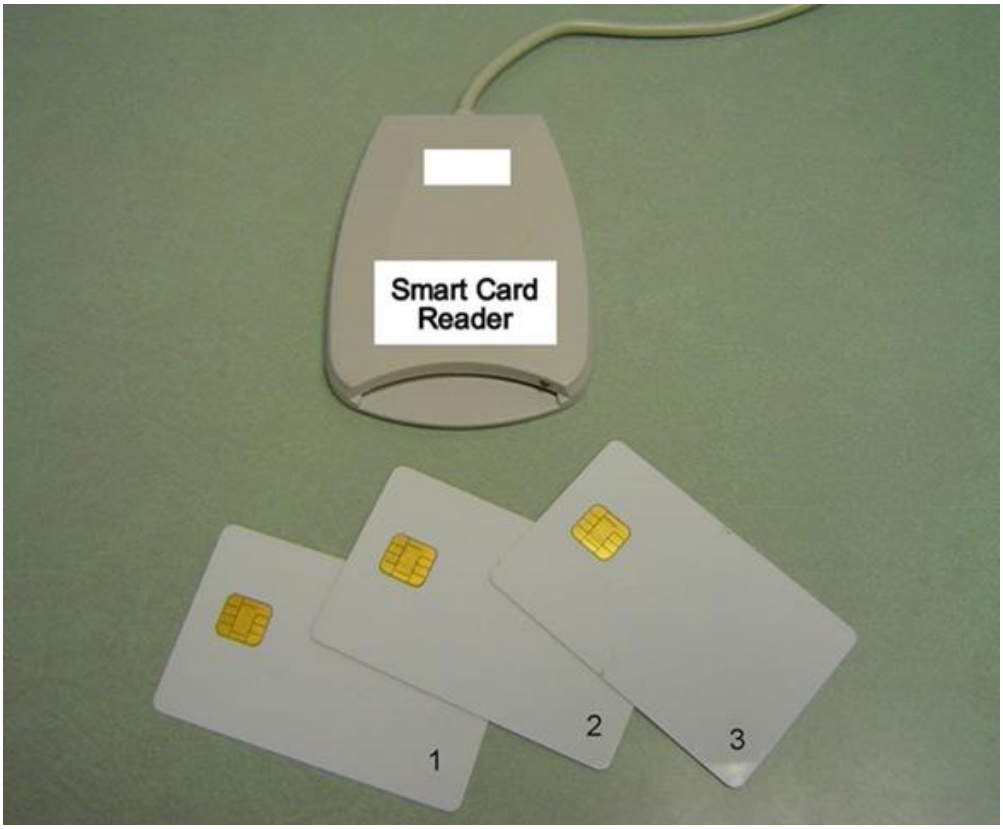
Kaikissa kerroksissa on erillinen kytkin ”HP ProCurve Switch 2600-8-PWR” langattoman verkon radioporttien käyttöön. Kytkin on malli, josta saadaan johdettua ethernet-verkkoa käyttäen sähkö ja verkkoyhteys radioporteille. Kyseiset kytkimet hankittiin langatonta verkkoa rakennettaessa huomioiden erityisesti radioporttien virransyöttö. Näistä kytkimistä on yhteys kerroskytkimiin, jotka reitittävät liikenteen rakennuksen runkoverkkoa pitkin keskuskytkimelle, jossa langattoman verkon kontrolleri sijaitsee.

Radioporttien liikenne on eroteltu kiinteästä verkosta kerroskytkimissä VLAN-verkoilla.

4.1.3 Tunnistautuminen ja salaus

Tunnistautuminen sisäverkkoon on toteutettu IAS *(Internet Authentication Service)* –nimisen palvelun avulla. Olemassa olevalle palvelimelle asennettu lisäpalvelu, joka hoitaa tunnistautumisen sisäverkkoon. IAS sijaitsee Microsoft Windows Server 2003 SP2 R2 –palvelimella. Samalla palvelimella on IAS:n käyttöön tarkoitettu RADIUS-palvelin.

Itse tunnistautuminen tapahtuu älykortille (kuva 12) asennetun sertifikaatin avulla. Jokainen kortti luodaan käyttäjäkohtaisesti ja myös sertifikaatti määritellään käyttäjäkohtaisesti. Kyseinen sertifikaatti varmistaa sen, että tunnistusta pyytävä langattoman verkon tukiasema on yrityksen verkossa eikä esimerkiksi ulkoisen hyökkääjän asentama laite. Lisäksi sertifikaatilla käyttäjä tunnistautuu verkkoon. Tunnistauduttaessa älykortti syötetään päätelaitteen kortinlukijaan ja käyttäjältä kysytään henkilökohtainen PIN-koodi, jolla älykortilla oleva sertifikaatti avataan.



Kuva 12. Älykortteja ja älykortinlukija

Kaikki asetukset langattoman verkon käyttöön on määritelty etukäteen ja ne jaetaan koneisiin Group Policy –ryhmäkäytäntöjen avulla automaattisesti uusia koneita asennettaessa. Asetukset pitävät sisällään käytetyt verkkojen nimet, kanavat ja tiedon tunnistautumisesta. Kyseisellä ratkaisulla pyritään ennakoimaan, jos verkkojen nimet tai muut ominaisuudet jatkossa muuttuvat.

Tunnistautumisessa langattoman verkon kontrolleri tarkistaa IAS-palvelun avulla RADIUS-palvelimelta avulla käyttäjän antamat kirjautumistiedot ja määrittelee sen perusteella, päästetäänkö käyttäjä verkkoon. Mikäli käyttäjän sertifikaatti vastaa palvelimella olevaa ja käyttäjätunnus on voimassa, muodostaa kontrolleri yhteyden ja toimittaa päätelaitteelle tarvittavat tiedot liikenteen salaamiseksi.

Tunnistautumisvaiheessa liikenne on salattu EAP-protokollalla. Kun langaton yhteys muodostetaan, salaus tapahtuu AES-algoritmilla ja säännöllisin väliajoin vaihtuvilla salausavaimilla. AES-algoritmista käytössä on vahvuudeltaan 256-tavuinen suojaus.

Vierailijaverkko on jaettu radioporteissa toiseen verkkoon eikä siinä ole käytössä minkäänlaista salausta. Itse vierailijaverkon liikenne on erotettu sisäverkosta kytkimissä VLAN-verkolla, ja yhteys reititetään suoraan runkokytkimestä erillisen palomuurin kautta ulos ADSL-linjaa pitkin (kuva 11).

Tunnistautuminen vierailijaverkkoon on toteutettu langattoman kontrollerin sisäisellä tunnushallinnalla ja tunnistautumissivulla. Kontrollerilla on sisäverkkoon jaettu verkkosivu, mihin voidaan ottaa yhteys selaimella ja sitä kautta luoda tunnukset vierailijoiden käyttöön. Tunnukset tallentuvat langattoman kontrollerin sisäiseen tietokantaan ja ovat voimassa oletuksena 24 tuntia.

Vierailijaverkkoon yhdistettäessä päätelaitteen selain siirtyy pakotetusti aloitussivulle, jossa kysytään tunnuksia. Tunnuksien syötön jälkeen kontrolleri vertaa niitä RADIUS-protokollalla omaan tietokantaansa. Mikäli tunnukset ovat voimassa, sallitaan kaikki verkkoliikenne ulkoverkkoon.

4.1.4 Haasteet käytössä ja parannusehdotukset

Yritys A:n langattomassa verkossa on ollut useita yksittäisiä ongelmia, mutta kokonaisuutena ja verkon käytettävyyden kannalta ne ovat häirinneet käyttöä melko vähän.

Verkkoa pystytettäessä oli kontrolleri vasta saapunut markkinoille. Tästä aiheutui ongelmia radioporttien hallinnassa eikä kaikkia portteja saatu aluksi käyttöön samanaikaisesti. Tähän kuitenkin saatiin pian päivitys kontrollerin ohjelmistoon, joka mahdollisti kaikkien porttien saamisen käyttöön samanaikaisesti.

Viime kesänä langattomassa verkossa alkoi esiintyä selvittämätöntä yhteyden katkeilua, jota yritettiin selvittää usean kuukauden ajan. Selvityksessä käytiin läpi käytännössä kaikki laitteet, joita verkossa oli, mutta ongelmaa ei kontrollerin ulkopuolelta löydetty. Lopulta ongelma ratkesi, kun koko kontrolleri takuuvaihdettiin uuteen kappaleeseen eikä yhteyden katkeilua sen jälkeen ole enää tapahtunut.

Yksittäisiä radioportteja on välillä hajonnut, mutta niiden vaihtaminen ei ole tuottanut ongelmia, eivätkä yksittäiset rikkinäiset portit heikennä merkittävästi verkon peittoaluetta. Verkossa on päällä automaattinen tehonsäätö, eli yksittäisen antennin rikkoutuessa viereiset antennit lisäävät tehoa kattaakseen rikkinäisen radioportin alueen. Verkon kattavuus on rakennuksessa muuten hyvä, mutta 9. kerroksessa on tehty remonttia ja siellä tarvittaisiin ainakin yksi radioportti lisää uusiin tiloihin.

Sertifikaattipohjaisessa tunnistautumisessa ilmeni ongelmia, kun palvelimelle muodostettiin uusi sertifikaatti edellisen voimassaolon umpeuduttua. Vanha sertifikaatti ei kuitenkaan poistunut palvelimelta automaattisesti, joten osan ajasta yhteyttä muodostettaessa päätelaiteet yrittivät varmentaa vanhentunutta sertifikaattia, jolloin yhteys ei muodostunut. Ongelma saatiin ratkaistua muuttamalla sertifikaattien vanhenemisen asetuksia ja varmistamalla, että jatkossa vanhat sertifikaatit poistuvat automaattisesti.

Sertifikaatit ovat tällä hetkellä verkossa vain yhdellä palvelimella, vaikka langallisen verkon tunnistautumiseen käytettävät palvelimet on kahdennettu. Tästä syystä langattoman verkon tunnistautumiseen käytettävän palvelimen rikkoutuessa ei yhteyttä langattomaan verkkoon saada muodostettua, vaikka

se langallista verkkoa käyttäen varapalvelimen avulla onnistuukin. Tämä tulisi huomioida jatkossa, jos langattomalle verkolle halutaan vikasietoisuutta. Vikasietoisuutta saataisiin haluttaessa lisättyä myös kahdentamalla langattoman verkon kontrolleri siihen tarkoitetulla varalaitteella.

Loppukäyttäjän kannalta näkyvin ongelma verkossa on tällä hetkellä vierailijaverkon kirjautumissivulla esiintyvä sertifikaattivaroitus. Sivun oletussertifikaatti osoittaa eri sivustolle kuin missä sivu sisäverkossa sijaitsee. Tämä ilmenee varsinkin uudemmissa internetselaimissa, erittäin näkyvänä varoituksena. Varoituksesta pääsee etenemään helposti, mutta loppukäyttäjän kannalta on epäedullista neuvoa jatkamaan sivustolle, josta selain varoittaa selkeästi. Ratkaisu ongelmaan olisikin selvittää, missä oletussertifikaatti sijaitsee palvelimella ja muokata se vastaamaan nykyistä kirjautumissivua.

4.1.5 Loppupäätelmät Yrityksestä A

Yritys A on mitoittanut verkon tarkasti omaan käyttöönsä ja valinnut laitteita, jotka ovat yhteensopivia muiden verkon laitteiden kanssa. Laitteiden hankinnan suunnitteluun on käytetty riittävästi aikaa ja ne on hankittu selvästi verkon toimivuuden ollessa hankinnan perusteena eikä niinkään edulliset kustannukset.

Verkossa on riittävästi laajennusvaraa, jos peittoaluetta tai verkon tiedonsiirtokapasiteettia halutaan vielä tulevaisuudessa kasvattaa. Tämänhetkinen radioporttien määrä on mitoitettu hyvin ja hidastumista useista samanaikaisista käyttäjistä johtuen ei ole vielä esiintynyt. Tulevaisuuden kannalta on hyvä huomioida mahdolliset uudet sovellukset yrityskäytössä, kuten IP- tai videopuhelut. Kyseiset palvelut vaativat huomattavasti enemmän tiedonsiirtokaistaa kuin nykyinen käyttö. Mikäli verkossa halutaan siirtää huomattavasti enemmän liikennettä, olisi se huomioitava uusilla, nopeamman standardin mukaisilla radioporteilla.

Verkon rakenne on toteutettu rakennuksen tiloihin sopivasti, ja kaikki katvealueet on saatu hyvin peitettyä. Verkon kattavuus on jopa niin hyvä, että verkon kattavuutta testatessa ei rakennuksen sisällä edes kellarissa tullut katkoksia tiedonsiirtoon.

Verkon hallinnointi on helppoa keskitetyn kontrollerin kautta ja verkon eri ominaisuuksien muokkaus onnistuu helposti. Kontrollerissa asetuksia pää-

see muokkaamaan selkeiden valikoiden kautta käyttämällä internetselainta. Tarvittaessa asetuksia pääsee muokkaamaan myös komentoriviltä, mikä mahdollistaa kaikkien laitteen asetusten hyvin tarkan säätämisen. Käytännössä kuitenkin kaikki normaalit toimenpiteet onnistuvat graafiseltakin puolelta.

Ongelmat verkon käytössä ovat olleet vaikutukseltaan pieniä, viallista kontrolleria lukuun ottamatta, ja ne on saatu ratkaistua nopeasti. Käyttäjät ovat olleet verkon toimintaan tyytyväisiä ja käytön helppouden myötä yhä useampi käyttäjä onkin neuvottelutiloissa tai muissa olosuhteissa turvautunut langattomaan verkkoon työpaikalla.

Tietoturvan kannalta Yritys A:n verkko on toteutettu kiitettävästi. Tällä hetkellä olevista tunnistautumis- ja salausmenetelmistä vahvimpana pidetään Yritys A:ssa käytössä olevaa älykortilla sijaitsevaa sertifikaattia ja AES-salausta. Kyseinen fyysisen tunnisteen käyttö vähentää ulkopuolisen henkilön pääsyn mahdollisuuden käytännössä olemattomaksi. Mahdollisesti hävinneet älykortit saadaan kuoletettua hetkessä, jolloin estetään käyttäjien huolimattomuudesta johtuvat tietoturvariskit.

AES-salaus, varsinkin käytettävä 256-tavun salausta käyttävä malli, luokitellaan tällä hetkellä murtamattomaksi. Tilanne varmasti muuttuu tulevaisuudessa, mutta tällä hetkellä verkon tietoturvaa ei olennaisesti pystyttäisi lisäämään millään toimenpiteillä. [5.]

Verkon tietoturvan lisäksi on huomioitu käytön helppous käyttäjille ja vierasverkon helppo käyttö. Näissäkin on Yritys A:ssa onnistuttu löytämään riittävän hyvä tasapaino käytettävyyden ja turvallisuuden kanssa. Älykortilla sisäverkon vaatii hieman ylimääräisiä toimenpiteitä, mutta tietoturvahyöty on kyseisessä yrityksessä nähty ylimääräisten toimenpiteiden arvoiseksi.

Vierailijaverkon tunnusten luonti ja hallinnointi on toteutettu riittävän helposti jatkuvan käytön kannalta.

4.2 Yritys B

Yritys B sijaitsee kahdessa kerroksessa sekä yhdessä etäpisteessä. Käyttäjiä yrityksessä on noin 130. Tarve langattomalle verkolle syntyi, kun yrityksen sisäverkkoon haluttiin päästä joustavasti eri puolilta yrityksen tiloja. Yri-

tyksessä oli myös neuvottelutiloja, mutta niihin ei verkkoa alun perin rakennettaessa nähty tarpeelliseksi hankkia langattomia yhteyksiä. Neuvottelutilat otettiin kuitenkin mukaan suunnitelmiin, kun verkon toimivuutta haluttiin parantaa myöhemmin.

Yrityksen etäpisteeseen on rakennettu suora verkkoyhteys ja langattoman verkon haluttiin kattavan myös etäpisteen käyttäjät. Neuvottelutiloja on sekä päätoimistolla että etäkonttorin tiloissa.

Lähtökohtana verkon rakentamisessa oli tulla toimeen mahdollisimman pienillä uusilla investoinneilla. Langatonta verkkoa ei katsottu kovin keskeiseksi osaksi yrityksen liiketoimintaa.

4.2.1 Laitteisto

Verkko rakennettiin aluksi itsenäisillä Ciscon valmistamilla tukiasemilla, mutta itsenäisten tukiasemien hallinta osoittautui erittäin hankalaksi ja yritykseen päätettiin hankkia langattomalle verkolle kontrolleri, jotta tukiasemia saatiin hallittua keskitetysti. Kontrolleria käyttämällä saatiin myös antennien välinen liikenne hallintaan, jolloin yrityksen tiloissa pystyi liikkumaan päätelaitteen kanssa, ilman että yhteys katkesi antennien välillä liikuttaessa.

Kontrollerin hankinnan yhteydessä päätettiin myös samalla määritellä verkkoon erillinen vierailijaverkko. Yksittäisillä tukiasemilla vierailijaverkkoon määrittelyä oli tutkittu, mutta se oli osoittautunut erittäin vaikeaksi toteuttaa. Kontrollerin avulla verkon määrittely onnistui helposti.

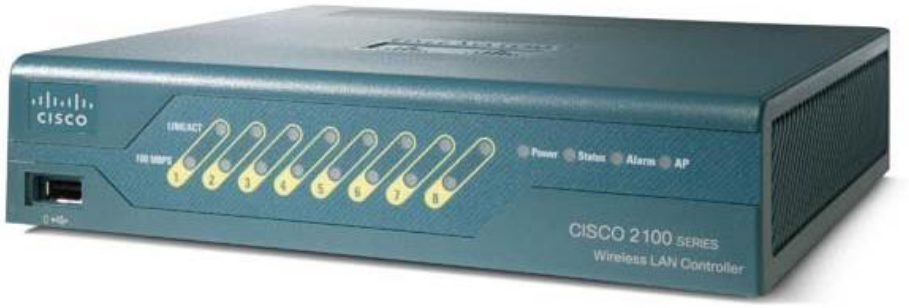
Verkon muut verkkolaitteet olivat Ciscon valmistamia, joten yhteensopivuuden vuoksi myös langattoman verkon laitteet päätettiin hankkia samalta valmistajalta.

Valmistajalta saatujen ohjeiden perusteella olemassa olevat, yksittäiset tukiasemat voitiin muuttaa itsenäisistä ohjelmistoista hallittuun ohjelmistoon. Ennen muutosta tukiasemien mallinimi oli ”AIR-AP1242AG” ja ohjelmiston päivityksen jälkeen ”AIR-LAP1242AG” (kuva 13). Kyseisen muutoksen ansiosta ei ollut tarpeellista hankkia muita uusia laitteita verkkoon kontrollerin lisäksi.

Langattoman verkon kontrolleriksi valittiin ”Ciscon AIR-WLC2106” (kuva 14), joka katsottiin ominaisuuksiltaan sopivaksi yrityksen tarpeisiin.

Cisco AIR-WLC2106 [9, 10]

- Radioportteja on enintään 6 kappaletta, ei laajennettavissa.
- Tukee RADIUS-tunnistautumista tukien EAP-TLS-protokollaa.
- Vierailijaverkon tunnushallinta ja tunnistautuminen on sisäänrakennettu kontrolleriin.
- Tunnistaa automaattisesti kiinteään verkkoon kytketyt radioportit. [9; 10]



Kuva 13. Cisco AIR-WLC2106 [9]

Cisco AIR-LAP1242AG [11]

- Mahdollisuus ohjelmistollisesti määritellä toimimaan joko itsenäisenä tukiasemana ilman kontrolleria tai pelkkänä radioporttina erillisen kontrollerin avulla.
- Saa virtansa joko sähköpistorasiasta muuntajalla tai ethernet-verkon avulla PoE-tekniikalla.
- Tukee 802.11a ja 802.11b/g verkkoja.
- Ei sisäänrakennettuja antenneja, jolloin vaaditaan erilliset ulkoiset antennit.
- Siinä on haluttaessa automaattinen tehonsäätö.

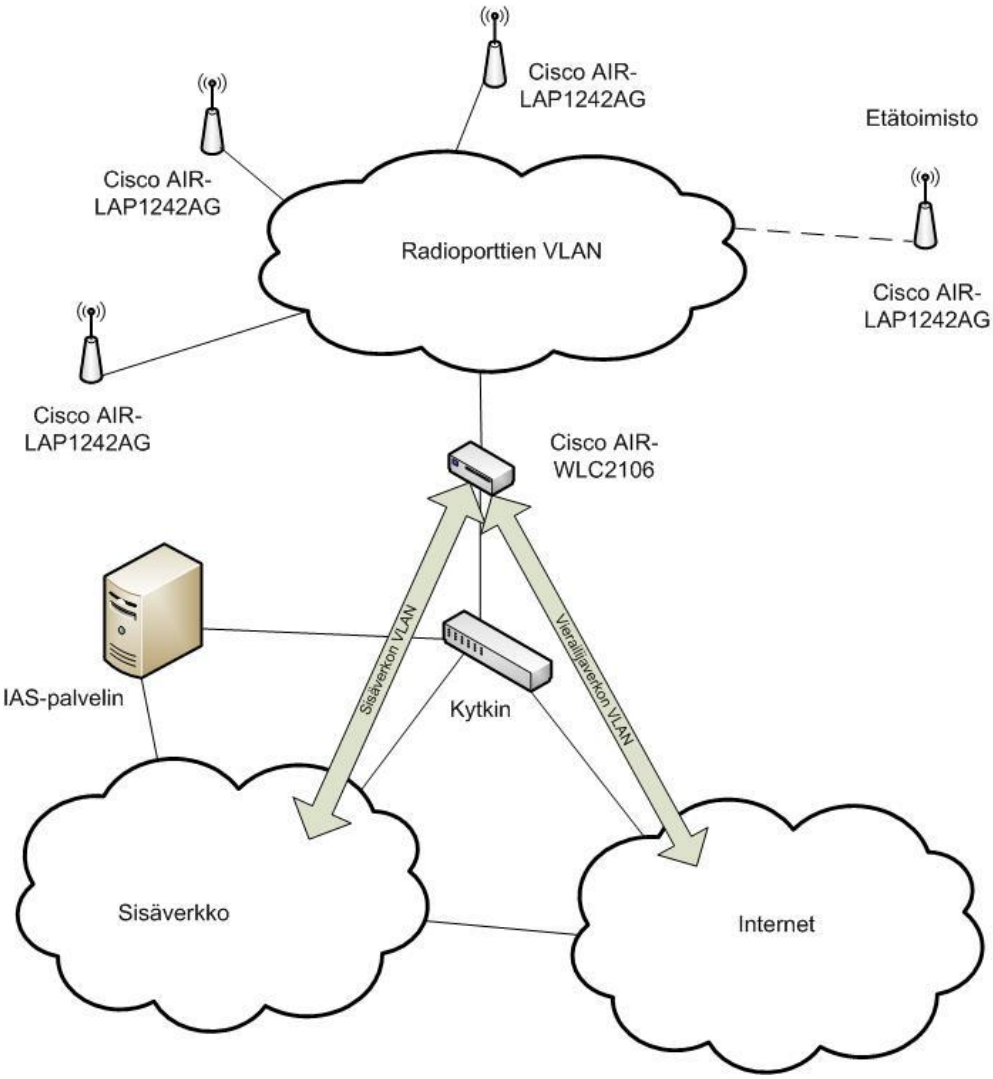
Kuva 14. Cisco AIR-LAP1242AG [11]

4.2.2 Verkon rakenne

Yrityksen verkko on Windows-pohjainen, joten verkossa on käytössä aktiivihakemisto ja ryhmäkäytännöt. Aktiivihakemistoa käytetään langattoman verkon yhteydessä sisäverkon käyttäjätunnusten hallinnointiin ja sertifikaattien luomiseen. Ryhmäkäytäntöjä käytetään asetusten määrittelyyn keskitetysti yrityksen työasemiin.

Radioportit on kytketty kiinteän verkon kautta kontrolleriin VLAN-verkon avulla. Myös vierailijaverkko ja sisäverkko on erotettu toisistaan VLAN-verkoilla (kuva 15).

Radioportteja on neljä kappaletta, joista kolme sijaitsee päätoimistolla ja yksi etäpisteessä. Kaikki liikenne kulkee muun verkon liikenteestä erillisessä VLAN-verkossa kontrollerille, joka hoitaa kirjautumisen joko sisäverkkoon tai ulkoverkkoon.



Kuva 15. Verkon rakenne Yrityksessä B

Liikenne kontrollerilta sisäverkkoon ja vierailijaverkkoon on eristetty omiin VLAN-verkkoihin, mutta se kulkee samojen fyysisten laitteiden kautta. Kuvassa 15 kyseinen rajaus on merkitty nuolilla.

Verkossa käytössä olevat kytkimet eivät ole PoE-mallisia, joten virta radioporteille tarjotaan normaalin sähköverkon kautta. Tukiasemat on tästä syystä sijoitettu pistorasioiden lähettyville.

Kontrollerilla on päällä niin sanottu ”Rogue AP detection” -toiminto eli haitallisen tukiaseman havaitseminen. Mikäli radioporttien lähettyville tuodaan vieraita tukiasemia, hälyttää kontrolleri siitä järjestelmän ylläpitäjille. Kontrollerilla olisi myös mahdollisuus yrittää sulkea verkosta vieraita tukiasemia, mutta sitä ei ole haluttu kytkeä päälle. Päällä ollessaan ominaisuus saattaa sulkea myös naapuritiloissa olevien yritysten tukiasemia.

Radioportit tarkkailevat koko ajan toisiaan. Mikäli yksittäinen radioportti rikkoutuu, osaavat viereiset laitteet lisätä automaattisesti tehoa kattaakseen vikaantuneen tukiaseman alueen.

4.2.3 Tunnistautuminen ja salaus

Langaton verkko on jaettu radioporteissa kahteen verkkoon, vierailijaverkkoon ja sisäverkkoon. Vierailijaverkon liikenne on salaamatonta, mutta verkkoon täytyy tunnistautua kirjautumissivun kautta. Kirjautumissivu aukeaa päätelaitteen internetselaimeen automaattisesti, kun yhteys on muodostettu vierailijaverkkoon. Kaikki vierailijaverkon tunnistautumiseen liittyvät toiminnot tapahtuvat kontrollerissa lukuun ottamatta vierailijaverkon salasanan muodostamista.

Kontrollerille on määritelty viikoittain vaihtuva salasana, jota hallinnoidaan erillisellä komentosarjalla. Komentosarja suoritetaan erillisellä palvelimella ja se luo satunnaisen merkkijonon salasanaksi. Lisäksi komentosarja vaihtaa automaattisesti uuden salasanan kontrollerille ja luo samalla internetsivun, josta tunnus on luettavissa. Tämän jälkeen komentosarja päivittää kyseisen sivun yrityksen sisäverkkoon, josta yrityksen henkilökunta voi ottaa salasanan vierailijoiden käyttöön.

Sisäverkkoon yhdistetään ja tunnistaudutaan automaattisesti, yrityksen koneille etukäteen määriteltyjen asetusten avulla. Asetukset jaetaan koneisiin verkon ryhmäkäytäntöjen avulla, jolloin niitä pystytään muokkaamaan ja jakelemaan uudestaan helposti. Verkkoon yhdistäminen ei vaadi käyttäjiltä mitään toimenpiteitä, koska yhteys on määritelty muodostumaan automaattisesti yrityksen langattoman verkon ollessa saatavilla.

Tunnistautuminen tapahtuu WPA2-Enterprise -tekniikalla, IAS-palvelimen ja siinä sisällä toimivan RADIUS-palvelimen avulla. Tunnistauduttaessa langattoman verkon kontrolleri varmistaa IAS-palvelimelta, onko käyttäjällä oikeus päästä verkkoon.

Tunnistautuminen varmennetaan sertifikaatilla, joka luodaan sisäverkon Active Directory -palvelimen avulla. Sertifikaatti on konekohtainen, ja se luodaan konetta asennettaessa. Kun verkkoon on onnistuneesti tunnistauduttu, salataan liikenne AES-salauksella. AES-salauksesta on käytössä vahvin 256-tavuinen versio.

4.2.4 Haasteet käytössä ja parannusehdotukset

Suurimpana haasteena Yrityksen B langattoman verkon pystytyksessä oli vanhojen tukiasemien muuttaminen radioporteiksi. Valmistaja oli toimittanut ohjelman, jolla asetukset oli tarkoitus asentaa automaattisesti, mutta sen käytössä tuli suuria ongelmia. Lopputuloksena jokainen tukiasema jouduttiin uuden ohjelmiston asentamista varten käymään läpi yksitellen.

Verkkoa asennettaessa huomattiin, että WPA2-AES-asetukset eivät asentuneet työasemiin ryhmäkäytäntöjen avulla automaattisesti. Asiaa tutkittiin ja ongelmaksi selvisi yrityksessä silloin käytössä ollut Windows XP -käyttöjärjestelmän Service Pack 2 –laajennus. Käyttöjärjestelmän valmistaja toimitti ongelmaan korjaustiedoston, eikä vastaavia ongelmia ole päivityksen jälkeen ilmennyt.

Osa käyttäjistä on myös raportoinut ongelmista erilaisten tietokantasovellusten käytössä langattoman verkon yli. Tämä ongelma saatiin rajattua kyseisten sovellusten ongelmaksi ja siihen saatiin sovellusten valmistajalta korjauspäivitys.

Vierailijaverkkoon kirjauduttaessa selain ohjautuu kirjautumissivulle. Sivuston sertifikaatissa on kuitenkin virheellinen tieto, joka näkyy käyttäjälle varoituksena virheellisestä sertifikaatista. Varoituksesta huolimatta kirjautuminen onnistuu, mutta visuaalisesti kyseinen varoitus on yrityksen kannalta epäedullinen. Ongelmaa tulisi yrittää ratkoa selvittämällä, mikä kohta sertifikaatissa on väärin ja luoda uusi, toimiva sertifikaatti sivustolle.

Verkon kattavuus mitattiin yrityksessä verkkoa pystytettäessä, mutta yrityksen tilat ovat sen jälkeen laajentuneet. Tästä syystä radioportteja tulisi hankkia lisää, mutta esteeksi saattaa osoittautua kontrollerin tuki vain kuudelle radioportille.

Tulevaisuudessa tulisikin selvittää tarvitaanko tiloihin kontrolleri, johon saisi kytkettyä useampia radioportteja. Valmistajan mallistosta kyseisiä malleja löytyy. Lähinnä tulisi selvittää laitteiston hankinta-ajankohta.

4.2.5 Loppupäätelmät Yrityksestä B

Yritys B:n verkko on toteutettu kustannustehokkaasti käyttämällä olemassa olevia laitteita ja hankkimalla vain välttämättömimmät lisälaitteet. Laitteet on

kuitenkin hankittu myös ottamalla huomioon verkossa olevat laitteet ja näin yhteensopivuusongelmilta on vältytty.

Verkon toimivuus on ollut riittävän hyvä ja peittoalue kattava. Kaikki käyttäjiä häiritsevät ongelmat on saatu ratkottua päivityksillä tai verkon asetuksia muuttamalla. Sisäverkon ja ulkoverkon käyttö on helppoa ja yksinkertaista. Käyttö ei vaadi käyttäjiltä ylimääräisiä toimenpiteitä, koska verkko on rakennettu lähtökohtanaan helppokäyttöisyys.

Verkon hallittavuus on helppoa ja tehokasta kontrollerin avulla. Asetusten jakelu työasemiin on helppoa ryhmäkäytäntöjen avulla.

Sisäverkkoon kirjautuminen on tietoturvaltaan riittävän hyvä ja langattoman verkon salaus riittävä yrityskäyttöön. Vierailijaverkon hallinta on toteutettu hieman erikoisella ratkaisulla. Kyseinen ratkaisu kuitenkin toimii, eikä siinä ole varsinaisia tietoturvaongelmia tai ongelmia käytössä

4.3 Yritys C

Yrityksellä on noin 400 käyttäjää, joista noin 100 sijaitsee kiinteästi Helsingin pääkonttorilla. Toimisto sijaitsee yhdessä kerroksessa, kolmeen siipeen jakautuneena. Kaksi siivistä on rajattu vain yrityksen työntekijöille ja kolmas siipi on varattu neuvotteluhuonekäyttöön. Lisäksi kaikki yrityksen vierailijat otetaan vastaan neuvottelutiloissa kolmannessa siivessä.

Tarve langattomalle verkolle muodostui kun, yrityksessä otettiin käyttöön kannettavia tietokoneita ja niillä haluttiin päästä yrityksen verkkoon toimiston tiloissa langattomasti. Myös muilta toimistoilta pääkonttorilla käyville työntekijöille haluttiin tarjota pääsy sisäverkkoon joustavasti. Lisäksi neuvottelutiloihin haluttiin järjestää vierailijoille pääsy internetiin.

4.3.1 Laitteisto

Langaton verkko on toteutettu Extreme Networksin laitteistolla. Laitteistoon kuuluu tällä hetkellä yksi kontrolleri, malli ”Summit WM20” (kuva 16) ja viisi tukiasemaa, malli ”Altitude 350-2” (kuva 17). Lisäksi verkossa on Juniperin valmistamia kytkimiä, joiden kautta radioportit on kytketty kontrolleriin. Vierailijaverkkoon tunnistautumista varten verkossa on erillinen palvelin, jossa toimii Arch Red –yrityksen valmistama tunnustenhallintasovellus.

Extreme Networks Summit WM20 [12]

- Ulkoisia antenneja saa kytkettyä enintään 16 kappaletta, laajennettavissa ohjelmistolla 32 kappaleeseen.
- Kontrolleri tukee enintään 512 samanaikaista käyttäjää.
- Tukee RADIUS-tunnistautumista, tukien EAP-TLS ja PEAP –protokollia.
- Tunnistaa automaattisesti kiinteään verkkoon kytketyt radioportit.

Kuva 16. Extreme Networks Summit WM20

Extreme Networks Altitude 350-2 [13]

- On yksinkertainen radioportti, joka vaatii kontrollerin toimintaansa.
- Saa virtansa ethernet-verkon yli PoE-tekniikalla.
- Tukee 802.11a- ja 802.11b/g-verkkoja.
- Radioportissa on sisäänrakennetut antennit. Radioportissa on mahdollisuus kytkeä ulkoiset lisäantennit tarvittaessa.
- Radioportissa on automaattinen tehonsäätö, jolla vältetään viereisten radioporttien häiritseminen liialla teholla. Tehonsäädöllä pyritään myös korvaamaan automaattisesti rikkoutunut tukiasema verkossa.

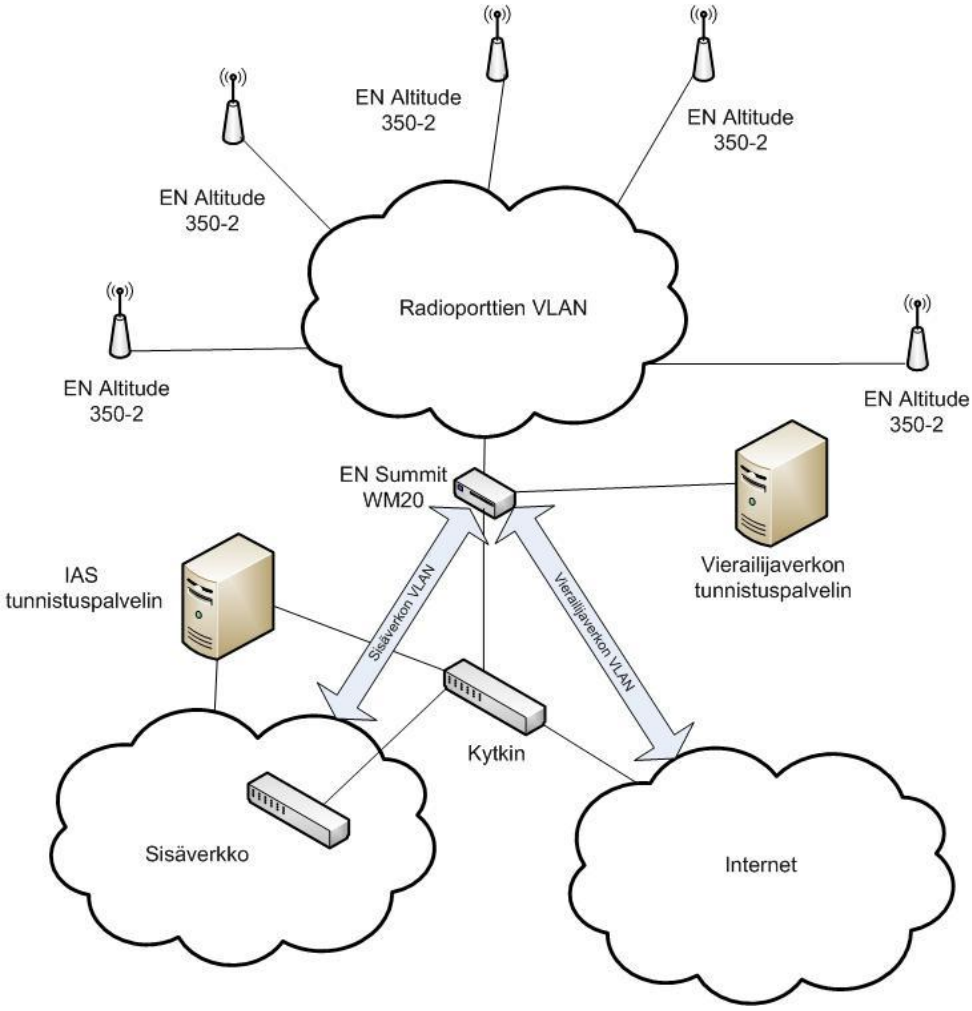
Kuva 17. Extreme Networks Altitude 350-2

Kontrollerissa on kytketty päälle toiminto, joka tarkkailee verkossa olevia langattomia tukiasemia. Mikäli verkossa havaitaan vieraita tukiasemia, kirjataan huomio lokitiedostoon. Jos vierailla tukiasemilla havaitaan sama nimi kuin yrityksen käyttämillä tukiasemilla, lähetetään verkon ylläpitäjälle ilmoitus verkossa olevasta, mahdollisesti hyökkääjän asentamasta, tukiasemasta.

Verkon muut laitteet ovat eri valmistajilta, kuten CISCOlta, Juniperilta ja HP:ltä. Mitään erityistä syytä ei ollut, jolla olisi päädytty valitsemaan juuri Extreme Networksin verkkolaitteet.

4.3.2 Verkon rakenne

Kontrolleri sijaitsee yrityksen kytkentätilassa ja radioportit on jaettu seuraavasti: kaksi kappaletta radioporteista on neuvottelutiloissa, kaksi kappaletta toisessa toimistosiivessä ja yksi kappale toisessa siivessä.



Kuva 18. Verkon rakenne yrityksessä C

Radioportit on eristetty muusta verkosta omaan VLAN-verkkoon, joka kulkee usean fyysisen reitittimen kautta. Kuvassa 18 kyseinen looginen kytkentä on kuvattu radioporttien omana VLAN-verkkonaan.

Vierailijaverkon ja sisäverkon liikenne on eristetty toisistaan VLAN-verkkojen avulla, mutta ne käyttävät samoja fyysisiä laitteita ja kytkentöjä. Kuvassa 18 kyseiset loogiset verkot on kuvattu nuolien avulla.

4.3.3 Tunnistautuminen ja salaus

Langaton verkko on jaettu radioporteissa kahteen eri mainostettavaan verkkoon, vierailijaverkkoon ja sisäverkkoon. Vierailijaverkon liikenne ei ole salattua, mutta tunnistautuminen on hoidettu erillisellä hallintapalvelimella, joka pitää sisällään vierailijatunnusten hallinnan ja itse tunnistautumiseen vaadittavat palvelut.

Palvelimella on tunnusten hallintaa varten verkkosivu, josta ylläpitäjä voi luoda vierailijoille tunnukset verkon käyttöön. Kun vierailija yhdistää vierailijaverkkoon ja avaa koneensa selaimen, reitittyy kaikki liikenne kyseiselle palvelimelle, joka tarjoaa näkyville sisäänkirjautumislomakkeen. Tässä vaiheessa muu kuin tunnistautumiseen liittyvä liikenne verkkoon on estetty.

Kun vierailija on syöttänyt saamansa tunnukset verkkosivulle, tunnistautuu vierailijan kone RADIUS-menetelmällä palvelimelle ja saa käyttöönsä normaalit verkkoyhteydet ylläpitäjän määräämäksi ajaksi. Kun aika umpeutuu, tunnukset lakkaavat toimimasta ja vierailija ohjautuu takaisin kirjautumissivulle ja muu liikenne verkkoon katkeaa.

Sisäverkon tunnistautuminen ja salaus on toteutettu WPA2-AES–tekniikalla. Tunnistautuminen verkkoon tapahtuu *PEAP* eli *protected EAP* -protokollan avulla erilliselle IAS-palvelimelle. IAS-palvelin tarkistaa RADIUS-protokollan avulla yrityksen verkosta käyttäjätunnuksen ja salasanan, sekä onko tunnus voimassa ja onko sillä sallittu pääsy langattomaan verkkoon. Tunnistautumisen jälkeen liikenne salataan AES-salauksella.

Tunnistautumiseen käytetään lisäksi konekohtaista sertifikaattia, joka luodaan yrityksen palvelimelle. Sertifikaatin avulla myös tunnistuspalvelimen aitous varmistetaan päätelaitteelle. Sertifikaatti luodaan ja asennetaan päätelaitteeseen automaattisesti asennuksen yhteydessä käyttäen avuksi Active Directoryn Group Policy -ryhmäkäytäntöjä.

4.3.4 Haasteet käytössä ja parannusehdotukset

Suurimpina haasteina verkon käytössä on huomattu selvittämättömät ongelmat yhteyden muodostamisessa sisäverkkoon. Osa koneista tunnistautuu verkkoon sertifikaatilla onnistuneesti, mutta ei saa IP-osoitetta palvelimelta. Tämä estää liikennöinnin verkossa täysin.

Ongelma ilmenee satunnaisesti, eikä sitä ole saatu rajattua mihinkään tiettyyn päätelaitteistoon, vaan ongelma esiintyy myös identtisillä päätelaitteilla, joissa on identtiset ohjelmistot. Ongelman on epäilty johtuvan laitteiston yhteensopivuusongelmista, mutta mitään varmaa selvitystä asiaan ei ole saatu.

Toinen ongelma verkossa ovat katvealueet tietyissä osissa toimistoa. Osa antenneista on rakenteiden takana, jolloin käyttäjät eivät saa häiriötöntä yhteyttä, mikä näkyy yhteyden katkeiluna ja hidasteluna.

Parannusehdotuksina yrityksen langattoman verkon toimintaan olisi selvittää yhteysongelmien perimmäinen syy. Ensimmäisenä olisi tärkeää selvittää, aiheutuvatko ongelmat mahdollisesti siitä, että suuri osa verkon laitteistosta on eri valmistajilta. Ongelma pitäisi tämän jälkeen saada rajattua tiettyyn osaan laitteistoa, ennen kuin mitään korjausehdotusta olisi järkevää antaa.

Verkkoon tulisi myös hankkia lisää radioportteja, jotta langattoman verkkoon kattavuutta saataisiin parannettua ja katvealueita poistettua. Lisäksi langattoman verkon käyttäjiä on koko ajan lisää, joten antennien rajallinen tiedonsiirtokaista saattaa tulla jossain välissä vastaan. Nopeus kuitenkin vielä riittää normaaliin toimistokäyttöön, joten uudemman 802.11n-standardin mukaisia, nopeampia antenneja tuskin tarvitaan, koska suurin osa päätelaitteista on vielä vanhaa 802.11g-standardia.

4.3.5 Loppupäätelmät Yrityksestä C

Yrityksen C langaton verkko on toteutettu eri valmistajien erillisillä laitteilla, mikä saattaa olla osasyynä yhteensopivuusongelmiin. Nykyään suurin osa langattomien verkkojen toiminnoista pyritään saamaan yksittäisiin laitteisiin, jolloin vältetään mahdolliset ongelmat laitteiden kesken. Erilisissä osissa on kuitenkin etuna se, että niitä saadaan vaihdettua tarvittaessa helposti. Laitteet ovat saattaneet olla ostettaessa edullisempi vaihtoehto hankkia erikseen kuin yksittäiseltä valmistajalta. Kyseisen laitteiston hankintahintaa ei tämän työn yhteydessä saatu selvitettyä.

Verkon laitteisto on tehoiltaan riittävää toimiston käyttäjille, ehkä jopa turhankin tehokas. Se suoriutuu varmasti hyvin myös tulevaisuudessa, vaikka verkon käyttäjämäärät kasvaisivat suuresti. Verkko on toteutettu fyysiseltä rakenteeltaan järkevästi, joten antenneja saadaan tarvittaessa lisättyä helposti.

Verkon ylläpito on helppoa kontrollerin hallintasivujen kautta. Kaikkiin toimintoihin löytyvät graafiset valikot ja käytännössä kaikkia verkon ylläpidossa ja hallinnassa tarvittavia asioita pääsee muutamaan helposti.

Tunnistautuminen sisäverkkoon on hoidettu käyttäjien kannalta riittävän joustavasti, ottaen kuitenkin huomioon tietoturvan käyttämällä sertifikaattia verkkoon yhdistettäessä. Vierailijaverkkoon yhdistäminen on helppoa ja tunnusten luominen vierailijoille on sujuvaa ja selkeää.

5 YHTEENVETO TUTKITUISTA RATKAISUISTA

Kaikissa kolmessa tutkitussa yrityksessä on langaton verkko toteutettu hieman eri tavoilla. Yksikään ratkaisuista ei noussut muiden edelle, vaan jokainen ratkaisuista toimi kohdeympäristössään riittävän hyvin ja jokaisessa ratkaisussa oli omat heikkoutensa.

Yritys C oli ainoa, jossa ympäristössä oli jatkuvia ja selvittämättömiä ongelmia, joten kyseistä ratkaisua langattoman verkon toteutukseen ei voi suositella.

Kaikki yleisimmät laitevalmistajat valmistavat langattoman verkon rakentamiseen tarkoitettuja laitteita. Tutkittujen yritysten perusteella voisi suositella, että verkko rakennetaan mahdollisuuksien mukaan käyttäen saman valmistajan laitteita kuin verkossa jo olemassa olevat laitteet. Muiden valmistajien laitteita voi suositella vain, jos ne on tarkkaan testattu yhteensopiviksi ennen hankkimista.

Useissa nykyaikaisissa verkkolaitteissa on jo langattoman verkon tarvitsemia ominaisuuksia, kuten PoE-virransyöttö tai modulaarinen rakenne, johon voi lisätä esimerkiksi kontrollerin. Näitä verkossa mahdollisesti olemassa olevia laitteita ja ominaisuuksia kannattaa verkkoa suunnitellessa ehdottomasti hyödyntää.

Nykyaikainen yritysverkko tulisikin rakentaa oikein mitoitetulla kontrollerilla ja siihen liitetyillä radioporteilla. Radioportteja on hyvä varata riittävästi, jotta verkko kattaa tarpeeksi suuren alueen ja ettei verkon tiedonsiirtokapasiteetti kärsi useasta käyttäjästä samalla alueella. Nykyaikainen verkko vaatii helppoa ja varmaa hallittavuutta, mikä voidaan käytännössä saavuttaa vain erillisen kontrollerin avulla.

Kaikki tutkitut verkon perustuivat 802.11g-standardiin ja sen mukaisiin tiedonsiirtonopeuksiin. Kaikissa tutkituissa yrityksissä valittu nopeus katsottiin riittäväksi. Mikäli yrityksen langattoman verkkoliikenteen katsotaan jatkossakin koostuvan lähinnä sähköpostiliikenteestä, ei varmasti ole perusteltua vaihtaa olemassa olevia 802.11g-standardin laitteita nopeushyödyn takia 802.11n-standardin laitteisiin.

Kokonaan uutta verkkoinfrastruktuuria pystytettäessä voisi olla perusteltua hankkia 802.11n-standardin mukaisia laitteita ottaen kuitenkin huomioon, että suuremmat nopeudet vaativat tuen myös verkon päätelaitteilta, kuten kannettavilta työasemilta. Tulevaisuudessa n-standardin päätelaitteet kuitenkin tulevat yleistymään. Nopeushyöty tulee ajankohtaiseksi otettaessa verkossa käyttöön enemmän tiedonsiirtokaistaa vaativia sovelluksia, kuten IP-puheluita.

Yhteistä kaikille verkoille oli ajantasainen tietoturva WPA2-Enterprise tunnistautumisen ja AES-salauksen avulla. Kyseisiä menetelmiä voidaankin pitää vähimmäistasona yritystasolla verkkoja rakennettaessa. AES-salausta kehitetään jatkuvasti ja siitä onkin olemassa jo monimutkaisempia malleja. Tällä hetkellä 256-tavuinen salaus on riittävä, mutta tulevaisuudessa voidaan varmempia malleja tarvittaessa ottaa käyttöön.

Yritys A oli myös ottanut tunnistautumiseen mukaan ulkoisen tunnistusvälineen, tässä tapauksessa älykortin. Ulkoista tunnistusvälinettä käyttävä tunnistautumismenetelmä on tietoturvan kannalta kaikkein varmin, mutta lisää käyttäjälle lisävaiheita verkkoon kirjauduttaessa. Käytön helppous kärsii ulkoisesta välineestä kuitenkin huomattavasti, joten voidaankin miettiä, onko kyseinen lisäturva tarpeellinen. [1; 2; 4.]

6 TULEVAISUUS

Yrityskäytössä tulevat tulevaisuudessa korostumaan IP-puhelut ja videoneuvottelut. Nämä vaativat verkon tiedonsiirtokapasiteettia huomattavasti enemmän kuin nykyinen, pääsääntöisesti sähköpostiliikenteestä muodostuva liikenne. Nykyinen 802.11g-standardi ei sovellu kyseisten sovellusten tiedonsiirtoon kapasiteettinsa ja suurien viiveidensä takia.

802.11n-standardi yrittääkin mahdollistaa suuremman tiedonsiirtokapasiteetin, mutta se ei yksinään todennäköisesti riitä esimerkiksi videopuheluita varten, vaan niitä varten on edelleen käytettävä kiinteää verkkoa tiedonsiirtoon.

Langattomat verkot ovat jatkossakin vain kiinteän verkon jatke, koska verkon häiriöherkkyys ja rajattu tiedonsiirtokapasiteetti yksittäisten tukiasemien alueella estää verkon käytön raskaampaan tiedonsiirtoon. Häiriöitä ja viiveitä verkkoon tulee rakennusten rakenteiden ja muiden tiedonsiirtolaitteiden lisäksi muun muassa samalla taajuusalueella toimivista mikroaaltouuneista.

Asiaa hankaloittaa rajallinen taajuuskaista, varsinkin kun jo tällä hetkellä samalla alueella toimivat *Bluetooth-tekniikka,* erilaiset langattomat lähettimet esimerkiksi langattomille hiirille ja näppäimistöille sekä muut samalla alueella olevat langattoman WLAN-verkot.

Rajalliselle taajuusalueelle on jatkossa tulossa myös uusi tekniikka *Wi-Fi Direct*, jolla pyritään korvaamaan laitteiden välisiä yhteyksiä. Tekniikan avulla on mahdollista muodostaa esimerkiksi kannettavan tietokoneen ja tulostimen välille langaton verkko ilman ulkopuolista tukiasemaa. Wi-Fi Directin avulla yritetään ratkoa AD-HOC-verkkojen ongelmia. Erityisesti uusi tekniikka pyrkii olemaan kevyempi ja helpommin muodostettavissa kuin nykyiset AD-HOC-verkot.

Mikäli vastaavia laitteita ilmestyy yrityskäyttöön runsaasti, ne tukkivat jo valmiiksi ruuhkaista aluetta runsaasti. N-standardi onneksi mahdollistaa 5 MHz:n alueen käytön, mutta sekin täyttyy varmasti nopeasti, jos Wi-Fi Direct -laitteet yleistyvät ja siirtyvät käyttämään kyseistä taajuusaluetta.

VIITELUETTELO

[1] Puska, Matti (2005). *Langattomat lähiverkot*. Talentum Media Oy.

[2] McCullough, Jack (2004). *Caution! Wireless Networking: Preventing a Data Disaster*. Wiley Publishing Inc.

[3] IEEE: *Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, verkkodokumentti [viitattu 13.2.2010], saatavissa: http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

[4] Järvinen, Petteri (2003). *Salausmenetelmät*. Docendo Finland Oy.

[5] National Institute of Standards and Technology. *Announcing the ADVANCED ENCRYPTION STANDARD (AES),* verkkodokumentti [viitattu 13.2.2010], saatavissa: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[6] HP, *HP ProCurve Wireless Edge Services xl Module*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://www.procurve.com/products/pdfs/datasheets/ProCurve_Wireless_Edge_Services_xl_Module.pdf.

[7] HP, *ProCurve Series 5300xl Switches*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://ftp.hp.com/pub/networking/software/5300xl-Install-Aug2006-59914750.pdf.

[8] HP, *HP ProCurve Radio Port 230*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://www.procurve.com/products/pdfs/datasheets/ProCurve_Radio_Port_230.pdf.

[9] Cisco, *Cisco 2100 Series Wireless LAN Controller*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps7206/ps7221/prod_qas0900aecd805aaa9c_ps7206_Products_Q_and_A_Item.html.

[10] Cisco, *Cisco 2100 Series Wireless LAN Controllers*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps7206/ps7221/product_data_sheet0900aecd805aaab9.html.

[11] Cisco, *Cisco Aironet 1240AG Series 802.11A/B/G Access Point*, verkkodokumentti [viitattu 30.1.2010], saatavissa: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c844.pdf.

[12] Extreme Networks, *Summit WM20 Controller*, verkkodokumentti [viitattu 31.1.2010], saatavissa: http://www.extremenetworks.com/libraries/products/DSSumWM20_1393.pdf.

[13] Extreme Networks, *Altitude 350-2 Access Point*, verkkodokumentti [viitattu 31.1.2010], saatavissa: http://www.extremenetworks.com/libraries/products/DSSUMALT3502_1037.pdf.