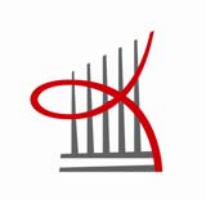


LANGATTOMAN TRAVELLER-VERKON KÄYTTÖÖNOTTO

Markus Saaristo

Opinnäytetyö
Marraskuu 2010
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut
Tampereen ammattikorkeakoulu

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

Markus Saaristo: Langattoman Traveller-verkon käyttöönotto
Opinnäytetyö 44 s.
Marraskuu 2010

Tämän opinnäytetyön tavoitteena oli tutkia langattomien verkkojen toimintaperiaatteita. Tämän lisäksi opinnäytetyön ohessa toteutettiin projekti, jossa Pilkington Automotive Finland Oy:n Ylöjärven toimipisteelle asennettiin langaton verkko.

Nykypäivänä langattomat verkot ovat jo osa arkipäiväistä tietotekniikkaa ja ne yleistyvät nopealla vauhdilla. Langaton verkko ilman sopivia tietoturvamenetelmiä on kuitenkin täysin turvaton, sillä periaatteessa kuka tahansa verkon kantoalueella pystyy siihen liittymään. Vaikka yleisesti yrityksissä tämä asia on huomioitu, varsinkin kotikäytössä törmää useasti langattomiin verkkoihin, joita ei ole suojattu millään tavalla.

Langatonta verkkoa suunniteltaessa tulisi miettiä miten tietoturva hoidetaan. Tässä työssä käydään läpi erilaisia keinoja suojautua langattoman verkon vaaroja vastaan. Tämän lisäksi työssä on lyhyesti kerrottu siitä, kuinka tilaajalle toteutettiin langaton verkko laajentamaan jo olemassa olevaa, kiinteää verkkoa.

Avainsanat WLAN, langaton, lähiverkko, traveller, access point, controller

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Network Services

Markus Saaristo: Wireless Traveller Network

Bachelor's thesis 44 pages
November 2010

The objective of this thesis was to study wireless Ethernet networks and also implement one. Today wireless networks are widely used in home and office networks. Office networks are usually secured in some way but many home networks are totally unsecured.

This thesis will take a look at the threats wireless technology is facing. It will also provide information on how to deal with these threats and make wireless network safe and secure for end-users.

This thesis was carried out as a project and the client for it was Pilkington Automotive Finland Oy, a company which business is based on glass industry. The goal was to establish both secure and reliable wireless network to extend the wired network in the office located at Ylöjärvi.

Keywords WLAN, wireless, local area network, access point, controller

SISÄLTÖ

1 JOHDANTO 8
1.1 Yleistä 8
1.2 Toimeksiantaja 9
1.3 Työn jakautuminen 9
1.4 Työn tavoitteet 10
2 LANGATTOMAT LÄHIVERKOT 11
2.1 Yleistä 11
2.2 Laitteet 11
2.3 Langattoman verkon arkkitehtuurit 12
2.3.1 Ad-Hoc 12
2.3.2 Infrastruktuuri 13
2.4 Wi-Fi-määritelmä 14
2.5 Tajuusalueet ja kanavat 14
2.5.1 2.4 GHz 14
2.5.2 5 GHz 15
2.6 Radiosignaalin kantavuus 16
2.7 Siirtotekniikat 17
2.7.1 Monikantoaaltomodulointi 17
2.7.2 Suorasekvenssihajaspekti 17
2.7.3 Taajuushyppelyhajaspektri 17
2.8 802.11 Standardeja 18
2.8.1 802.11 18
2.8.2 802.11a 18
2.8.3 802.11b 18
2.8.4 802.11g 18
2.8.5 802.11n 19
2.9 Muita 802.11 standardeja 19
2.10 Muita standardeja 20
2.10.1 HiperLAN/1 20
2.10.2 HiperLAN/2 20
3 LANGATTOMAN LÄHIVERKON TIETOTURVA 21
3.1 Tietoturvan tarve 21
3.2 Tietoturvauhat 22
3.3 Tietoturvan tavoitteet ja määrittely 23
4 SALAUSMENETELMÄT 24
4.1 WEP-protokolla 24
4.2 WPA-protokolla 24
4.3 WPA2-protokolla 25
5 AUTENTIKOINTI 26

5.1 Pre-Shared Key 26
5.2 802.1x 27
6 EXTENSIBLE AUTHENTICATION PROTOCOL 29
6.1 EAP-TLS 30
6.2 EAP-TTLS 30
6.3 EAP-PEAPv0/MSCHAPv2 31
7 CAPWAP 33
8 CASE 34
8.1 Valmistautuminen 34
8.2 Käyttöönotto 35
8.2.1 Tukiasemien sijoittelu 35
8.2.2 Reititys ja osoiteavaruus 35
8.2.3 Tukiasemien konfigurointi 37
8.2.4 Salaus ja autentikointi 37
8.3 Ongelmat 39
8.4 Parannusehdotukset 40
8.4.1 Tietoturva 40
8.4.2 Vierailijaverkko 41
9 YHTEENVETO 42
LÄHTEET 43

LYHENNELUETTELO

802.11	IEEE:n kehittämä standardi langattomille lähiverkoille
AD	Active Directory; käyttäjätietokanta ja hakemistopalvelu
AES	Advanced Encryption Standard; vahva salausmenetelmä, jota mm. WPA2 käyttää
AP	Access Point; langaton tukiasema
CAPWAP	Control And Provisioning of Wireless Access Points; IETF:n standardoima protokolla, jota käytetään langattomien tukiasemien keskitettyyn hallintaan
CCK	Complementary Code Keying; tiedonsiirrossa käytettävä koodaustekniikka
DES	Data Encryption Standard; tiedon salausmenetelmä
DHCP	Dynamic Host Configuration Protocol; tekniikka, jolla päätelaitteet saavat IP-asetukset automaattisesti
DSSS	Direct Sequence Spread Spectrum; suorasekvenssihajaspektri, langattomaan tiedonsiirtoon käytetty tekniikka
EAP	Extensible Authentication Protocol; käyttäjien tunnistukseen tarkoitettu protokolla
ETSI	European Telecommunications Standards Institute; eurooppalainen telealan standardisoimisjärjestö
FHSS	Frequency Hopping Spread Spectrum; tajuushyppelyhajaspektri, langattomaan tiedonsiirtoon käytetty tekniikka
IEEE	Institute of Electrical and Electronics Engineers; teknillinen järjestö, joka muun muassa määrittelee tietotekniikkaan liittyviä standardeja
IETF	Internet Engineering Task Force; internet-protokollien standardoinnista vastaava organisaatio
IP-osoite	Internet Protocol address, IP-address; koneen yksilöivä tieto, jonka perusteella tieto kulkee esim. internetissä
MIMO	Multiple-Input, Multiple-Output; tekniikka, jossa langattomaan tiedonsiirtoon käytetään useampaa antennia yhtä aikaa
OFDM	Orthogonal Frequency Division Multiplexing; langattomaan tiedonsiirtoon käytetty tekniikka

OSPF	Open Shortest Path First; reititysprotokolla
PSK	Pre-Shared Key; esijaettu avain
RADIUS	Remote Authentication Dial In User Service; käyttäjien tunnistukseen sekä käyttöoikeuksien myöntämiseen käytettävä palvelin
RC4	Rivest Cipher 4; salausalgoritmi, jota mm. WEP ja WPA käyttävät
SSID	Service Set Identifier; langattoman lähiverkon verkkotunnus
TKIP	Temporal Key Integrity Protocol; salausavaimien vaihtoon käytettävä protokolla
VLAN	Virtual Local Area Network; virtuaalinen lähiverkko
VPN	Virtual Private Network; näennäinen yksityinen verkko, tapa, jolla verkkoja voidaan yhdistää julkisen verkon yli yksityisesti ja salatusti
WEP	Wired Equivalent Privacy; datan suojaamiseen tarkoitettu protokolla
WLAN	Wireless Local Area Network; langaton lähiverkko
WPA	Wi-Fi Protected Access; datan suojaamiseen tarkoitettu protokolla, joka kehitettiin paikkaamaan WEP:n heikkouksia
WPA2	Wi-Fi Protected Access 2; datan suojaamiseen tarkoitettu protokolla, joka laajentaa alkuperäistä WPA-standardia

1 JOHDANTO

1.1 Yleistä

Vielä reilu kymmenen vuotta sitten eivät langattomat verkot olleet hyvin yleisiä. Niitä oli käytössä, mutta verrattuna nykypäivään niitä oli hyvin vähän. Nykypäivänä langaton verkko on kuitenkin osa arkipäivän tietotekniikkaa ja se on käytössä niin yritysmaailmassa kuin kotitalouksissakin. Myös esimerkiksi matkapuhelimet ovat kehittyneet vuosituhannen alun malleista ja nykyisin myös puhelimella, kuten monilla muillakin laitteilla, voi käyttää langatonta verkkoa hyödykseen.

Langattomuus tuo mukanaan myös uusia haasteita ja tietoturvauhkia. Tieto ei siirry enää johtoa pitkin vaan radioteitse joka suuntaan ja näin ollen tähän tietoon on helpompi päästä käsiksi kuin perinteisissä verkoissa. Kerrostaloissa naapuri voi urkkia mitä langattomassa verkossasi tapahtuu, sillä radioaallot liikkuvat myös naapurisi suuntaan. Tästä syystä langattomassa verkossa tapahtuva tiedonsiirto tulee salata. Nykypäivänä poikkeuksetta lähes kaikki kuluttajakäyttöön tarkoitetut langattomat tukiasemat tarjoavat tiedon salauksen melko yksinkertaisin toimenpitein.

Monesti kuulee myös puhuttavan siitä, kuinka vanhemmat salausmenetelmät eivät enää riitä suojaamaan tietoa, sillä ne on helppo murtaa. Tämä pitää osittain paikkansa. Yrityskäytössä, jossa verkossa saattaa liikkua myös salaista materiaalia, vanhentuneet salausmenetelmät eivät riitä. Mutta kotikäytössä monesti myös tällaiset toimenpiteet tiedon suojaamiseksi ovat usein täysin riittäviä. Pääsääntönä voidaan pitää, että huonokin suojaus on suojaus ja näin ollen parempi kuin ei mitään.

Koska langattomaan verkkoon pystyy liittymään mistä tahansa verkon kuuluvuusalueelta, esimerkiksi naapurin olohuoneesta, tulee verkko suojata myös salasanalla. Tällä toimenpiteellä estetään verkon luvaton käyttö, eli tehdään ns. käyttäjän autentikointi.

1.2 Toimeksiantaja

Työn toimeksiantajana toimi lasiteollisuudessa toimiva Pilkington Automotive Finland Oy. Pilkington on yksi maailman johtavia lasinvalmistajia ja sillä on pitkät perinteet lasiteollisuudessa, sillä yritys on perustettu jo vuonna 1826. Pilkington pysyi yksityisessä omistuksessa aina vuoteen 1970 asti, jolloin se listattiin ensimmäistä kertaa Lontoon pörssissä.

Lontoon pörssissä yhtiö pysyi aina vuoteen 2006 saakka, jolloin siitä tuli Japanilaisen NSG Groupin (listattu Tokion pörssissä) kokonaan omistama tytäryhtiö. Tämän jälkeen konsernin rakennus- ja autoteollisuuden tuotteita on markkinoitu Pilkingtonin brändin alla sen vahvan menestyksen ja hyvän tunnettavuuden vuoksi. Yhdistymisen myötä NSG Groupista tuli yksi maailman hallitsevia lasinvalmistajia. Yhtiön pääliiketoimintana on valmistaa rakennus- ja ajoneuvolaseja. Sillä on noin 32 000 työntekijää, valmistusta 29 eri maassa neljällä mantereella sekä myyntiä 130 maassa (This is Pilkington 2010).

Pilkingtonin www-sivuilta (Pilkington Suomessa 2010) selviää, että Suomessa Pilkington Automotive Finland Oy:llä työskentelee noin 1200 ihmistä. Ajoneuvolasia valmistavia tehtaita on Laitilassa, Ylöjärvellä ja Tampereella. Tämän lisäksi Automotive Finland Oy:n alle kuuluvat Nivalassa ja Forssassa erityislaseja rakennusteollisuudelle valmistavat tehtaat sekä toistaiseksi toiminnan keskeyttänyt Lahden Lasitehdas Oy. Näiden lisäksi Espoossa toimii varaosalasien tukkuliike ja Laitilan Automotive tehtaan vieressä toimiva, laivojen vaativia lasituksia toimittava Pilkington Marine. (Pilkington Suomessa 2010.)

1.3 Työn jakautuminen

Työ jakautui kahteen erilliseen osioon, käytännönosioon eli itse tehtävään sekä teoriaosioon eli tähän raporttiin. Vaikka eri osiot on pääsääntöisesti tehty eri aikaan, käytäntö ensin ja teoria sitten, raportin kirjoittaminen alkoi kuitenkin jo silloin, kun itse käytäntöä ei ollut kokonaisuudessaan suoritettu. Työn raportointi osiolle on varattu myös enemmän aikaa kuin mitä käytännönosuudelle.

1.4 Työn tavoitteet

Työn ensisijaisiin tavoitteisiin kuului se, että työn tilaaja on tyytyväinen lopputulokseen. Mikäli tilaaja olisi ollut tyytymätön, olisi asetettuja tavoitteita voitu pitää epäonnistuneina, vaikka muilla mittareilla mitattuina tavoitteet olisikin saavutettu. Tavoitteena oli löytää myös sellainen opinnäytetyön aihe, joka tuntuisi mielenkiintoiselta, eikä työ kävisi missään vaiheessa liian rasittavaksi tai pahimmassa tapauksessa kävisi niin, että mielenkiinto loppuisi kokonaan. Oman oppimisen kannalta asetettuihin tavoitteisin kuului omien tietojen ja taitojen kehittäminen sekä uusien asioiden oppiminen.

Kaikki yllämainitut tavoitteet täytettiin hyvin. Tilaaja oli työhön tyytyväinen eikä opinnäytetyönaihe alkanut missään vaiheessa tuntua liian raskaalta. Tämän lisäksi sain matkan varrella huomattavasti lisää tietoa langattomista verkoista sekä niiden toimintaperiaatteista.

2 LANGATTOMAT LÄHIVERKOT

2.1 Yleistä

Langattomien lähiverkkojen historia ulottuu 1980-luvun puolivälin paikkeille, jolloin Motorola kehitti ensimmäisen WLAN-tuotteen, Altairin. Kuten Altairissa ja myös muissa tuon ajan ja 1990-luvun alun WLAN-tuotteissa, ongelmana oli se, että valmistajat tekivät omia ratkaisujaan ja ajoivat omia innovaatioitaan. Näin ollen standardeja ei päässyt syntymään ja kuluttajat joutuivat sitoutumaan yhden valmistajan tuotteisiin.

Tätä varten IEEE (Institute of Electrical and Electronics Engineers) perusti vuonna 1990 ryhmän, jonka tarkoitus oli kehittää langattoman lähiverkon standardeja. Ryhmä julkaisi ensimmäisen 802.11-standardin vuonna 1997. Puskan (2005, 15) mukaan ensimmäisen standardin vaatimaton tiedonsiirto sekä yhteensopivuuden vajavuudet pakottivat ryhmää kuitenkin jatkamaan standardointityötään, jonka seurauksena nykypäivänä WLAN-standardeja on useita sekä valmistajien laitteet ovat monesti hyvin yhteensopivia.

Vaikka langattomat lähiverkot tarjoavat nykypäivänä teoriassa jopa 600 Mbit/s:n tiedonsiirtonopeuden, ei niistä kuitenkaan ole vielä yrityksen ainoaksi verkoksi. Langattomat lähiverkot soveltuvat parhaiten täydentämään yrityksen lähiverkkoa esimerkiksi neuvotteluhuoneissa tai muissa paikoissa, joihin ei kaapelia pystytä tai haluta vetää. Ne toimivat hyvin myös pienissä konttoreissa tai kotioloissa. Langattoman verkon tukiasemat (AP, Access Point) täytyy kuitenkin liittää toisiinsa tai muuhun verkko infrastruktuuriin yleiskaapeloinnilla, joten täydellisestä langattomasta verkosta ei voida puhua.

2.2 Laitteet

Langattomassa lähiverkossa käytettävät laitteet ovat hyvin samankaltaisia kuin perinteisessä Ethernet-verkossa käytetyt vastaavat laitteet. Pääasiallisesti langattoman verkon laitteet voidaan jakaa kolmeen ryhmään: sovittimiin, tukiasemiin sekä laiteohjaimiin.

Sovittimilla tarkoitetaan päätelaitteessa olevaa korttia tai piiriä, joka mahdollistaa liittymisen langattomaan verkkoon. Nykyisin lähes kaikissa kannettavissa tietokoneissa on

sisäänrakennettu WLAN-sovitin, jolla voidaan muodostaa yhteys langattomaan verkkoon.

Tukiasema mahdollistaa langattomien laitteiden liittymisen verkkoon ja on toimintaperiaatteiltaan hyvin samanlainen kuin Ethernet-verkon kytkin. Tukiasema voi toimia myös langattomana etäsiltana tai reitittimenä, mutta yleisesti tukiasema yhdistetään langallisesti kiinteään verkkoon. WLAN-verkko voidaan rakentaa myös ilman tukiasemaa Ad-Hoc-arkkitehtuurilla (katso 2.3.1).

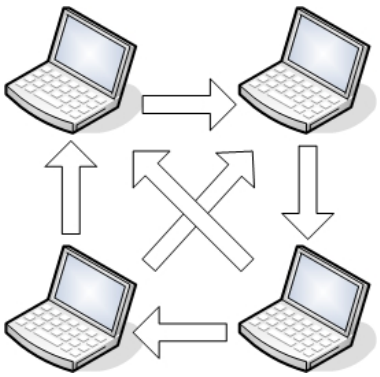
Laiteohjaimella (Controller) eli kontrollerilla voidaan hallita useampia tukiasemia kerralla sekä automatisoida erilaisia tehtäviä. Kontrollerin toimintaperiaatteista on lisää luvussa 7.

2.3 Langattoman verkon arkkitehtuurit

2.3.1 Ad-Hoc

Ad-Hoc-verkkomallissa (kuvio 1) ei tarvita ollenkaan tukiasemia, vaan verkon laitteet kommunikoivat suoraan toisilleen. Tästä johtuen verkon kantama jää lyhyeksi ja verkon toimintavarmuus pienenee, sillä kaikkien verkon laitteiden tulisi olla yhteydessä toisiinsa verkon täyden toimintakyvyn takaamiseksi.

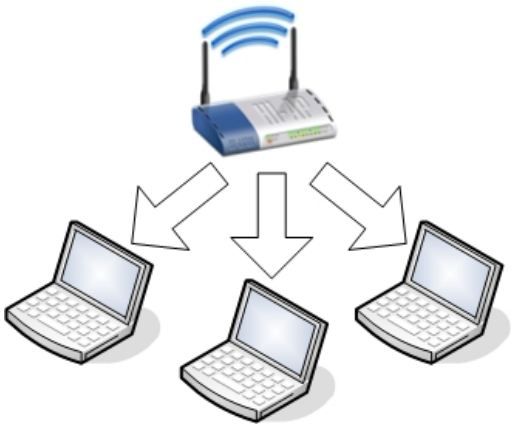
Ad-Hoc-verkkomallia ei suositellakaan pysyväisasennukseen, vaan sen suurimmat edut ovat sen nopeus ja yksinkertaisuus, kun tarvitaan väliaikaista, muutaman koneen yhdistävää langatonta verkkoa, esimerkiksi palaverin ajaksi.



Kuvio 1. Ad-Hoc-verkkomalli

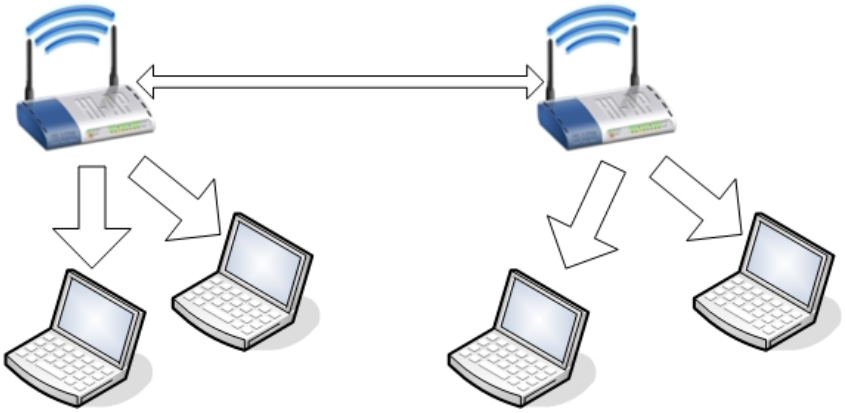
2.3.2 Infrastruktuuri

Infrastruktuurilla tarkoitetaan langattomia lähiverkkoja, jotka on liitetty vähintään yhdellä tukiasemalla langalliseen lähiverkkoon. Tukiaseman alueella voi olla useita päätelaitteita, jotka ovat tukiaseman kautta yhteydessä muuhun verkkoon. Jos tukiasemia on verkossa ainoastaan yksi, kutsutaan tällaista verkkoa BSS:ksi (Basic Service Set). Esimerkki BSS-verkosta on esitetty kuviossa 2.



Kuvio 2. Infrastruktuuriverkko (BSS)

Mikäli verkossa on useampia BSS:iä, jotka muodostavat yhteisen aliverkon, kutsutaan sitä Extended Service Setiksi (ESS). Useampia ESS:iä voidaan liittää toisiinsa esimerkiksi Ethernetin avulla (kuvio 3). ESS-järjestelmässä käytetään yleensä roaming-tekniikkaa, jolloin langattomalla verkkoyhteydellä varustettu pääte osaa ottaa automaattisesti yhteyden uuteen tukiasemaan, kun se poistuu aikaisemman tukiasemansa vaikutusalueelta (Syrjälä 2001).



Kuvio 3. Infrastruktuuriverkko (ESS)

2.4 Wi-Fi-määritelmä

Wi-Fi on yleisesti käytetty nimi langattomille verkkotuotteille. Termin on yleisesti luultu olevan lyhennys sanoista ”Wireless Fidelity”, mutta näin ei kuitenkaan ole. Wi-Fi on ainoastaan termi, jolla tarkoitetaan 802.11-standardin kanssa yhteensopivia laitteita. Wi-Fi Alliance omistaa oikeudet Wi-Fi-tuotemerkkiin ja on tarkemmin määritellyt, että ”Wi-Fi on mikä tahansa langaton (WLAN) tuote, joka pohjautuu IEEE:n 802.11-standardeihin”.

Wi-Fi:ä tukevat monet erilaiset laitteet, kuten kännykät, pelikonsolit, tietokoneet, kämmenmikrot. Laitteiden, jotka on Wi-Fi-sertifioitu (Wi-Fi Certified) Wi-Fi Alliancen toimesta, on luvattu toimivan myös yhdessä. Esimerkiksi Wi-Fi-sertifioidulla kannettavalla voidaan ottaa yhteyttä Wi-Fi-sertifioituun tukiasemaan huolimatta siitä, minkä valmistajan kannettava tai tukiasema on kyseessä.

2.5 Tajuusalueet ja kanavat

Tietoliikenteessä, kuten myös esimerkiksi mikroissa ja tutkissa, käytetään mikroaaltoja. Mikroaaltoalueella on kaksi vapaasti käytettävää radiotaajuusaluetta: 2.4 GHz sekä 5 GHz. Näitä radiotaajuusalueita käytetään myös langattomissa lähiverkkoyhteyksissä. Suurin ero 2.4 ja 5 GHz:n radiotaajuuksilla on niiden taajuuksien leveyksissä. Siinä missä 2.4 GHz:n radiotaajuus on verrattain kapea, on 5 GHz taajuus huomattavasti leveämpi.

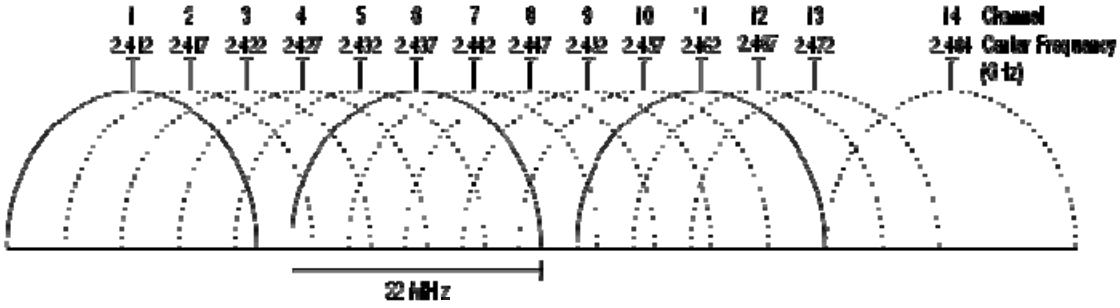
2.5.1 2.4 GHz

2.4 GHz:n radiotaajuudella toimivat langattomat lähiverkot, kuten 802.11b ja 802.11g, toimivat samalla taajuudella kuin moni muukin elektroninen laite. Tällaisia laitteita ovat mm. langaton puhelin, autotallin ovenavaaja, mikroaaltouuni sekä itkuhälytin. Nämä laitteet voivat häiritä langattoman lähiverkon toimintaa ja hidastaa sitä, pahimmassa tapauksessa katkaista yhteyden. Tämän lisäksi myös muut lähellä sijaitsevat langattomat lähiverkot voivat käyttää samaa radiotaajuutta. Mikäli verkoilla on kantamaa niin, että

ne osuvat toistensa peittoalueille, kuten monesti esimerkiksi kerrostaloissa tapahtuu, voivat verkot häiritä keskenään toisiaan.

2.4 GHz:n Wi-Fi radiotaajuus on tästä syystä jaettu useampaan pienempään taajuuteen tai ”kanavaan”. Suomessa ja suurimmassa osassa Eurooppaa näitä kanavia on käytössä 13 kun taas USA:ssa kanavia on käytössä 11 (Geier 2002). Japanissa käytössä on ainoastaan yksi kanava, kanava 14.

Huomioitavaa on, että kanava kertoo taajuuden keskivaiheen jota käytetään (esim. kanavan yksi keskitaajuus on 2.412 GHz ja kanavan kaksi keskitaajuus on 2.417 GHz). Eri kanavien väliin jää vain 5 MHz levyinen taajuus. Koska esim. 802.11g käyttää suunnilleen 22 MHz levyistä taajuutta, sen signaali ulottuu n. 11 MHz kanavan keskivaiheen molemmille puolille. Tästä johtuen 2.4 GHz:n Wi-Fi – signaali johtaa päällekkäisyyksiin muiden kanavien kanssa. Näin ollen käyttöön jää ainoastaan kolme kanavaa, kanavat 1, 6 ja 11, jotka eivät mene päällekkäin muiden kanavien kanssa (Geier 2002). Kuviossa 4 on esitetty 2.4 GHz:n keskitaajuudet ja kuinka käytössä oleva signaali ulottuu keskitaajuuden molemmille puolille.



Kuvio 4. 2.4 GHz:n Wi-Fi kanavat (Wikipedia 2010a)

2.5.2 5 GHz

Viestintäviraston tiedotteesta selviää, että langattomille lähiverkoille on varattu 5 GHz:n alueelta seuraavat taajuudet: 5150 – 5350 MHz ja 5470 – 5725 MHz (Langattomat lähiverkot (RLAN) 5 GHz:n taajuusalueella 2002). Kuten 2.4 GHz:n taajuudet, eivät nämäkään taajuudet ole varattu pelkästään langattomille lähiverkoille. 5 GHz:n taajuudella on kuitenkin vähemmän muita haittatekijöitä kuin 2.4 GHz:n taajuudella. Tämän lisäksi 5

GHz:n taajuus on paljon leveämpi, eli sillä on useampia kanavia, kuin 2.4 GHz:n taajuudella.

Tästä johtuen 5 GHz:n radiotaajuuden käyttö saattaa olla hyödyllistä varsinkin silloin, kun pienelle alueelle joudutaan sijoittamaan monta tukiasemaa tai mikäli tukiasemien sijoittamisalueella on paljon muita häiriötekijöitä. 5 GHz:n taajuusalueelta voidaan valita useita toisistaan kauempana olevia kanavia, jolloin tukiasemien signaalit eivät mene päällekkäin toistensa kanssa. Tällöin tulee ainoastaan huomioida standardien asettamat rajat. Mikäli halutaan käyttää 5 GHz:n taajuusaluetta, tulee 802.11-standardiksi valita joko 802.11a tai 802.11n.

2.6 Radiosignaalin kantavuus

Radiosignaalien etenemistä on vaikea ennakoida tai mallintaa. Koska verkon suorituskykyyn ja kantavuuteen vaikuttavat monet asiat, on langattoman verkon suunnittelussa ja testauksessa otettava huomioon tiettyjä asioita. Näitä ovat mm. tukiasemien ja päätelaitteiden sijoittelu. Hakalan ja Vainion (2005, 153) mukaan mikroaallot eivät läpäise hyvin kiinteitä esteitä, kuten seiniä, ovia ja ne heijastuvat helposti takaisin erilaisista pinnoista. Tästä johtuen tukiasemat tulisi sijoittaa siten, että niillä on suora, esteetön yhteys päätelaitteisiin.

Langaton verkko saattaa toisinaan ulottua pidemmälle kuin on tarkoitettu, esimerkiksi rakennuksen ulkopuolelle. Tällöin verkon luvaton kuuntelu ja käyttö on helpompi toteuttaa. Näitä tietoturvauhkia voidaan välttää käyttämällä aikaa tukiasemien sijoitteluun ja kuuluvuusmittausten tekemiseen.

Myös 5:n ja 2.4 GHz:n taajuuksilla on itsessään eroja signaalin kantavuuden ja kuuluvuuden suhteen. 5 GHz:n radiotaajuudella signaalin katoaminen (attenuation) on suurempaa kuin 2.4 GHz:n taajuudella ja signaalin kulkeminen esteiden läpi on heikompaa (IEEE 802.11 Standards, facts & channels 2005).

2.7 Siirtotekniikat

2.7.1 Monikantoaaltomodulointi

Orthogonal Frequency Division Multiplexing, OFDM, on tekniikka, jossa data lähetetään samanaikaisesti useampaa eritaajuista kantoaaltoa käyttämällä. Hakalan ja Vainion mukaan (2005, 155) esimerkiksi 802.11a ja 802.11g käyttävät tätä tekniikkaa tiedonsiirron ylittäessä 20 Mbit/s.

2.7.2 Suorasekvenssihajaspekti

Direct Sequence Spread Spectrum, DSSS, lähettää varsinaisen datan lisäksi koodausbittejä (chipping code), joiden avulla signaalia voidaan lähettää useammalla vaihtuvalla taajuudella. Vastaanottava laite rakentaa datan uudelleen yhdistämällä eri taajuuksilta luetut signaalit käyttäen samaa koodausbittiä. Koodausbittien avulla voidaan myös rakentaa osa siirron aikana turmeltuneista biteistä uudestaan. Koodausbittien käyttö lisää datan määrää hieman, mutta DSSS on FHSS-tekniikkaa huomattavasti tehokkaampi.

Koodausbittien lisäksi käytetään CCK-koodausta (Complementary Code Keying), joka mahdollistaa suuremman tietomäärän lähettämisen yhtenä signaalina. Hakala ja Vainio toteavat (2005, 155), että mm. 802.11b sekä 802.11g käyttävät tätä modulointia kun tiedonsiirtonopeus on alle 20 Mbit/s.

2.7.3 Taajuushyppelyhajaspektri

Frequency Hopping Spread Spectrum, FHSS, perustuu siihen, että signaalia siirretään useilla ajan mukaan vaihtuvilla taajuuksilla. Tekniikalla ei ole enää merkitystä nykyisissä langattomissa verkoissa. Vaikka FHSS on DSSS-tekniikkaa hitaampi, on se myös samalla DSSS:ää vastustuskykyisempi häiriöille.

2.8 802.11 Standardeja

2.8.1 802.11

Vuonna 1997 IEEE (Institute of Electrical and Electronics Engineers) kehitti ensimmäisen 802.11 standardin. Ensimmäinen standardi esittää, että 2.4GHz:n radiotaajuudella käytetään joko DSSS-, FHSS- tai infrapunatekniikkaa datan siirtämiseen (Bing 2002, 2). Näistä infrapunaa ei ole otettu kaupalliseen käyttöön. 802.11 standardi tukee nopeuksia vain 2 Mbit/s saakka ja tämä ei ole tarpeeksi nopeaa nykypäivän ohjelmille, joten standardia on laajennettu useampaan otteeseen.

2.8.2 802.11a

802.11a valmistui vuonna 1999. Se eroaa alkuperäisestä 802.11 standardista käyttämällä 5 GHz:n radiotaajuutta, jolla se saavuttaa jopa 54 Mbit/s siirtonopeuden. 802.11a käyttää OFDM modulointia ja jos signaali heikkenee esim. pidentyneen matkan tai esteiden takia, siirtonopeus laskee automaattisesti pienemmäksi, jotta yhteys ei katkea.

2.8.3 802.11b

802.11b laajennus valmistui myös vuonna 1999. Se käyttää samaa 2.4 GHz:n radiotaajuutta kuin alkuperäinen 802.11, mutta tarjoaa suuremman tiedonsiirtonopeuden aina 11 Mbit/s asti käyttäen DSSS modulointia. Kuten myös 802.11a, 802.11b voi automaattisesti laskea tiedonsiirtonopeutta, mikäli signaali heikkenee. Signaalin parantuessa nousee nopeus automaattisesti parhaaseen mahdolliseen. (Bing 2002, 3.) 802.11b:llä on yhteensä neljä eri tiedonsiirtonopeutta: 11, 5.5, 2 ja 1 Mbit/s.

2.8.4 802.11g

Vuonna 2003 esitelty 802.11g on kolmas laajennus 802.11 standardiin. Se yhdistää a- ja b-standardien hyvät puolet yhdeksi standardiksi tarjoamalla maksimissaan 54 Mbit/s

tiedonsiirtonopeuden 2.4 GHz radiotaajuudella. 802.11g on myös taaksepäin yhteensopiva 802.11b:n kanssa, mutta mikäli näitä käytetään yhdessä, tiedonsiirtonopeus rajoittuu 802.11b:n asettamaan 11 Mbit/s. 802.11g käyttää sekä DSSS että OFDM moduloin-tia.

2.8.5 802.11n

Viimeisin 802.11 standardin laajennus on 802.11n. Se on suunniteltu kasvattamaan tiedonsiirtonopeutta a- ja b-standardien 54 Mbit/s:stä jopa 600 Mbit/s. Käytännössä nopeudet jäävät 100 Mbit/s ja 200 Mbit/s väliin ja näin ollen se vastaa pitkälti perinteistä 100 Mbit/s Ethernetiä.

802.11n standardin nopeuden takana on uusi MIMO-tekniikka (multiple-input, multiple-output), joka käyttää useampaa antennia yhtä aikaa. Tämä antaa tasaisemman kantaman ja mahdollistaa useat samanaikaiset ilmakanavat ja näin ollen nopeamman tiedonsiirron. 802.11n toimii sekä 2.4 GHz:n että 5 GHz radiotaajuuksilla ja on näin ollen yhteen sopiva niin a-, b- kuin g-standardien kanssa. (IEE 802.11 Standards, facts & channels 2005.) Taulukossa 1 on vertailtu eri 802.11 standardeja keskenään.

Taulukko 1. IEEE-standardien vertailua (Wikipedia 2010b)

IEEE standardi	Max nopeus	Todellinen nopeus	Käytetty taajuusalue	Siirtotekniikka	Kantama ulkona (noin)	Kantama sisällä (noin)
802.11	2 Mbps	2 Mbps	2,4 Ghz	DSSS / FHSS	100 m	20 m
802.11a	54 Mbps	~30 Mbps	5,0 Ghz	OFDM	120 m	35 m
802.11b	11 Mbps	~6 Mbps	2,4 Ghz	DSSS	140 m	38 m
802.11g	54 Mbps	~22 Mbps	2,4 Ghz	OFDM / DSSS	140 m	38 m
802.11n	~600 Mbps	~100-200 Mbps	2,4 Ghz 5,0 Ghz	OFDM	250 m	70 m

2.9 Muita 802.11 standardeja

Ylläkuvattujen standardien lisäksi IEEE on julkaissut myös muita 802.11 laajennuksia. Seuraavassa tärkeimpiä.

802.11e: sisältää palvelunlaatuun (Quality of Service, QoS) liittyviä parannuksia. Tätä standardia pidetään erittäin tärkeänä viive-herkille protokollille, kuten esimerkiksi VoIP:lle (Voice over IP).

802.11i: sisältää langattoman verkon turvallisuuteen liittyviä parannuksia. 802.11i tunnetaan paremmin nimellä WPA2, joka korvasi WEP-salauksen ja paransi alkuperäistä WPA:ta.

802.11h: määrittelee lisämäärityksiä 5 GHz:n taajuuden käytölle Euroopassa.

2.10 Muita standardeja

802.11-standardin lisäksi markkinoilla on myös toinen standardi, ETSI:n (European Telecommunications Standards Institute) HiperLAN, joka on eurooppalainen vastine 802.11-standardille. Käytännössä 802.11-standardilla on kuitenkin monopoliasema WLAN-tuotteissa myös Euroopassa. Käytössä on ollut myös HomeRF-standardi, jota ei nykyään kuitenkaan enää kehitetä tai käytetä.

2.10.1 HiperLAN/1

Ensimmäisen HiperLAN (High Performance Radio LAN) version suunnittelu aloitettiin vuonna 1991, kun ensimmäisen 802.11 version suunnittelu oli jo käynnissä. HiperLA-Nin tavoite oli korkeampi tiedonsiirtokapasiteetti kuin 802.11:ssa ja se mahdollistaakin 23,5 Mbit/s tiedonsiirtonopeuden. Standardiksi HiperLAN hyväksyttiin vuonna 1996.

2.10.2 HiperLAN/2

Kasvavan tiedonsiirron tarpeisiin ETSI standardoi HiperLANin toisen version vuonna 2000. HiperLAN/2:n fyysinen kerros on hyvin samanlainen kuin 802.11:ssa ja perustuu OFDM-tekniikkaan. HiperLAN/2 käyttää 5 GHz:n taajuutta ja pystyy 54 Mbit/s tiedonsiirtonopeuteen eli samaan kuin tällä hetkellä laajimmin käytössä oleva 802.11g. HiperLAN/2:ssa on keskitytty myös tietoturvan parantamiseen. Se käyttää tietojen salaamiseen DES- ja 3DES-algoritmeja.

3 LANGATTOMAN LÄHIVERKON TIETOTURVA

3.1 Tietoturvan tarve

Langaton lähiverkko on usein hyvin helppo saada toimimaan perusasetuksilla. Monesti, varsinkin kotikäyttöön suunnatuissa tukiasemissa, käyttäjältä ei vaadita muita toimenpiteitä kuin verkkopiuhan sekä sähköjohdon kytkeminen. Tämän jälkeen verkko on ”valmis” käytettäväksi. Tällaisen asennuksen jälkeen verkko sekä tukiasema ovat kuitenkin täysin turvattomia ja sisältävät ainakin seuraavia uhkia.

- Mikä tahansa WLAN-yhteyksiä hyödyntävä laite pystyy liittymään verkkoon ja mikäli tukiasema vielä levittää SSID-tunnusta, kuten hyvin usein oletuksena on tapana, ei verkossa ole mitään salaista.

- Vaikka SSID-tunnus olisikin piilotettu, on se silti melko helppo saada selville salakuuntelemalla verkkoa ja tätä kautta liittyä verkkoon.

- Kaikki liikenne työaseman ja tukiaseman välillä tapahtuu täysin salaamatta. Luvaton käyttäjä voisi helposti salakuunnella liikennettä ja kerätä kaikkea sellaista käyttäjän tietoa, kuten salasanoja tai käyttäjätunnuksia, jota ei erikseen salata sovelluskerroksella.

- Tukiaseman hallintatunnuksia ei ole vaihdettu ja ne on erittäin helppo jopa arvata. Oletustunnukset löytyvät myös valmistajien www-sivuilta.

- Vaikka hallintatunnukset vaihdettaisiinkin, ei http- tai telnet-liikennettä ole salattu ja käyttäjätunnukset sekä salasanat siirretään verkon yli selväkielisenä. Mikäli verkkoa ei ole suojattu, voidaan uudet hallintatunnukset saada selville kuuntelemalla verkkoliikennettä.

3.2 Tietoturvauhat

Langattomassa verkossa esiintyy hyvin samanlaisia uhkia kuin perinteisessä langallisessakin verkossa. Vaikka langattomassa verkossa on myös hyviä puolia tietoturvan kannalta, kuten esimerkiksi käyttäjien autentikointi, tuo langattomuus mukanaan myös uusia uhkia.

- Liikenteen salakuuntelu, joka on mahdollista myös rakennuksen ulkopuolelta.

- Tukiaseman häirintä, jossa tukiasemaa kuormitetaan turhilla pyynnöillä. Tukiaseman häirintä on toimintaperiaatteiltaan hyvin samanlainen kuin DoS-hyökkäys (Denial of Service).

- Verkossa liikkuvan datan muokkaus ns. Man in the middle-menetelmällä, jossa hyökkääjä asettuu lähettävän ja vastaanottavan laitteen väliin. Lähetetty tieto ei päädy suoraan vastaanottajalle, vaan välissä oleva taho saa tiedon ensiksi. Tässä vaiheessa keskellä oleva taho voi muuttaa tai lukea tietoa, ennen kuin välittää tiedon oikealle vastaanottajalle.

- Tukiasema voidaan korvata toisella, luvattomalla tukiasemalla eli ns. Roque Access Pointilla. Tämä laite voidaan määritellä ohjaamaan käyttäjien ensimmäinen sisäänkirjautuminen uuteen kohteeseen, joka kerää käyttäjätunnukset ja salasanat. Tämän jälkeen palautetaan virheilmoitus väärästä salasanasta, ja seuraava yhteys ohjataan oikeaan osoitteeseen. (Puska 2005, 68.)

- Yleensä päämääränä on tietojärjestelmään tunkeutuminen. Tätä päämäärää varten käytetään muita keinoja. Langattoman verkon salakuuntelulla voidaan selvittää salasanoja ja käyttäjätunnuksia ja koska langaton verkko on osa yrityksen tietoverkkoa, on hyökkääjällä mahdollisuus päästä tätä kautta käsiksi myös yrityksen muihin tietojärjestelmiin.

3.3 Tietoturvan tavoitteet ja määrittely

Tietoturvan tavoite ja varsinkin sen määrittely on laaja ja monimutkainen prosessi. Lyhyesti voidaan kuitenkin todeta, että tietoturvan tavoite verkoista puhuttaessa on suojata verkkoa luvattomalta käytöltä ja käyttäjiltä.

Varsinkin langattomassa verkossa, jossa tiedonsiirtoon käytetään radioaaltoja, on liikenteen kaappaaminen ja kuuntelu sekä verkkoon liittyminen huomattavasti helpompaa kuin langallisessa verkossa (Hakala & Vainio 2005, 167). Tästä syystä johtuen tulisi langattoman verkon käyttäjät autentikoida sekä käyttäjien lähettämä ja vastaanottama data salata. Langattomiin verkkoihin on suunniteltu useita erilaisia ratkaisuja parantamaan käyttäjän ja verkon tietoturvaa. Verkon tietoturvaa määrittäessä tulisi ainakin seuraavat asiat ottaa huomioon.

- Verkon käyttötarkoitus, eli onko kyseessä avoin vai suljettu verkko.

- Miten käyttäjien tunnistus verkossa tapahtuu? Onko jokaisella käyttäjällä henkilökohtaiset tunnukset vai käytetäänkö valmiiksi jaettua avainta (Pre-Shared Key, PSK).

- Datan salaukseen liittyvät ongelmat ja kuinka vahvasti WLAN-verkossa liikkuva data tulee suojata.

Kun verkon tarpeet on pystytty määrittelemään, tulee seuraavaksi pystyä määrittelemään tavat, joilla halutut tarpeet saavutetaan. Hankalan tästä asiasta saattaa tehdä se, että eri tarpeiden saavuttamiseksi on useita eri ratkaisuja. Esimerkiksi datan salaukseen on useita eri mahdollisuuksia aina yksinkertaisimmasta WEP-salauksesta aina yritystason VPN-tunneleihin asti. Myös käyttäjien tunnistamiseen löytyy eri vaihtoehtoja valmiiksi jaetuista salasanoista käyttäjät paremmin identifioivaan 802.1x ja Radius-autentikointiin.

4 SALAUSMENETELMÄT

4.1 WEP-protokolla

WEP-protokolla (Wired Equivalent Privacy) on langattoman verkon perusmekanismi, jolla pyritään turvaamaan liikenteen luottamuksellisuus (Hakala & Vainio 2005, 168). Se perustuu kiinteisiin, sekä verkkokortille että tukiasemalle kerrottuihin salausavaimiin, joiden maksimipituus on 128 bittiä. WEP-protokolla käyttää samaa avainta sekä autentikointiin että liikenteensalaukseen, eikä se sisällä mekanismiä salausavainten automaattiseen vaihtoon, vaan liikenteen salaamiseen käytetään jatkuvasti samaa avainta.

Tästä johtuen salausavain pystytään suht helposti murtamaan, kuten Samuli Kotilainen on Tietokonelehden artikkelissa jo vuonna 2003 kertonut.

> Wepissä käytettävässä 64-tai 128-bittisessä rc4-salauksessa ei itsessään ole mitään vikaa. Salausalgoritmin yhteydessä käytetään kuitenkin niin sanottua alustusvektoria, joka standardin mukaan toteutettuna on liian heikko. Tietynlaiset alustusvektorit antavat vihjeitä verkon salausavaimesta, joten liikennettä riittävän kauan kuunneltuaan voi avaimen selvittää yksinkertaisesti laskemalla. (Kotilainen 2003.)

WEP toimii pääsääasiassa liikenteen salauksessa ja mikäli käyttäjät halutaan luotettavasti myös tunnistaa, ei siihen riitä enää WEP:n tarjoama useille käyttäjille tarkoitettu yhteinen avain.

4.2 WPA-protokolla

WEP-protokollassa esiintyvien puutteiden vuoksi Wi-Fi Alliance kehitti WPA-protokollan (Wi-Fi Protected Access). WPA:ta voi käyttää kahdessa eri muodossa: WPA-Personal (useasti WPA-PSK) tai WPA-Enterprise (WPA). Näiden suurimmat erot ovat käyttäjien autentikoinnissa. WPA-Personalia käytettäessä autentikointi suoritetaan ennalta määritellyllä avaimella. Enterprise taas tarjoaa käyttäjien autentikoinnin 802.1x-standardin avulla.

WPA käyttää salaukseen samaa RC4-algoritmiä kuin WEP:kin, mutta WPA-protokolla eroaa WEP:stä sen käyttämän avaintenjaon johdosta. Siinä missä WEP käyttää kiinteää salausavainta, WPA:n avaintenjako perustuu TKIP:iin (Temporal Key Integrity Protocol). Autentikointi tapahtuu joko WPA-Personal tai WPA-Enterprise tavalla, jonka jälkeen Hakalan ja Vainion mukaan (2005, 168) TKIP generoi uuden salausavaimen dynaamisesti aina 10 000 paketin välein. Tämän pitäisi estää se, että hyökkääjä ei pysty keräämään tarpeaksi paketteja laskeakseen salausavaimen. WPA:lla on mahdollista käyttää myös vahvempaa AES-salausta, mutta AES-tuki on valinnainen ja riippuu laitevalmistajien ohjaintuesta.

Muuttuvan salausavaimen lisäksi TKIP sisältää *Message Integrity Code* (MIC) toiminnon, joka varmentaa siirretyn paketin oikeellisuuden. MIC:n käyttö varmistaa, että paketti ei ole muuttunut matkalla, eikä lähde- tai kohdeosoitetta ole muutettu. (Bing 2002, 127.) Vaikka TKIP onkin suuri parannus WEP:n käyttämään salaukseen, on WPA:n keskeisimmät ongelmat kuitenkin TKIP:n käyttämässä RC4-salauksessa, joka on sama salaus jota myös WEP käyttää.

Parannetun salauksen lisäksi WPA-Enterprise hyödyntää myös EAP-protokollaa (Extensible Authentication Protocol), jonka avulla käyttäjät pystytään luotettavasti tunnistamaan. EAP-protokollista lisää luvussa 6.

4.3 WPA2-protokolla

WPA2 (Wi-Fi Protected Access 2) on kansantajuinen nimi IEEE:n 802.11i-standardille, joka luotiin laajentamaan vanhaa WPA:ta. WPA2:n ja WPA:n suurin ero on niiden käyttämät salausalgoritmit. Siinä missä WPA käyttää salaukseen TKIP/RC4:ää, käyttää WPA2 salaukseen järeämpää AES:ia (Advanced Encryption Standard). AES itsessään sisältää salausavaimen dynaamiseen vaihtoon tarvittavat toiminnot.

Kuten WPA:ta, myös WPA2:sta voidaan käyttää kahdessa eri muodossa: WPA2-Personal sekä WPA2-Enterprise. WPA 2 on taaksepäin yhteensopiva WPA:n kanssa (Wi-Fi Alliance 2010).

5 AUTENTIKOINTI

Jokaisen langattomaan verkkoon liittyvän laitteen on ensiksi autentikoitava, eli tunnistettava itsensä verkon tukiasemalle. Verkkoon voidaan tehdä myös ns. avoin autentikointi, jossa tunnistautuminen tapahtuu palvelutunnisteen (Service Set Identification, SSID) avulla. Tässä tapauksessa SSID:n tulee olla sama sekä päätelaitteella että tukiasemalla, eikä erillisiä määrityksiä tarvita.

Tällainen ”autentikointi” ei kuitenkaan tarjoa tietoturvaa, sillä tukiasemat yleislähettävät SSID:tä selväkielisinä tasaisin väliajoin mainostaakseen verkkoaan. Vaikka SSID:n lähetys ei tukiasemassa olisi päällä, on se silti helppo salakuunnella liittyvien laitteiden liittymisviesteistä.

Seuraavassa on esitelty yleisimmin käytettyjä autentikointi menetelmiä, joilla verkon tietoturvaa voidaan parantaa.

5.1 Pre-Shared Key

Ensimmäinen ja samalla rajoittunein vaihtoehto käyttäjien autentikoinnissa on esijaettu avain (Pre-Shared Key, PSK). PSK:n toiminta perustuu siihen, että päätelaitteelle sekä tukiasemalle on molemmille kerrottu etukäteen sama avain. Tunnusta ei siirretä selväkielisenä ilmateitse, vaan käytetään ns. haaste-metodia (Niemi 2003).

Tässä metodissa tukiasema pyytää päätelaitetta salaamaan lähettävän viestin päätelaitteen omalla avaimella. Mikäli tukiasema pystyy tämän jälkeen purkamaan viestin omalla avaimellaan, voidaan todeta, että avaimet ovat samat ja yhteys muodostetaan. Muussa tapauksessa yhteys puretaan.

Tällä metodilla käyttäjät voidaan henkilökohtaisesti tunnistaa ainostaan siten, että jokaista käyttäjää kohden tukiasemalle syötetään oma avain. Tämä ei kuitenkaan ole suuremmissa verkoissa järkevää, eikä monesti edes mahdollista johtuen tukiasemien tukemien avainten määrästä. PSK käytetään yleisesti kuitenkin kotiverkoissa sekä pienempi-

en yritysten verkoissa, joissa kalliimman ja hankalamman 802.1x-autentikoinnin käyttö ei ole järkevää.

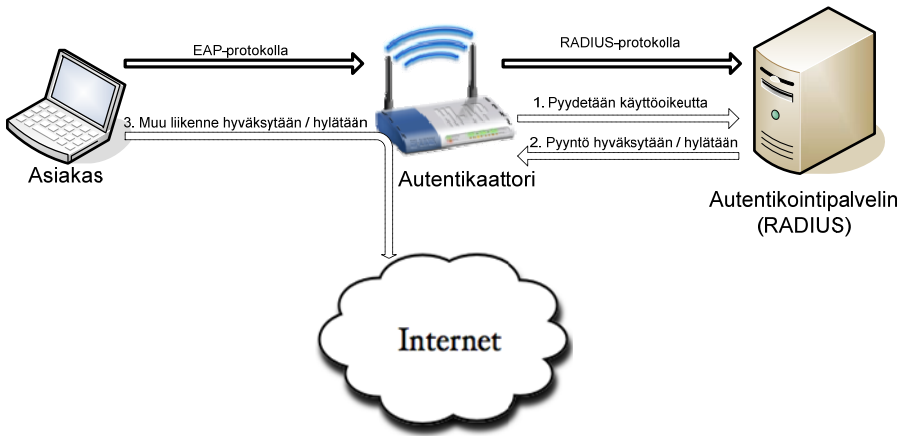
5.2 802.1x

802.1x Port Based Authentication, eli porttiperustainen autentikointi, estää luvattoman asiakaslaitteen kommunikoinnin verkon liityntäpisteen kautta ja määrittelee asiakkaan verkon käyttöä porttien ja todennuspalvelimen avulla. 802.1x on suunniteltu käytettäväksi kaikissa IEEE 802-verkoissa, eli mm. Ethernet ja WLAN-verkoissa. Ethernet-verkoissa verkon liityntäpiste on aktiivilaitteen, esimerkiksi kytkimen, portti ja WLAN-verkossa liityntäpiste on tukiaseman looginen portti.

Menettelyssä on kolme osapuolta: asiakaskone (Suplicant), autentikaattori (Authenticator) sekä käyttäjän todentava palvelin (Authentication Server). Kun asiakaskone yrittää ottaa yhteyttä verkkoon, autentikaattori avaa laitteelle portin jossa sallitaan ainoastaan autentikointiliikenne. Kaikki muu liikenne, kuten HTTP tai DHCP, estetään siihen asti, kunnes autentikointipalvelin varmistaa päätelaitteen identiteetin.

Käyttäjien tunnistamiseen liittyvät sanomat siirretään asiakkaan ja autentikaattorin välillä käyttäen EAP-protokollaa, josta lisää seuraavassa luvussa. Autentikaattorin kapsuloi EAP-viestin Radius formaattiin ja lähettää sen autentikointipalvelimelle (802.1X Port-Based Authentication HOWTO 2004). Autentikointiprosessin aikana autentikaattori ainoastaan välittää viestejä asiakkaan ja autentikointipalvelimen välillä. Kun autentikointi on suoritettu, sallitaan myös muun tyyppinen liikenne autentikointipalvelimen ilmoittamien oikeuksien mukaisesti. 802.1x-autentikoinnin toimintaperiaatteita on kuvattu kuviossa 5.

Autentikointipalvelimina käytetään yleensä RADIUS-palvelimia (Remote Authentication Dial-In User Service). Ne hoitavat käyttäjien tunnistuksen (authentication), määrittelevät käyttäjien oikeudet verkon resursseihin (authorisation) ja ylläpitävät verkonhallinnassa tarvittavia tietoja (accounting) (Hakala & Vainio 2005, 170). Tästä prosessista käytetään myös nimitystä AAA-protokolla.



Kuvio 5. 802.1x:n toimintaperiaate

6 EXTENSIBLE AUTHENTICATION PROTOCOL

EAP eli Extensible Authentication Protocol on käyttäjien tunnistukseen tarkoitettu protokolla, joka alun perin suunniteltiin käytettäväksi Point-To-Point-protokollan (PPP) kanssa. Myöhemmin se on laajentunut käytettäväksi myös langallisissa verkoissa sekä WLAN-verkoissa. Kwanin (2003) mukaan EAP sekoitetaan useasti autentikointiprotokollaksi, mutta se ei määrittele turvallisuusprotokollia tai mekanismejä autentikointi prosessille. Kwan (2003) jatkaa myös, että EAP määrittelee ainoastaan miten autentikointiviestit vaihtuvat asiakkaan, autentikaattorin ja autentikointipalvelimen välillä.

EAP:lla on mahdollista käyttää eri autentikointimetodeita, joilla kaikilla on eri ominaisuuksia. Näitä ominaisuuksia vertailemalla voidaan tehdä paras valinta omaa verkkoa varten. Kaikille metodeille yhteistä on kuitenkin se, että ne toimivat linkkikerroksella ja näin ollen ne eivät tarvitse IP-osoitetta toimiakseen (Kwan 2003). Tämä toimii hyvin DHCP-pohjaisissa verkoissa, sillä autentikointi tapahtuu ennen kuin asiakas saa IP-osoitteen DHCP-palvelimelta.

Tämän lisäksi EAPilla on myös muita etuja:

- Toimii useiden autentikointipalvelimien kanssa (Esim. RADIUS)
- Se on standardi, joka toimii useiden valmistajien laitteilla
- Se ei kuormita autentikaattoria paljoa, sillä autentikaattori saa kaiken tiedon suoraan autentikointipalvelimelta. Ainoa tieto joka autentikaattorin tulee tietää, on autentikointipalvelimen lähettämä Hyväksy/Hylkää viesti, jonka mukaan autentikaattori sallii tai rajoittaa liikennettä.

Eri EAP-metodeja on käytössä yhteensä noin 40. Suuri osa näistä metodeista on jo vanhentuneita ja niissä on vakavia tietoturva-aukkoja tai ne ovat muuten sellaisia, joita ei yleisesti käytetä. Listalle mahtuu myös muutamia hieman laajemmin levinneitä metodeja kuten Ciscon kehittämä EAP-LEAP ja sen korvannut EAP-FAST. Seuraavassa on kuitenkin käyty läpi vain muutamat oleellisimmat ja käytetyimmät metodit.

6.1 EAP-TLS

EAP-TLS (Transport Layer Security) on alkuperäinen EAP-standardi, jota tukee kaikki laitevalmistajat. EAP-TLS:ää pidetään yhtenä turvallisimmista EAP-standardeista, sillä TLS-suojatun yhteyden lisäksi se tarvitsee sekä palvelin- että asiakassertifikaatin.

Asiakassertifikaattien käyttö on juuri se osa, joka antaa EAP-TLS:lle sen autentikointi vahvuuden. Se, että pääsee käsiksi käyttäjän käyttäjätunnuksiin, ei vielä riitä järjestelmään murtautumiseksi. Mikäli asiakassertifikaatit säilytetään esimerkiksi älykortilla tai vastaavalla, tulisi järjestelmään pyrkivän henkilön päästä vielä fyysisesti käsiksi laitteeseen, jolla sertifikaattia säilytetään. Asiakassertifikaattien käyttö tekee EAP-TLS:stä kuitenkin myös hankalasti ylläpidettävän ja tämän seikan takia sitä ei ole otettu laajalti käyttöön.

6.2 EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) laajentaa alkuperäistä EAP-TLS-standardia. EAP-TTLS:n on kehittänyt yhteistyössä FunkSoftware ja Certicom. Vaikka EAP-TTLS on muuten hyvin laajalti tuettu, sille ei kuitenkaan löydy natiivia tuke esimerkiksi Microsoftin Windows käyttöjärjestelmistä. Tästä syystä EAP-PEAP-protokolla on nykypäivänä laajemmin käytössä.

TTLS tarvitsee palvelin sertifikaatin, mutta se eroaa alkuperäisestä TLS:stä siinä, että vaikka se voi vaatia myös asiakkaan sertifioimista, niin se ei ole pakollista. Tämä helpottaa varsinkin ylläpitotehtäviä ja tästä syystä TTLS on suositumpi kuin alkuperäinen TLS. TTLS on ”kahden vaiheen” protokolla, joka ensimmäisessä vaiheessa perustaa suojatun TLS-tunnelin ja toisessa vaiheessa siirtää autentikointitiedot tämän tunnelin läpi.

Gastin (2004) mukaan TTLS käyttää TLS-tunnelia vaihtaakseen AVP-arvoja (Attribute-Value Pairs) hyvin samalla tavalla kuin RADIUS-palvelinkin. Gast (2004) jatkaa vielä, että AVP mekanismin johdosta TTLS pystyy autentikoimaan käyttäjän käyttämällä lähes mitä tahansa käytettävissä olevaa autentikointimenetelmää. Näitä ovat mm. kaikki

EAP:in tukemat metodit, mutta myös vanhemmat metodit kuten PAP, CHAP, MS-CHAP ja MS-CHAPv2.

Siinä missä PEAP siirtää ainoastaan käyttäjän salasanan suojattua TLS-yhteyttä pitkin, TTLS suojaa myös käyttäjän käyttäjänimen. Tällä voidaan estää tietynlaiset DoS-hyökkäykset (Denial of Service), joilla lukitaan käyttäjän tunnus kirjautumalla oikealla käyttäjänimellä ja väärällä salasanalla useita kertoja peräkkäin.

6.3 EAP-PEAPv0/MSCHAPv2

EAP-PEAPv0 (Protected EAP) on Ciscon, Microsoftin ja RSA Securityn yhteistyönä kehittämä EAP-standardi. EAP-TLS:n jälkeen EAP-PEAPv0 on yleisimmin tuettu EAP-standardi laitevalmistajien osalta. Sille löytyy natiivi tuki mm. suurimmasta osasta Microsoftin ja Ciscon tuotteita. Juuri tämän laajan tuen ansiosta PEAP on nykyään alalla hyvin yleisesti käytetty.

PEAP on ominaisuuksiltaan hyvin samantapainen kuin EAP-TTLS. PEAP:ssa, kuten myös TTLS:ssä, palvelimen sertifioiminen on välttämätöntä, mutta asiakkaan sertifioiminen on optionaalista. Tämän lisäksi PEAP rakentaa yhteyden aluksi TLS-tunnelin samalla tavalla kuin TTLS.

PEAP eroaa TTLS:stä siinä, että kun TTLS voi käyttää melkein mitä tahansa autentikointimenetelmää TLS-tunnelin lävitse käyttäjän autentikointia varten, PEAP muodostaa vain ulomman TLS-tunnelin. Tämän tunnelin läpi ajetaan toista, sisempää EAP-protokollaa, jolla varsinainen autentikointi suoritetaan. PEAP tarjoaa siis vain ”suojakerroksen” muille EAP-protokollille, kuten turvattomammalle EAP-MD5-protokollalle.

Vaikka PEAP:sta on käytössä eri versioista, niin yleensä puhuttaessa pelkästä PEAP:sta tarkoitetaan sillä juuri EAP-PEAPv0/MSCHAPv2 versiota, jonka sisempänä EAP-protokollana toimii EAP-MSCHAPv2. Mm. Microsoft viittaa juuri tähän protokollaan käyttäessään termiä PEAP. MSCHAPv2:n avulla voidaan käyttää ulkoista käyttäjätietokantaa, kuten esimerkiksi Active Directorya (Gast 2004). Sisempi EAP-protokolla voi kuitenkin olla mikä tahansa muu EAP-protokolla, pois lukien PEAP:in ja TTLS:n.

PEAP voi tarjota mm. seuraavia parannuksia muille EAP-standardeille:

- Viestin todennuksen (kolmannet osapuolet eivät voi vääristää tai lisätä EAP-viestejä)
- Viestin salauksen (kolmannet osapuolet eivät voi lukea suojattuja EAP-viestejä)
- Palvelimen autentikointi asiakkaalle
- Salausavaimen vaihto
- EAP-pakettien fragmentointi ja uudelleen kasaus, mikäli tarvetta (pitkille EAP-viesteille)

7 CAPWAP

CAPWAP (Control And Provisioning of Wireless Access Points) on IETF:n standardoima protokolla, jota käytetään langattomien tukiasemien keskitettyyn hallintaan WLAN-laiteohjaimen eli kontrollerin avulla. CAPWAP pohjautuu Ciscon LWAPP-protokollaan (Lightweight Access Point Protocol) (Control And Provisioning of… 2009).

CAPWAP:n ajatus on siirtää kaikki "äly" tukiasemilta kontrollerille. Näin WLAN-verkon hallinta ja ylläpito helpottuvat, kun jokaista tukiasemaa ei tarvitse konfiguroida erikseen. Kontrollerin tehtävänä on tarjota mm.

- keskitetty hallinta verkon ylläpidolle
- yleiset asetukset tukiasemille
- tukiasemien virran ja radioiden hallinta
- yhtenäiset turvallisuus- sekä liikenneasetukset tukiasemille.

Kontrollerin merkitys korostuu varsinkin suuremmissa verkoissa. Jos verkossa ei ole kontrolleria, jouduttaisiin 20 tukiaseman verkossa tapahtuva muutos konfiguroimaan käsin jokaiseen tukiasemaan. Kontrollerin avulla riittää, että muutos tehdään pelkästään kontrollerille, joka tämän jälkeen päivittää tukiasemien tiedot.

Tämän lisäksi kontrolleri pystyy myös tarkkailemaan liikennettä ja mukautumaan erilaisiin tilanteisiin. Esimerkiksi jos yksi tukiasema menee rikki, kontrolleri saa tiedot tästä ja säätää muiden tukiasemien lähetystehoa niin, että muut tukiasemat pystyvät yhdessä kattamaan myös rikkoutuneen tukiaseman alan.

8 CASE

8.1 Valmistautuminen

Ennen kuin varsinaisen langattoman verkon asennusta päästiin aloittamaan tuli yrityksen runkoverkkoon tehdä muutoksia. Näistä muutoksista suurin oli yrityksen käyttämän vanhan runkokytkimen vaihtaminen uuteen, reititysominaisuuksilla varustettuun kytkimeen. Vaihto jouduttiin tekemään sen takia, että langaton verkko toimii omana aliverkkonaan, eikä ilman reitittävää laitetta tätä verkkoa olisi voitu reitittää osaksi yrityksen muuta verkkoa. Reititys olisi voitu tehdä myös lisäämällä uusi reititin verkkoon, mutta reitittävän kytkimen käyttö nähtiin järkevämmäksi vaihtoehdoksi muutamastakin syystä.

Keskuskytkimen ja eri osastoiden jakopisteiden välinen runkoverkko oli valmiiksi kuitukaapelia, mutta vanhassa runkokytkimessä, eikä kaikissa jakopisteissä sijaitsevissa kytkimissä, ollut mahdollisuutta liittää kuituliitäntöjä. Ainoana liitäntä mahdollisuutena näissä kytkimissä oli käyttää RJ45-liitäntöjä. Tästä syystä kuitukaapelin molemmissa päissä käytettiin medianmuuntimia, joilla kuituliitäntä pystyttiin vaihtamaan RJ45-liitännäksi.

Mediamuuntimien käyttö heikensi verkon toimintavarmuutta. Useasti medianmuuntimet eivät yltäneet laadultaan kytkimien tasolle ja varsinkin useamman vuoden käytössä olleet mediamuuntimet alkoivat hajoilla omia aikojaan. Mediamuuntimien lisäksi vanha runkokytkin rajoitti verkon maksiminopeutta, sillä kytkimen portit pystyivät toimimaan maksimissaan 100 Mbit/s nopeudella.

Uusi runkokytkin sekä uudet kytkimet jakopisteissä mahdollistivat kuitenkin kuitukaapelin suoran liittämisen kytkimiin ja mediamuuntimista päästiin eroon. Runkoverkon nopeutta pystyttiin nostamaan 100 Mbit/s nopeudesta 1000 Mbit/s nopeuteen ja medianmuuntimien poiston myötä myös verkon toimintavarmuus parani.

8.2 Käyttöönotto

Kun runkoverkon muutokset oli tehty, päästiin rakentamaan langatonta Traveller-verkkoa. Traveller on yrityksen verkosta käyttämä nimi, joka toimii myös verkon SSID-tunnuksena.

8.2.1 Tukiasemien sijoittelu

Verkon suunnittelu aloitettiin miettimällä tukiaseman sijoituspaikkoja. Suurempia kuuluvuus mittauksia ei ollut syytä tehdä, sillä ensimmäiset tukiasemat sijoitettiin auditorioon sekä neuvotteluhuoneeseen. Niiden kantaman oli tarkoitus peittää ainoastaan kyseessä olevat kohteet, eikä pidemmälle kantamalle ollut sen suurempaa tarvetta. Tästä syystä tukiasemien sijoituspaikkoja mietittiin enemmän esteettiseltä kannalta.

Tukiasemat yritettiin sijoittaa mahdollisimman piiloon ja niin, että johdot olisivat mahdollisimman lyhkäisiä ja niitä olisi mahdollisimman vähän. Tämän johdosta tukiasemissa päätettiin käyttää PoE-moduuleja (Power over Ethernet). PoE-moduulien käyttö mahdollisti virtalähteen ja sähköjohdon piilottamisen siihen ristikytkentäkaappiin, johon tukiasema oli liitetty. Itse tukiasema tarvitsi ainoastaan yhden RJ45-kaapelin, jonka läpi kulki Ethernet-liikenteen lisäksi myös virta.

8.2.2 Reititys ja osoiteavaruus

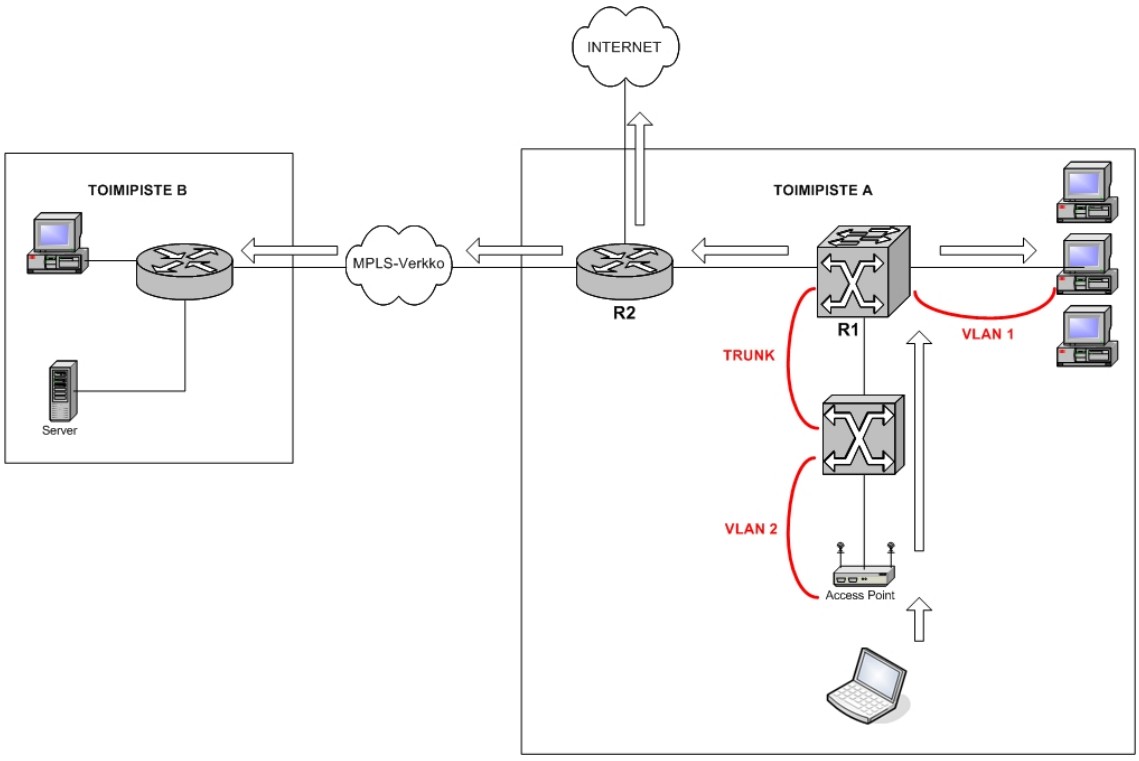
Uudelle Traveller-verkolle varattiin kokonaan oma aliverkko. Verkoksi valikoitui x.x.x.x-verkko 24-bittisellä verkkomaskilla, kun Ylöjärven toimipisteen kiinteä verkko toimii x.x.x.x-verkossa 21-bittisellä verkkomaskilla. Koska molemmat verkot, langaton ja langallinen, toimivat omina verkkoinaan samoilla fyysisillä laitteilla, päätettiin verkot jakaa omiin VLAN-verkkoihinsa (Virtual LAN).

Koska yrityksen langallinen verkko oli valmiiksi sijoitettu jo yhteen VLAN:iin, VLAN 1, ei tätä päätetty muuttaa, vaan uudelle Traveller-verkolle päätettiin luoda oma VLAN. Travellerin VLAN:ksi tuli näin ollen VLAN 2. Kytkinten väliset yhteydet muutettiin

Trunk-linkeiksi, jotta ne tukisivat useamman VLAN:in liikennöintiä. Tämän jälkeen sen kytkimen portti, johon tukiasema oli liitetty, määriteltiin kuuluvaksi VLAN 2:een.

Verkkojen reititys päätettiin hoitaa OSPF (Open Shortest Path First) pohjaisella IP-reitityksellä. OSPF-otettiin käyttöön runkokytkimellä R1 ja se asetettiin mainostamaan verkkoja x.x.x.x /24 sekä x.x.x.x /21. Reunareitittimelle R2 ei tarvitse erikseen kertoa uuden verkon olemassaolosta, vaan se oppii sen R1:ltä.

Runkokytkin reitittää Traveller-verkosta tulevan liikenteen kohdeosoitteesta riippuen joko toimipisteen muuhun sisäverkkoon tai ulkoreitittimelle R2. Ulkoreititin jatkoreitittää liikenteen eteenpäin joko internettiin tai yrityksen muihin toimipisteisiin MPLS-verkon läpi kuvion 6 osoittamalla tavalla.



Kuvio 6. Verkon reititys sekä VLAN-verkot

8.2.3 Tukiasemien konfigurointi

Tukiasemien konfigurointi suoritettiin CAPWAP-protokollaa hyväksikäyttäen. Tukiasemia ei konfiguroitu yksitellen käsin, vaan tukiasemien asetusten tekemiseen käytettiin kontrolleria.

Vaikka muutama tukiasema olisikin ollut suhteellisen helppo ja nopea konfiguroida myös manuaalisesti, helpottaa kontrollerin käyttö uusien tukiasemien lisäämistä verkkoon. Näin kaikki tukiasemat saadaan käyttämään mm. samoja turvallisuus- ja liikenneasetuksia, kuten salausta, autentikointimenetelmiä sekä 802.11-protokollan valintaa, joten verkko säilyy yhdenmukaisena ja helpommin hallittavana.

Koska kyseessä on kansainvälinen yritys ja kaikkien toimipisteiden Traveller-verkot, niin Suomessa kuin muuallakin maailmassa, on haluttu pitää samanlaisina ja helpommin hallittavina, on kontrollerit päätetty sijoittaa yrityksen datakeskukseen Saksaan. Näin ollen ainoastaan tukiasemat sijoitetaan eri toimipisteille, mutta kaikki yrityksessä käytössä olevat tukiasemat saavat tietonsa Saksassa sijaitsevilta kontrollereilta.
Tämänlainen keskittäminen tuo etuja verkkojen ylläpitoon ja yhtenäistämiseen. Mikäli joka maassa olisi oma ylläpitäjä tai ylläpitäjät, olisi melko todennäköistä, että jossain vaiheessa yhtenäisyys eri maiden verkkojen välillä alkaisi murentua. Myös vian etsintä olisi tällaisessa tapauksessa huomattavasti vaikeampaa.

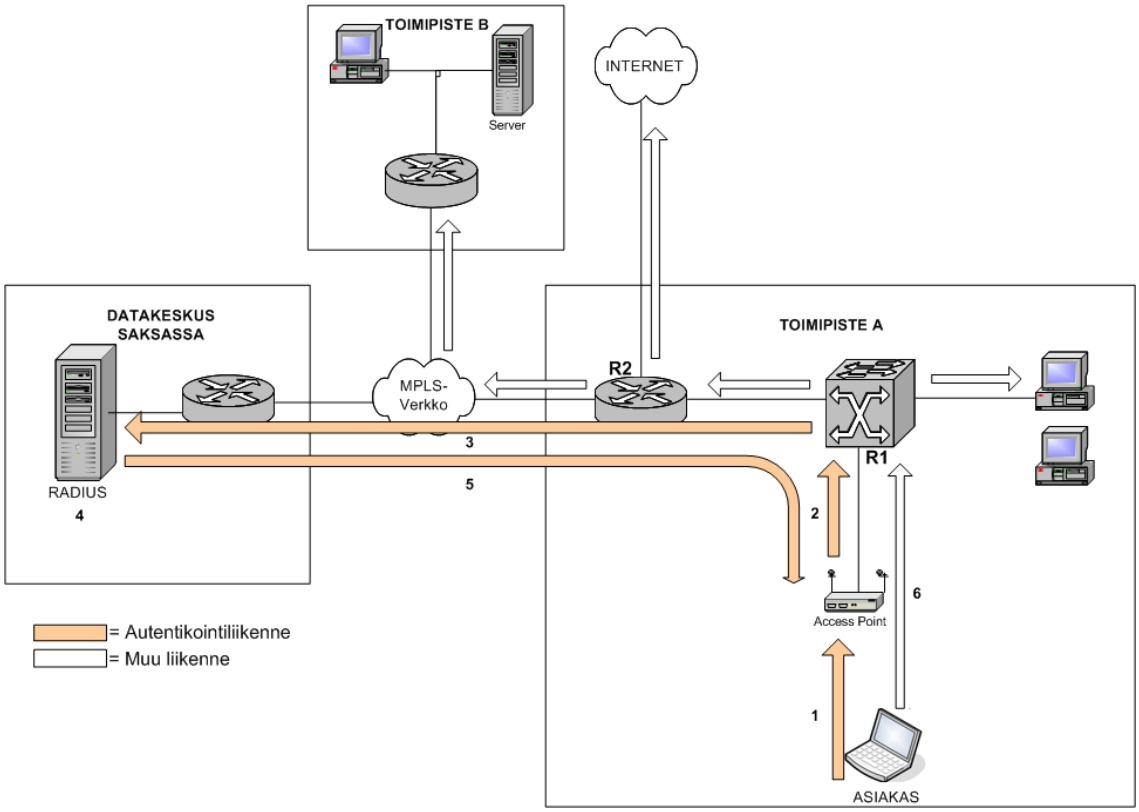
8.2.4 Salaus ja autentikointi

Verkossa liikkuvan tiedon salaukseen tukiaseman ja asiakkaan välillä päätettiin käyttää WPA-protokollaa ja TKIP-salausta. WPA2-protokollaa tai vahvempaa AES-salausta ei käytetty sen takia, että yrityksessä on käytössä vielä jonkin verran vanhempia kannettavia, jotka eivät tue WPA2:sta tai AES:ia.

Käyttäjien tunnistus suoritetaan käyttäen 802.1x-autentikointia ja RADIUS-palvelinta. RADIUS-palvelimena verkossa toimii Windows 2003 Server, joka on liitetty yrityksen domainiin ja palvelimelle on asennetu Active Directory. Näin ollen RADIUS pystyy käyttämään yrityksessä jo valmiiksi olevaa AD-tietokantaa käyttäjien tunnistukseen, eikä Traveller-verkon käyttäjiä varten tarvitse luoda uutta käyttäjätietokantaa.

Verkkoon kirjauduttaessa viestit päätelaitteen ja tukiaseman välillä hoidetaan käyttäen EAP-protokollaa ja sen määrityksiä. Eri EAP-protokollista käyttöön on valittu EAP-PEAP, joka toimii ulompana EAP-protokollana. Sisempänä EAP:na toimii EAP-MSCHAPv2. Juuri EAP-MSCHAPv2:n käyttö mahdollistaa AD-tietokannan hyväksikäytön käyttäjien tunnistuksessa. Koska PEAP:ssa palvelinsertifikaattien käyttö on valinnaista, on palvelinsertifikaateista päätetty luopua kokonaan.

Kontrollereiden tapaan RADIUS-palvelin on päätetty sijoittaa yrityksen datakeskukseen Saksaan, jolloin samalla RADIUS-palvelimella voidaan palvella yrityksen kaikkien Traveller-verkkojen autentikointia. Kuviossa 7 on esitetty, että kaikki liikenne ei kulje kuitenkaan Saksan kautta, vaan ainoastaan autentikointiliikenne. Autentikoinnin jälkeen liikenne reititetään normaaliin tapaan riippuen sen määränpäästä.



Kuvio 7. Autentikointi verkossa

1. Langaton päätelaite kirjautuu verkkoon ja lähettää EAP-paketin tukiasemalle.

2. Tukiasema vastaanottaa kirjautumispyynnön. Koska RADIUS on käytössä, tukiasema uudelleen kapsuloi EAP-paketin RADIUS-paketiksi ja estää muun liikenteen päätelaitteelta tukiasemalle. Kohdeosoitteeksi pakettiin tukiasema kirjaa asetuksistaan löytyvän RADIUS-palvelimen IP:n ja lähettää paketin omalle yhdyskäytävälleen R1:lle.

3. Yhdyskäytävänä toimiva reitittävä kytkin R1 ohjaa paketin edelleen verkon reunareitittimelle R2, joka tämän jälkeen reitittää RADIUS-paketin eteenpäin kohti määränpäätänsä MPLS-verkon läpi.

4. Kun RADIUS-paketti saapuu määränpäähänsä RADIUS-palvelimelle, palvelin vertaa paketissa olevaa käyttäjätunnusta sekä salasanaa omasta tietokannastaan löytyviin tietoihin.

5. Mikäli käyttäjätunnus löytyy tietokannasta ja salasana täsmää, RADIUS-palvelin lähettää hyväksy-viestin takaisin tukiasemalle.

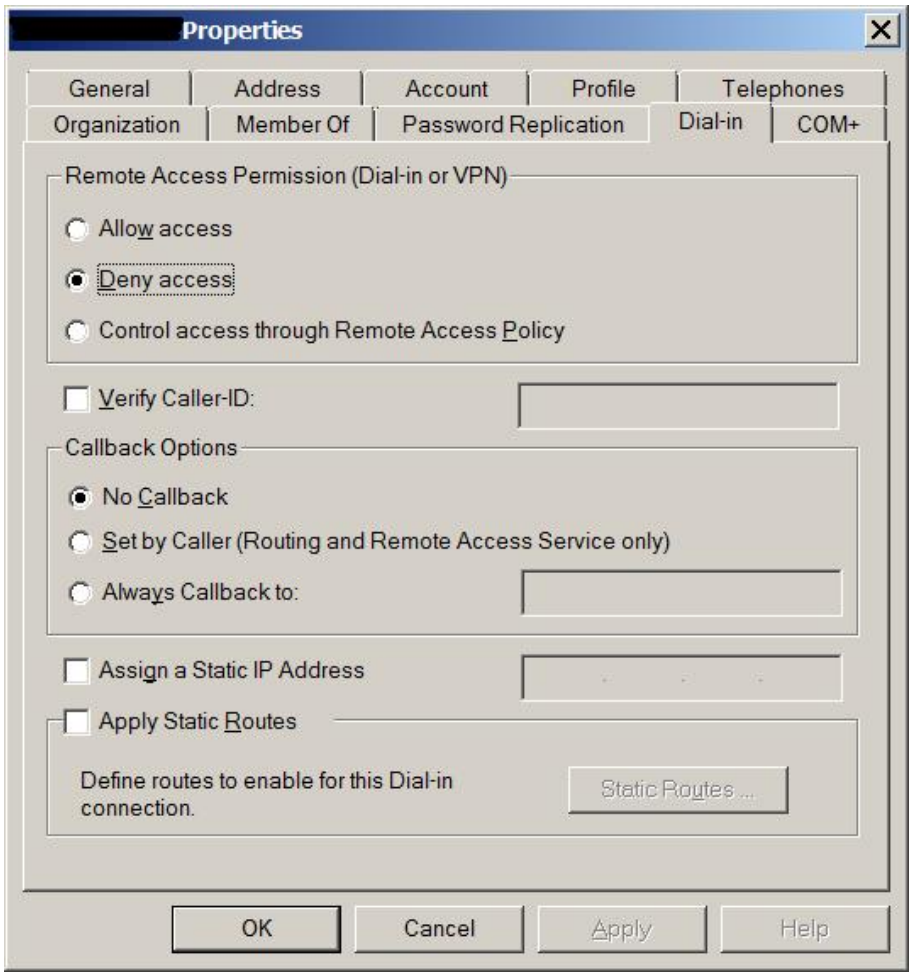
6. Tukiasema sallii tämän jälkeen liikenteen verkkoon RADIUS-palvelimen antamien, tarkempien liikennerajoitusten mukaan. Tämän jälkeen liikenne reititetään normaaliin tapaan riippuen kohdeosoitteesta.

8.3 Ongelmat

Usealla käyttäjällä oli ongelmia liittyä Traveller-verkkoon, vaikka asetukset koneella oli oikein sekä käyttäjillä oli voimassa olevat tunnukset Active Directoryssä. Aluksi ongelman ajateltiin aiheutuvan viallisista verkkokortin ajureista, mutta tämä pystyttiin melko nopeasti unohtamaan, sillä ongelmia esiintyi useammalla eri merkkisellä ja mallisella koneella. Osa käyttäjistä kertoi myös, että ovat pystyneet käyttämään muita langattomia verkkoja koneillaan.

Kun ongelmaa alettiin selvittää kontrollerilta, huomattiin, että näiden käyttäjien kirjautumispyynnöt evätään sen takia, että kirjautumisen yhteydessä ei lähetetä salasanaa ol-

lenkaan. Syyksi paljastui käyttäjien AD-profiileissa oleva esto (kuvio 8), joka esti VPN- ja Dial-in-yhteydet. Vaikka langatonta verkkoa ei voi laskea kummankaan kategorian yhteydeksi, niin Traveller-verkossa käyttäjät tunnistava RADIUS on nimensä mukaisesti Dial-in-palvelin, ja myös Windows käsittelee tätä tällä tavoin. Tästä syystä AD:ssa oleva esto vaikuttaa myös langattoman verkon toimintaan käyttäjien kirjautumisen osalta.



Kuvio 8. Active Directoryn asetus, joka estää käyttäjää kirjautumasta Traveller-verkkoon

8.4 Parannusehdotukset

8.4.1 Tietoturva

Tällä hetkellä verkkoon kirjautuvat käyttäjät todennetaan vertaamalla syötettyä käyttäjätunnusta sekä salasanaa Active Directorystä löytyviin tietoihin. Mikäli käyttäjänimi ja salasana täsmäävät, verkon käyttö sallitaan. Muussa tapauksessa verkon käyttö estetään. Active Directoryn käyttö tarjoaa käyttäjien yksilöivän tunnistamisen sekä parantaa tieto-

turvaa, kun jokainen käyttäjä käyttää omia tunnuksiaan eikä käytössä ole esijaettua avainta.

Verkon tietoturvaa voitaisiin parantaa kuitenkin entisestään niin, että käyttäjätunnuksen sekä salasanan lisäksi varmistettaisiin, että myös liittyvä päätelaite löytyy AD:sta. Tämä estäisi sen, että luvattomilla laitteilla ei verkkoon pystyisi liittymään. Nykyisillä asetuksilla kiinteään verkkoon ei pysty liittymään luvattomalla koneella, mutta langattoman verkon kautta se on mahdollista.

8.4.2 Vierailijaverkko

Langatonta verkkoa voitaisiin käyttää tarjoamaan myös ns. vierailija-yhteyttä yrityksessä vieraileville ulkopuolisille henkilöille, kuten yhteistyökumppaneille ja asiakkaille. Tämä voitaisiin saavuttaa mm. niin, että tukiasemille luotaisiin Traveller SSID:n lisäksi vielä toinenkin SSID, esimerkiksi Visitor.

Tukiasema yleislähettäisi (broadcast) näitä molempia SSID:tä ja käyttäjän tulisi valita, kumpaan verkkoon hän haluaa liittyä. Traveller-verkkoa käyttävät käyttäjät todennettaisiin normaaliin tapaan RADIUS-palvelimen avulla. Visitor-verkko voitaisiin suojata esimerkiksi esijaetulla avaimella.

Visitor-verkko sijoitettaisiin erilliseen VLAN-verkkoon, joka reititettäisiin ainoastaan internettiin. Näin Visitor-verkko olisi täysin erillinen verkko yrityksen kiinteästä verkosta sekä langattomasta Traveller-verkosta.

9 YHTEENVETO

Koko opinnäytetyöprosessi sujui omasta mielestäni hyvin. Ennen opinnäytetyön aloittamista määritellyt tavoitteet täyttyivät ja opinnäytetyötä tehdessä sekä raporttia kirjoittaessa olen oppinut paljon uutta liittyen langattomiin verkkotekniikoihin. Tietoteknisen oppimisen lisäksi työ auttoi minua hahmottamaan myös sen, kuinka kansainvälisessä yrityksessä toimitaan.

Opinnäytetyön käytännönosuus hoitui hyvin ja ilman suurempia ongelmia. Uusi langaton verkko otettiin yrityksessä loppukäyttäjien keskuudessa vastaan hyvillä mielin, eikä nurinoita sen toimintavarmuudesta ole liiemmin kuultu. Myös sen helppo käyttöönotto on saanut kiitosta.

Tämän valmiina olevan ratkaisun päälle on helppoa lähteä laajentamaan langatonta verkkoa myös muille toimipisteille. Raportin valmistumishetkellä marraskuussa 2010 verkko olikin jo laajentunut käsittämään useampia toimipisteitä. Raportointi osuus sujui myös hyvin ja koska sille oli varattu tarpeeksi aikaa, ei kiirettä päässyt muodostumaan missään vaiheessa. Raportti venyi hieman alkuperäisestä suunnitelmasta, mutta monesti kokonaisuus muovautuu vasta kirjoitusvaiheessa.

LÄHTEET

802.1X Port-Based Authentication HOWTO. 2004. The Linux Documentation Project. Luettu: 17.9.2010.
http://tldp.org/HOWTO/html_single/8021X-HOWTO

Bing, B. 2002. Wireless Local Area Networks. New York: John Wiley & Sons.

Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification. 2009. Internet Engineering Task Force. Luettu: 6.10.2010.
http://www.ietf.org/rfc/rfc5415.txt

Gast, M. 2004. TTLS and PEAP comparison. Luettu: 28.9.2010.
http://www.opus1.com/www/whitepapers/ttlsandpeap.pdf

Geier, J. 2002. Assigning 802.11b Access Point Channels. Luettu: 20.9.2010.
http://www.wi-fiplanet.com/tutorials/article.php/972261/Assigning-80211b-Access-Point-Channels.htm

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: WS Bookwell.

IEEE 802.11 Standards, facts & channels. 2005. Air802 LLC. Luettu: 16.4.2010.
http://www.air802.com/ieee-802.11-standards-facts-amp-channels.html

Jaakohuhta, H. 2000. Lähiverkot: Ethernet. Helsinki: IT Press.

Kwan, P. 2003. White Paper: 802.1x Authentication & Extensible Authentication Protocol (EAP) Luettu: 16.9.2010.
http://www.foundrynet.com/pdf/wp-8021x-authentication-eap.pdf

Kotilainen, S. 2003. Wlan-verkon tietoturva. Tietokone lehti. Luettu: 4.8.2010.
http://www.tietokone.fi/lehti/tietokone_4b_2003/wlan_verkon_tietoturva_3501

Langattomat lähiverkot (RLAN) 5 GHz:n taajuusalueella. 2002. Viestintävirasto. Luettu: 27.9.2010.
http://viestintavirasto.fi/index/viestintavirasto/asiakastiedotteet/radiotaajuudet/2002/P_12.html

Niemi, J. 2002. WLAN-Turvallisuus. Luettu: 10.8.2010.
http://www.cs.helsinki.fi/group/turvasem/papers/niemi_wlan.pdf

Pilkington Suomessa. 2010b Pilkington. Luettu: 12.10.2010.
http://www.pilkington.com/europe/finland/finnish/about+pilkington/default.htm

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Gummerus Kirjapaino Oy.

Syrjälä, M. 2001. WLAN – Langaton lähiverkko. Luettu: 23.8.2010.
http://users.tkk.fi/mjsyrjal/wlan.html

This is Pilkington. 2010. Pilkington. Luettu: 12.10.2010.

http://www.pilkington.com/resources/10052_tip_finn_fin.pdf

Wi-Fi Alliance. 2010. Featured Topics: WPA2. Wi-Fi Alliance. Luettu: 4.8.2010. http://www.wi-fi.org/knowledge_center/wpa2

Wikipedia 2010a. 2010.. IEEE 802.11g-2003. Luettu:16.4.2010. http://en.wikipedia.org/wiki/IEEE_802.11g-2003

Wikipedia 2010b. 2010. IEEE 802.11. Luettu: 17.9.2010. http://en.wikipedia.org/wiki/IEEE_802.11