**TEKNIIKKA JA LIIKENNE**

**Tietotekniikka**

**Tietoliikennetekniikka**

**INSINÖÖRITYÖ**

# LANGATON LÄHIVERKKO JA IEEE-STANDARDIT

**Työn tekijä: Jesse Rampanen**

**Työ hyväksytty: ___. ___. 2010**

**Jukka Louhelainen**
**lehtori**

**ALKULAUSE**

Tämä insinöörityö tehtiin kypsyysnäytetyöksi insinööritutkintoa varten. Kiitän Jukka Louhelaista, joka suostui lyhyellä varoitusajalla valvomaan insinöörityötäni.

Helsingissä 8 .4 .2010

Jesse Rampanen

**TIIVISTELMÄ**

**Työn tekijä:** Jesse Rampanen

**Työn nimi:** Langaton lähiverkko ja IEEE-standardit

**Päivämäärä:** 8. 4. 2010 **Sivumäärä:** 51 s.

**Koulutusohjelma:** Tietotekniikka

**Suuntautumisvaihtoehto:** Tietoliikennetekniikka

**Työn ohjaaja:** lehtori Jukka Louhelainen

Tässä insinöörityössä perehdytään langattomiin lähiverkkoihin ja niissä käytettäviin tekniikoihin. Langattomat yhteydet ovat jo luultavasti yleisin tapa muodostaa yhteys verkkoon, ja yhä useammat mobiililaitteet ovat jollakin tapaa yhteydessä verkkoon.

Langattomat lähiverkot perustuvat ilmatiellä radiotaajuuksilla tapahtuvaan tiedonsiirtoon. WLAN-laitteet toimivat lupavapaalla ISM-taajuusalueella ja käyttävät sekä 2,4 GHz:in että 5 GHz:in taajuusalueita tiedonsiirtoonsa. Nykyisillä standardeilla päästään jo teoriassa 600 Mbps nopeuksiin, mutta käytännön nopeudet jäävät näistä vielä huomattavasti.

Käyttäjien ja tarjottujen palveluiden määrät kasvavat koko ajan, jolloin tarvitaan tehokkaampia menetelmiä käyttää radiotaajuuksilla tapahtuvaa tiedonsiirtoa hyväksi. Palvelujen tarjoama laatu myös paranee samaa tahtia, kun itse päätelaitteiden ja verkon suorituskyky kasvaa.

Koska yhä henkilökohtaisemmat ja kriittisemmät palvelut siirtyvät verkkoon, käyttäjien ja palvelujen välinen tiedonsiirto tulisi myös suojata mahdollisimman hyvin. Uudet standardit keskittyvät myös pelkän suorituskyvyn lisäämisen ohella parantamaan tietoturvaa, jolloin palveluiden käyttäminen on entistä turvallisempaa.

Insinöörityössä keskitytään WLAN-verkkojen peruskäsitteisiin ja syvennytään tarkemmin uudempiin IEEE:n määrittelemiin standardeihin.

**Avainsanat:** WLAN, langaton lähiverkko, IEEE, Wi-Fi

Metropolia

**ABSTRACT**

**Name:** Jesse Rampanen

**Title:** Wireless Local Area Network and IEEE-standards

**Date:** 8. 4. 2010 **Number of pages:** 51

**Department:** **Study Programme:**

Information Technology Communications and Data Networks

**Instructor:** Jukka Louhelainen, Lecturer

The purpose of this thesis was to investigate WLAN networks and the techniques that are used. Wireless connections are probably the main way to connect to a network and a growing number of mobile stations are somehow connected to networks.

WLAN networks use radio waves to transfer information by air. WLAN stations operate in the license free ISM radio bands and use 2,4 GHz and 5 GHz frequencies to transfer information. With current standards it is theoretically possible to achieve data rates up to 600 Mbps, but in practice the data rates are much lower.

The number of users and services is constantly growing so it is necessary to develop more powerful methods to utilize the used radio frequencies. As the mobile equipment is developing the quality of the offered services is also getting better.

It is important to secure the data transfers between users and services, because even more critical and personal services are converted to be used in the Internet. New standards improve the performance of the networks, but they also make the communications more secure.

This thesis focuses mainly on WLAN concepts and concentrates more precisely on the newer standards defined by IEEE.

**Keywords:** WLAN, Wireless Local Area Network, IEEE, Wi-Fi

**SISÄLLYS**

**ALKULAUSE**

**TIIVISTELMÄ**

**ABSTRACT**

**KÄSITELUETTELO**

**KÄSITELUETTELO**

| | |
|---|---|
| AP | Access Point; langaton tukiasema. |
| BSS | Basic Service Set; yhden AP:n kantoalueen verkko. |
| CAPWAP | Control and Provisioning of Wireless Access Points; tukiasemien ja WLAN-kontrollien välinen protokolla. |
| CCK | Complement Code Keying; koodaustekniikka. |
| CCMP | Counter Mode with CMC-MAC Protocol; WLAN-verkoissa käytettävä salausprotokolla. |
| DBPSK | Differential Binary Phase-Shift Keying; modulointitekniikka. |
| DQPSK | Differential Quadrature Phase-Shift Keying; modulointitekniikka. |
| DS | Distribution System; tukiasemien taustalla oleva runkoverkko. |
| DSSS | Direct Sequence Spread Spectrum; suorasekvenssihajaspektri. |
| EAP | Extensible Authentication Protocol; todennuksessa käytettävä protokolla. |
| ESS | Extended Service Set; useamman BSS:n muodostama verkko. |
| FEC | Forward Error Coding; virheenkorjauksessa käytettävä koodaus. |
| FHSS | Frequency-Hopping Spread Spectrum, taajuushyppelyhajaspektri. |
| IEEE | Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan järjestö. |
| IETF | Internet Engineering Task Force; protokollia standardoiva järjestö. |
| ISM | Industrial, Scientific and Medical; luvista vapaa taajuusalue. |
| LWAPP | Lightweight Access Point Protocol; tukiasemien ja WLAN-kontrollien välinen protokolla. |
| MAC | Media Access Control –kerros; yksi OSI-mallin kerroksista. |
| Mbps | Megabytes per second; datanopeusyksikkö (Mb/s). |
| MIMO | Multiple-Input Multiple-Output; useiden lähetys- ja vastaanottoantennien käytön mahdollistava tekniikka. |
| MPDU | MAC Packet Data Unit. |
| NAS | Network Access Server; verkkoon yhdistämisessä käytettävä yhteyspiste. |
| OFDM | Orthogonal Frequency-Division Modulation; modulointitekniikka, jossa tieto siirretään useilla taajuuskanavilla samanaikaisesti. |
| OSI | OSI-malli; yhdistelmä tiedonsiirtoprotokollien kerroksista. |

| | |
|---|---|
| PMK | Pairwise Master Key; 802.11i –salauksessa käytettävä avain. |
| PN | Packet Number; paketin numero. |
| PSK | Pre-Shared Key; ennen verkkoon yhdistämistä jaettu salausvain. |
| QAM | Quadrature Amplitude Modulation; amplitudimodulaatioon pohjautuva modulaatiotekniikka. |
| RC4 | Rivest Cipher 4; WEP-salauksessa käytettävä algoritmi. |
| RF | Radio Frequency; radiotie, radiotaajuus. |
| RSN | Robust Security Network; 802.11i –standardia noudattava verkko. |
| SDM | Spatial Division Multiplexing; modulaatiotekniikka, jossa lähetetään samoja tai eri bittivirtoja jokainen omalla, rinnakkaisella kaistalla. |
| SNR | Signal-to-Noise Ratio; signaalikohinasuhde. |
| Spatiaalinen | Geometrinen, avaruudellinen, tilan puolesta oleva. |
| SSID | Service Set Identifier; langattoman lähiverkon tunnus. |
| STBC | Space-Time Block Coding; langattomassa tiedonsiirrossa käydetty tekniikka. |
| TK | Temporal Key; väliaikainen salausavain. |
| TKIP | Temporal Key Integrity Protocol; 802.11 –standardin turvallisuusprotokolla. |
| WEP | Wired Equivalent Privacy; 802.11 –standardien käyttämä salausmenetelmä. |
| Wi-Fi | Wireless Fidelity; WLAN-tuotteista käytteävä nimitys. |
| WLAN | Wireless Local Area Network; langaton lähiverkko. |
| WLC | WLAN-kontrolleri; laite, jolla hallinnoidaan langattomia tukiasemia. |
| WPA | Wi-Fi Protected Access; WEP-salauksessa kehitetty paranneltu salausmenetelmä. |

# 1 JOHDANTO

Tietoliikenneyhteydet ja verkostoituminen ovat yhä keskeisempiä tarpeita ja vaatimuksia nykyisessä yhteiskunnassa. Ihmisten käyttämät hyöty- ja viihdepalvelut siirtyvät yhä enemmän sähköisiksi verkkopalveluiksi, jolloin palveluiden tarve ja käyttö kasvavat. Koska osa verkkoon siirtyvistä palveluista voi olla ihmisille välttämättömiä, myös palvelujen saatavuus kasvaa. Jotta palvelut olisivat saatavilla verkoissa, tulee niitä käyttävillä ihmisillä olla jokin yhteys itse palveluun.

Suurimmalla osalla työasemia ja kannettavia mobiililaitteita on jokin verkkoyhteys, mutta luultavasti suosituin ja eniten käytetty verkkoyhteys on WLAN, eli langaton lähiverkko. Tässä insinöörityössä keskitytäänkin pelkästään tähän langattomaan lähiverkkotekniikkaan.

IEEE-järjestö on kehittänyt yhtenäisiä IEEE 802.11 –standardeja, joiden avulla eri valmistajien ja mahdollisesti eri tekniikoita käyttäville laitteille on kehitetty yhteisiä standardeja. Näiden avulla eri laitteille on saatu määriteltyä muun muassa samat käytettävät tiedonsiirtomenetelmät ja yhtenevät viestintäprotokollat, joiden avulla laitteet voivat kommunikoida keskenään. Nykyään monet IEEE 802.11 –standardeja käyttävät laitteet tunnetaan myös Wi-Fi–laitteina, jolloin ne ovat saaneet Wi-Fi Alliancen hyväksynnän.

Tässä insinöörityössä käydään läpi langattomien lähiverkkojen peruskäsitteitä ja keskitytään tarkemmin IEEE:n määrittelemiin uusiin 802.1x- ja 802.11i–standardeihin, jotka parantavat WLAN-verkkojen tietoturvaa ja 802.11n–standardiin, jolla saadaan käyttöön uusia verkon suorituskykyä parantavia tekniikoita.

# 2 IEEE-STANDARDIT

## 2.1 IEEE 802.11

802.11 on alkuperäinen standardi, joka julkistettiin vuonna 1997 ja täsmennettiin vuonna 1999. Standardi määrittelee alimman, fyysisen kerroksen OSI-mallissa sekä siirtokerroksen alemman MAC-kerroksen. Siirtotavoiksi määritellään 2,4 GHz:n tai 5 GHz:n ISM-alueilla toimivat radioaallot tai 850-950 nanometrin aallonpituusalueella toimiva infrapuna. [1.]

Standardi määrittelee käytettäviksi verkkotopologioiksi Ad Hoc –verkon, jossa mobiiliasemat ovat suoraan yhteydessä toisiinsa sekä tukiasemiin pohjautuvan verkon, jossa mobiiliasemat suorittavat liikennöinnin tukiasemien kautta.

ISM-alueella tapahtuvan datan siirron tulee sääntöjen mukaan perustua hajaspektritekniikkaan, ja IEEE 802.11 käyttää sekä suorasekvenssi-hajaspektriä että taajuushyppelyä. [2.]

## 2.2 IEEE 802.11a

Myös IEEE 802.11a –laajennuksen kehitystyö aloitettiin vuonna 1997, ja se ratifioitiin vuoden 1999 lopulla. Laajennus parantaa fyysisen kerroksen toimintaa eikä vaikuta muihin ylempiin kerroksiin. Standardin hyötyinä ovat parempi suoja häiriöitä vastaan ja suuremmat saavutettavat nopeudet. Suurin saavutettava nopeus on 54 Mbit/s. Tämä saavutetaan käyttämällä QAM-modulointia. Nopeutta voidaan tarpeen tullen alentaa käyttäen eri modulaatiotekniikoita ja FEC-tasoja.

802.11a hyödyntää 300 MHz:n levyistä kaistaa 5 GHz:n taajuusalueella. Käytetty kaista on jaettu kolmeen 100 MHz:n alueeseen eri lähetystehoilla välitettyjen signaalien mukaan. Laajennus käyttää OFDM-modulointia fyysisellä tasolla ja laajennuksesta käytetäänkin nimitystä OFDM PHY. [3, s. 267.]

## 2.3 IEEE 802.11b

802.11b-standardi on laajennus alkuperäiseen IEEE 802.11 -suositukseen ja sillä voidaan saavuttaa suurempia nopeuksia aina 11 Mbit/s asti käyttäen samaa lisensoimatonta 2,4 GHz:n ISM-taajuuskaistaa kuin alkuperäisessäkin suosituksessa. 802.11b–laajennus on myös taaksepäin yhteensopiva 802.11–suosituksen kanssa, joten laajennuksen avulla voidaan käyttää myös 1 ja 2 Mbit/s nopeuksia samoilla vastaanottimilla. [3, s. 267-268.]

Alhaisemmilla 1 ja 2 Mbit/s nopeuksilla käytetään DBPSK- ja DQPSK-modulointeja. Näitä nopeuksia käytetään huonompien olosuhteiden vallitessa. Suosituksen avulla saavutetaan suurempia 5,5 ja 11 Mbit/s nopeuksia käyttämällä CCK-modulointia. [4, s. 240.]

## 2.4 IEEE 802.11g

802.11g on kolmas laajennus alkuperäiseen IEEE 802.11 -standardiin. Laajennus toimii samalla 2,4 Ghz:n taajuuskaistalla kuin 802.11b, mutta tällä standardilla voidaan saavuttaa 54 Mbit/s datanopeus. 802.11g-laitteet ovat taaksepäin yhteensopivia 802.11b-laitteiden kanssa.

802.11g-laajennuksessa käytetään useampia eri modulaatiotekniikoita riippuen datanopeudesta. 1 ja 2 Mbit/s nopeuksissa käytetään DBPSK-, DQPSK- ja DSSS-modulaatioita. 5,5 ja 11 Mbit/s nopeuksilla käytetään CCK-modulointia. OFDM-modulaatiotekniikkaa käytetään eri datanopeuksilla aina 54 Mbit/s asti.

Standardin suuri suosio on aiheuttanut ongelmia käytön ja tiheyden kanssa etenkin tiheästi asutuilla seuduilla. Häiriöiden vähentämiseksi Euroopassa on käytössä neljä ei-päällekkäistä, 20 MHz välein olevaa kanavaa. USA:ssa ja muissa maissa on käytössä kolme kanavaa 25 MHz välein toisistaan. [5.]

## 2.5 IEEE 802.11n

802.11n-protokolla tarjoaa useita parannuksia fyysisessä kerroksessa ja MAC-alikerroksessa, joista on suuria hyötyjä langattomassa tiedonsiirrossa. Tärkeimmät parannukset ovat:

- Multiple-input multiple-output –tekniikka. MIMO hyödyntää signaalien monimuotoisuutta sekä kahdentumista käyttämällä useita lähetys- ja vastaanottoantenneja. MIMO parantaa myös luotettavuutta ja bittinopeutta.
- 40 MHz:in toiminta liittää viereiset kanavat toisiinsa kanavien väleihin varatun tilan kanssa ja tuplaten datanopeuden. Tämä myös parantaa bittinopeutta MIMO-tekniikan lisäksi.
- Kehysten kokoaminen vähentää 802.11-overheadia sulauttamalla paketteja toisiinsa. Parannus varmistaa myös sen, että isompi määrä korkeammasta bittinopeudesta on ohjelmien käytettävissä. Tästä aiheutuu parempi suoritusteho.
- Taaksepäin yhteensopivuus sallii aikaisempia 802.11a/b/g/n-laitteiden olemassaolon ja antaa käyttäjille mahdollisuuden päivittää laitteistoaan ajan kanssa. Toisin sanoen aiempia verkkoja on yksinkertaisempaa päivittää uutta protokollaa tukevaksi.

Lopullinen 802.11n -protokolla ei eronnut suuresti aikaisemmasta, laajemmin hyväksytystä draft 2.0 –versiosta. Käyttäjät, jotka ovat hankkineet draft 2.0 -laitteita, voivat jatkaa entisten laitteiden käyttöä ilman laitteistojen tai ohjelmistojen uusimisia. [7.]

### *2.5.1 MIMO*

MIMO on yksi tärkeimmistä 802.11n–protokollan tarjoamista parannuksista. Sen avulla mahdollistetaan parempi luotettavuus ja saavutetaan suurempia nopeuksia kuin 802.11a/b/g–protokollia käyttämällä samassa radio-spektrissä.

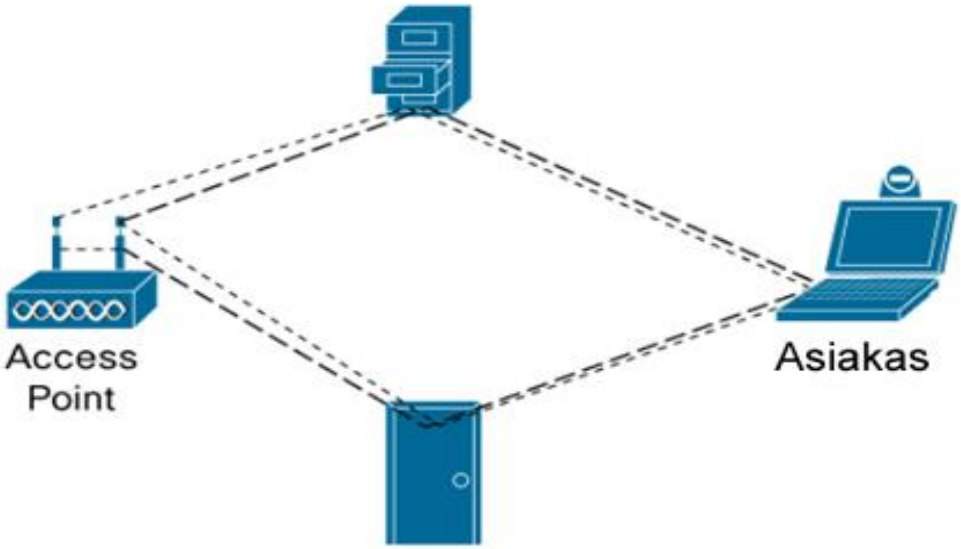
Normaaleissa single-input single-output -yhteyksissä (SISO) radiosignaalin siirtämän informaation mahdollinen määrä riippuu siitä, kuinka paljon vastaanotetun signaalin voimakkuus ylittää kohinan voimakkuuden vastaanottimessa. Parempi signaalikohinasuhde mahdollistaa suuremman informaatiomäärän siirtämisen signaalissa ja paremman mahdollisuuden signaalin vastaanottamiseen. Korkeammalla signaalikohinasuhteella on mahdollista vähentää verkosta löytyviä kuolleita kohtia sekä ylläpitää haluttua datanopeutta ympäristön vaikutuksen vähentyessä.

Kun alhaisin haluttuun datanopeuteen riittävä signaalikohinasuhde on saavutettu, kaikki ylimääräinen saavutettu SNR on lisähyötyä. Tämän avulla voidaan parantaa datanopeutta, kasvattaa signaalin kantomatkaa tai kumpaakin. [7.]

### *2.5.2 Monitie-eteneminen MIMO-tekniikassa*

Sisätiloissa WLAN-tekniikkaa käytettäessä on harvinaista, että radiosignaali siirtyisi suorinta ja lyhintä mahdollista reittiä. Sisätiloissa lähettimen ja vastaanottimen välillä on harvoin suoraa näköyhteyttä ja kaikki esteet näiden välillä heikentävät siirrettävää signaalia.

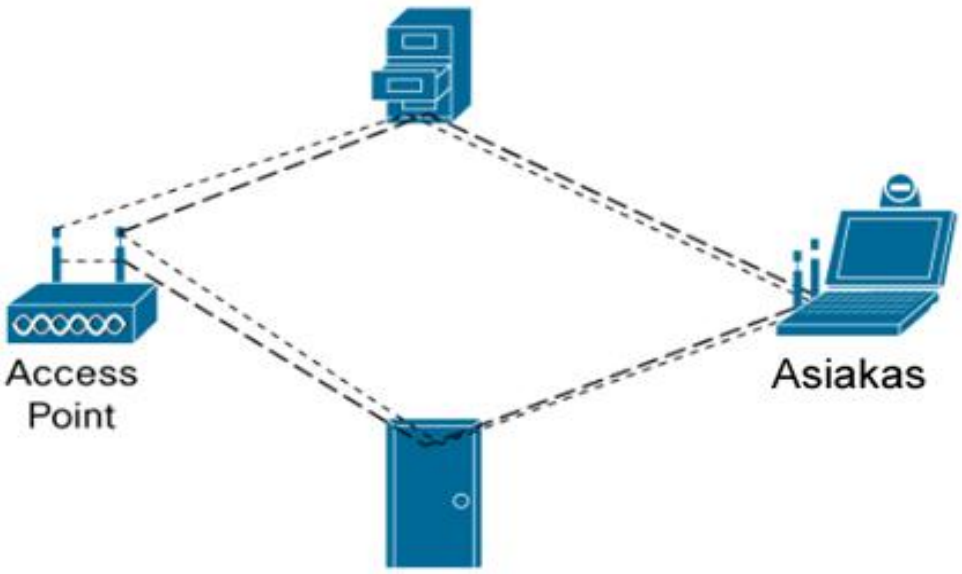
Suurin osa ympäristön pinnoista kuitenkin heijastaa radiosignaaleja. Samaan aikaan lähteneet signaalit saapuvat vastaanottimeen eri suunnista ja eri aikaan riippuen kulkemansa matkan pituudesta, eli kyseessä on monitie-eteneminen. SISO-yhteyksissä signaalien väliset viiveet aiheuttavat vastaanotetun signaalin muuttumista, koska erivaiheiset signaalit häiritsevät toisiaan.




*Kuva 1. Monitie-eteneminen* [7.]

MIMO-tekniikkaa käytettäessä radiolaite lähettää useita signaaleja samaan aikaan ja käyttää monitie-etenemistä hyödykseen. Eri signaalit voivat olla lähes samankaltaisia, jolloin voidaan parantaa luotettavuutta tai ne voivat sisältää täysin eri informaatiota, jolloin yhteyden suorituskyky paranee. Yksinkertaisimmillaan jokainen signaali lähetetään käyttäen omaa antennia. Jokainen antenni vastaanottaa eri signaalia, ja eri signaalit yhdistetään keskenään. MIMO siis tarjoaa kolme tärkeää ominaisuutta:

- mahdollisuuden käyttää useita lähetysantenneja parantaakseen signaalikohinasuhdetta vastaanottimessa
- mahdollisuuden käyttää useita vastaanottoantenneja parantaakseen signaalikohinasuhdetta vastaanottimessa (tunnetaan nimellä MIMO-ekvalisaatio)
- mahdollisuuden lähettää kahta tai useampaa signaalia samanaikaisesti käyttäen samaa spektriä. Jokaista siirrettyä signaalia kutsutaan spatiaaliksi virraksi ja tapaa lähettää useita spatiaaleja virtoja samalla taajuuskaistalla kutsutaan nimellä Spatial Division Multiplexing (SDM). 802.11n mahdollistaa maksimissaan neljän spatiaalin virran käytön.




*Kuva 2. Spatial Division Multiplexing* [7.]

MIMO-linkit kuvaavat, miten yksi laite lähettää informaatiota toiseen laitteeseen. Parametreina ovat lähetysantennien lukumäärä langattomassa tukiasemassa ja vastaanottoantennien lukumäärä asiakkaan päässä. Jokainen antenni mahdollistaa yhden spatiaalisen datavirran, joten 802.11n mahdollistaa parhaimmillaan 4x4–konfiguraation käytön.

802.11n määrittelee joukon erilaisia tiedonvälitysvaihtoehtoja riippuen MIMO-linkissä olevien lähetys- ja vastaanottoantennien lukumääristä. Osaa antenneista käytetään SDM:ää varten. Jos kaikkia antenneja ei vaadita multipleksaukseen, niitä voidaan käyttää parantamaan yhteyden signaalikohinasuhdetta. Huomattavia parannuksia saadaan aina 2x3- tai 3x2–konfiguraatioon asti, mutta tästä eteenpäin muutokset eivät ole enää suuria. [7.]

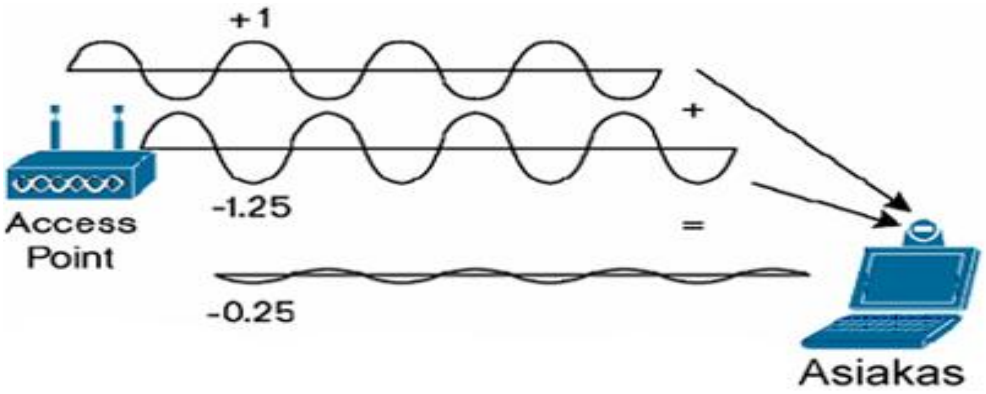
### *2.5.3 Signaalikohinasuhdetta parantavat tekniikat*

Kun käytettävissä on useampia lähetysantenneja kuin spatiaaleja datavirtoja, MIMO-linkin signaalikohinasuhdetta voidaan parantaa muutamalla eri tekniikalla. Tekniikoita ovat

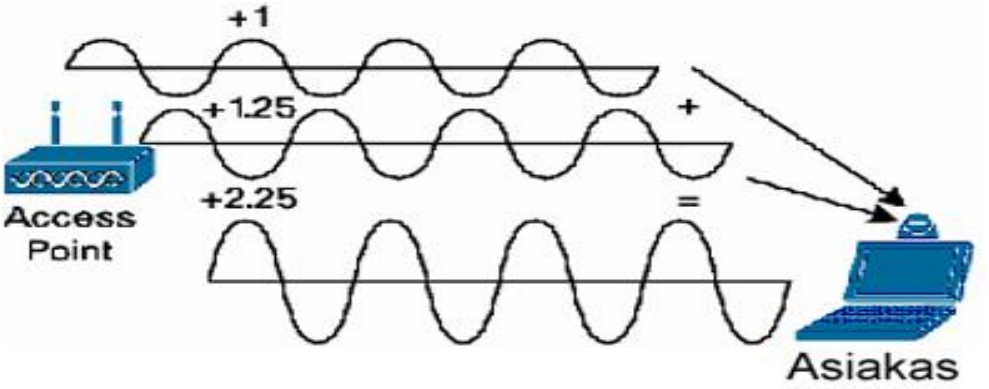
- transmit beamforming
- Space Time Block Coding (STBC)
- spatial expansion
- antennien valinta.

Transmit beamforming

Kun käytössä on useampi lähetysantenni, jokaisen antennin lähettämä signaali asetetaan vastaanottimessa siten, että vastaanotetun signaalin laatu paranee huomattavasti. Vastaanotetut signaalit saapuvat vastaanottimeen eri aikaan ja eri vaiheisina, koska ne matkaavat eri pituisia matkoja. Eri vaiheiset vastaanotetut signaalit heikentävät vastaanotetun signaalin kokonaisvoimakkuutta. Kun signaaleja säädetään lähettimessä, vastaanotetun signaalin voimakkuus voidaan maksimoida parantaen signaalikohinasuhdetta. Transmit beamforming tekee tämän jokaiselle signaalissa olevalle yksittäiselle alikantoaallolle.




*Kuva3. Tuhoava häiriö* [7.]




*Kuva 4. Transmit beamforming käytössä* [7.]

Jotta menetelmä toimisi, sekä langattoman tukiaseman sekä asiakaslaitteen tulee kummankin tukea samoja asetuksia. Menetelmä ei voi toimia, jos lähettimellä ei ole tietoa vastaanottimen vastaanottamasta signaalista. 802.11n-laajennukseen onkin standardoitu protokolla näitä tiedonsaanti-menetelmiä varten.

Transmit beamforming on tärkein menetelmä parantaa datanopeutta lähetettäessä dataa yhteen vastaanottimeen. Lähetettyjen signaalien vaiheita ei voida säätää suotuisimmiksi, jos kyseessä on yleis- tai ryhmälähetys. Menetelmä ei kasvata langattoman tukiaseman peittoaluetta, koska tämän määrittelee tukiaseman mahdollisuus vastaanottaa yleisesti lähetettyjä signaaleja. [7.]

Space Time Block Coding (STBC)

Menetelmä jakaa lähetettävän datan lohkoihin ja jakaa lohkot kahdeksi datavirraksi. Kumpikin datavirta lähetetään käyttäen omaa antennia. Toisen antennin datavirrassa lohkot on järjestelty uudelleen. Koska sama informaatio lähetetään kahteen kertaan, data voidaan vastaanottaa luotettavammin.

Jokainen datalohko lähetetään kahteen kertaan käyttäen eri antennia, jolloin hyödynnetään suurin mahdollinen signaalien vaihtelevuus. Tämä menetelmä

laskee datanopeuden puoleen, mutta tarjoaa paremman mahdollisuuden vastaanottaa signaalin oikein, koska vastaanottimen käytössä on monta eri versiota lähetetystä signaalista. Menetelmä siis yhdistää kaikki vastaanotetut signaalit siten, että niistä on mahdollista saada suodatettua niin paljon informaatiota kuin mahdollista. STBC-menetelmää voi käyttää sekä täsmälähetyksissä että yleis- ja ryhmälähetyksissä. [7.]

Spatial Expansion

Menetelmää käytetään, jos käytössä on vähän spatiaaleja datavirtoja ja useita lähetysantenneja. Tällöin tarkoituksena on estää tahaton tiedonvälitys satunnaisiin suuntiin, joka tapahtuu normaalisti, kun signaalit jaetaan usealle eri antennille.

Menetelmässä lähetetään alkuperäisen signaalin kopioita eri antenneista. Lähetetyt signaalit ovat niin kaikuja alkuperäisestä lähetetystä signaalista ja menetelmä toimii parhaiten ympäristöissä, joissa ei ole pitkiä, monitie-etenemisestä johtuvia kaikuja vaan vähän lyhyitä kaikuja. Menetelmä luo suurempaa vaihtelua yksittäisille alikantoaalloille, jolloin eri alikantoaaltojen kokonaisvaihtelu tasoittuu.

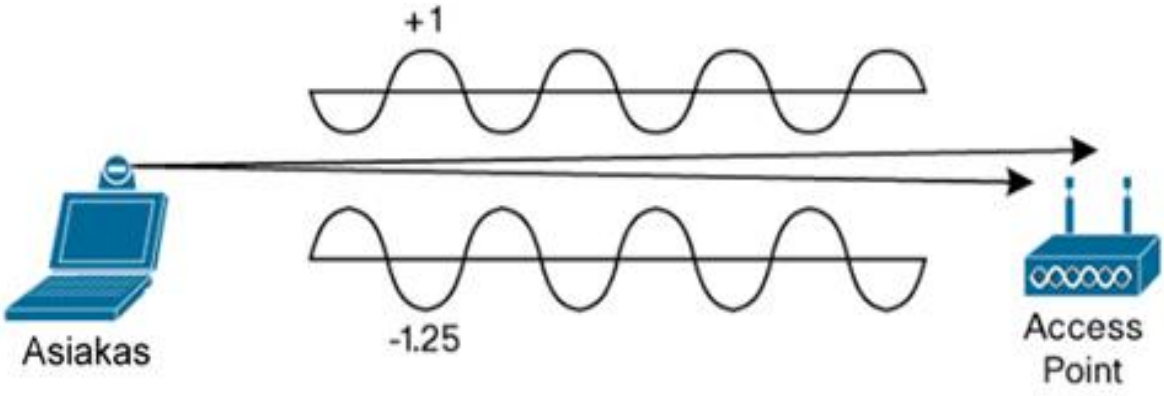
Koska menetelmällä ei lähetetä lisäinformaatiota, se parantaa pelkästään signaalikohinasuhdetta.

Antennin valinta

Menetelmää käytetään eniten 802.11a/b/g–standardeja tukevissa langattomissa tukiasemissa. Näissä on useimmiten vain yksi RF-ketju, joten useita antenneja vaativat menetelmät eivät näissä laitteista paranna nopeutta tai signaalikohinasuhdetta. Menetelmässä valitaan vain millä antennilla olisi parastaa lähettää informaatiota asiakkaalle. Antennin valinta ei optimoi itse signaalia millään lailla vaan sillä valitaan pelkästään paras reitti tiedonvälitykselle. [7.]

### *2.5.4 MIMO-ekvalisaattori*

MIMO-ekvalisaattori mahdollistaa vastaanottimessa eri antennien vastaanottamien signaalien yhdistämisen. Yhtä vastaanottoantennia käytettäessä saapuvat signaalit voivat häiritä toisiaan niin paljon, että ne kumoavat toisensa. Jos käytössä on toinen vastaanottoantenni, käytettävä signaali on mahdollista vastaanottaa suuremmalla varmuudella. Menetelmää kutsutaan myös nimellä spatiaalinen vaihtelevuus ja se tarjoaa parannuksia signaalikohinasuhteeseen. MIMO-ekvalisointi on tapa parantaa langattoman tiedonsiirron luotettavuutta ja ennakoitavuutta. [7.]




*Kuva 5. MIMO-vastaanotin haravoimassa useaa signaalia* [7.]

### *2.5.5 Spatial Division Multiplexing (SDM)*

Useiden antennien käyttö yhdistettynä SDM:ään tarjoaa mahdollisuuden käyttää jokaista spatiaalia datavirtaa kuljettamaan omaa informaatiota. Tämän avulla saavutetaan suuria nopeuden kasvuja. Aikaisemmat 802.11a/b/g–standardit sallivat vain yhden spatiaalin datavirran lähetyksen samanaikaisesti.

Käytettäessä SDM-tekniikkaa kahteen datavirtaan linkissä tarvitaan vähintään kaksi lähetys- ja vastaanottoantennia. Käyttämällä kahta lähetys- ja vastaanottoantennia on mahdollista tuplata linkin datanopeus, mutta

maksiminopeuden saavuttamisesta tulee hankalampaa mitä useampia spatiaaleja virtoja käytetään. Tällöin vaaditaan korkeaa signaalikohina-suhdetta, joten laitteiden välisten etäisyyksien tulee olla lyhyemmät, jotta muiden laitteiden lähetykset eivät haittaisi yhteyttä. [7.]

### *2.5.6 802.11n-standardin parannukset radiotekniikkaan*

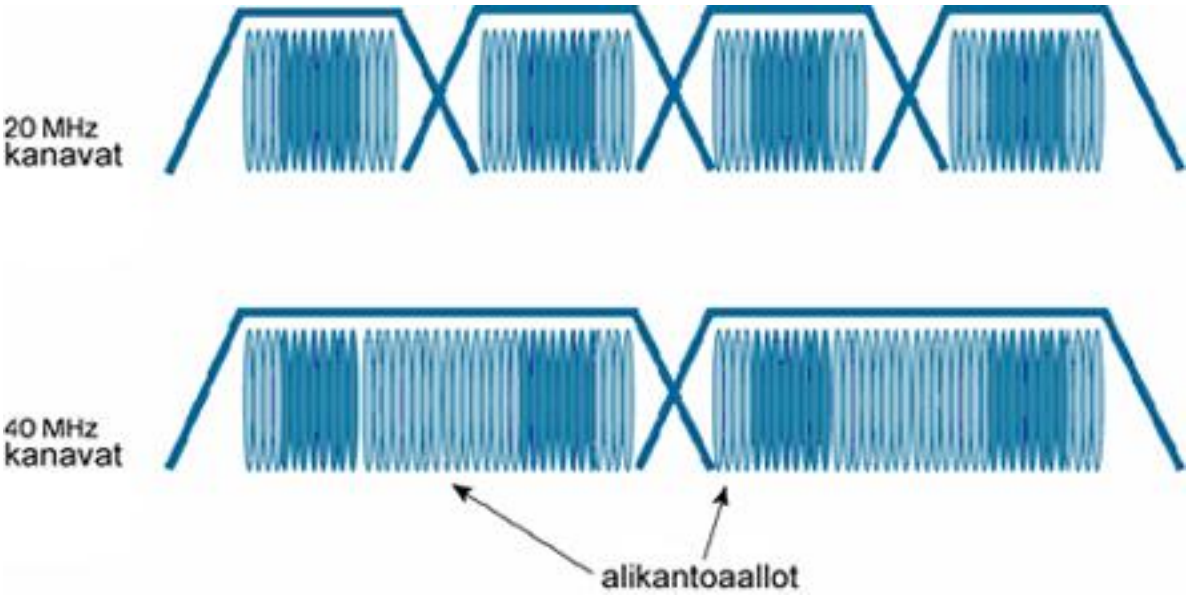
MIMO-tekniikan lisäksi 802.11n tekee useita muita muutoksia radiotekniikkaan, jotta langattomien lähiverkkojen suoritusteho parantuisi. Tärkeimmät muutokset ovat kasvattu kanavan leveys, korkeammat modulointinopeudet ja vähentynyt overhead.

#### 20 ja 40 MHz:n kanavat

Alkuperäinen 802.11-standardi sekä 802.11b-laajennus käyttävät 22 MHz:n levyisiä kaistoja ja jokaisten radiokanavien välit ovat 25 MHz. 802.11a ja 802.11g kumpikin käyttää 20 MHz:n levysiä kaistoja. Koska 802.11g-standardi on laajennus aiempiin standardeihin. Myös 802.11g asettaa radiokanavansa 25 MHz:n välein. Datan suhde kaistanleveyteen on tärkeä mittasuhde mitatessa radioyhteyden tehokkuutta. Tätä suhdetta kutsutaan spektritehokkuudeksi ja sitä mitataan laskemalla sekunnissa siirtyvien bittien määrä suhteessa taajuuteen. Käyttäen samaa tekniikkaa kuin 802.11a ja 802.11g -standardeissa jotkin alkuperäiset WLAN-järjestelmät voivat saavuttaa 108 Mbps nopeuksia. Nämä järjestelmät voivat tuplata nopeutensa käyttämällä kahta eri kanavaa samanaikaisesti. Tätä kutsutaan kanavaliitokseksi. Tällä menetelmällä spektritehokkuus on sama kuin alunperin, mutta kanavan taajuuskaista on tuplaantunut 40 MHz:iin. Tämä on yksinkertainen menetelmä datanopeuden tuplaamiseksi.

802.11n käyttää sekä 20 MHz:n että 40 MHz:n kanavia. Myös tässä standardissa 40 MHz:n kanavat ovat kaksi vierekkäistä 20 MHz:n kanavaa liitettynä yhteen. 802.11n-standardi hyödyntää 20 MHz:n kanavien alussa ja lopussa olevaa pientä tyhjää tilaa, jotka ovat olemassa vierekkäisten

kanavien häiriöiden vähentämiseksi. Käytettäessä 40 MHz:n kanavia kyseisiä alemman kanavan lopussa olevaa ja ylemmän kanavan alussa olevia tyhjiä tiloja ei tarvita häiriöiden välttämiseksi, vaan näitä tiloja voidaan käyttää tiedonsiirtoon. Tällä tavalla 802.11n saavuttaa vähän yli kaksinkertaisen nopeuden siirtyessään 20 MHz:n kanavista 40 MHz:n kanaviin. [7]




*Kuva 6. 20 MHz:n ja 40 MHz:n kanavat* [7.]

Suuremmat modulointinopeudet

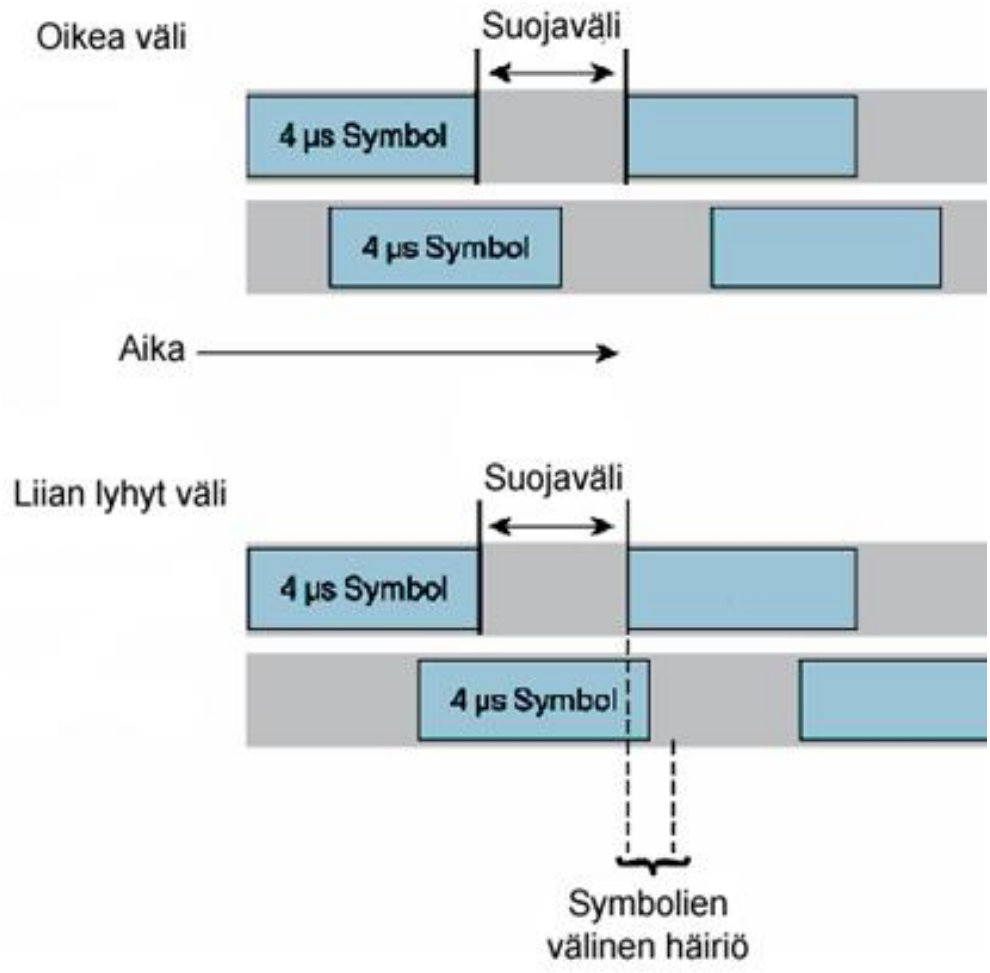
802.11a- ja 802.11g-standardit ottavat käyttöönsä OFDM-moduloinnin. Tämä modulointi jakaa radiokanavan suureen määrään pienempiä kanavia, joissa jokaisella kanavalla on oma alikantoaalto. Jokainen alikantoaalto pystyy siirtämään eri informaatiota. 802.11a- ja 802.11g-standardeissa yksi symboli kestää neljä mikrosekuntia, joka sisältää 800 nanosekunnin suojavälin. Korkeimmalla datanopeudella, 54 Mbps, jokainen symboli kuljettaa 216 databittiä. Virheenkorjausbittien kanssa jokainen symboli sisältää 288 bittiä. Jotta näin monta bittiä saadaan pakattua yhteen alikantoaaltoon, alintokantoaalto moduloidaan käyttäen 64-QAM -modulointia.

802.11n-standardi käyttää myös OFDM-modulointia ja samaa symboli-nopeutta, mutta lisää alikaantoaaltojen määrää 20 MHz:n kanavissa 48:sta 52:een. 802.11n tarjoaa vastaanottimelle kahdeksan käytettävää datanopeutta. Näiden muutosten avulla voidaan saavuttaa 65 Mbps nopeus käyttäen yhtä lähetys- ja vastaanottoantennia. Kun MIMO-tekniikan mahdollistamat neljä lähetys- ja vastaanottoantennia otetaan käyttöön, valittavana on 32 eri lähetysnopeutta käyttäen 20 MHz:n levyisiä kanavia. Tällöin teoreettinen maksiminopeus on 260 Mbps.

Kun siirrytään käyttämään 40 MHz:n kanavia, alikantoaaltojen määrä kasvaa 108 kappaleeseen asti. Tällöin teoreettinen maksinopeus kasvaa 540 Mbps asti käyttämällä neljää antennia kummassakin päässä. [7.]

Lyhyempi suojaväli

Jokaisessa OFDM-symbolissa oleva suojaväli on aika, jolla pyritään vähentämään symbolien välisiä häiriöitä. Häiriöt johtuvat symbolien viivästyneistä saapumisista, kun uutta symbolia aletaan vastaanottamaan ennen kuin edellinen symboli on ehditty vastaanottamaan lopullisesti. Tästä aiheutuva häiriö laskee linkin signaalikohinasuhdetta.




*Kuva 7.* Suojavälit [7]

Olosuhteiden salliessa 802.11n-standardissa on mahdollista lyhentää oletuksena käytettävää 800 nanosekunnin suojaväliä 400 nanosekuntiin. Tämä lyhentää symbolin kestoaikaa neljästä nanosekunnista 3,6 nanosekuntiin kasvattaen symbolinopeutta ja samalla tietenkin myös datanopeutta. Tämän muutoksen avulla voidaan saavuttaa suuremmat 288 Mbps nopeus käyttäen 20 MHz:n kanavia ja 600 Mbps nopeus käyttäen 40 MHz:n kanavia. [7.]

### *2.5.7 MAC-kerroksen muutokset*

Tarvitaan myös muita muutoksia, joita pelkkä datanopeuden kasvatus ei tarjoa. OSI-mallin siirtokerroksen alla oleva MAC-alikerros määrittelee muun muassa vuoronvarauksen ja kehysten väliset ajat. Alikerroksen protokolla sisältää ylimääräistä aikaa, joka kuluu tietojen käsittelyyn (overhead). Tähän kuuluvat niin kehysten välit ja jokaisesta kehyksestä lähetetyt kuittaukset. Suurimmilla nopeuksilla pelkästään tämä ylimääräinen aika voi olla pidempi kuin yhden datakehyksen kesto.

Kehyksien yhdistämisellä voidaan vähentää overhead yhdistämällä kaksi tai useampi kehys yhdeksi lähetykseksi. Kun useat kehykset lähetetään yhdessä lähetyksessä, kehysten mahdolliset törmäykset ja kehysten selvittelyihin kuluvat ajat lyhenevät. 802.11n kasvattaa tätä menetelmää käyttämällä kehysten kokoa moninkertaisesti.

Menetelmällä on myös rajoituksia. Kaikki lähetykseen yhdistetyt kehykset tulee lähettää samaan sijaintiin. Kaikki lähetettävät kehykset tulee myös luonnollisesti lähettää samaan aikaan, josta saattaa syntyä viivettä. Myös lähetettävän kehyksen maksimikoko määrittyy sen mukaan, kuinka nopeasti lähetin ja vastaanotin liikkuvat toisiinsa nähden.

Kun kehyksien yhdistäminen ei ole mahdollista, 802.11n tarjoaa menetelmän lähettää kehyksiä yhtenä virtana samaan päämäärään. Tämä menetelmä lyhentää välitettyjen kehyksien välisiä aikoja. 802.11e -laajennuksessa määritellään vastaavanlainen kyky, mutta 802.11n parantaa tätä menetelmää lyhentämällä kehysten välistä aikaa entisestään. Aika, jolloin kehyksiä on mahdollista lähettää, kasvaa, kun kehyksien välisiä tyhjiä hetkiä lyhennetään. [7.]

### *2.5.8 802.11n yhteenveto*

- Parempi signaalikohinasuhde parantaa tiedonsiirron luotettavuutta, koska vaaditaan suurempaa häiriötä pilaamaan lähetykset. Myös suurempi käyttäjätiheys on tällöin sallittu.
- Kun käytetään MIMO-tekniikkaa ja useampia antenneja yhteyden kuuluvuusaluetta saadaan parannettua ja katvealueita vähennettyä.
- Spatial Division Multiplexing, 40 MHz:n kanavat ja lyhennetty suojaväli parantavat datanopeutta verrattuna aiempiin standardeihin.
- Parannukset 802.11-MAC-alikerroksessa tarjoaa paremman suoritus-kyvyn suurilla nopeuksilla. [7.]

| 802.11 standardi | Taajuus (GHz) | Kanavan leveys (MHz) | Mahdolliset datanopeudet | MIMO-virtoja | Käytetty modulaatio |
|---|---|---|---|---|---|
| - | 2.4 | 20 | 1 ja 2 | 1 | DSSS |
| a | 5<br>3.7 | 20 | 6, 9, 12, 18, 24, 36, 48 ja 54 | 1 | OFDM |
| b | 2.4 | 20 | 1, 2, 5.5 ja 11 | 1 | DSSS |
| g | 2.4 | 20 | 1, 2, 6, 9, 12, 18, 24, 36, 48 ja 54 | 1 | OFDM ja DSSS |
| n | 2.4 ja 5 | 20<br>40 | 15, 30, 45, 60, 90, 120, 135 ja 150 | 4 | OFDM |

*Kuva 8. 802.11 –standardit* [6]

## 2.6 Muita IEEE-standardeja

802.11 LMSC -ryhmä on julkaissut muitakin valmiita tai kehitteillä olevia standardeja. Näitä ovat muun muassa

- 802.11d, joka sisältää uusia kenttiä tukiasemien levitysviesteihin, joilla kerrotaan laitteen sijaintimaa. Tämän avulla langaton laite osaa valita itse käytettävän taajuuskaistan, jota kyseisen tukiaseman on luvallista käyttää.
- 802.11e, joka sisältää toimintoja verkon palvelunlaadun (Quality of Service) parantamiseksi. Tämän avulla tukiasemat voivat priorisoida liikennettä, jotta halutun lähetyksen odotusaika on pienempi mikä vähentää viivettä näiden tukiasemien kautta.
- 802.11h, joka sisältää muutoksia 5 GHz:n taajuusaluetta käyttäville laitteille Euroopassa. Laajennus sisältää myös tuen älykkäämmällä taajuusalueen vaihdolle, jos kanavalla esiintyy runsaasti häiriötä sekä tuen langattomien laitten virransäästöominaisuuksille. [2.]
- 802.11j, joka sisältää erityisesti Japania koskevia määrityksiä. Laajennuksella sallitaan langattoman lähiverkon käyttö 4.9 – 5 GHz:n välisellä taajuusalueella, jotta standardi noudattaisi paremmin Japanissa määrättyjä sääntöjä koskien radiotaajuuksien käyttöä.
- 802.11k, joka sisältää määrittelyt radioresurssien ylläpitoa varten. Laajennus määrittelee ja paljastaa radio- ja verkkoinformaation, jotta mobiilin langattoman lähiverkon hallinnointi ja ylläpito on helpompaa.
- 802.11r, joka sallii liikkellä olevien langattomien laitteiden jatkuvan kommunikoinnin. Tämä saadaan aikaan käyttämällä nopeita ja turvallisia kanavanvaihtoja tukiasemasta toiseen.
- 802.11w, joka sisältää määrityksiä kasvattamaan hallinnointiin käytettävien kehysten turvallisuutta.
- 802.11y, joka sallii suuritehoisten Wi-Fi –laitteiden toimimisen 3650-3700 MHz:n taajuuskaistalla Yhdysvalloissa. [6.]

# 3 WLAN-LAITTEET

Langattomat lähiverkot koostuvat useimmiten seuraavista rakenteellisista komponenteista.

## 3.1 Päätelaite

Päälaite on langaton laite, jolla voidaan liittyä WLAN-verkkoon. Päätelaite on useimmiten asiakkaan tietokone tai matkapuhelin, mutta kaikki langattomat IEEE 802.11 –standardia hyödyntävät laitteet voivat toimia päätelaitteina. Nykyään myös tulostimet ja muut kuluttajatuotteet voivat liittyä osaksi langatonta lähiverkkoa. [8, 2.2.]

## 3.2 Access Point – yhteyspiste (AP)

Yhteyspisteet toimivat langattomien lähiverkkojen tukiasemina. Ne lähettävät majakkasanomia tietyin väliajoin, jolloin yhteyspisteiden kantoalueilla olevat laitteet voivat havaita niiden olemassaolon. Päätelaitteet tunnistavat yhteyspisteet niiden välittämien Service Set Identifier –tunnusten (SSID) perusteella, jolloin he tietävät mihin verkkoon yhteyspisteen kautta voi olla mahdollista päästä.

Yhteyspisteet toimivat langattomien ja langallisten verkkojen välisinä siltoina, joiden avulla langattomien laitteiden on mahdollista päästä käsiksi saman verkon langalliseen osaan. Yhteyspisteet voivat myös yhdistää langattomia päätelaitteita toisiinsa. Yhteyspisteet voivat myös hoitaa päätelaitteiden tunnistuksen niille määritellyillä tunnistusmenetelmillä ja voivat täten myös estää tuntemattomien laitteiden pääsyn verkkoon. [9, s. 131 – 136.]

## 3.3 Sillat

WLAN-silloilla voidaan yhdistää kaksi tai useampi lähiverkko toisiinsa langattomasti, joiden välillä ei muuten olisi yhteyttä. Koska langattomien lähiverkkojen väliset etäisyydet voivat olla suurempia, silloissa käytetään erillisiä antenneja lähiverkkojen yhdistämisiä varten. Lähiverkkojen välinen etäisyys tulee kuitenkin olla vain muutama kilometri ja suunta-antennien välillä tulee olla näköyhteys.

Siltaparit tulee määrittää käyttämään samoja yhteys- ja salausasetuksia, jotta yhdistäminen olisi mahdollista. Yksi silloista tulee myös määrittää juurisillaksi (root bridge), jotta yksi tai useampi muu silta tietää, mihin niiden tulee yhdistää. [9, s. 175-178.]

## 3.4 WLAN-kontrolleri

WLAN-kontrollerit (WLC) on kehitetty helpottamaan ja nopeuttamaan suurien verkkojen hallinnointia. Kun verkko kasvaa suureksi ja yhteyspisteitä on runsaasti, eri yhteyspisteiden ylläpito ja asentaminen käy työlääksi. WLC helpottaa verkon hallinnointia ottamalla aiemmin yhteyspisteiden hoitamat autentikointi- ja assosiointitoimenpiteet hallintaansa. Tällaisessä ympäristöissä yhteyspisteitä kutsutaan nimellä Lightweight Access Point (LAP) ja LAP:t välittävät kaikki hallinnointia ja dataa sisältävät paketit suoraan kontrollerille. WLC siis hoitaa pakettien vaihdannan langattomien päätelaitteiden ja verkon muun osan välillä. LAP:t toimivat tällöin vain pelkkinä liitäntäpisteinä verkkoon pääsyä varten. LAP:eiden ylläpito ja asennus helpottuu, koska jokainen WLC:hen rekisteröity LAP lataa vaadittavat asetukset suoraan kontrollerilta. [10.]

### *3.4.1 Lightweight Access Point Protocol (LWAPP)*

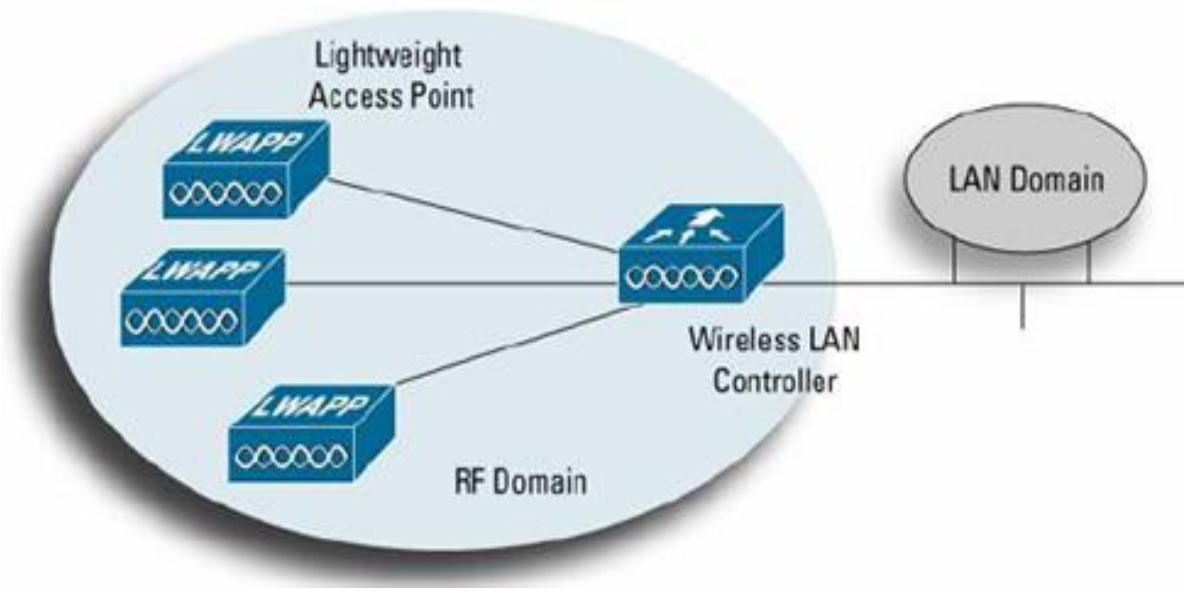
LWAPP-protokollaa alettiin kehittää, jotta eri valmistajien laitteet pystyisivät kommunikoimaan keskenään tehokkaammin ja joustavammin. LWAPP-protokolla standardisoi yhteyspisteiden ja WLAN-laitteiden välisen tiedonvälitysprotokollan. Protokollan tarkoituksena on

- vähentää yhteyspisteissä tapahtuvaa tiedonkäsittelyä, jolloin yhteyspisteen prosessointitehoa kyetään käyttämään tehokkaammin verkkoon pääsyn hallintaan.
- mahdollistaa keskityn järjestelmän liikenteen käsittelyyn, autentikointiin ja salaukseen.
- tarjota yleisen salaus- ja siirtotekniikan eri valmistajien laitteille.

Protokollan avulla on mahdollista suunnitella verkot laitteiden kapasiteettien pohjalta ilman, että verkkoa suunnitellessa tarvitsee pohtia laitteiden yhteensopivuuksia. LWAPP tarjoaa myös turvalliset verkkopalvelut OSI-mallin toisella ja kolmannella kerroksella, vaikka käytössä olisi eri valmistajien laitteita.

LWAPP-protokollan käyttö mahdollistaa seuraavia toimintoja:

- yhteyspisteiden havainnointi, informaation vaihto ja konfigurointi
- yhteyspisteiden varmennus ja ohjelmiston hallinta
- datapakettien kapselointi, jakaminen ja alustus
- yhteyspisteen ja päätelaitteen välisen kommunikoinnin kontrollointi ja hallinnointi.




*Kuva 9. WLAN-kontrolleri keskitettynä yhteyksien ja oikeuksien hallinnoijana* [10]

### *3.4.2 LWAPP-protokolla toiminnassa*

Protokolla esittelee käsitteen ”jaettu-MAC”, joka tarkoittaa kykyä erotella 802.11–protokollan osia reaaliajassa. Käytännössä tämä tarkoittaa, että yhteyspisteet voivat käsitellä tiettyjä MAC-hallinnointia sekä verkkoon-

pääsyjä ja WLAN-kontrollerit hoitavat autentikointia sekä suojausten ylläpitoa samaan aikaan.

LWAPP-protokolla mahdollistaa useita parannuksia. Protokolla parantaa hallinnointia tarjoamalla yhden käyttöliittymän, jolla voidaan hallinnoida suuren verkon käytäntöjä ja suojauksia. Hallinnoinnin avulla kaikille verkon laitteille voidaan helposti asettaa haluttuja asetuksia. Protokolla helpottaa yhtenäisten suojausasetusten asettamista laitteisiin. Protokollan avulla voi myös helposti havaita ja estää verkkoon kohdistuneita hyökkäyksiä. LWAPP:ta käytettäessä verkkojen toiminta nopeutuu ja tämä nopeuttaa myös verkosta toiseen liittymistä. Verkonhallinnoinnin nopeutuminen parantaa myös reaaliaikaisten sovellusten toimimista kyseisessä verkossa. [11.]

### *3.4.3 Control and Provisioning of Wireless Access Points protocol (CAPWAP)*

Uudemmissa kontrollereissa käytetään CAPWAP-protokollaa, joka pohjautuu aiempaan LWAPP-protokollaan. Vaikka yhteyspisteet käyttäisivät LWAPP-protokollaa, yhteyspisteet voivat havaita ja yhdistää CAPWAP-protokollaa käyttäviin WLAN-kontrollereihin, eli kumpaakin protokollaa käyttäviä laitteita voidaan käyttää samassa verkossa. [10.]

# 4 WLAN-VERKKOMALLIT

IEEE 802.11 –standardi määrittelee kaksi erilaista verkkomallia.

## 4.1 Ad Hoc –verkkomalli

Ad Hoc –yhteys tunnetaan myös nimellä peer-to-peer-verkko. Tässä mallissa kahden tai useamman päätelaitteen kommunikointi tapahtuu suoraan näiden päätelaitteiden välillä eikä kommunikointiin tarvita laitteiden välisiä langattomia tukiasemia.

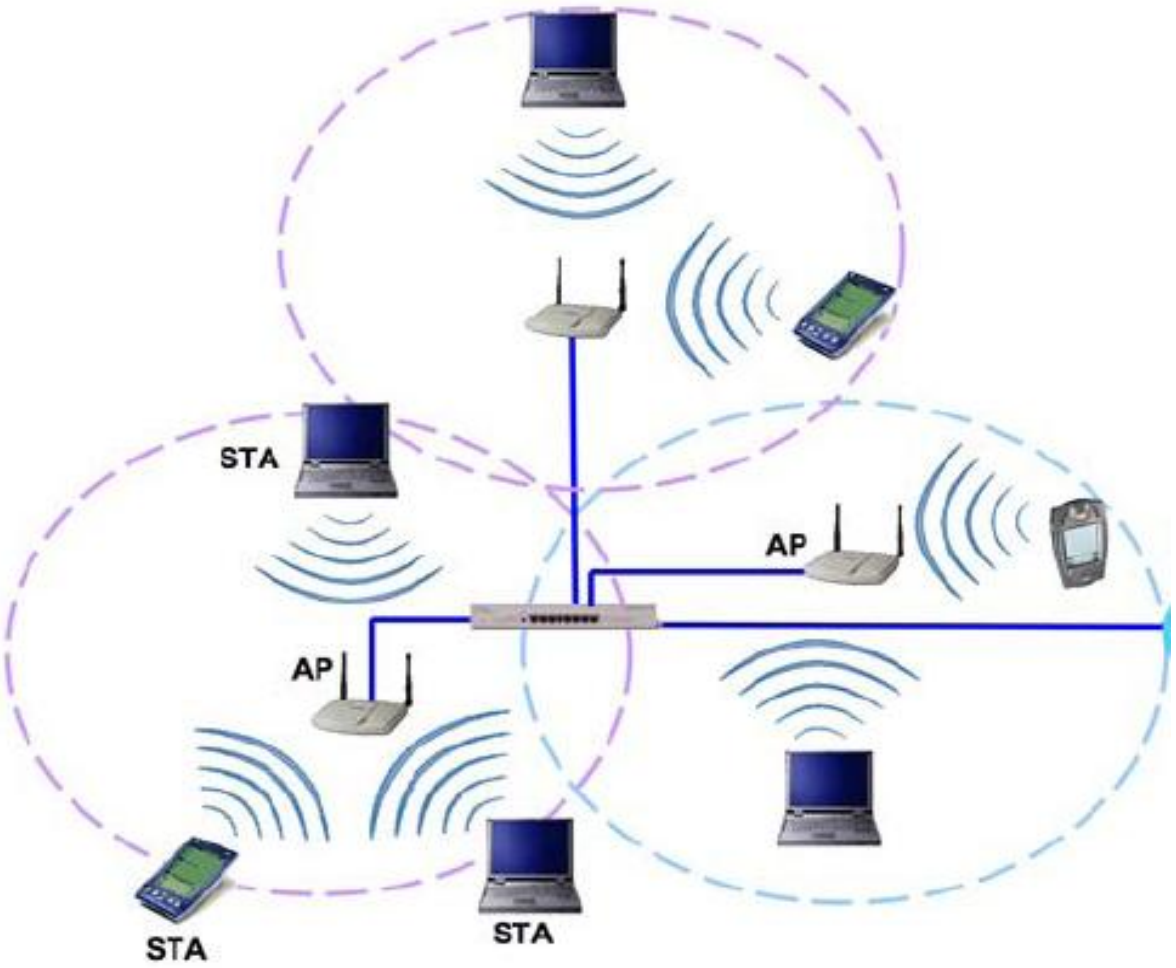

*Kuva 10. Ad Hoc –verkko* [8]

Kuvan ympyrä esittää Ad Hoc –verkon kantoaluetta, jonka sisällä laitteet kommunikoivat keskenään. Laitteiden tulee pysyä toistensa kantamien alueella, jotta laitteiden havainnointi ja niiden välinen kommunikointi on mahdollista. Ad Hod –malli ei määrittele roaming-mahdollisuutta, joten päätelaitteet eivät voi siirtyä toisen verkon alueelta toiselle yhteyden aikana.

Ad Hoc –verkon etuna on, että niitä voidaan luoda periaatteessa koska tahansa käyttäjien tarpeen mukaan. Haittapuolena on kuitenkin, että Ad Hoc –verkko ei voi kommunikoida ulkopuolisen verkon kanssa. [8, 2.2.1]

## 4.2 Infrastruktuuri-verkko

Infrastruktuuriverkossa WLAN-verkko koostuu yhdestä tai useammasta Basic Service Setistä, jotka ovat WLAN-verkkojen perustana toimivia rakenneosia. Jokainen BSS sisältää yhden AP:n sekä vähintään yhden päätelaitteen. Päälaitteet tunnistavat access pointit niiden lähettämien Service Set Identifierin perusteella, joita AP:t lähettävät yleisviesteinä kantoalueellaan. SSID toimii langattomien tukiasemien ja niihin yhdistyneen verkon tunnistetietona eli nimenä.




*Kuva 11. Infrastruktuuri-verkko* [8]

AP:t yhdistävät päätelaitteet distribution system –järjestelmään, jonka kautta päätelaitteiden on mahdollista olla yhteydessä verkon langallisiin osioihin tai ulkopuolisiin verkkoihin. DS-järjestelmän ja usean BSS:n käyttö antavat mahdollisuuden luoda suurempi verkkoja. Useaa Basic Service Setia käyttävä verkko tunnetaan myös nimellä Extended Service Set.

Päätelaitteet voivat liikkua verkon alueella ja tarvittaessa yhdistää toiseen langattomaan tukiasemaan. Tämä edellyttää sitä, että tukiasemat on asetettu tarpeeksi lähekkäin toisiaan nähden ettei niiden välille muodustu katvealueita. Tämä roaming-ominaisuus mahdollistaa päätelaitteiden liikkumisen verkon alueella ja verkkoyhteyden katkeamattomuuden, vaikka yhden tukiaseman kantoalueelta siirryttäisiin pois. [8, 2.2.2.]

# 5 KÄYTETYT SIIRTOTEKNIIKAT

## 5.1 Direct Sequence Spread Spectrum (DSSS)

DSSS-tekniikassa kantoaaltoa vaihemoduloidaan käyttäen näennäis-satunnaisia tavuja, joilla on paljon lyhyempi kestoaika kuin itse tietoa sisältävillä biteillä. Tämän vuoksi yhtä alkuperäistä bittiä vastaa useamman bitin sarja moduloidussa signaalissa. DSSS-tekniikkaa käyttämällä alkuperäinen signaali lähetetään kertomalla datasignaali kohinasignaalin kanssa. Kohinasignaali on itseasiassa näennäissatunnainen sarja, jonka taajuus on paljon alkuperäistä signaalia korkeampi.

Lähetetty signaali muistuttaa kohinaa, mutta haluttu datasignaali voidaan palauttaa poistamalla kohina. Tämä tapahtuu kertomalla vastaanotettu signaali samalla näennäissatunnaisella sarjalla, jolla kyseinen signaali alunperin luotiin. Jotta palautusprosessi onnistuisi, lähetys- ja vastaanotto-sekvenssien tulee olla synkronoidut. [12.]

## 5.2 Frequency-hopping Spread Spectrum (FHSS)

Taajuushyppelyä käyttämällä signaalin lähetys näyttää tapahtuvan satunnaisilla taajuuskanavilla, eli signaali hyppii kanavalta toiselle tietyin väliajoin. Lähetys tapahtuu kuitenkin muuttamalla signaalin lähetystaajuutta näennäissatunnaisen algoritmin mukaisesti. Signaalin vastaanottaminen onnistuu suorittamalla saman algoritmin mukainen sarja synkronoidusti lähettäjän kanssa. Satunnaislukugeneraattori määrittelee hyppysekvenssin. Tämä sekvenssi on sekä lähettäjän että vastaanottajan tiedossa.

Taajuushyppely voidaan toteuttaa joko hitaalla tai nopealla hyppelyllä. Hitaalla hyppelyllä voidaan lähettää useita bittejä käyttäen samaa taajuutta, kun taas nopealla hyppelyllä lähetetään yhtä bittiä usealla eri taajuudella. [3, s. 251-252.]

### 5.3 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM-tekniikkaa käyttämällä lähetetty signaali levitetään leveämmälle taajuuskaistalle. Tekniikassa käytetään useita eri kantoaaltoja ja käytettävissä oleva spektri jaetaan useaksi kanavaksi, joista jokaisella voidaan lähettää yhtä kantoaaltoa.

Tekniikassa käytetään taajuuskaistaa tehokkaasti hyödyksi asettamalla vierekkäiset kanavat lähemmäksi toisiaan kuin normaalisti. Tämä on mahdollista tekemällä kaikki kantoaallot ortogonaalisiksi toisiinsa nähden, jolloin vierekkäiset kantoaallot eivät häiritse toisiaan. Jokainen kantoaalto käyttää kapeaa taajuuskaistaa, josta johtuen bittinopeus on alhaisempi ja jokaisen lähetettävän bitin kesto on suurempi. Koska koko taajuuskaista hyödynnetään tehokkaasti, tekniikka mahdollistaa suuriakin nopeuksia. [3, s. 255-256.]

## 6 WLAN-TIETOTURVA

### 6.1 Wired Equivalent Privacy (WEP)

WEP oli sisällytettynä alkuperäisessä IEEE 802.11 -standardissa, joka ratifioitiin vuonna 1999. Mekanismi merkattiin vanhentuneeksi salausmenetelmäksi vuonna 2004.

Tavallinen 64-bittinen WEP käyttää 40-bittistä salausavainta, johon lisätään 24-bittinen alustusvektori. Alustusvektori lähetetään aina salaamattomana kehyksen parissa ensimmäisessä bitissä. Koska samaa salausta käytetään kaikissa kehyksissä, verkon salaus on suhteellisen helppo murtaa seuraamalla alustusvektoreita ja laskemalla näiden avulla verkon salattu avain. Käytössä on myös 128- ja 256-bittisiä WEP-järjestelmiä. Näissäkin alustusvektorin pituus on sama, joten vain WEP-avaimen pituus muuttuu.

WEP-tunnistus toteutetaan normaalisti jaetun avaimen menetelmällä. Tunnistustilanteessa päätelaitteen ja yhteyspisteen välillä tapahtuu seuraavanlainen liikennöinti:

- Päätelaite lähettää Authentication Request –pyynnön yhteyspisteelle.
- Yhteyspiste lähettää satunnaisen, salaamattoman haastetekstin päätelaitteelle.
- Päätelaite salaa haastetekstin käyttämällä WEP-avaintaan ja lähettää salatun vasteen takaisin yhteyspisteelle.
- Yhteyspiste purkaa vasteen omalla avaimellaan ja vertaa lähettämäänsä ja purkamaansa tulosta. Jos tulokset ovat samat, tunnistus hyväksytään.

WEP-salaus on suhteellisen helposti murrettavissa, koska alustusvektorit ovat lyhyitä ja kaikki kyseissä verkossa olevat laitteet käyttävät aina samaa määrättyä salausavainta. Nykyään suositellaankin käytettäväksi esimerkiksi turvallisempaa WPA2-salausta. [13.]

## 6.2 Wi-Fi Protected Access (WPA)

WPA kehitettiin korvaamaan WEP-salaus ja korjaamaan tässä esiintyneet heikkoudet, eli WEP:in käyttämät staattiset salausavaimet ja lyhyet alustusvektorit. WPA:ssa tukiaseman ja päätelaitteen välinen liikennöinti salataan käyttäen pakettikohtaisia 128 bitin salausavaimia. Avainparit luodaan muuttuvasti ja pakettikohtaisesti. WPA-salauksessa valvotaan myös pakettien eheyttä, jossa jokainen paketti tarkistetaan mahdollisten muutosten varalta. Tätä tapahtumaa kutsutaan MIC–toiminnoksi (Message Integrity Check).

Kun käyttäjä tunnistautuu verkon käyttäjäksi WPA-salausta käyttämällä, kirjautumispalvelin tai tukiasema luo käyttäjälle yksilöllisen pääavainparin session ajaksi. TKIP-protokolla toimittaa käyttäjälle avaimen, jonka avulla protokolla luo dynaamisesti pakettikohtaiset avaimet kaikille verkkoon

lähetetyille paketeille ja salaa ne. Käyttämällä WPA-salausta saadaan miljoonittain erilaista salausavaimia, joita jokaista voidaan käyttää salaamaan kukin verkossa välitetty paketti. Salausavainta vaihdetaan automaattisesti jokaisen 10 000 paketin välein.

Kun käytetään MIC-toimintoa, lähettäjä ja vastaanottaja laskee jokaiselle paketille tarkistussumman. Tarkistussummia verrataan pakettien eheyden takaamiseksi. Jos tarkistussummat eivät ole samat, paketin oletetaan joutuneen muutoksen kohteeksi ja se hylätään. Jos virheellinen paketti havaitaan, MIC-toiminta voi autentikoida kaikki verkon käyttäjät uudelleen ja estää uudet tunnistautumispyynnöt tietyksi ajaksi. [14.]

### 6.3 Remote Authentication Dial In User Service (RADIUS)

RADIUS-protokolla tarjoaa keskitetyn todennuksen, valtuutuksen ja tilastoinnin (Authentication, Authorization and Accounting, AAA) hallinnan tietokoneille, jotka yhdistävät verkkoon ja käyttävät sen palveluita.

RADIUS on protokolla, jota suoritetaan sovelluskerroksella ja se käyttää UDP:ta siirtoon. RADIUS-palvelimella on kolme funktiota:

- todentaa käyttäjät tai laitteet ennen kuin niille suodaan pääsy verkkoon
- valtuuttaa käyttäjät tai laitteet tietyille verkkopalveluille
- tilastoida palvelujen käyttö.

RADIUS-palvelimet käyttäjät AAA-menetelmää hallinnoidakseen verkkoon pääsyä. Hallinnointi tapahtuu kahdessa eri vaiheessa. [15.]

### *6.3.1 Todennus ja valtuutus*

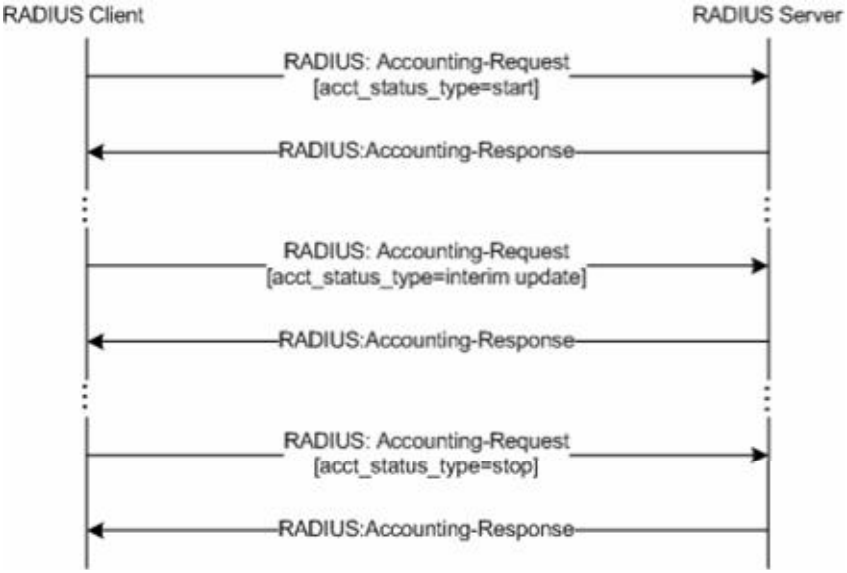
Käyttäjä tai tietokone lähettää pyynnön Network Access Serverille (NAS) saadakseen pääsyn verkon resursseihin. NAS lähettää RADIUS-palvelimelle Access Request –viestin, eli pyytää todennusta käyttäen RADIUS-protokollaa. Pyyntö sisältää pääsyyn vaadittavat tiedot, jotka ovat useimmissa tapauksissa käyttäjätunnus ja salasana. Pyyntö voi sisältää myös muita tietoja käyttäjästä.

RADIUS-palvelin tarkastaa vastaanotettujen tietojen oikeellisuuden ja vertaa käyttäjän lähettämiä tietoja palvelimen tietokantaan tallennettuihin tai ulkoisen tietokannan tietoihin. Palvelin palauttaa yhden kolmesta mahdollisesta vastauksesta NAS:lle:

- Access Reject –käyttäjältä evätään kokonaan pääsy verkkoon. Syynä voivat olla virheelliset tai puutteeliset tunnukset,
- Access Challenge –palvelin pyytää käyttäjältä lisää tietoja yhdistämistä varten kuten esimerkiksi toista salasanaa,
- Access Accept –käyttäjän pääsy verkkoon sallitaan. Palvelin tarkastaa usein käyttäjän valtuudet käyttää sen verkossa pyytämiä palveluja. Käyttäjälle voidaan myös sallia vain osa kaikista mahdollisista palveluista.

### *6.3.2 Tilastointi*

Kun NAS sallii pääsyn verkkoon, RADIUS-palvelimelle lähetetään Accounting Start –viesti, jolla ilmoitetaan käyttäjän verkkoon pääsyn alkaminen. Viesti sisältää käyttäjän tietoja, verkko-osoitteen, verkkoon kytkeymisen sijainnin sekä uniikin istuntotunnisteen.




*Kuva 12. RADIUS-viestien vaihtoa* [15]

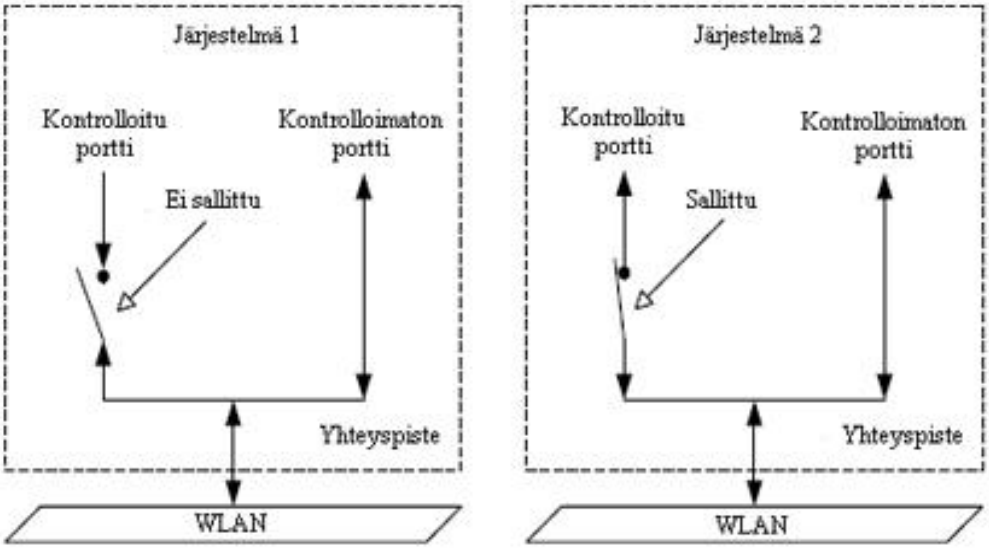
NAS voi lähettää väliajoin päivitysilmoituksen palvelimelle, jolla päivitetään aktiivisen istunnon tietoja. Tietoja ovat istunnon kesto ja käsitellyn datan määrä. Kun käyttäjä katkaisee yhteyden, NAS lähettää palvelimelle ilmoituksen tilastoinnin lopettamisesta. Ilmoitus sisältää lopulliset tiedot istunnon kestosta, siirretystä datasta ja syyn yhteyden katkeamiseen. [15.]

# 7 TIETOTURVALLISUUTTA PARANTAVAT IEEE-STANDARDIT

## 7.1 802.1x

Porttikohtaisella todentamisella voidaan estää luvattomien asiakaslaitteiden pääsy suojattuun verkkoon ja täten estää sitä käyttämästä verkon tarjoamia palveluita. Asiakaslaite voi samoin keinoin estää todentamattoman järjestelmän yhdistämästä itseensä. Kun asiakaslaite kytketään johonkin 802.1x –standardia käyttävän verkon porttiin, järjestelmä vaatii käyttäjää todentamaan itsensä. Todentamisprosessin tuloksena järjestelmä päättää sallitaanko käyttäjän pääsy verkkoon vai hylätäänkö se. Jos asiakaslaitteen pääsy verkkoon estetään, verkkoportin tilaksi määritellään ei-sallittu. Portti

on niin kauan ei-sallitussa tilassa, kunnes jonkin asiakaslaitteen todentaminen hyväksytään. Tällöin verkkoportti menee sallittuun tilaan ja käyttäjä pääsee käyttämään verkkoa ja sen tarjoamia palveluja. Kun asiakaslaite kytkeytyy irti verkosta, verkkoportti palaa ei-sallittuun tilaan.




Kuva 13. 802.1x –kontrolloidut portit [16.]

Kontrolloimaton portti sallii datan siirron asiakaslaitteen ja verkon välillä riippumatta käyttäjän todentamisen tilasta. Kontroilloitu portti mahdollistaa datan siirtämisen verkon ja asiakaslaitteen välillä vain, kun käyttäjä on todennettu ja portti on tämän johdosta sallitussa tilassa. Järjestelmä voi suorittaa todentamisen uudelleen myös tietyin väliajoin. [16.]

Todentamisprosessi

Käyttäjän todennuksessa tapahtuu seuraavat vaiheet

1) Asiakaslaite liittyy verkkoon ja yrittää päästä käsiksi verkon tarjoamiin palveluihin. Asiakaslaitteen ja liityntäpisteen yhteys muodostuu, mutta kontrolloidun portin tilaksi määritellään ei-sallittu. Asiakaslaitteen kaikkii muu kuin linkkitason kommunikointi estetään. Kommunikointi tapahtuu käyttäen EAP over WLAN –protokollaa (EAPOW).

2) Autentikaattori vastaa lähettämällä EAP-Request–paketin ja kysyy asiakkaan identiteettiä.

3) Asiakas vastaa autentikaattorille ja lähettää identiteetti-informaation EAP-Response –paketissa.

4) Autentikaattori välittää asiakkaan tiedot eteenpäin autentikointi-palvelimelle käyttäen vaadittavaa protokollaa. EAP-standardi tukee useaa eri autentikointipalvelinta, mutta yleisimmin käytetty palvelin ja protokolla on RADIUS. Tässä tapauksessa autentikaattorin ja autentikointipalvelimen välinen liikennöinti tapahtuu käyttämällä RADIUS-protokollaa.

5) Autentikointipalvelin vastaa autentikaattorille haasteella ja määrittää asiakaslaitteelle käytettävän EAP-autentikointimenetelmän, jota myös palvelin tukee. Haaste lähetetään palvelimelta autentikaattorille käyttäen yhä RADIUS-protokollaa.

6) Autentikaattori välittää haasteen asiakkaalle käyttämällä EAPOW-protokollaa.

7) Asiakaslaite tarkastaa haasteen ja määrittelee voiko se tukea pyydettyä EAP-autentikointimenetelmää. Jos asiakas ei voi tukea pyydettyä menetelmää, se yrittää neuvotella muista käytettävistä autentikointi-menetelmistä. Jos asiakaslaite tukee pyydettyä autentikointia, se vastaa ja lähettää tunnistustiedot.

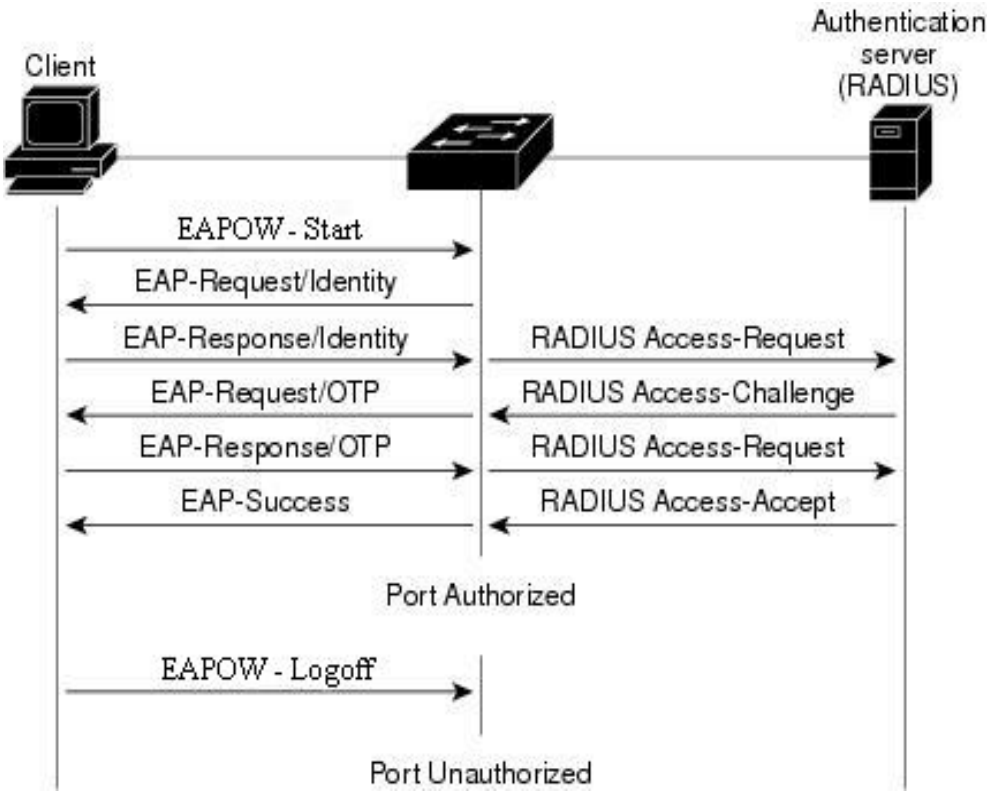
8) Autentikaattori välittää saadut tunnistustiedot palvelimelle käyttäen RADIUS-protokollaa.

9) Jos käyttäjän tunnistustiedot ovat oikeat ja löytyvät tietokannasta, autentikointipalvelin todentaa ja valtuuttaa asiakkaan käyttämään verkkoa ja

lähettää autentikaattorille Access-Accept-viestin. Muutoin asiakkaan pääsy verkkoon hylätään ja autentikaattorille välitetään Access-Reject–viesti.

10) Autentikaattori vastaanottaa palvelimen viestin ja määrittelee viestin perusteella portin tilan.

11) Kun asiakas poistuu verkosta, asiakas lähettää EAPOW-Logoff –paketin autentikaattorille. Tämän jälkeen autentikaattori kytkee verkkoportin takaisin ei-sallittuun tilaan. [17.]




*Kuva 14. 802.1x –todentamisprosessi* [15]

## 7.2 802.11i

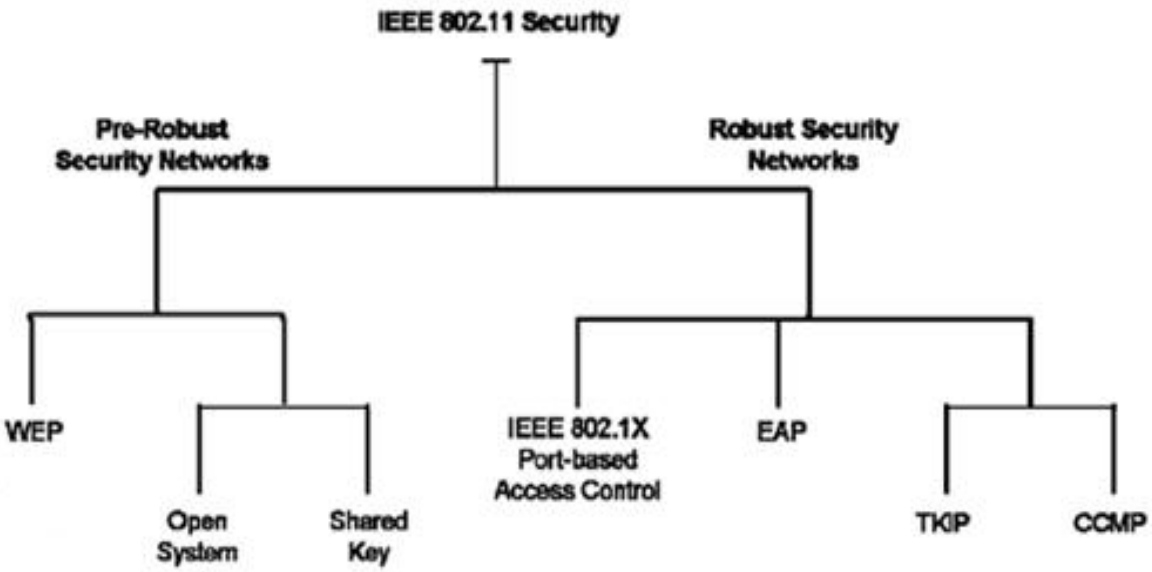
802.11i -protokolla, joka tunnetaan myös nimellä WPA2, on parannus alkuperäiseen IEEE:n määrittelemään 802.11-standardiin ja se määrittelee uusia tietoturvamekanismeja langattomille lähiverkoille. 802.11i korvaa aikaisemman WEP-salausmenetelmän vahvemmalla salausmenetelmällä, jota se käyttää yhteyspisteen ja asiakkaiden välillä siirrettävien datapakettien salaukseen. Uusi protokolla korvaa myös aikaisemmat autentikointi-määrittelyt.

Aikaisempi WEP-salausmenetelmä sisältää paljon vakavia turvallisuus- ja ylläpito-ongelmia, jonka takia kehitettiin parempi Wi-Fi Protected Access –salausmenetelmä. WPA:ssa otettiin käyttöön TKIP-protokolla, joka pohjautui WEP:issä käytettyyn RC4-salausalgoritmiin.

802.11i–protokollan keskeisiä käsitteitä ovat autentikointiin käytetty 802.1x -protokolla, turvallisuusyhteyksien seuraamiseen tarkoitettu Robust Security Network sekä tiedon luottamuksellisuuden ja eheyden varmistavat CCMP- ja TKIP-protokollat. [18.]

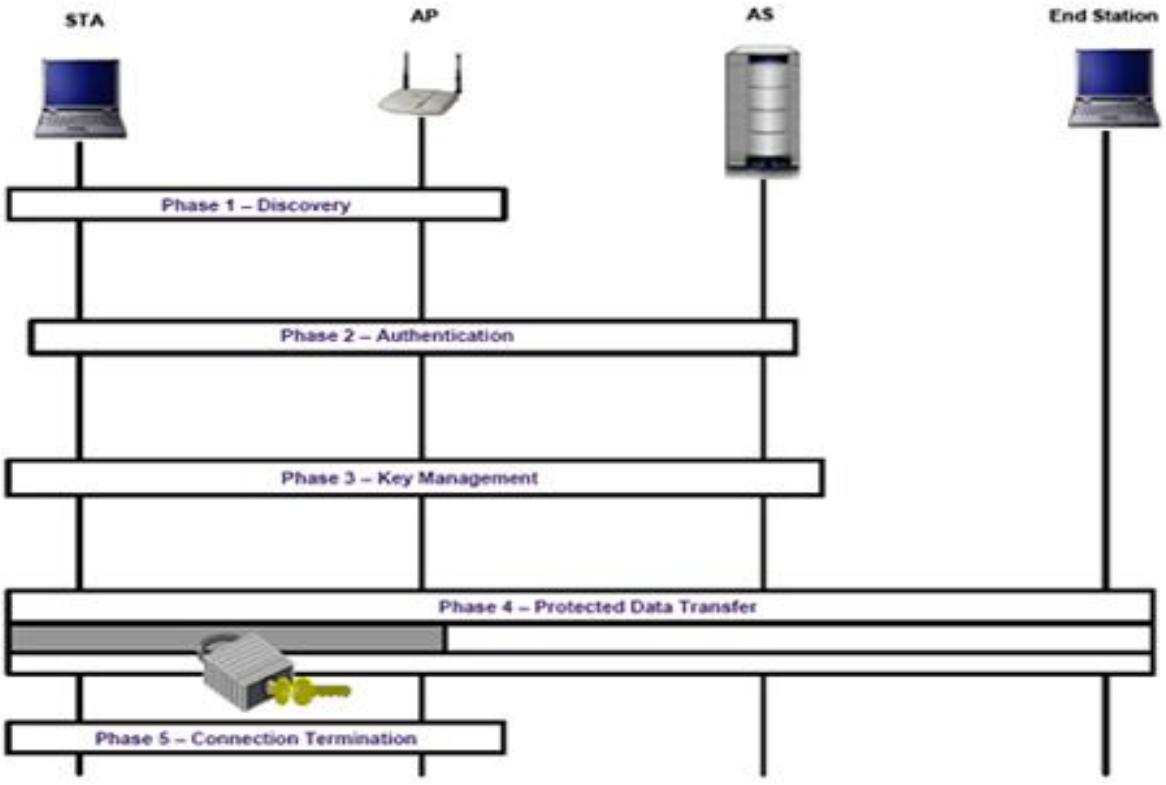
### *7.2.1 Robust Security Network (RSN)*

Kun 802.11i–protokolla otetaan käyttöön, IEEE 802.11 –standardi tarjoaa kaksi eri turvallisuusluokkaa. Pre-RSN –luokka sisältää alkuperäisen 802.11-standardin turvallisuusominaisuudet, jossa autentikointi tapahtuu käyttämällä jaettua avainta ja liikenteen salaus tapahtuu käyttämällä WEP-salausta. Uusilla tarjotuilla turvallisuusominaisuuksilla mahdollistetaan RSN-luokka, joka tarjoaa vahvemman suojauksen korjaamalla WEP-salauksessa havaitut puutteet ja jolla voidaan varmistaa vastaanotetun datan eheys ja luotettavuus.




*Kuva 15. 802.11 turvallisuus* [8]

RSN tarjoaa liikenteen suojauksen ainoastaan yhdessä linkissä, eli joko langattoman tukiaseman ja päätelaitteen tai kahden päätelaitteen välillä. RSN toimii myös pelkästään langattomassa verkossa, eli sitä ei voi hyödyntää esimerkiksi saman verkon langallisessa osassa. Muissa tapauksissa tulee käyttää muita mahdollisia turvallisuusmenetelmiä. [8.]




*Kuva 16. RSN-toiminnan vaiheet* [8]

802.11i –standardi määrittelee RSN-verkon langattomaksi verkoksi, joka sallii RSN-assosiaatioiden (RSNA) luomisen. RSNA on turvallisuusyhteys, jonka 802.11i on muodostanut käyttämällä nelisuuntaista kättelyä (4-Way Handshake). Tämä kättely vahvistaa, että kummatkin kättelyn osapuolet omaavat oikeat avaimet, synkronoi väliaikaisten avainten käytön ja vahvistaa käytetyt koodausmenetelmät.

RSN-toiminnan voidaan ajatella tapahtuvan viidessä eri vaiheessa:

**Vaihe 1: havainnointi**

Havainnointi on ensimmäinen vaihe luodessa RSNA:ta. Tässä vaiheessa asiakas havaitsee verkon, johon haluaa olla yhteydessä. Verkko löydetään ja tunnistetaan tukiaseman lähettämistä viesteistä. Havainnointivaiheessa asiakas ja tukiasema neuvottelevat muun muassa SSID:sta, tuetuista datanopeuksista sekä turvallisuuskäytännöistä. Tukiasema esittää tukemansa asetukset, ja vain näitä tukevat asiakkaat voivat yrittää yhdistää tähän verkkoon.


*Kuva 17. Yhtespiesteiden majakkaviestit* [8]

**Vaihe 2: autentikointi**

Kun havainnointivaihe on suoritettu onnistuneesti, asiakas siirtyy todentamaan identiteettiään langattomalle lähiverkolle. Tässä vaiheessa estetään luvaton pääsy verkkoon. Molemminpuolinen autentikointi mahdollistaa WLAN-verkon todentavan itsensä asiakkaalle, jolloin asiakas tietää olevansa yhteydessä oikeaan verkkoon. Autentikointi tapahtuu 802.1x–standardin mukaisesti käyttäen valittua EAP-protokollaa.

**Vaihe 3: Avainten luonti, hallinta ja jakaminen**

Avaintenhallinta

Alkuperäinen 802.11–standardi käytti manuaalisti luotuja ja syötettyjä WEP-avaimia. 802.11i–estandardi määrittelee kaksi avainhierarkiaa RSNA:lle, jotka määrittelevät avainten väliset suhteet. Nämä avainhierarkiat ovat pariavainhierarkia (Pairwise Key Hierachy, PMK), jota on tarkoitus käyttää täsmälähetyksien (unicast) suojaamiseen sekä ryhmäavainhierarkia (Group Key Hierarchy), jota on tarkoitettu käytettävän ryhmä- ja yleislähetyksien (multicast ja broadcast) suojaamiseen.

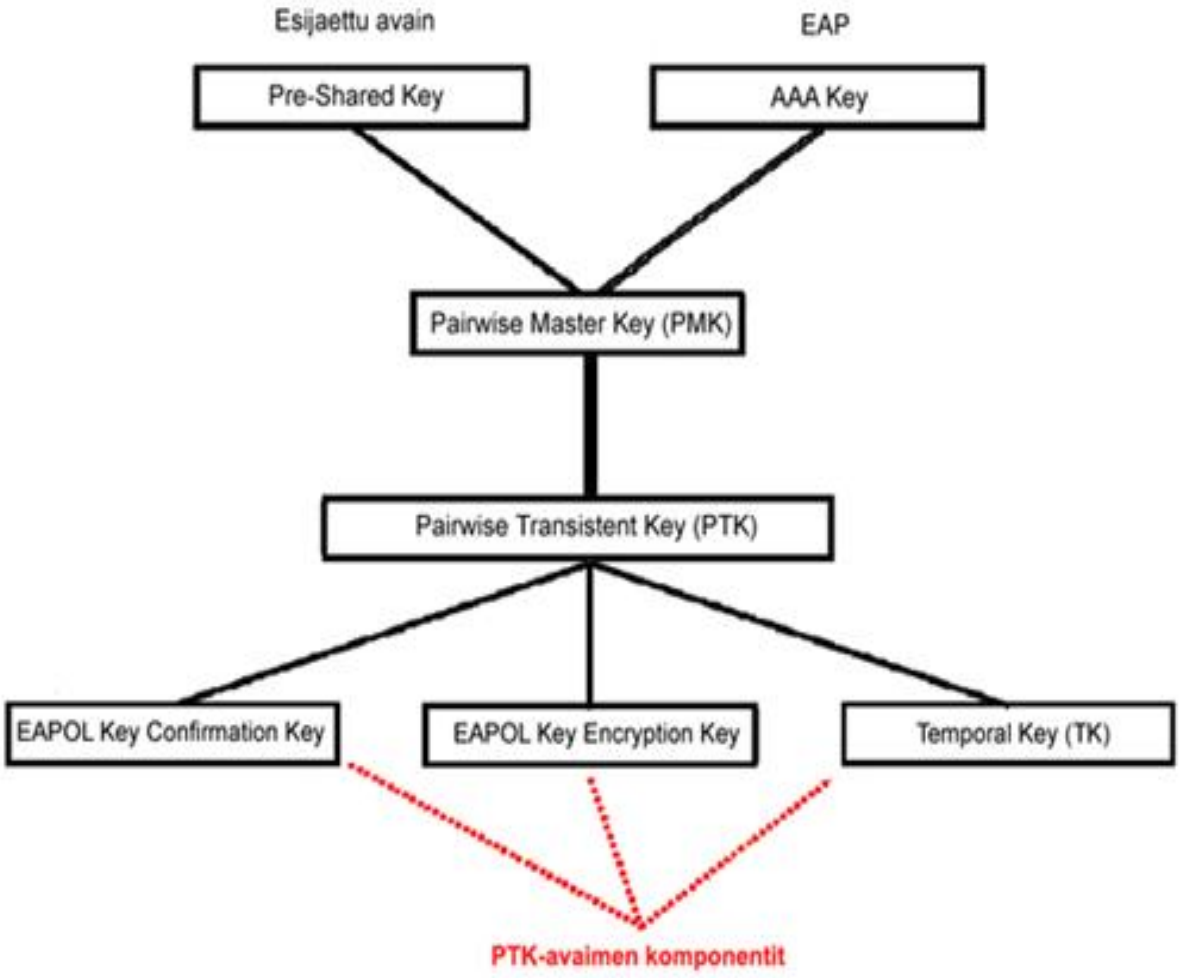
Pariavainhierarkia

**Pre-Shared Key (PSK)** on staattinen avain, joka toimitetaan autentikointipalvelimelle ja asiakkaalle ulkoista reittiä pitkin ennen yhteyden muodostamista. 802.11–standardi ei määrittele kuinka PSK-avaimet tulee luoda tai jakaa, vaan se jää avainten käyttäjien päätettäväksi.

**Authentication, Authorization and Accounting Key (AAAK),** joka tunnetaan myös nimellä Master Session Key (MSK), toimitetaan tukiasemalle EAP-protokollan mukana, kun RSNA-yhteyttä muodostetaan. Avain vaihdetaan aina, kun asiakas autentikoituu WLAN-verkkoon. Avainta käytetään sen voimassaolon ajan tai sen aikaa, kunnes asiakas

autentikoituu uudelleen. Avaimen toimitustapa valikotuu sen mukaan, mitä menetelmää valittu EAP-autentikointimenetelmä käyttää avaimen luomiseen.

Käytettyä pääavainta, joko PSK:ta tai AAAK:ta, käytetään muodostamaan pariavain (PMK). PMK on avainten luomiseen käytetty avain, jota yhdessä tukiaseman ja asiakkaan MAC-osoitteen kanssa käytetään luomaan uusi Pairwise Transient Key (PTK). Käyttämällä tukiaseman ja asiakkaan MAC-osoitteita saadaan aikaan suojaus datan kaappaamista vastaan.




*Kuva 18. Pariavainhiearkia* [8]

PTK koostuu seuraavista avaimista:

- **EAPOL Key Confirmation Key (EAPOL-KCK)**, jota käytetään varmistamaan asiakkaan tukiasemalle lähetettävien kontrollikehysten eheys ja alkuperä alustaessa RSN-verkkoa.
- **EAPOL Key Encryption Key (EAPOL-KEK)**, jota käytetään suojaamaan avaimia ja dataa tiettyjen RSNA-toimenpiteiden aikana.
- **Temporal Key (TK)**, jota käytetään suojaamaan itse asiakkaan liikennöinti.

Ryhmäavainhierarkia

Ryhmäavainhierarkia koostuu vain yhdestä Group Temporal Key (GTK) – avaimesta. Tukiasema luo avaimen itse ja välittää avaimen siihen yhteydessä oleville asiakkaille. Avaimen luontiin ei siis käytetä tukiaseman tai asiakkaiden tietoja.

Avainten luonti ja jakaminen

Avainten luonti- ja jakamisvaihe (Key Generation and Distribution, KGD) on viimeinen vaihe autentikoinnissa. Vaiheen tarkoituksena on muun muassa vahvistaa PMK-avaimen olemassaolo, varmistaa suojausavainten tuoreus, hoitaa TK-avainten asettamiset laitteissa sekä varmistaa salausmenetelmän valinta.

KGD-vaiheita on kahdenlaisia: nelisuuntainen kättely (4-Way Handshake) ja ryhmäkättely (Group Handshake). Kummassakin vaiheessa tarkistetaan viestien eheys ja suoritetaan viestien salaus.

4-Way Handshake

Vaihe alkaa nelisuuntaisella kättelyllä, jonka aikana asiakkaan ja tukiaseman välillä vaihdetaan neljä kehystä dataa. Kättelyn aikana asiakkaan ja tukiaseman välillä siirretään neljä kehystä lisää.

Jos kättely tapahtuu onnistuneesti, asiakas ja tukiasema ovat autentikoituneet molemminpuoleisesti ja 802.1x–standardin hallinnoimat portit avataan liikennöintiä varten.

Ryhmäkättely (Group Key Handshake, GSK)

Kättelyä käytetään, kun tukiasema lähettää uuden väliaikaisen ryhmäavaimen (GTK) asiakkaalle. Kättely on tarpeellinen, jos halutaan tukea ryhmä- ja yleislähetyksiä. Kun ryhmäkättely on suoritettu onnistuneesti, 802.1x–standardin kontrolloima portti avataan ja normaali liikennöinti sallitaan.

**Vaihe 4: suojattu datan siirto**

Kun edelliset vaiheet on suoritettu onnistuneesti, tukiaseman ja asiakkaan välisen liikennöinnin voidaan vahvistaa olevan suojattu. Tämän vaiheen aikana tukiasema ja asiakas voivat vaihtaa informaatiota turvallisesti ja liikennöinti on suojattu käyttäen havainnointivaiheessa valittuja tiedon luottamuksellisyys- ja eheysprotokollia.

Kun datan siirto kohdistetaan yhdelle vastaanottajalle (unicast), käytetään PTK-avainta liikenteen suojauksessa. Suojauksiin lukeutuu kehysten salaus ja eheyden tarkistus. Kehyksin käytetään myös autentikointia, joilla voidaan varmistua kehysten alkuperästä.

Kun dataa siirretään ryhmä- tai yleislähetyksissä, tukiaseman ja asiakkaiden väliset liikennöinnit suojataan käyttämällä CCMP-protokollaa.

**Vaihe 5: yhteyden lopettaminen**

Viimeisessä vaiheessa asiakkaan ja tukiaseman väliset kytkökset poistetaan ja langaton yhteys lopetetaan. Syitä tähän vaiheeseen joutumiseen voivat olla yhteyksien katkeaminen tai kättelyjen ja avainten voimassaolon päättyminen. Vaihe palauttaa tukiaseman ja asiakkaan alkuperäiseen tilaan.

Yhteyden lopettamisessa tapahtuu seuraavat vaiheet:

- Tukiasema epätodentaa asiakkaan,
- Turvallisuuskytkökset poistetaan,
- Salauksessa ja suojauksessa käytetyt väliaikaiset avaimet poistetaan,
- 802.1x –standardin hallinnoima portti palautaa estetty-tilaan [8.]

### *7.2.2 Datan luottamuksellisuus- ja eheysprotokollat*

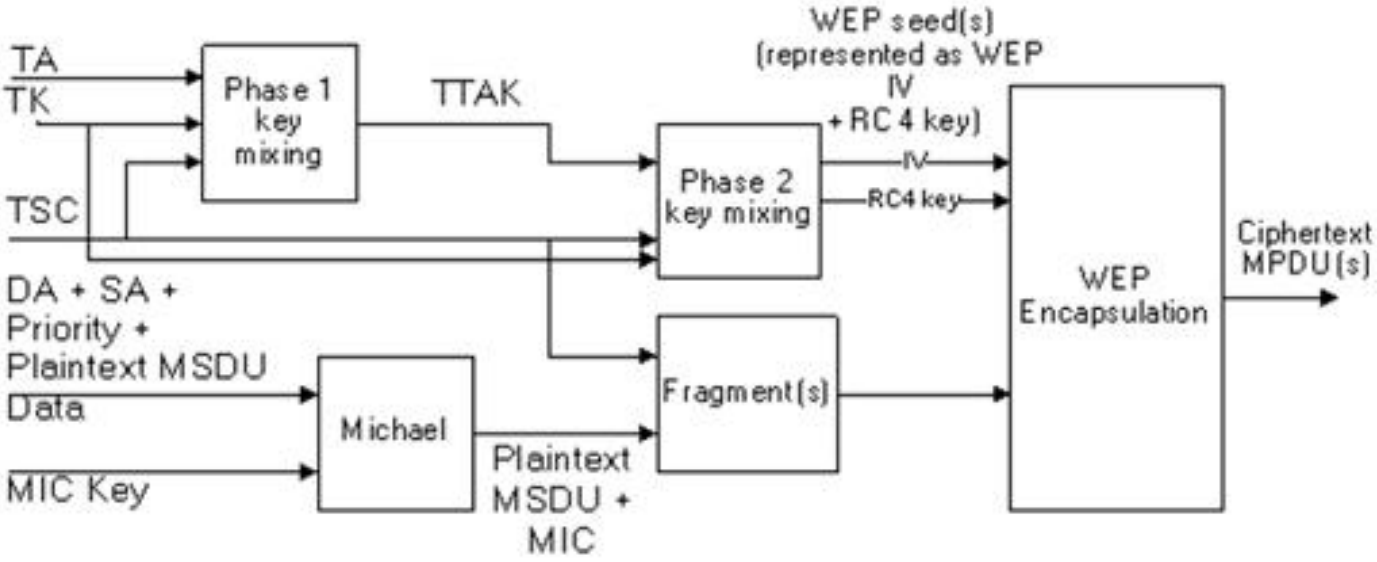
802.11i–standardi määrittelee kaksi RSNA:n kanssa käytettävää protokollaa, joilla voidaan varmistua datan luottamuksellisuudesta ja eheydestä. CCMP-protokollaa tulisi käyttää aina, kun halutaan luoda RSN-assosiaatioita 802.11-laitteilla. TKIP-protokollaa tulisi käyttää laitteiden kanssa, jotka tukevat pelkästään WEP-salausta.

### *7.2.3 Temporal Key Integrity Protocol (TKIP)*

TKIP parantaa aiemmin käytettyä WEP-protokollaa. Lähetin laskee ja lisää kehyksiin Message Intregrity Check –eheystarkastuskoodin (MIC). Vastaanotin vahvistaa kehysten MIC-koodin ja hylkää kaikki väärän koodin

sisältävät kehykset. MIC tarjoaa turvan kehysten väärentämistä vastaan. TKIP käyttää myös TKIP Sequence Counter –laskuria (TSC), jonka avulla vastaanotin voi hylätä kaikki epäjärjestyksessä tulevat kehykset. Tämän avulla saadaan suojaus kehysten uudelleenkäyttöä vastaan. TKIP myös käyttää myös tiettyjä funktioita, joilla se yhdistää muun muassa väliaikaiset avaimet ja TSC-laskurit satunnaiseksi WEP-luvuksi. Vastaanotin selvittää TSC-laskurin vastaanotetusta kehyksestä ja käyttää sitä laskeakseen WEP-luvun, jota se tarvitsee purkamaan kehysten salauksen oikein.

TKIP-kapselointi



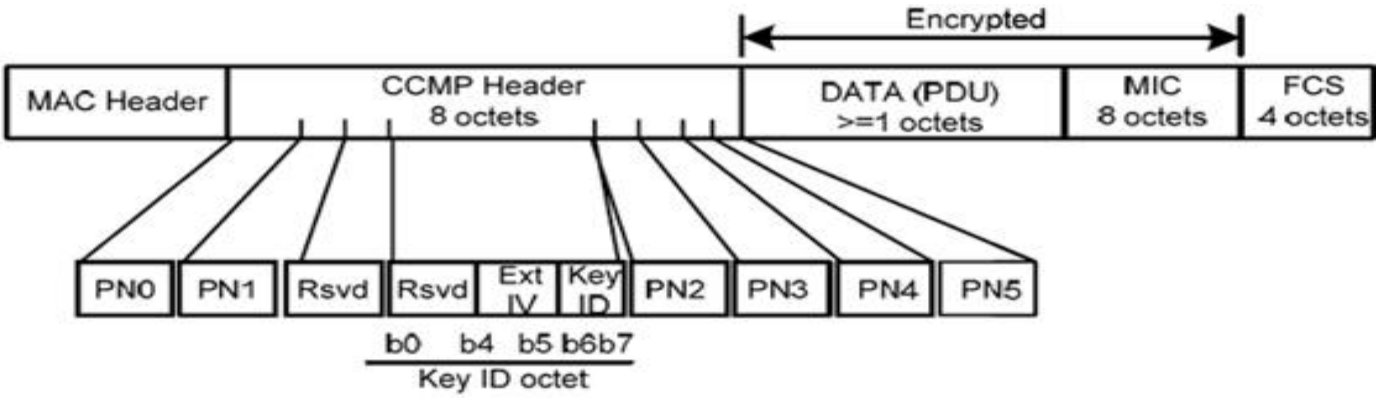

*Kuva 19. TKIP-kapselointi kaavakuvana [8]*

TKIP-protokollan MIC-eheystarkistus suojaa lähetettävät datakehykset ja MIC lisätään kehysten datakenttiin. Tarvittaessa datakehykset voidaan jakaa pienempiin osiin, jolloin TKIP muuttaa TSC-laskimen arvoja jokaiselle kehykselle. TKIP laskee jokaiselle kehykselle oman satunnaisen WEP-luvun. WEP-salaus käyttää oletuksena laskettua WEP-lukua WEP-avaimena.

### *7.2.4 CTR with CBC-MAC Protocol (CCMP)*

CCMP-protokolla pohjautuu AES-salausalgoritmiin. Protokolla yhdistää AES-salauksessa käytettyjä CCM-menetelmiä, joista Counter Mode (CTR) on luottamuksellisuuden ja Cipher Block Chaining Message Authentication Code (CBC-MAC) todennuksen sekä eheyden varmistamiseen.

CCM määrittelee MIC-eheystarkistukseen käytettävän kahdeksan oktettia. CCM vaatii tuoreen väliaikaisen avaimen jokaista sessiota varten. CCM käyttää myös 48-bittistä pakettinumeroa (PN) jokaista suojattua kehystä varten.

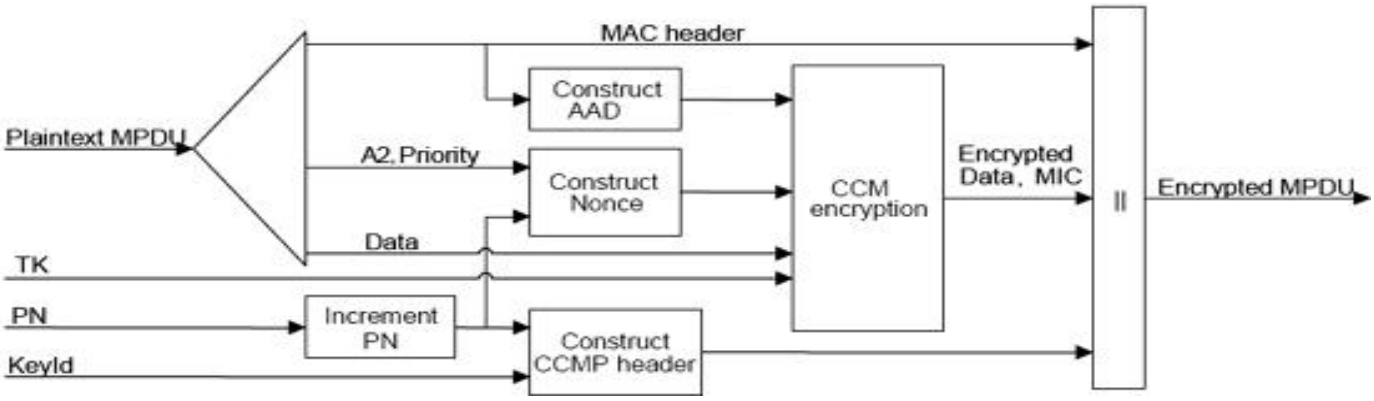



*Kuva 20. CCMP Mac Protocol Data Unit* [8]

CCMP-protokollan käyttö laajentaa alkuperäisä MPDU:ta (MAC Protocol Data Unit) 16 oktetilla, joista kahdeksan oktettia käytetään CCMP-otsikkokenttään ja kahdeksan oktettia MIC-eheystarkistuskenttään. Pakettinumero on 48-bittinen luku, joka esitetään kuuden oktetin sarjana. PN0 on pakettinumeroista tärkeydeltään alhaisin ja PN5 tärkein.

Key ID –oktetin ExtIV-alikenttä ilmaisee, että CCMP-otsikkokenttä laajentaa MPDU:n otsikkoa yhteensä kahdeksalla oktetilla. WEP-salausta käytettäessä MPDU:n otsikkokenttä vie neljä oktettia. CCMP-protokollaa käyttävä ExtIV-bitti asetataan siis aina arvoon 1.

CCMP-kapselointi




*Kuva 21. CCMP-kapselointi* [8]

CCMP salaa ja kapseloi MPDU:ssa siirretyn leipätekstin tekemällä seuraavat toimenpiteet:

- Pakettinumeroa kasvatetaan, jotta jokainen MPDU saa oman pakettinumeron. Samaa pakettinumeroa ei koskaan käytetä kahdesti käyttäessä samaa väliaikaista avainta (TK). Tässä vaiheessa MPDU:ta ei ei vielä muokata.
- MPDU-otsikon sisältämiä kenttiä käytetään muodostamaan lisäautentikointidataa (additional authentication data, AAD). CCM-algoritmi tarjoaa eheydensuojauksen kentille, jotka sisällytetään AAD:hen. MPDU:n otsikkokentät, jotka saattavat muuttua uudelleenlähetyksen yhdeytessä, piilotetaan laskettaessa AAD:ta.
- CCM muodostaa Nonce-lohkon käyttäen hyväksi MPDU:n pakettinumerosta sekä osoite- (A2) ja prioriteettikentästä. Kentän arvo on asetettu nollaksi. Nonce tarkoittaa lukua, jota tullaan käyttämään vain kerran (number used once, Nonce).
- Asetetaan uusi pakettinumero ja avaintunniste (KeyID) CCMP-otsikkoon.
- Käytetään väliaikaista avainta, AAD:ta, nonce-lohkoa sekä MPDU:n sisältämää dataa ja muodostetaan salattu teksti (cipher text) sekä MIC. [19, 8.3.]

# 8 EAP-PROTOKOLLAT

Extensible Authentication Protocol (EAP) on usein langattomissa verkoissa ja Point-to-Point –yhteyksissä (PPP) käytetty tunnistusrunkorakenne. EAP ei itsessään ole mikään tietty tunnistusmenetelmä, vaan se tarjoaa erilaisia funktiota ja tunnistusmenetelmiä, joita kutsujaan nimellä EAP-metodit. Metodeja on useita kymmeniä, ja suurin osa niistä on Internet Engineering Task Forcen kehittämiä, mutta on olemassa myös valmistajakohtaisia tunnistusmetodeja.

Kun EAP otetaan käyttöön Network Access Server –laitteen toimesta, nykyiset EAP-metodit voivat tarjota turvallisen tunnistusmenetelmän sekä voivat neuvotella turvallisen Pair-wise Master Keyn asiakkaan ja NAS:in välille. PMK:ta voidaan käyttää langattomaan salaussessioon, joka käyttää TKIP- tai CCMP-salausta.

EAP ei itsessään ole protokolla vaan se vain määrittää viestien muodon. Jokainen EAP:ta käyttävä protokolla määrittelee tavan kapseloida EAP-viestit protokollan omien viestien sisään. 802.1x–standardia käytettäessä kapselointia kutsutaan nimellä EAPOL (EAP over LAN) ja EAPOW (EAP over WLAN). [20.]

## 8.1 LEAP

Lightweight Extensible Authentication Protocol (LEAP) EAP-metodi, jota Cisco Systems kehitteli ennen IEEE:n ratifioimaa 802.11i –standardia. LEAP:in tärkeitä ominaisuuksia ovat vaihtuvat WEP-avaimet sekä molemminpuolinen tunnistus langattoman päätelaitteen ja RADIUS-palvelimen välillä. LEAP sallii käyttäjien suorittaa tunnistuksen usein ja jokaisella uudella, onnistuneella tunnistautumisella käyttäjä saa uuden WEP-avaimen. Usein vaihdetulla WEP-avaimella pyritään estämään avainten murtaminen.

LEAP vaatii asiakkaan ja autentikaattorin molemminpuolista todentamista. Asiakas todentaa ensin itsensä autentikaattorille ja sen jälkeen

autentikaattori autentikoi itsensä asiakkaalle. Jos kumpikin autentikointi onnistuu, verkkoyhteys sallitaan. LEAP pohjautuu poikkeuksellisesti käyttäjätunnuksen ja salasanan käyttöön

Menetelmässä kuitenkin heikkouksia, koska LEAP käyttää tunnistus-protokollaa, jossa käyttäjän tiedot eivät ole hyvin suojattuja. Vahvemmat tunnistusprotokollat lisäävät satunnaisia bittejä käyttäjän tietoihin, mutta Ciscon vastaus oli opastaa käyttäjiä käyttämään monimutkaisempia salasanoja tai siirtyä käyttämään toista, EAP-FAST –tunnistusprotokollaa. [21.]

## 8.2 EAP-TLS

EAP-Transport Layer Security on avoin standardi, jota langattomien laitteiden valmistajat tukevat laajalti. EAP-TLS:aa pidetään yhä yhtenä turvallisimmista EAP-standardeista vaikka sitä harvemmin enää käytetään. Standardi käyttää PKI:ta turvaamaan liikennöinnin RADIUS- tai muun tunnistuspalvelimen kanssa. EAP-TLS pohjautuu 802.1x/EAP arkkitehtuuriin. [20.]

RADIUS-tunnistuspalvelin välittää varmenteen käyttäjälle ja pyytää vastauksena käyttäjältä omaa varmennetta. Käyttäjä vahvistaa palvelimen varmenteen ja vastaa EAP-vastausviestillä, joka sisältää käyttäjän varmenteen ja samalla aloittaa neuvottelun käyttöön otettavista salaus- ja pakkausalgoritmeista. Kun palvelin on vahvistanut käyttäjän palauttaman varmenteen, palvelin lähettää vastauksena salaustekniikan määrittelyt kyseistä sessiota varten. [22.]

## 8.3 EAP-FAST

EAP-FAST (Flexible Authentication via Secure Tunneling) on Cisco Systemsin suunnittelema protokolla, jonka on tarkoitus paikata LEAP:ista löytyneitä heikkouksia. Protokolla muodostaa TLS-tunnelin, jossa käyttäjän tiedot varmennetaan.

EAP-FAST sisältää kolme vaihetta:

- **Vaihe 0:** on vapaaehtoinen. Tässä vaiheessa Protected Access Credential (PAC) asetetaan manuaalisesti tai dynaamisesti. Tämä asetus tulee normaalisti tehdä vain kerran RADIUS-palvelinta varten.
- **Vaihe 1:** käyttäjä ja tunnistuspalvelin käyttävät PAC:ta muodostaakseen TLS-tunnelin.
- **Vaihe 2:** käyttäjätiedot vaihdetaan käyttäen salattua tunnelia. [17.]

### 8.4 EAP-MD5

EAP-MD5 on standardi, joka käyttää käyttäjätunnusta ja salasanaa valtuuksina autentikoinnissa. Viestien vaihdossa jokainen paketti suojataan allekirjoittamalla jokainen paketti. Tällä voidaan taata, että EAP-viestit ovat aitoja. EAP-MD5 on tehokas ja suorittaa toimenpiteitä nopeasti, mutta se ei käytä PKI-varmenteita vahvistaakseen asikkaita tai tarjoamaan vahvaa salausta suojaamaan asiakkaan ja autentikointipalvelimen välisiä viestejä. Tästä johtuen EAP-MD5–protokolla on haavoittuvainen kaappauksia ja salakuunteluja vastaan.

Protokolla onkin parhaimmillaan langallisissa verkoissa, joissa EAP-asiakas on suoraan kytkeytyneenä autentikaattoriin ja salakuuntelun sekä viestin kaappaamisen mahdollisuus on alhainen. Langattomissa verkoissa suositellaan käyttämään vahvempia EAP-autentikointeja. [20.]

### 8.5 EAP-TLS

EAP-TLS (Transport Level Security) tarjoaa vahvan suojauksen vaatien sekä asiakkaan että autenkointipalvelimen käyttämään PKI-varmenteita. EAP-viestit suojataan salakuuntelulta käyttämällä TLS-tunnelia asiakkaan ja autentikointipalvelimen välillä. Sekä asiakkaalla että palvelimella tulee olla omat PKI-varmenteet. Varmenteiden jako suurelle osalle asiakkaita ja palvelimia on työlästä ja ylläpidosta tulee hankalaa. [20.]

### 8.6 EAP-TTLS

EAP-TTLS-protokolla (Tunneled TLS) on lisäys EAP-TLS–protokollaan ja tarjoaa vahvemman salauksen ilman asikkaan ja autentikointipalvelimen välisiä varmenteita. Protokolla kyllä tukee molemminpuolista autentikointia, mutta vaatii varmenteen käyttöä pelkästään palvelimelta. Asiakas autentikoituu palvelimelle käyttäen käyttäjätunnusta ja salasanaa. Protokolla helpottaa ylläpitoa, mutta säilyttää silti vahvan suojauksen ja autentikoinnin.

TLS-tunnelia voidaan käyttää suojaamaan EAP-viestit ja jo olemassa olevaa varmennepalvelua, kuten esimerkiksi RADIUS:ta, voidaan käyttää uudelleen autentikointiin. Protokolla on myös taaksepäin yhteensopiva muiden autentikointiprotokollien kanssa. EAP-TTLS–protokollan heikkoutena on, että sitä voidaan huijata lähettämään tietoja, kun TLS-tunneli ei ole käytössä. Vaikka protokolla on laajalti tuettu, muun muassa Microsoft Windowsissa ei ole valmista tukea protokollalle. [20.]

### 8.7 PEAP

Protected EAP –protokolla on samankaltainen EAP-TTLS–protokollan kanssa ja käyttää molemminpuolista autentikointia. PEAP-protokollaa on ehdotettu korjaamaan EAP-protokollasta löytyneitä heikkouksia. PEAP sallii muiden EAP-autentikointimenetelmien käytön ja suojaa niiden lähetykset käyttämällä salattua TLS-tunnelia. PEAP-asiakas autentikoituu suoraan autentikointipalvelimen avulla ja autentikaattori toimii vain välikappaleena. Autentikaattorin ei välttämättä tarvitse ymmärtää käytettyä EAP-protokollaa. Tunnelin salauksen avaimet lähetetään käyttämällä palvelimen julkista avainta. Itse asiakkaan autentikointitiedot lähetetään salattuna TLS-tunnelin sisällä ja ovat täten turvassa salakuuntelulta. [23.]

# 9 YHTEENVETO

Työssä tutustuttiin langattomien lähiverkkojen peruskäsitteisiin, verkkojen rakenneosiin ja verkoissa käytettyihin tekniikoihin. Langattomat lähiverkot ovat arkipäivää miltei kaikkien työpaikoilla ja kotioloissa, joten verkkoa käytetään niin hyöty- kuin viihdekäytössä.

Verkkojen yleistyminen ja käyttäjämäärien kasvu ovat luonnollisesti lisänneet huolta käyttäjien ja tiedonsiirtojen turvallisuudesta. Tästä johtuen suuri osa tätä insinöörityötä keskittyi tietoturvallisuutta lisääviin protokolliin ja menetelmiin. Insinöörityössä keskityttiin myös suurelta osin langattomien lähiverkkojen suorituskykyä parantaviin tekniikoihin. Viimeisimmät IEEE:n ratifioimat standardit mahdollista suuremmat tiedonsiirtonopeudet, koska verkkojen ja käyttäjien määrä kasvaa koko ajan entisestään. Tästä johtuen tarvitaan tehokkaammin toimivia verkkoja ja laitteita.

IEEE jatkaa uusien standardien kehittelyä kokoajan, koska käyttäjien ja palvelijen vaatimukset kasvavat myös kokoajan. Tälläkin hetkellä IEEE:n kotisivujen aikajanasta voi nähdä, että kehityksen alla on noin kymmenen eri standardia tai uutta laajennusta, joiden kaikkien on suunniteltu valmistuvan parin vuoden sisällä. Vain aika näyttää mihin asti nykyisillä standardeilla voidaan päästä ja mihin asti IEEE meidät lopulta vielä vie.

**VIITELUETTELO**


[1] Wikipedia: *IEEE 802.11 (legacy mode)*, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: **http://en.wikipedia.org/wiki/IEEE_802.11_%28legacy_mode%29 ,**

[2] Wikipedia: *IEEE 802.11*, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: http://fi.wikipedia.org/wiki/802.11 ,

[3] Nicopolitidis, Petros – Obaitat, Mohammad Salameh – Papadimitriou, Georgios I. – Pomportsis, Andreas, *Wireless Networks.* John Wiley & Sons Ltd 2003 ,

[4] Granlund, Kaj, *Langaton Tiedonsiirto*. Docendo, 1. painos, Porvoo 2001 ,

[5] Wikipedia: *IEEE 802.11g-2003*, verkkodokumentti [viitattu 15. 2. 2010].Saatavissa: ***http://en.wikipedia.org/wiki/IEEE_802.11g-2003*** ,

[6] Wikipedia: *IEEE 802.11*, verkkodokumentti [viitattu 4. 3. 2010]. Saatavissa: http://en.wikipedia.org/wiki/IEEE_802.11 ,

[7] Cisco Systems White Paper, 802.11n: The Standard Revealed, verkkodokumentti [viitattu 29. 3. 2010]. Saatavissa: http://www.laureatesonline.net/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-427843_v1.pdf ,

[8] National Institute of Standards and Technology, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, verkkodokumentti [viitattu 3. 4. 2010]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf ,

[9] Puska, Matti, *Langattomat lähiverkot*, Gummerus Oy, Jyväskylä 2005 ,

[10] Cisco Systems, Wireless LAN Controller (WLC) FAQ, verkkodokumentti [viitattu 5. 4. 2010]. Saatavissa: http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml ,

[11] Cisco Systems White Paper, *Understanding The Lightweight Access Point Protocol (LWAPP)*, verkkodokumentti [viitattu: 5. 4. 2010]. Saatavissa: http://www.conticomp.com/PDF/LWAPP_td.pdf ,

[12] Wikipedia: *Direct-sequence Spread Spectrum*, verkkodokumentti [viitattu 23. 2. 2010]. Saatavissa: http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum ,

[13] Wikipedia: *Wired Equivalent Privacy*, [viitattu 9. 3. 2010]. Saatavissa: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy ,

[14] Wikipedia: *Langattoman lähiverkon tietoturva*, verkkodokumentti [viitattu 11. 3. 2010]. Saatavissa: http://fi.wikipedia.org/wiki/WLAN_tietoturva#WPA2_.28AES.29 ,

[15] Wikipedia: *RADIUS*, verkkodokumentti [viitattu: 11. 3. 2010]. Saatavissa: http://en.wikipedia.org/wiki/RADIUS ,

[16] IEEE Computer Society, *IEEE 802.1x-2004*, verkkodokumentti [viitattu 21. 3. 2010]. Saatavissa: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf ,

[17] Ironshield White Paper, *802.1x Authentication & Extensible Authentication Protocol (EAP)*, verkkodokumentti [viitattu: 11. 3. 2010]. Saatavissa: **http://www.foundrynet.com/pdf/wp-8021x-authentication-eap.pdf ,**

[18] Airtight Networks, 802.11i – WLAN/Wireless Security Knowledge Center, verkkodokumentti [viitattu: 4. 4. 2010]. Saatavissa: http://www.airtightnetworks.com/home/resources/knowledge-center/80211i.html ,

[19] IEEE Computer Society, IEEE Std 802.11i -2004, verkkodokumentti [viitattu: 3. 4. 2010]. Saatavissa: http://download.www.techstreet.com/cgi-bin/pdf/free/461163/802.11i-2004.pdf ,

[20] Wikipedia: Extensible Authentication Protocol, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol ,

[21] Wikipedia: Lightweight Extensible Authenticatio Protocol, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: http://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol ,

[22] Cisco Systems, EAP-TLS Deployment Guide for Wireless LAN Networks, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml#wp39021 ,

[23] Wikipedia: Protected Extensible Authentication Protocol, verkkodokumentti [viitattu 15. 2. 2010]. Saatavissa: http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol