TEKNILLINEN KORKEAKOULU

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Mikko Sannikka

PALVELUNLAATU LANGATTOMISSA LÄHIVERKOISSA

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 29.3.2009

Työn valvoja:	Dosentti Kalevi Kilkki
Työn ohjaaja:	DI Vesa Hirsmäki

TEKNILLINEN KORKEAKOULU Elektroniikan, tietoliikenteen ja automaation tiedekunta Tietoliikennetekniikan koulutusohjelma	DIPLOMITYÖN TIIVISTELMÄ
Tekijä Mikko Sannikka	Päiväys 29.3.2009
	Sivumäärä 104
Työn nimi Palvelunlaatu langattomissa lähiverkoissa	
Professuuri Tietoverkkotekniikka	Koodi S-38
Työn valvoja Dosentti Kalevi Kilkki Työn ohjaaja DI Vesa Hirsmäki	

Kriittisen liikenteen määrä myös langattoman verkon yli on kasvamassa. Tässä työssä tutkittiin IEEE 802.11 -standardin mukaisia langattomia lähiverkkotekniikoita (WLAN, Wireless Local Area Network) sekä langattomien lähiverkkojen palvelunlaatua. Lisäksi perehdyttiin palvelunlaadun toteutumiseen keskeisesti liittyviin käsitteisiin palvelutasonhallinta (SLM, Service Level Management) sekä palvelutasosopimukset (SLA, Service Level Agreement). Langattomien lähiverkkojen palvelunlaatua tutkittiin keskittymällä erityisesti kriittisen liikenteen kuljetukseen. Kirjallisuustutkimusta ja sen tuloksia käytettiin hyödyksi asiakasprojektina toteutetuissa mittauksissa.

Mittaukset toteutettiin Noval Networksin toimintatapaa ja mittausjärjestelmää apuna käyttäen Salon kaupungin verkkoon tehdyillä laatumittauksilla. Mittausten avulla selvitettiin pääterveyskeskuksen langattoman verkon laatua ja samalla todennettiin, miten kriittinen liikenne kulkee langattoman lähiverkon yli. Tulosten perusteella arvioitiin yleisellä tasolla vaatimuksia langattomalle lähiverkolle kriittisen liikenteen kuljetuksen osalta. Verkon viiveet sekä pakettihävikit osoittautuivat erittäin mataliksi ja langattoman verkon todettiin soveltuvan hyvin myös kriittiselle liikenteelle.

Avainsanat: QoE, QoS, SLA, SLM, VoWLAN

Helsinki University of Technology
Faculty of Electronics, Communications and Automation

Abstract of the Master's Thesis

Author
Mikko Sannikka

Date
29.3.2009

Number of pages
104

Name of the Thesis
Quality of Service in wireless local area networks

Professorship
Networking Technology

Code
S-38

Supervisor
Dosent Kalevi Kilkki

Instructor
M.Sc. Vesa Hirsmäki

The amount of critical traffic over wireless networks is growing rapidly. This thesis focuses on IEEE 802.11 standard and its Wireless Local Area Network (WLAN) technologies. Besides the technology, Quality of Service (QoS) and important factors behind that were examined. In addition Service Level Management (SLM) and Service Level Agreements (SLA), key concepts related to achieving QoS targets, were studied. This thesis examines the QoS in WLANs focusing especially in critical traffic. The results of literature study were used for measurement in a customer project.

Practical measurements were conducted using Noval Networks' approach and measurement system. The measurements itself were carried out in the city of Salo, one of Noval Networks' customer. The target for the project was to find out the quality of Salo's health center's wireless network and also to find out if the critical traffic will transfer over WLANs without problems. The results were used to evaluate the needs for WLANs while using quality-critical traffic. The delays and packet losses of Salo's WLAN network seemed to be very low and network suits fine also for critical traffic.

Keywords: QoE, QoS, SLA, SLM, VoWLAN

Alkulause

Tämä diplomityö on tehty Noval Networksille. Työn kokeelliseen osioon liittyvät mittaukset suoritettiin Noval Networksin asiakkaan, Salon kaupungin pääterveysasemalla.

Haluan tässä yhteydessä ensinnäkin kiittää diplomityöni valvojaa, dosentti Kalevi Kilkkiä lukuisista neuvoista ja suosituksista aina alkusuunnittelusta diplomityön viimeistelyyn asti. Lisäksi kiitän DI Vesa Hirsmäkeä diplomityön ohjauksesta neuvoineen ja vinkkeineen. Asiakasta, Salon kaupunkia ja Ville Maimosta haluan kiittää mittausprojektin mahdollistamisesta ja hyvästä yhteistyöstä mittausten toteuttamiseksi. Lisäksi Noval Networksin projektitiimistä haluan kiittää Jussi Repoa ja Teemu Salmensuuta avustuksesta mittausten toteuttamisessa.

Noval Networksin teknologiajohtaja Jari Reinikaista sekä toimitusjohtaja Erkki Tuomea haluan kiittää mahdollisuudesta diplomityön tekoon Noval Networksissa. Kiitokset myös muille Noval Networksin työntekijöille loistavasta työilmapiiristä.

Lisäksi haluan kiittää perhettäni ja ystäviäni tuesta opintojen ajalta.

Lopuksi haluan osoittaa kiitokset kihlatulleni Lauralle korvaamattomasta ja sinnikkäästä avusta koko opiskelujeni ajan.

Helsingissä, maaliskuun 29. päivänä, 2009

Mikko Sannikka

Sisällysluettelo

Lyhenteet

3G	Third Generation Mobile Technology
4G	Fourth Generation Mobile Technology
AAA	Authentication Authorization Accounting
AC	Access Category
ACK	Acknowledgement Code
ADPCM	Adaptive Differential Pulse-Code Modulation
AES	Advanced Encryption Standard
AF	Assured Forwarding
AIFS	Arbitary InterFrame Space
AP	Access Point
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
BE	best-effort
BER	Bit Error Rate
BSS	Basic Service Set
CAP	Controlled Access Phase
CAPEX	Capital Expenditures
CBWFQ	Class-Based Weighted Fair Queuing
CC	Control Contention
CDMA	Code Division Multiple Access
CELP	Code-Excited Linear Prediction
CFP	Contention Free Period
CP	Contention Period
CQ	Custom Queuing
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function

DiffServ	Differentiated Services
DIFS	Distributed Coordination Function Interframe Space
DLP	Direct Link Protocol
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DTPC	Dynamic Transmit Power Control
EDCA	Enhanced Distributed Channel Access
EF	Expedited Forwarding
EKG	ElektroKardioGrafia
ErtPS	Extended real-time Packet Service
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FBSST	Fast Basic Service Set Transition
FCFS	First Come – First Served
FDD	Frequency Division Duplexing
FEC	Forwarding Equivalency Class
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIFO	First In – First Out
Flash-OFDM	Fast Low-latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing
FTP	File Transfer Protocol
HC	Hybrid Controller
HCCA	Hybrid Coordination Function Controlled Channel Access
HCF	Hybrid Coordination Function
HIPERLAN	HIgh PErformance Radio Local Area Network
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSUPA	High Speed Uplink Packet Access
HTTP	HyperText Transfer Protocol
IAPP	Internet Access Point Protocol
ICMP	Internet Control Message Protocol

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	Internet Protocol Multimedia Subsystem
IntServ	Integrated Services
IP	Internet Protocol
IR	InfraRed
ISM	Industrial, Scientific and Medical
IT	Information Technology
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAN	Local Area Network
LLC	Logical Link Control
LLQ	Low-Latency Queuing
LSP	Label Switched Path
LSR	Label Switched Router
MAC	Medium Access Control
MIMO	Multiple In – Multiple Out
MOS	Mean Opinion Score
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NAV	Network Allocation Vector
NLOS	Non Line Of Sight
NMT	Nordisk Mobiltelefon
nrtPS	non-real-time Polling/Packet Service
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OPEX	Operating Expense
OSI	Open Systems Interconnection Reference Model
PC	Point Coordinator
PCF	Point Coordination Function
PCM	Pulse-Code Modulation
PCMCIA	Personal Computer Memory Card International Association

PESQ	Perceptual Evaluation of Speech Quality
PHB	Per Hop Behaviour
PIFS	Point Coordination Function Interframe Space
PQ	Priority Queuing
PSQA	Pseudo-Subjective Quality Assessment
PSQM	Perceptual Speech Quality Measure
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RED	Random Early Detection
RIO	Random Early Detection with In/Out
RR	Round-Robin
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
rtPS	real-time Polling/Packet Service
RTS	Request To Send
SDP	Session Description Protocol
SIFS	Short Interframe Space
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Service Level Management
SLO	Service Level Objective
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSID	Service Set IDentifier
STUN	Simple Traversal of User Datagram Protocol Through Network Address Translation
TBTT	Target Beacon Transition Time
TC	Traffic Category
TCP	Transmission Control Protocol
ToS	Type of Service

TXOP	Transmit Opportunity Limit
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VoWIP	Voice over Wireless Internet Protocol
VoWLAN	Voice over Wireless Local Area Network
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WEP	Wireless Equivalent Privacy
WFQ	Weighted Fair Queuing
WiFi	Wireless Fidelity
WiMAX	Worldwide interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wireless Fidelity Protected Access
WRED	Weighted Random Early Detection
WRR	Weighted Round-Robin
WWW	World Wide Web

1. Johdanto

1.1 Tutkimuksen tausta

Internetin tietoverkot suunniteltiin ja rakennettiin alun perin ilman kunnollista panostusta palvelunlaatuun, sillä silloisten sovellusten vaatimukset ja tarpeet eivät olleet yhtä lailla sidoksissa laatuun kuin nykyään. Tärkeintä oli saada muodostettua yhteys tietokoneiden välille sillä nopeudella, mitä kulloinenkin tekniikka salli. Palvelunlaatuun alettiin kiinnittää enemmän huomiota vasta kun huomattiin, että tietoverkoissa tapahtuvaan liikennöintiin pitää pystyä vaikuttamaan, jotta voidaan parantaa liikennöintivarmuutta ja nopeutta sekä voidaan välittää tärkeä liikenne ensisijaisesti muuhun liikenteeseen verrattuna.

Langattomuudesta on tullut iso asia viime vuosina. Langattomat lähiverkot tulivat koteihin ja yrityksiin ennen kaikkea kannettavien tietokoneiden käytön yleistyessä. Ne lisäsivät innostusta tietokoneiden käyttöön, kun käyttäjä ei enää ollutkaan niin sidottu tiettyyn fyysiseen paikkaan kuin aiemmin. Nyt langattomia tekniikoita käytetään sekä laajemmassa mittakaavassa mobiileina laajakaistatekniikoina että lähiverkoissa yhdistämään langattomat työasemat ja muut päätelaitteet tukiaseman kautta langalliseen IP (Internet Protocol)-verkkoon, eli pakettikytkentäiseen Internet-verkkoon. Kaupungeissa julkisilla paikoilla yleistyneet asiakkaille tarkoitetut alueet, joista on langaton yhteys Internetiin esimerkiksi ravintoloissa ja kahviloissa ovat yksi uusi ilmiö langattomuuden saralla. Usein ravintolasta saa pyytäessään (tai pientä maksua vastaan) tarvittavan salasanan, jolla langattomaan verkkoon kytkeydytään. Myös täysin salaamattomia verkkoja löytyy, jolloin kuka tahansa pystyy kytkeytymään kyseiseen verkkoon. Usein tämä ei kuitenkaan tarkoita, että verkkoon saisi kytkeytyä kuka tahansa. Varsinkin kerrostaloissa suojaamaton verkko mahdollistaa kantoalueella asuvien naapureiden ilmaisen Internet-käytön naapurin suojaamattoman verkon yli.

Langattomien verkkojen palvelunlaadun kehittämisestä ei löydy vielä samalla lailla tutkimustietoa kuin palvelunlaadusta langallisissa verkoissa. Aihe on toisaalta hyvin ajankohtainen, sillä langattomat ratkaisut ovat yleistyneet varsin nopeasti viime vuosina.

Palvelunlaatua ja palvelunlaatuvaatimuksia ei voida suoraan tuoda langallisen verkon puolelta, sillä langattomuus asettaa palvelunlaadun toteutumiselle enemmän vaatimuksia kuin perinteinen langallinen ratkaisu. Haasteena on saada taattua kriittiselle liikenteelle riittävä palvelunlaatu kuitenkin niin, että myös ns. laatutakeeton best-effort -liikenne saa riittävästi kaistaa käyttöönsä.

Yhtenä mielenkiintoisena aihealueena on laadullisesti kriittisen puheliikenteen siirtäminen langattoman lähiverkon yli täysin IP-pohjaiseen verkkoon (VoWLAN, Voice Over Wireless Local Area Network). Puheen kuljettamisesta IP-verkon yli (VoIP, Voice over Internet Protocol) VoWLAN eroaa siinä, että puhe kulkee osan matkaa langattoman lähiverkon yli ilmateitse. VoWLAN nähdäänkin haastajana perinteisille mobiilipuheluille ja on yksi mobiilioperaattoreiden suurimmista huolenaiheista. Puheliikenne asettaa omat erikoishaasteensa langattomien verkkojen palvelunlaadulle. Sujuvan puheliikenteen takaamiseksi pakettihävikkiä tai viivettä ei saisi ilmetä liikaa ja toisaalta kaistaa pitäisi olla riittävästi. Palvelunlaadulliset ongelmat aiheuttavat suurempaa päänvaivaa ilmarajapinnassa kuin täysin langallisissa ratkaisuissa.

1.2 Tutkimuskysymykset

Diplomityössäni keskityn tutkimaan palvelunlaatua langattomissa verkoissa. Langattoman lähiverkon palvelunlaatuun liittyen tutkitaan erillisenä tapauksena VoWLAN:ia sekä käydään tapaustutkimuksena läpi palvelunlaadun selvittämistä ja mittaamista langattomissa lähiverkoissa Noval Networksin ratkaisulla. Aihetta käsitellään seuraavien tutkimuskysymysten kautta:

1. Miten langattomuus vaikuttaa palvelunlaatuun?
2. Millainen on kriittisen liikenteen (puheliikenteen) laadullinen ero käytettäessä langatonta ja langallista lähiverkkoyhteyttä (VoWLAN vs. VoIP)?
3. Millaisia kehitystoimenpiteitä palvelutasonhallintaan keskittyneen yrityksen tulisi huomioida omassa palvelukonseptissaan palvelutasonhallintaan ja palvelunlaatuun liittyen? Vaikuttaako langattomuus jollain lailla toimenpiteisiin? Erityistapauksena tutkitaan asiaa Noval Networksin ja sen asiakkaan kannalta selvittämällä palvelunlaadun toteutumista kriittisen liikenteen kuljetuksessa.

1.3 Tutkimuksen rajaus

Tutkimus rajattiin koskemaan palvelunlaatua langattomissa lähiverkoissa. Langattomista pitkän kantaman verkoista käydään perustasolla läpi tärkeimmät (WiMAX, @450, 3G), muutoin pitäydytään lähiverkoissa. Perinteisiin langallisiin lähiverkkoihin viitataan lähinnä vain VoIP:ia koskevassa osiossa, sillä tämä tutkimus keskittyy muutoin langattomiin yhteyksiin niiden tarjoaman haasteellisuuden ja toisaalta langallisista verkoista tehtyjen tutkimusten suuren määrän vuoksi.

Tapaustutkimuksena selvitetään WLAN-verkon laatua Noval Networksin asiakkaan verkossa Noval Networksin omalla, NetEye -nimisellä mittausjärjestelmällä. Lopuksi mietitään kehitysehdotuksia Noval Networksin toimintatavalle koko SLM(Service Level Management)-toiminnan kannalta.

1.4 Yleisesti tietoliikennealan toimijoista

Tietoliikennealan toimijoiksi voidaan yleisellä tasolla laskea loppukäyttäjä, verkko-operaattori ja palveluoperaattori/palveluntarjoaja. Verkko-operaattori vastaa fyysisestä tietoliikenneverkosta ja liikennöinnistä, kun palveluoperaattori puolestaan tarjoaa sovelluspalvelut fyysisen verkon päällä. Lisäksi toimijoihin voidaan mieltää esimerkiksi asennuspalveluiden toimittajat sekä päätelaitevalmistajat ja maahantuojat. Täytyy kuitenkin huomata, että toimijat voidaan määritellä eri tekniikoiden yhteydessä hieman toisistaan poiketen tapauskohtaisesti, eli eri toimijoiden välinen rajapinta on toisinaan häilyvä.

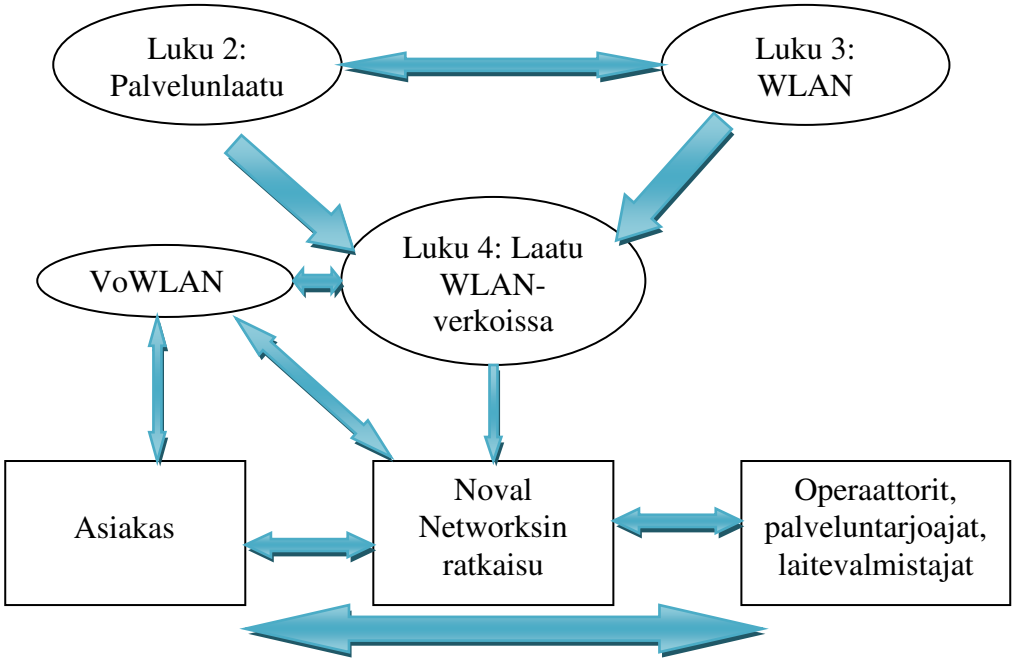
1.5 Tutkimusmenetelmät

Tutkimuksessa käytettäviä tutkimusmenetelmiä ovat kirjallisuustutkimus sekä mittaukset Noval Networksin NetEye-tuotteella. Teoreettisen osion ja mittaustulosten perusteella analysoidaan saavutettuja tuloksia.

Kirjalliset lähteet pitävät sisällään akateemisia julkaisuja, alan kirjallisuutta, ’white paper’-julkaisuja, www-julkaisuja ja kirjoituksia sekä ajankohtaisia lehtiartikkeleita.

1.6 Tutkimuksen rakenne

Kuvassa 1 on kuvattu diplomityön rakenne.



Kuva 1. Diplomityön rakenne

Tutkimuksessa käydään ensin läpi palvelutasosopimukset, niiden määritelmät ja tavoitteet sekä selvitetään tarkemmin käsitteen *palvelunlaatu* sisältöä tutkimalla mistä palvelunlaatu ja palvelunlaadun mittaaminen koostuvat, minkälaisia tekniikoita käytetään ja mihin palvelunlaadulla sekä palvelunlaadun mittaamisella ylipäätään pyritään. Seuraavaksi käsitellään langattomia lähiverkkoja, niiden taustaa ja kehitystä sekä sitä, minkälaisia erityispiirteitä langattomissa verkoissa on langallisiin verkkoihin verrattuna.

Kappaleessa neljä osiot yhdistetään käsitteen palvelunlaatu langattomissa lähiverkoissa alle. Osiossa selvitetään, miten tilanne palvelunlaadun osalta muuttuu siirryttäessä langattomiin verkkoihin. Erikoistapauksena tästä käydään läpi laatukriittisen puheliikenteen kuljetus langattoman lähiverkon yli (VoWLAN) ja selvitetään, mihin VoWLAN:ia voidaan käyttää sekä mitä erityispiirteitä VoWLAN tuo palvelunlaadun mittaamiseen. Lisäksi VoWLAN:ia vertaillaan ominaisuuksien osalta VoIP:iin. Samassa

osiossa myös käydään lyhyesti läpi käsitteen VoWIP sisältö ja siihen liittyvät langattomat verkkotekniikat, mutta pääasiassa tutkimus käsittelee ainoastaan lähiverkkoja.

Lopuksi käydään tapaustutkimuksen avulla läpi tilannetta Noval Networksin kannalta esittelemällä ensin Noval Networksin SLM-kokonaisuus. Tämän jälkeen selvitetään osin asiakasverkon mittausten avulla langattoman verkon häiriötekijöitä sekä palvelunlaadun toteutumista kriittisen liikenteen kuljetuksessa. Samalla selvitetään, miten hyvin Noval Networksin tarjoama palvelukokonaisuus soveltuu palvelunlaadun mittaamiseen sekä palvelutasonhallinnan jatkuvaan parantamiseen langattomissa verkoissa. Lisäksi selvitetään mahdollisia kehityskohteita asiakasverkon ja Noval Networksin toiminnalle.

2. Palvelunlaadun toteutuminen tietoliikenneverkoissa

Perinteisessä suurimmalta osin TCP (Transmission Control Protocol)-pohjaisessa IP-liikennöinnissä Internetissä pakettien kuljetus tapahtuu best-effort -periaatteen mukaisesti. Tällöin jokaista pakettia kohdellaan tasavertaisesti, eli jokaisella paketilla on yhtäläiset mahdollisuudet tulla välitetyksi eteenpäin. Toisaalta ruuhkatilanteessa mikä tahansa paketti saatetaan tiputtaa. Kyseinen pelkästään best-effort -liikenteeseen perustuva malli on ollut käytössä pitkään, sillä best-effort vaatii käytännössä toimiakseen sen, että suurin osa liikenteestä käyttää TCP:tä. Varsinkin IP-liikennöinnin alkuvaiheessa laadulliset seikat jätettiin huomiotta; kaikki liikenne oli keskenään samanarvoista.

2.1 SLM – palvelutasonhallinta

Ennen kaikkea liikeyrityksille tärkeä palvelutasonhallinta (SLM, Service Level Management) edesauttaa käyttäjän kokeman laadun onnistunutta toteuttamista ja toteutumista. Palvelutasonhallinta kuvaa jatkuvaa, asiakkaan tarpeiden mukaista palvelun tuottamista ja laadukkuuden toteutumisen seurantaa sekä näihin liittyviä toimenpiteitä. Palvelutasonhallinnan tärkein päämäärä onkin liiketoimintakriittisten palveluiden toimivuuden ja laadun ja sen myötä asiakkaan tyytyväisyyden sekä taloudellisen kannattavuuden varmistaminen ja kasvattaminen. Palvelutasonhallintaan liittyvät oleellisesti palvelutasosopimukset (SLA, Service Level Agreement). Näillä tarkoitetaan palveluntarjoajan ja asiakkaan välisiä kirjallisia sopimuksia, joihin on kirjattu määritellyt palvelutasotavoitteet (SLO, Service Level Ojectives)[1].

Palvelutasonhallinta seuraa toteutunutta palvelutasoa verraten sitä määritettyihin palvelutasotavoitteisiin. Palvelutasohallinnan avulla hallitaan ja parannetaan osapuolten välistä palvelutasoa. Mikäli jokin palvelutasosopimuksessa määritelty palvelutasotavoite ei täyty, on palveluntarjoaja velvoitettu korvaukseen sopimuksen mukaisesti. Sanktioiden perimmäinen idea ei kuitenkaan ole palveluntarjoajan rankaiseminen virheistä, vaan luottamuksen ja yhteistyön lisääminen osapuolten välille sekä ennen kaikkea molemminpuolinen pyrkimys parempaan laatuun. Sanktioilla

saadaan taattua asiakkaalle tietty laatu ja toisaalta palveluntarjoaja saadaan kiinnostumaan enemmän myös oman verkkonsa resurssien seurannasta sekä päivittämisestä. Lisäksi palveluntarjoaja pystyy palvelutasonhallinnan avulla helpommin jakamaan verkkonsa resurssit tehokkaasti parantaen näin kustannustehokkuutta. Toisaalta palvelutasosopimuksilla ja palvelutasonhallinnalla ylipäätään voidaan myös varmistaa, että asiakkaan odotukset eivät kasva jatkuvasti ylittäen palvelun realistiset toteutusmahdollisuudet, vaan asiakaskin on selvillä tarjottavasta palvelusta, sen laadusta ja laajuudesta.

Palvelutasonhallintaan kuuluu oleellisena osana jatkuva-aikainen laadun parantaminen. Usein tämä toteutetaan asiakkaan ja palveluntarjoajan välisillä, esim. kuukausittain pidettävillä laatu- ja seurantapalavereilla, joissa käydään läpi edellisen kuun toteutuneet palvelutasot sekä selvitetään mahdollisia ongelmatilanteita ja niiden syitä. Lisäksi pyritään miettimään mahdollisia kehitysideoita ja korjaavia toimenpiteitä jatkoa ajatellen. Palveluntarjoaja myös raportoi asiakkaalle säännöllisesti palveluista.

2.1.1 SLA - palvelutasosopimukset

Palvelutasosopimuksessa kuvataan sopimusosapuolten eli asiakkaan ja palveluntarjoajan keskenään sopimat palveluiden yksityiskohdat. Palvelutasosopimukseen on määritelty kirjallisesti sovitut tavoitearvot, joihin palveluntarjoaja sitoutuu tarjotessaan asiakkaalle tiettyä palvelua. Palvelutasosopimuksessa pyritään kuvaamaan toimivuuden kannalta kriittiset kohteet, joiden vaikutus koko palvelun toimivuuteen on oleellisen suuri. Kyseisille kriittisimmille kohteille on määritelty tietyt saatavuuden arvot, joiden rajoissa kohteiden tulee toimia. Mikäli raja alittuu, palveluntarjoaja joutuu maksamaan asiakkaalle sopimuksen mukaisesti sanktioita. Usein tärkeimpänä kohteena pidetään IT-palvelun kokonaiskäytettävyyttä. Palvelutasosopimukset tukevat osaltaan palvelutasonhallintaa ja antavat hyvän pohjan palvelutasonhallinnan toteuttamiselle. Tärkeä vaade palvelutasosopimusten suhteen on se, että ne ovat täysin yksiselitteisiä, jotta tulkinnanvaraa ei pääse syntymään. Ei saisi siis päästä syntymään tilannetta, jossa sopimukseen on kirjattu, että lyhyet katkokset eivät vaikuta kokonaiskäytettävyyteen, sillä palveluntarjoajalla ja asiakkaalla saattaa olla täysin erilaiset käsitykset lyhyestä

katkoksesta ja sen vaikutuksista liiketoimintaan. Edellä mainitun takia SLA-sopimukset pitää määritellä tarkasti ja yksiselitteisesti.

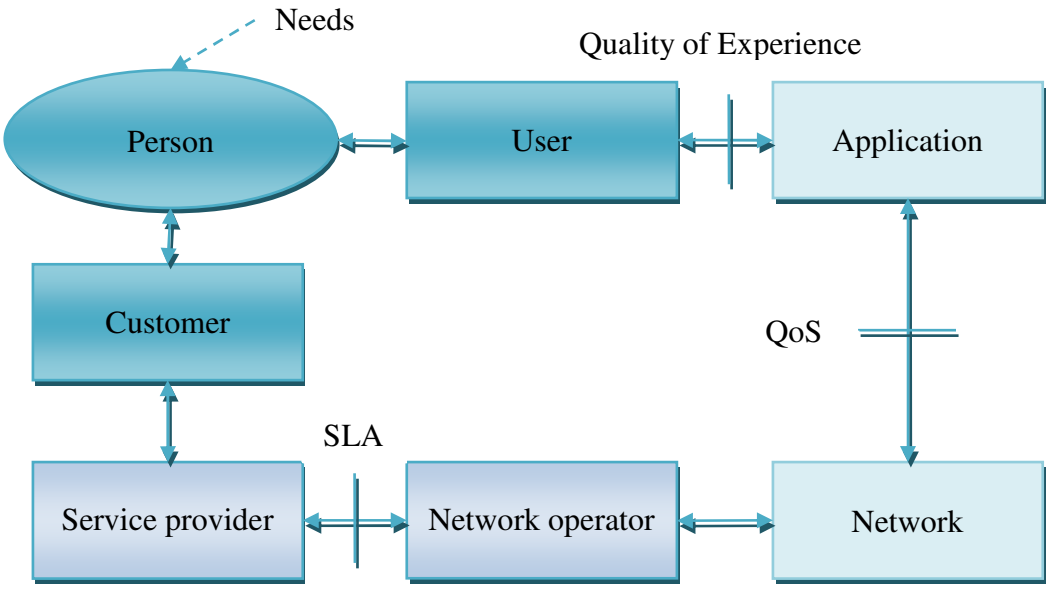
2.1.2 SLO - palvelutasotavoitteet

Palvelutasotavoitteet ovat yksittäisiä, teknisiä laatumääreen tavoitearvoja, jotka tuovat yleisellä tasolla kuvatut SLA:t todenmukaisemmiksi ja joita on helpompi mitata käytännössä. Palvelutasotavoitteiden tulee olla asiakkaankin kannalta ymmärrettäviä. Toisaalta on tärkeää pystyä hahmottamaan, miten yksittäisistä alemman tason palvelutasotavoitteista saadaan koottua asiakkaalle määriteltävä ylemmän tason palvelutasokuvauskokonaisuus.

2.2 Palvelunlaatu, palvelunlaatuparametrit ja käyttäjän kokema laatu

Palvelutasonhallinnan perimmäisenä ideana on liiketoiminnan tukemisen lisäksi pyrkiä takaamaan mahdollisimman hyvä käyttäjän kokema tietoliikennepalveluiden laadukkuus (QoE, Quality of Experience). QoE kuvaa palvelun laadukkuutta nimenomaan käyttäjän kannalta ja se on erotettu tässä tutkimuksessa palvelunlaatutoimenpiteistä, eli parametreista ja mekanismeista, joilla laatua parannetaan. Jälkimmäisessä tapauksessa puhutaan QoS:stä (Quality of Service). On kuitenkin huomioitava, että yleisesti kirjallisuudessa puhutaan usein QoS:stä ylipäätään palvelunlaadusta ja laadukkuudesta puhuttaessa. Tässä tutkimuksessa *palvelunlaatu* -käsitettä käytetään puhuttaessa aiheesta yleisellä tasolla, *QoE* kuvastaa käyttäjän kokemaa laatua ja *QoS* taas menetelmiä ja mekanismeja, joita käytetään *palvelunlaadun* parantamiseen [2].

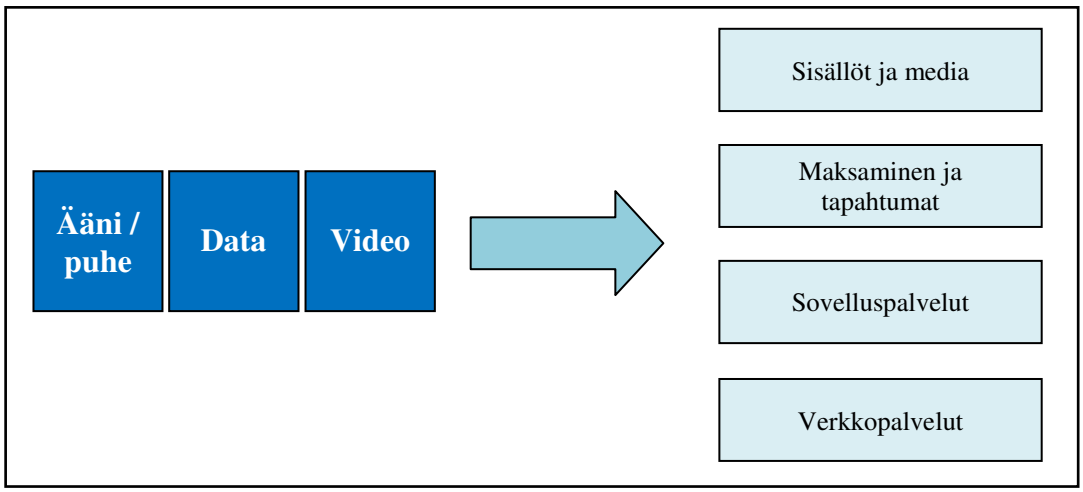
Alla olevassa kuvassa on kuvattu eri toimijoiden suhteet SLA:han, QoS:ään ja QoE:hen liittyen.



Kuva 2. Kilkki: Framework for analyzing communications ecosystem. Muokattu alkuperäisestä kuvasta [2]

Kuvassa yksittäisellä henkilöllä (Person) on tarpeita (Needs), joiden tyydyttämiseksi hän tilaa tietynlaisen palvelun palveluntarjoajalta (Service provider), jolloin henkilö on asiakas (Customer). (Loppu)käyttäjäksi (User) henkilö muuttuu käyttäessään jotain sovellusta (Application). Palveluntarjoaja on taas vastaavasti yhteydessä verkko-operaattoriin (Network operator) fyysisen verkon vuokrauksen osalta. SLA-sopimukset solmitaan sekä välille asiakas – palveluntarjoaja (palveluoperaattori) että palveluntarjoaja – verkko-operaattori. Huomioitavaa kuvassa on QoS:n ja QoE:n sijainti. QoS kuvastaa verkon (Network) ja sovelluksen välistä rajapintaa, kun taas Quality of Experience (QoE) eli käyttäjän kokema laatu kuvaa nimenomaan käyttäjän ja sovelluksen välistä rajapintaa, eli sitä laatua, minkä käyttäjä kokee käyttäessään tiettyä palvelua tai sovellusta. Tämä onkin tärkein mittari sekä loppukäyttäjän kannalta, että myös verkko-operaattorin ja palveluntarjoajan kannalta, sillä asiakkaan tyytyväisyyden maksimoiminen on paras kassavirran tae. Usein QoS-mekanismit edesauttavat QoE:n kasvamista, mutta aina ei näin ole. Tästä syystä QoE on erotettu omaksi osiokseen, sillä vain se kuvastaa loppukäyttäjän ja samalla asiakkaan kokemaa laatua.

Lisääntynyt puhe- ja videodatan hyödyntäminen tietoverkoissa sekä tärkeiden palveluiden kasvanut määrä on tuonut haasteita liikennöinnin suhteen. Nykyään vaaditaan yhä useammin, että tiettyjen pakettien on päästävä eteenpäin varmasti ja lyhyessä ajassa. Erilaiset reaaliaikaiset sovellukset kaipaavat laadukasta ja nopeaa tiedonsiirtoa toimiakseen kunnolla. Verkkokonvergenssi eli erilaisten osioiden (tv, puhe, data) integroituminen yhteen on omiaan kasvattamaan vaatimuksia verkon suhteen. Ylipäätään ollaan menossa vertikaalisesta palveluarkkitehtuurista horisontaaliseen. Aiemmin jo ATM:n (Asynchronous Transfer Mode) yhteydessä tavoiteltu eri osioiden yhdistäminen hiipui Internetin myötä. Internetissä jokainen tietotyyppi on oma itsenäinen kokonaisuutensa (video, puhe, data). Nykyään ja tulevaisuudessa asiat nähdään kuitenkin ennemminkin erilaisina palveluelementteinä, joita voidaan yhdistellä ja muokata tarpeen mukaan kuvan 3 mukaisesti. IMS (IP Multimedia Subsystem) on tärkeä tekijä konvergenssin edesauttajana. Se on standardoitu multimediakontrolliteknologia pakettikytkentäisiä verkkoja ja erilaisia liityntätyyppejä varten (esim. WLAN, UMTS, WiMAX, @450, joista jatkossa enemmän). IMS mahdollistaa erilaisten päätelaitteiden välisen kommunikoinnin käytetystä liityntätekniikasta ja verkosta riippumatta [3]. Täytyy kuitenkin huomioida, että myös IMS sisältää haasteita ja ongelmia, jotka ovat omiaan ainakin viivästyttämään verkkokonvergenssin toteutumista.



Kuva 3. Verkkokonvergenssi. Muokattu alkuperäisestä kuvasta [4]

QoS pyrkii vastaamaan kasvaneiden vaatimusten aikaansaamiin haasteisiin pakettien luokittelun sekä priorisoinnin avulla. QoS-parametrien avulla pyritään hyödyntämään tarjolla oleva kapasiteetti mahdollisimman hyvin ja takaamaan tietyille sovelluksille tai palveluille riittävän hyvä laatu. QoS:llä tarkoitetaan kaikkia niitä mekanismeja ja toimenpiteitä, joiden avulla pyritään takaamaan hyvä ja vaaditunlainen toimivuus sovelluksille [5]. Käyttäjät taas näkevät tilanteen usein sovellustason kannalta. Mikäli sovellus ei toimi toivotulla tavalla, ei käyttäjä voi tietää tarkemmin, onko kyse verkon ruuhkautumisesta, sovelluksen hitaudesta vai jostain muusta. Käytännössä siis QoS:n eli palvelunlaadun mekanismien avulla yritetään saada käyttäjän kokema QoE mahdollisimman korkeaksi.

QoS:n avulla paketeille voidaan määritellä erilaisia prioriteettiluokkia sen mukaan, mitä asiakas on palvelusta valmis maksamaan ja miten tärkeänä asiakas näkee tietyn palvelun toimivuuden. Tällöin tietyntyyppinen liikenne saa paremman kohtelun muuhun liikenteeseen verrattuna. Ruuhkatilanteessa paketteja lähdetään tiputtamaan ei-priorisoiduista paketeista eli best-effort -liikenteestä alkaen. QoS ei itse sinänsä tarjoa lisää kaistaa vaan mahdollistaa käytettävissä olevan kaistan mahdollisimman tehokkaan käytön. Täytyy siis pitää mielessä, että korkeamman prioriteetin määrittely tietyille paketeille ei kuitenkaan lisää käytettävissä olevien resurssien määrää. Näin ollen priorisoidut paketit saavat paremman liikennöintimahdollisuuden ei-priorisoitujen pakettien kustannuksella.

2.2.1 QoS-parametrit

QoS:n avulla pyritään minimoimaan IP-verkon pakettihävikkiä, viivettä ja viiveen vaihtelua sekä toisaalta joiltain osin maksimoimaan läpäisykykyä. Kuten edellä on kuitenkin huomioitu, QoS ei tarjoa lisää läpäisykykyä vaan mahdollistaa senhetkisen läpäisykyvyn paremman jaon eri pakettien kesken. Kaikki edellä mainitut suureet ovat palvelunlaatuparametreja, jotka liittyvät oleellisesti verkon toimivuuteen sekä tiedonsiirtokykyyn ja vaikuttavat näin ollen suoraan asiakkaan kokemukseen. Yleisimmät palvelunlaatuparametrit ovat:

- Pakettihävikki
- Viive

- Viiveen vaihtelu (jitter)
- Läpäisykyky (kaistanleveys)

Pakettihävikki kuvaa sitä, miten suuri osa lähetetyistä paketeista ei saavu vastaanottajalle asti. Yleensä luku kuvataan prosentteina, eli esimerkiksi 1 %:n pakettihävikki tarkoittaa sitä, että keskimäärin joka sadas paketti tippuu matkalla eikä saavu ikinä vastaanottajalle asti.
Viive on yksi tärkeimmistä palvelunlaatuparametreista. Se kuvaa aikaa, joka yhdellä paketilla kuluu sen kulkiessa lähettäjältä vastaanottajalle. Usein puhutaan myös *latenssista.*
Viiveen vaihtelulla (engl. *jitter*), joka vaikuttaa haitallisesti ennen kaikkea puheliikenteeseen, kuvataan aikaa, jonka verran edellä mainittu *viive* vaihtelee tutkittavalla välillä.
Läpäisykyky eli *kaistanleveys* mielletään yleensä palvelunlaatuparametriksi, vaikka sitä voidaan sanoa myös määrä (quantity)-parametriksi. Se kuvaa sitä, miten paljon dataa verkko pystyy tietyllä hetkellä kuljettamaan.

2.2.2 Ruuhkanhallinta

Verkkoresurssien mahdollisimman tehokas ja halutunlainen jakaminen sekä samalla palvelunlaatuparametrien hyvä toteutuminen aikaansaadaan useiden erilaisten mekanismien avulla. Verkon päätelaitteissa voidaan ottaa käyttöön erilaisia ruuhkanhallinta- ja ajoitusmenetelmiä, jolloin pakettien kulkeutumista verkossa pystytään säätelemään. Osa paketeista voidaan ruuhkatilanteessa laittaa puskuriin odottamaan lähetystä eteenpäin ja toisaalta menetelmästä riippuen osa paketeista voidaan ruuhkatilanteessa tiputtaa.

Tässä työssä erotellaan ruuhkanhallintamenetelmät ja ajoitusmenetelmät (engl. *scheduling*) toisistaan. Suurin ero kahden edellä mainitun välillä on se, että ajoitusmenetelmät hoitavat pakettien välityksen tietyssä järjestyksessä reitittimiltä eteenpäin. Ruuhkanhallintamenetelmät taas hoitavat ylimääräisten pakettien tiputtamisen, mutta eivät huolehdi pakettien välityksestä eteenpäin [6].

Liikenteen luokittelun yhteydessä otetaan käyttöön käsite *vuo*. Vuolla tarkoitetaan paketteja tai eräänlaista sarjaa peräkkäisiä tosiinsa kuuluvia paketteja, joilla on sama lähdeosoite sekä määränpää ja samanlaiset laadulliset vaatimukset keskenään. Verkon laitteet jakavat paketit omiin voihinsa edellä mainittujen kriteerien perusteella. Tietyn vuon liikenne ohjataan sitten halutun ajoitusmekanismin mukaisesti eteenpäin. Verkkolaitteiden pitää siis ensinnäkin hoitaa pakettien luokittelu omiin voihinsa ja toisaalta huolehtia ajoitusmenetelmistä, joiden perusteella voiden liikenne ohjataan eteenpäin.

Purskeisesta liikenteestä johtuen verkkolaitteet saattavat toisinaan ruuhkautua. Tällöin pitää olla tiedossa, minkälaista menettelyä käytetään pakettien käsittelyssä ja välittämisessä eteenpäin. Erilaiset menetelmät vaikuttavat pakettien kulkemiseen vasta siinä vaiheessa, kun reitittimelle alkaa kasautua paketteja. Menetelmästä riippuen paketit joutuvat joko odottamaan verkkolaitteen puskurissa tietyn ajan ennen jatkolähetystä tai vaihtoehtoisesti osa paketeista tiputetaan kokonaan.

Yksinkertaisimmassa menetelmässä paketit lähetetään eteenpäin siinä järjestyksessä, jossa ne reitittimelle saapuvat. Ruuhkan sattuessa voidaan joko ohjata kaikki paketit yhteen ja samaan jonoon FIFO-periaatteen (First In – First Out) mukaisesti (puhutaan myös FCFS, eli First Come First Served -periaatteesta) lähettäen paketit eteenpäin tulojärjestyksessä, tai vaihtoehtoisesti ohjata paketteja useampaan jonoon, joita palvellaan eri prioriteeteilla. Erilaisia ajoitusmenetelmiä on olemassa useita. FIFO:n lisäksi tunnetuimpia ovat esimerkiksi PQ (Priority Queuing), CQ (Custom Queuing), WFQ (Weighted Fair Queuing), WRR (Weighted round-robin), CBWFQ (Class-based Weighted Fair Queuing) ja LLQ (Low-Latency Queuing). Mahdollista on myös käyttää jo ennakoivasti erilaisia ruuhkanhallintamenetelmiä, kuten tail drop, RED (Random Early Detection), RIO (Random Early Detection In/Out) tai WRED (Weighted Random Early Detection), mutta adaptiiviset ajoitusmenetelmät mahdollistavat tarkemman palvelunlaadullisen liikenteen erottelun välitettäessä paketteja eteenpäin[7].

Alla olevassa taulukossa 1 on kuvattu yleisimmät jonotusmekanismit, joiden perusteella valitaan ruuhkautumistilanteissa ylimääräisten pakettien tiputtamisesta.

Taulukko 1. Tunnetuimmat ruuhkanhallintamenetelmät [6]

Menetelmä	Kuvaus	Vahvuudet	Heikkoudet
Tail drop	Jos jono on täysi, saapuva paketti tiputetaan. Muutoin paketti menee jonon viimeiseksi	Yksinkertainen algoritmi	Puskurin koon ollessa suuri viive kasvaa turhan suureksi
RED	RED alkaa tiputtaa satunnaisia paketteja lineaarisesti kasvavalla todennäköisyydellä, kun tietty alempi kynnysarvo on saavutettu. Kun päästään ylempään kynnysarvoon, toimii RED tail dropin tapaan ja tiputtaa jatkossa kaikki paketit	Antaa hyvissä ajoin tietoa ruuhkan lisääntymisestä, jolloin lähettäjä osaa hidastaa lähetysnopeutta (perustuu siis TCP:n ominaisuuteen säädellä lähetysnopeuttaan). Kohtalaisen pieni jononpituus sekä suuri läpäisy	Osa puskurin vapaasta tilasta hukataan tiputtamalla paketteja osittain jo ennen jonon täyttymistä. Toisaalta ruuhkatilanteessa paketteja tippuu paljon, eli keskimääräinen jonon koko vaihtelee paljon
RIO	Verrattavissa RED:iin, mutta sillä lisäyksellä, että paketit jaettu kahteen luokkaan, ”In” ja ”Out” – profiiliin. Out-luokassa pienempi minimikynnysarvo, joten Out-luokasta aletaan tiputtaa ensin paketteja. Kun jonon koko kasvaa, myös In-luokasta aletaan tiputtaa paketteja	RED:iin verrattuna saadaan haluttu In-luokan liikenne välitettyä paremmin Out-liikenteen kustannuksella	Toimii vastaavalla tavalla kuin RED, joten osa puskurin tilasta hukataan tiputettaessa osa paketeista aikaisessa vaiheessa
WRED	Myös WRED pohjautuu RED:iin. Käyttää lisänä IP-paketin otsikkokentän IP-Precedence – arvoa painottamaan heikomman arvon paketin pudotustodennäköisyyttä	QoS toteutuu aiempiin verrattuna paremmin. Monipuolisempaa ja paremmin yksilöityä liikenteenhallintaa eri luokkien ja kynnysarvojen johdosta	Ei-priorisoitu liikenne kärsii aiempiin verrattuna enemmän WRED:iä käytettäessä. Ei-IP-liikenne myös alimmassa luokassa

Tail drop on yksinkertaisin menetelmä tiputtaen jonon täyttyessä paketteja pois. Käytännössä tämä tarkoittaa sitä, että verkkolaite ei voi estää korkean prioriteetin pakettiakaan tippumasta, mikäli jono on täynnä. Tämän takia on olemassa esim. WRED:n tapaisia ruuhkanhallintamenetelmiä, joissa voidaan ennakoivasti hallita jonoa niin, ettei se täyty äärimmilleen. Tämä tapahtuu tiputtamalla jonon kasvaessa osa alemman prioriteetin paketeista pois, vaikkei jono vielä täynnä olekaan. Näin korkean prioriteetin paketit pääsevät todennäköisemmin tippumatta eteenpäin. Sekä RED että

WRED soveltuvat kuitenkin lähinnä TCP-liikenteelle, ja UDP (User Datagram Protocol)-liikenne vaatii toimiakseen toisenlaisia menetelmiä.

Taulukossa 2 kuvataan yleisimpiä ajoitusmenetelmiä, sekä niiden vahvuuksia ja heikkouksia.

Taulukko 2. Tunnetuimmat ajoitusmenetelmät [6],[7]

Menetelmä	Kuvaus	Vahvuudet	Heikkoudet
FIFO	Yksinkertainen best-effort konsepti, jossa paketteja palvellaan saapumisjärjestyksessä. Ei vaadi verkkolaitteilta erityistä konfigurointia	Yksinkertaisuus ja helppous, ei vaadi verkkolaitteilta erikoisuuksia. Tasoittaa hyvin purskeita, kun kuormitus on pieni	Kun kuormitus korkea, aiheutuu kaikille paketeille viivettä/hävikkiä ja myös korkean prioriteetin liikenne kärsii. Ei sovi kriittiselle liikenteelle
PQ	PQ määrittelee neljä jonoa (high-, medium-, normal- ja low-luokat) ja purkaa jonot tyhjäksi aina korkeimmasta prioriteetista alkaen	Varmistaa puheliikenteen kulun pienelläkin kaistalla. Korkean prioriteetin paketit hyvässä asemassa	Sekä heikkoutena että vahvuutena voi pitää sitä, että PQ toimii täysin korkea-prioriteettisten pakettien ehdoilla
CQ	Erona PQ:hon se, että CQ ei varmista korkean prioriteetin jonon läpimenoa pienemmän prioriteetin kustannuksella. Tärkeälle liikenteelle varataan tietty kaista ja muulle liikenteellekin minimikaista	Parantaa alemman prioriteetin liikenteen tilannetta PQ:hon verrattuna	Konfigurointi vaikeaa, korkean prioriteetin paketit hieman huonommassa asemassa kuin PQ:ssa
WFQ	Jaottelee liikenteen eri liikennevirtojen perusteella ja asettaa erityyppiset liikennevirrat eri jonoihin. Jokaista jonoa palvellaan yhtäaikaisesti	Suuret datamäärät eivät kuluta kaikkea kaistaa ja estä pienten, usein tärkeiden datamäärien kulkua	Ei sovellu suurinopeuksisille yhteyksille. Laskenta aiheuttaa ylimääräistä kuormaa
WRR	Perinteinen RR (round-robin) purkaa jokaisesta jonosta vuo-ronperään paketin tasapuolisesti, WRR taas mahdollistaa eri jonoille annettavat erilaiset painoarvot, jolloin tiettyjen jonojen paketteja saadaan hieman nopeammin eteenpäin	Monipuolistettu versio RR:stä. Saadaan nopeutettua tärkeiden pakettien lähetystä eteenpäin	Ei riittävän hyvä reaaliaikaiselle liikenteelle

CBWFQ	WFQ:n tapainen, mutta liikenteen jaottelu luokittelun avulla. Tällöin liikennevirtoja voidaan laittaa myös samaan jonoon. Tietyn luokan liikenteelle on lisäksi mahdollista allokoida haluttu kaista	Monipuolinen ja paranneltu versio WFQ:sta	Monimutkainen. Ei kovin nopeille yhteyksille
LLQ	Mahdollistaa prioriteettijonon luomisen, jolloin tälle varataan tietty kaista ja tämä jono tyhjennetään PQ-periaatteen mukaisesti ennen muita. Lisäksi muut jonot CBWFQ:n tavoin luokitteluperiaatteella ja kaistanvarauksella	Reaaliaikaiset sovellukset saavat tarvitsemansa kaistan ja toisaalta dataliikenteellekin pystytään optimoimaan halutut käsittelytavat	Monimutkainen

Edellä kuvatut menetelmät pyrkivät kaikki jakamaan paketteja verkkolaitteelta eteenpäin tietyllä tavalla. Perimmäisenä ajatuksena voidaan pitää sitä, että tärkeälle korkeasti priorisoidulle liikenteelle tulee taata riittävä kaista kuitenkin niin, että myöskään pienemmällä prioriteetilla oleva liikenne ei tukkeutuisi täysin. Tärkeintä on saada säilytettyä kaistan suhteellinen jako loppukäyttäjien välillä halutunlaisena.

2.2.3 MPLS

Yksi nykyään varsin yleisesti käytetty verkonhallintaratkaisu MPLS (MultiProtocol Label Switching) on IETF:n (Internet Engineering Task Force) kehittämä arkkitehtuuri, jonka tavoitteena on tehostaa reititystä IP-verkoissa ja näin epäsuorasti mahdollistaa palvelunlaadun parempi toteutuminen [8]. MPLS-arkkitehtuurin ideana on parantaa IP-verkoissa perinteisesti vallalla olevaa tilannetta, jossa verkon jokainen reititin tekee reitityspäätöksen itsenäisesti tutkittuaan IP-paketin otsikkokenttää. MPLS-verkossa paketin eteen lisätään eräänlainen vakiokokoinen leima (label), jonka perusteella paketti kulkeutuu oikeaan kohteeseen haluttua reittiä pitkin. Leiman avulla paketti määritellään kuuluvaksi tiettyyn FEC:iin (Forwarding Equivalency Class). FEC on ryhmä paketteja, jotka ohjataan samalla tavalla eteenpäin. MPLS-ominaisuuksilla varustetut LSR-reitittimet (Label Switched Router) ohjaavat paketit leimojen perusteella eteenpäin seuraavalle reitittimelle ja lisäävät uuden oikean leiman paketin otsikkokenttään. Polku, jota pitkin paketti MPLS-verkossa kulkee, on nimeltään Label-switched Path (LSP). MPLS-verkon reunalle saavuttuaan paketin MPLS-leima poistetaan [8].

MPLS-verkkoteknologia sopii hyvin kuvan ja puheen kuljettamiseen. Verkko on nopea toipumaan verkkolaitteen tai linkin kaatumisesta [9] ja kaiken kaikkiaan MPLS-verkko mahdollistaa QoS:n hyvän toteuttamisen ja toteutumisen, vaikkei se suora synonyymi QoS:lle tai palvelunlaadulle olekaan.

2.2.4 Yhdistetyt palvelut - Integrated Services (IntServ)

Yhdistetyt palvelut on arkkitehtuuri, jossa jokaiselta paketin välittävältä IP-verkon laitteelta pyydetään palvelunlaadullista resurssivarausta, joka tehdään vuopohjaisesti [10]. Varauksiin käytetään merkinantoprotokollaa, usein RSVP:tä (Resource Reservation Protocol). Arkkitehtuurikonsepti voidaan jakaa kahteen osaan, kontrolliosaan sekä dataosaan. Kontrolliosa on vastuussa varausten tekemisestä ja dataosa itse liikenteen kuljetuksesta kontrolliosan varausten perusteella.

IntServ-arkkitehtuuria ei ole otettu laajalti käyttöön osittain sen takia, että malli ei ole kovin skaalautuva erityyppisiin verkkoihin. Signaloinnin suhteen IntServ muodostaa point-to-point -yhteyden, jota ylläpidetään vuokohtaisesti. Se on kohtalaisen raskas arkkitehtuuri, sillä varaukset tulee tehdä jokaiselle verkon solmulle, joka tukee IntServiä.

2.2.5 Eriytetyt palvelut - Differentiated Services (DiffServ)

Jo pitkään huomattavasti IntServiä käytetympi arkkitehtuuri DiffServ eli *eriytetyt palvelut* on OSI-mallin 3. verkkokerroksen arkkitehtuuri [11],[12]. Se on käytännössä vastakohta edellä kuvatulle IntServ -arkkitehtuurille, sillä DiffServ ei vaadi päästä-päähän signalointia IntServin tapaan. Se ei myöskään pyydä jokaiselta laitteelta palvelunlaadullista resurssivarausta, kuten IntServ. DiffServ luokittelee paketit IP-otsikkotiedoista löytyvän ToS-kentän (Type of Service) arvon mukaan. Luku kuvaa paketin prioriteettiarvoa ja ensimmäistä kuutta bittiä ToS-kentässä kutsutaan myös DSCP:ksi (DiffServ Code Point). DiffServiä käyttävässä verkossa liikenne luokitellaan DSCP:n perusteella erilaisiin luokkiin ja näiden pohjalta valitaan hyppykohtaiset säännöt, PHB (Per Hop Behaviour), jotka liitetään pakettiin DSCP-tunnisteen avulla. PHB määrittelee sen, miten kutakin luokkaa tulisi kohdella. Resurssit allokoidaan

liikenneluokkakohtaisesti, kun IntServissa allokointi tapahtuu vuokohtaisesti. Toisin sanoen mikäli DiffServissä jokin tietyn luokan vuo alkaa kuluttaa enemmän resursseja, on se pois muilta kyseisen luokan voilta. Tämän johdosta DiffServ-verkossa mitataan ja säännöstellään voita. DiffServ määrittelee kolme erilaista PHB:ta eli liikenneluokkaa, jotka prioriteettijärjestyksessä ovat EF (Expedited Forwarding) eli parannettu palvelu, AF (Assured Forwarding) eli taattu palvelu sekä BE (best-effort) eli normaali palvelu [11]. Kahden ensin mainitun luokan paketteja ei saa pilkkoa.

Edellä mainituista DiffServ-palveluluokista EF on suunniteltu takaamaan parhaimman laadun. Sen tarkoituksena on tarjota päästä-päähän laatua alhaisilla viiveen, viiveen vaihtelun ja pakettihävikin arvoilla sekä toisaalta taatulla kaistalla. EF on suunniteltu ennen kaikkea reaaliaikaisen tiedon siirtoon ja se soveltuukin hyvin esimerkiksi UDP-protokollalle ja sen käyttämille reaaliaikasovelluksille.
AF taas tarjoaa BE-liikenteeseen verrattuna parempaa palvelua tarjoamalla erilaisia tasoja, joille varataan jokaiselle jokin tietty minimikaista. AF soveltuu TCP-liikenteelle, sillä TCP-pakettien lähetyksessä pystytään tarvittaessa pienentämään lähetysikkunan kokoa reagoiden näin pakettien tippumisiin.
Kolmas luokka, BE, on tarkoitettu datapaketeille, jotka eivät vaadi erityistä QoS:ää.
Huomionarvoista kuitenkin on, että DiffServ ei pysty takaamaan tiettyä päästä-päähän laatua. Ennemminkin se mahdollistaa verkon resurssien mahdollisimman hyvän hyödyntämisen palveluluokkien mukaisesti.

2.3 Yhteenveto

Operaattoreiden ja palveluntarjoajien täytyy olla jossain määrin jatkuvasti kiinnostuneita tarjoamiensa tietoliikenneverkkojen palvelunlaadusta. Itse QoS-mekanismien käyttöönoton edellytyksenä on kuitenkin se, että operaattori hyötyy rahallisesti näiden käyttöönotosta ja hyödyntämisestä. Mikäli näin ei ole, ei operaattoreilla ole kiinnostusta kehittää tai edes ottaa käyttöön erillisiä QoS-mekanismeja, sillä eri verkkolaitteet vaativat lisämekanismeja ja päivitystä sekä konfigurointia, jotta niissä pystytään ottamaan mahdollisimman hyvät ja monipuoliset QoS-ominaisuudet kunnolla käyttöön. Mikäli laiteinvestointeihin kuluvat kustannukset (CAPEX) sekä investointeihin liittyvän työvoiman käytön kustannukset (OPEX) eivät

jatkossa tuota riittävästi rahaa yritykselle, ei yrityksellä ole mielenkiintoa lähteä viemään QoS:n kunnollista toteuttamista eteenpäin [13].

Operaattorilla on mahdollisuus varata kaistaa käyttöön niin paljon, että sitä on kaikille käyttäjille aina riittävästi. Vaikka runkoverkossa vapaa käyttämätön kaista ei merkittävä kustannustekijä olekaan, tämä ei aina kuitenkaan ole kustannustehokas ratkaisu ja tulee operaattorille kalliiksi varsinkin radiotiellä, sillä suurimman osan ajasta kaistaa olisi vapaana suurin osa tarjotusta. Parempi vaihtoehto onkin keskittyä ottamaan kaikki hyöty irti QoE:stä ja QoS:stä, jolloin pyritään pääsemään mahdollisimman optimaaliseen tilanteeseen, jossa kaista on mahdollisimman hyvin käytössä jatkuvasti, mutta jossa liikennöinti toisaalta sujuu kuitenkin hyvin myös verkon ruuhkatilanteissa. Tämä kaikki vaatii kuitenkin verkon tarkkaa tuntemusta ja osaamista ja edesauttaa osaltaan pitämään kiinnostuksen palvelunlaatua kohtaan edelleen kohtalaisen alhaisena.

Asiakkaan kannalta eri QoE-tasoihin pohjautuva hinnoittelumalli on hyödyllinen, sillä tällöin asiakkaalla on mahdollisuus maksaa haluamansa tasoisesta palvelusta. Hinnoittelu voi perustua esimerkiksi sovittuun yhteysnopeuteen, tiedonsiirtoviiveeseen, viiveen vaihteluun, pakettihävikkiin tai siirron tärkeysjärjestykseen. Palvelunlaatu paranee, kun asiakkaan täytyy maksaa vain tarvitsemastaan palvelusta. Mikäli asiakas kokee senhetkisen laatutason olevan liian alhainen, voi hän lisämaksua vastaan nostaa laatuluokitusta haluamalleen tasolle. Huomioitavaa kuitenkin on, että tavallisen loppukäyttäjän tapauksessa mahdolliset laadulliset parannuskeinot jäävät käytännössä kaistan kasvattamiseen tarvittaessa maksua vastaan. Yritysmaailmassa tilanne on kuitenkin tältä osin monipuolisempi ja esimerkiksi sopimuksentekovaiheessa pystytään määrittelemään operaattorin ja asiakkaan välillä yhteiset sovitut laatumääreiden arvot riippuen asiakkaan maksuhalukkuudesta ja tietoliikenneyhteyden toimintavarmuustason tarpeesta.

3. Langattomat verkot

Tässä osiossa käydään läpi yleinen kuvaus langattomista lähiverkoista sekä selvitetään erilaisten langattomien verkkotekniikoiden ominaisuuksia myös lähiverkkojen ulkopuolelta (WiMAX, @450, 3G). Pääasiassa keskitytään kuitenkin WLAN-käsitteen sisältöön.

3.1 Yleisesti langattomista verkkotekniikoista

Langattomat teknologiat ovat yleistyneet tietoliikenneverkoissa viime vuosina tekniikan kehittyessä, kysynnän kasvaessa ja tarjonnan monipuolistuessa. Ihmisten tottuessa uuteen tekniikkaan sitä aletaan pitää nopeasti itsestäänselvyytenä, joten tekniikan tulee pysyä mukana kehityksessä, jotta käyttäjät saadaan pidettyä tyytyväisinä vaatimusten kasvaessa. Langattomien tekniikoiden kantamat ovat pidentyneet, nopeudet kasvaneet ja käyttäjämäärät lisääntyneet, joten on oleellista käydä läpi tämän hetkistä tilannetta langattoman tarjonnan osalta, jotta jatkossa pystytään selvittämään puheen kulkua langattoman verkon yli. Tässä yhteydessä on kuitenkin hyvä huomioida, että langattomuuden lisääntyessä langalliset ratkaisut ovat kuitenkin edelleen tärkeässä roolissa. Esimerkiksi langattomatkin yhteydet yhdistyvät langattoman alkumatkan jälkeen kiinteään runkoverkkoon, eli ainoastaan viimeinen, loppukäyttäjälle näkyvä linkki on langaton.

VoIP-tekniikka (Voice over Internet Protocol) tarkoittaa puheen kuljetusta IP-verkon yli. Käytännössä puheenkuljetuksessa käytettävät tietoliikenneverkot ja sen pohjalta puheenkuljetus voidaan jakaa kolmeen erilliseen osioon; VoIP-käsitettä käytetään langallisissa IP-verkoissa, VoWIP-käsitettä (Voice over Wireless Internet Protocol) taas langattomissa IP-verkoissa (eli käytännössä WMAN-verkoissa (Wireless Metropolitan Area Network) ja VoWLAN:ia (Voice over Wireless Local Area Network) langattomissa lähiverkoissa. Huomioitavaa kuitenkin on, että usein VoIP-käsitettä käytetään kuvaamaan ylipäätään IP-puhetta riippumatta siitä, käytetäänkö langallista vai langatonta yhteyttä. Edellä mainittuja tutkitaan lähemmin neljännessä kappaleessa,

mutta lyhennelmät avattiin selvyyden vuoksi jo tässä vaiheessa, sillä langattomien verkkotekniikoiden yhteydessä käsitteet nousevat toisinaan esiin.

Nykypäivän langattomat verkkotekniikat voidaan mieltää lyhyen- ja pitkän kantaman teknologioiksi. VoWIP-kelpoiset pitkän kantaman langattomat verkkotekniikat pitävät sisällään WiMAX:in (Worldwide interoperability for Microwave Access), Flash-OFDM:n (Fast Low-latency Access with Seamless Handoff - Orthogonal Frequency Division Multiplexing), jonka pohjalta Suomessa on käytössä verkko-operaattori Digitan nimeämä @450-verkko, sekä 3G:n (Third Generation Mobile Technology). VoWLAN-tekniikka taas tarkoittaa puheen kuljettamista lyhyen kantaman langattoman lähiverkon, eli WLAN-verkon yli. Toisaalta VoWIP mielletään usein laajempana terminä VoWLAN:iin verrattuna tarkoittaen sitä, että VoWIP-konseptiin lasketaan usein mukaan myös WLAN. Langattomista verkkotekniikoista WLAN, WiMAX sekä @450 käyttävät kaikki OFDM:ää, kun taas mobiilipuolen 3G käyttää CDMA:ta [14].

Seuraavaksi käydään ensin lyhyesti läpi pitkän kantaman langattomia tekniikoita ja sen jälkeen jatkossa keskitytään tarkemmin lyhyen kantaman WLAN-tekniikkaan.

3.2 WiMAX

WiMAX on IEEE:n (Institute of Electrical and Electronics Engineers) määrittelemä standardi 802.16 [15]. Kyseessä on langaton laajakaistateknologia, josta käytetään myös WirelessMAN (Wireless Metropolitan Area Network) nimeä, mutta joka on WiMAX-foorumin myötä saanut itselleen nykyisin yleisesti käytetyn nimen WiMAX.

WiMAX:ia pidetään pääasiassa langallisen laajakaistayhteyden korvaajana syrjäseuduilla, joissa operaattoreiden ei käytännössä ole mahdollista toteuttaa langallista kupari- tai kuituyhteyttä niiden kalleuden, vähäisen asukasmäärän ja pitkien etäisyyksien vuoksi. Ensimmäinen versio WiMAX:sta (802.16-2004) ei mahdollistanut liikkumista ollenkaan, mutta uudempi mobiili-WiMAX (802.16e-2005) tuo parannuksen myös tähän ja mahdollistaa liikkuvuuden osittain jopa ajoneuvonopeuksissa asti [15]. IEEE:n kehitystyön tuloksena on lisäksi tulossa uusi 802.16m standardi, joka mahdollistaa liikkumattomassa käytössä jopa 1Gbps

yhteysnopeuden ilmarajapinnan yli. Tämän mahdollistaa MIMO:n (Multiple Input/Multiple Output) käyttö. 802.16m ei kuitenkaan ole suoranaisesti osa WiMAX:ia, mutta tulee IEEE:n ilmoituksen mukaan toimimaan sekä WiMAX:in että 4G:n (Fourth Generation Mobile Technology) kanssa [16]. WiMAX:in on sanottu alusta alkaen tukevan myös puhe- ja ääniliikennettä pienen latenssinsa ansiosta.

Tällä hetkellä WiMAX:in teoreettinen maksiminopeus on noin 70Mbit/s, mutta todellisuudessa nopeus jää usein maksimissaan noin 10Mbit/s nopeuteen, kun etäisyyttä tukiasemaan on kymmenisen kilometriä. Aiemmin vaadittiin näköyhteys tukiasemaan, mutta 802.16e toi pienemmän taajuuden ansiosta mukanaan NLOS-ominaisuuden (Non Line-Of-Sight), jolloin näköyhteyttä ei enää välttämättä tarvita.

WiMAX perustuu OFDMA:han (Orthogonal Frequency Division Multiple Access) ja lisäksi käytössä on FDD (Frequency Division Duplexing), joka mahdollistaa eri lähetys- ja paluukanavan, jolloin data voi kulkea yhtä aikaa molempiin suuntiin. 802.16 standardin arkkitehtuuri koostuu neljästä eri kerroksesta; sovituskerros (Convergence Layer), MAC(Medium Access Control)-kerros, kuljetuskerros (Transmission Layer) sekä fyysinen kerros (Physical Layer) [15]. Suomessa WiMAX toimii 3,5 MHz:n taajuusalueella.

3.3 @450

@450 on Digitan tarjoama entisen NMT (Nordisk Mobiltelefon)-verkon lopettamisen jälkeen vapautunut 450 MHz:n taajuusalueen digitaalinen matkaviestinverkko. @450-verkko on toteutettu Flash-OFDM -tekniikalla, eli ortogonaalisella taajuusjakoisella kanavoinnilla. Radiolähete sisältää useita kantoaaltoja, joita tarpeen mukaan jaetaan käyttäjien tiedonsiirtoon. Flash-etuliite viittaa nopeaan ja katkeamattomaan lyhyen vasteajan yhteyteen. Tekniikassa käytetään taajuusjakoista kahdennusta tarkoittaen sitä, että tulo- ja lähtökaista kulkevat eri taajuuskaistoilla. Yhden radiokantoaallon kaistanleveys on 1,25MHz, joten sekä tulo- että lähtökaista mahtuvat hyvin yhdelle taajuuskaistalle [17].

Digita toimii verkko-operaattorina myyden verkon kapasiteettia palveluoperaattoreille. Palveluoperaattorit sitten taas myyvät kyseisen verkon palveluita loppuasiakkaille. @450-verkossa on mahdollista hankkia korkean prioriteetin liittymä. Ruuhkatilanteessa tällainen liittymä saa etuoikeuden matalan prioriteetin liittymään nähden. @450-verkko ei kuitenkaan tue eri liikennetyyppien välistä priorisointia ainakaan vielä tässä vaiheessa ollenkaan.

@450 käyttää Mobile IP -tekniikkaa päätelaitteiden löytämiseksi ja tunnistamiseksi. Kaikki liikenne kulkee Digitan hallinnassa olevan kotireitittimen (engl. *Home Agent*) kautta. Myös verkon päätelaitteiden autentikoinnit tapahtuvat Digitan hallinnassa olevan AAA-palvelimen kautta. Flash-OFDM teknologian tarjoama teoreettinen maksiminopeus asiakkaalle päin on 5,3Mbit/s ja asiakkaalta verkkoon päin 1,8Mbit/s. Käytännössä maksiminopeus asiakkaan suuntaan on noin 1Mbit/s – 1,5Mbit/s ja asiakkaalta verkkoon päin 300kbit/s - 500kbit/s. Tällä hetkellä 1Mbit/s nopeuksinen yhteys on suurin, mitä markkinoilla on tarjolla. Keskimääräinen pakettien yksisuuntainen päästä-päähän -viive on noin 50ms, mikä mahdollistaa esimerkiksi VoIP:n käytön [17]. @450:n etuna esimerkiksi WiMAX:iin verrattuna on liikkuvuus. @450 toimii suurissakin nopeuksissa ja Digitan mukaan yhteys ei katkea 150 - 200 km/h nopeuksissakaan. Lisäksi tukiaseman vaihto onnistuu ilman yhteyden katkeamista toisin kuin WiMAX:ssa.

3.4 3G

3G on yleistynyt lyhenne kolmannen sukupolven matkapuhelintekniikoille. Yleisimmin tunnettu määritelmä on ITU-T:n (International Telecommunication Union - Telecommunication Standardization Sector) luoma [18]. Sen mukaan kolmannen sukupolven matkapuhelinjärjestelmän tulee tukea suuria bittinopeuksia, sallia joustava liikkuvuus sekä tukea multimediapalveluita. Kolmannen sukupolven matkapuhelinjärjestelmät perustuvat pakettikytkentäiseen, laajakaistaiseen nopeaan tiedonsiirtoon sekä Internet-yhteensopivuuteen. 3G:lle ei ole määritelty tarkkaa minimitiedonsiirtonopeutta, mutta rajana voidaan pitää 256 kbit/s nopeutta ja kykyä siirtää puheen lisäksi muutakin dataa.

Yksi tärkeimmistä 3G-standardeista on UMTS (Universal Mobile Telecommunications System). ETSI:n (European Telecommunications Standards Institute) määrittelemä UMTS:n radiorajapinta WCDMA (Wideband Code Division Multiple Access) on 3G-verkoissa yleisimmin käytetty radiorajapinta, eli tukiaseman ja päätelaitteen välinen ilmarajapinta. Se on maailmanlaajuinen standardi ja mahdollistaa pakettipohjaiset palvelut perustuen CDMA:han (Code Division Multiple Access) eli koodijakotekniikkaan. CDMA:ssa käyttäjät allokoidaan samalle taajuuskaistalle, mutta erotetaan toisistaan koodien avulla.

WCDMA:n päälle on kehitetty suurempiin nopeuksiin pystyvä HSPA (High Speed Packet Access), joka jakaantuu HSDPA:han (High Speed Downlink Packet Access) sekä HSUPA:han (High Speed Uplink Packet Access). HSPA on eräänlainen ohjelmistopäivitys WCDMA:lle. Perimmäisenä ideana on siirtonopeuden kasvattaminen. HSDPA nopeuttaakin liikennettä verkosta asiakkaalle päin kasvattamalla tehokkuutta ja vähentämällä linkin latenssia mahdollistaen näin esimerkiksi interaktiivisuuden paremman toteutumisen. Tämän hetkinen teoreettinen maksiminopeus asiakkaalle päin on 14.4 Mbit/s ja asiakkaalta verkkoon päin 5,8 Mbit/s (kun HSUPA käytössä). Tällä hetkellä operaattorit ovat Suomessa käytännössä jo päivittäneet tai päivittämässä 3,6 Mbit/s nopeuden tekniikkaa ylöspäin 7,2 Mbit/s nimellisnopeuteen. Operaattorit kuitenkin tarjoavat nykyisin maksimissaan viiden megabitin nopeutta. Elisa ja muut operaattorit ovat kuitenkin luvanneet, että viimeistään vuoden 2009 aikana operaattorit tulevat tarjoamaan jo 10 Mbit/s nopeuksista kaistaa verkosta asiakkaalle päin [19].

Suomalaisista teleoperaattoreista ainakin Elisa on päivittänyt HSPA-verkkoaan myös HSUPA:n osalta ja se on ilmoittanut ottaneensa käyttöön elokuussa 2007 myös HSUPA-tekniikan, jossa tiedonsiirtonopeus asiakkaalta verkkoon päin saadaan nousemaan alkuvaiheessa maksimissaan 1,4 megabittiin sekunnissa aiemman maksimin 384 kbit/s sijaan [19]. HSUPA on laajennettu kattamaan Elisan koko 3G-verkon vuoden 2008 aikana.

3.5 WLAN

WLAN on tarkoitettu datan siirtämiseen yhtä lailla kuin perinteinen langallinen lähiverkkokin, mutta tässä tapauksessa kyse on nimenomaan ilmateitse ilman kaapeleita radioaalloilla (tai infrapunalla) kulkevasta datasta. Toinen yleistynyt nimi WLAN:lle on WiFi. Standardi WLAN:in takana on Yhdysvalloissa kehitetty IEEE 802.11, ja tarkemmin ottaen nykyään käytössä ovat lähinnä 2,4 GHz:n taajuusalueella toimivat 802.11b (11Mbit/s) sekä 802.11g (54Mbit/s) [20], [21]. WLAN:ksi voidaan laskea 802.11 standardin lisäksi myös esimerkiksi ETSI:n kehittämä kilpaileva eurooppalainen standardi HIPERLAN, mutta tässä työssä rajataan tutkimus selvästi tunnetuimpaan ja käytetyimpään 802.11-standardiin.

3.5.1 OSI-mallin WLAN-kerrokset

802.11-standardi määrittelee OSI-mallin mukaiset kaksi alinta kerrosta; fyysisen kerroksen sekä siirtoyhteyskerrokselta MAC-tason (Medium Access Control). Siirtoyhteyskerroksen LLC-tasoa (Logical Link Control Layer) ei tässä yhteydessä käsitellä tarkemmin, sillä se toimii kuten LAN-verkoissa yleensäkin määrittäen rajapinnan verkkokerrokseen. Fyysinen kerros tarjoaa MAC-tasolle palveluita ja huolehtii resurssien varaamisesta sekä liikenteen lähettämisestä ja vastaanottamisesta. Alkuperäiselle 802.11-standardin mukaiselle fyysiselle kerrokselle on kolme erilaista vaihtoehtoa jakaa radiosignaali halutulle kaistalle; taajuushyppelevä hajaspektritekniikka (FHSS, Frequency Hopping Spread Spectrum), suorasekvenssihajaspektritekniikka (DSSS, Direct Sequence Spread Spectrum) sekä infrapuna (IR, infrared) [21]. Edellä mainituista FHSS sekä DSSS toimivat ISM-kaistalla (Industrial, Scientific and Medical) 2,4 – 2,4835 GHz:n taajuusalueella, jonka käyttämiseksi ei vaadita erityistä lupaa, vaan taajuusalue on lisenssivapaa mahdollistaen kyseisellä taajuudella operoimisen missä päin maailmaa tahansa. Verrattuna esimerkiksi 5 GHz:n taajuusalueeseen 2,4 GHz taajuusalueen etuja ovat parempi kantama ja pienemmät vaatimukset lähetysteholle, sillä korkeampi taajuus läpäisee huonommin erilaisia materiaaleja ja toisaalta vaimenee nopeammin kuin matalataajuuksinen signaali. 802.11b-standardi ei kuitenkaan enää käytä FHSS:ää, vaan DSSS:ää. Myöskään infrapunaratkaisut eivät ole olleet enää aikoihin todellinen vaihtoehto, sillä

ne vaativat aina näköyhteyden kohteeseen, joten nykyään selvästi käytetyin ratkaisu on suorasekvenssihajaspektritekniikka, eli DSSS [20], [21].

DSSS käyttää jatkuvasti 22 MHz:n levyistä taajuusaluetta, jolle lähetettävä data levitetään siruksi(chip) tai sirpalekoodiksi(chipping code), eli jaetaan pieniin osiin ja lähetetään koko taajuusalueella yhtenä signaalina. Ongelmaksi muodostuu tällöin muiden signaalien aiheuttamat häiriöt. Ratkaisuna on sekoittaa lähtevä signaali kohinaa muistuttavaan kantoaaltoon. Esimerkiksi 802.11b-standardissa yksi bitti levitetään 11 bitiksi, jolloin ulkopuolinen tarkkailija käsittää signaalin kohinaksi. Taajuusalue on jaettu osittain päällekkäisiksi kanaviksi, jolloin lähekkäin sijaitsevat tukiasemat saattavat häiritä tosiaan, vaikka käyttäisivätkin eri kanavia. Kanavia on 13 kappaletta, ja kaikki ovat siis 22 MHz leveydeltään [22]. DSSS:n tarjoama maksiminopeus on IEEE 802.11b-standardin tarjoama 11 Mbit/s, ja tämä maksiminopeus jaetaan kaikkien DSSS:ssä samalla alueella (esimerkiksi saman tukiaseman alueella) olevien päätelaitteiden kesken. DSSS tarjoaa melko pienen latenssiajan, joten esimerkiksi VoWLAN:n käyttö on mahdollista. Toisaalta ongelmana DSSS:ssä on se, että 802.11b-standardin maksiminopeudella (11 Mbit/s) voi olla vain kolme erillistä kanavaa, jolloin enemmän päätteitä sisältävässä verkossa saattaa ilmetä tiedonsiirron hidastumista ja yhteyden katkeilua.

Alkuperäisessä 802.11-standardissa määritellään kaksi MAC-protokollaa: DCF (Distributed Coordination Function) sekä PCF (Point Coordination Function) [23]. Siirtoyhteyskerroksen MAC-osakerroksen DCF käyttää aina CSMA/CA:ta (Carrier Sense Multiple Access with Collision Avoidance) eli kilpailuvarausta, sillä WLAN-standardeista on haluttu tehdä yhteensopivia useiden erilaisten tiedonsiirtotekniikoiden kanssa myös tulevaisuudessa. Tästä syystä yksi yhteinen protokolla on oleellinen. Kilpavarauksessa tarkistetaan ensin, onko linjalla muita käyttäjiä. Mikäli on, odotetaan hetken aikaa ennen uutta yritystä. Erona Ethernetin CSMA/CD-käytäntöön (Carrier Sense Multiple Access with Collision Detection) on se, että linjalta vetäydytään ennen törmäyksiä, ei vasta niiden jälkeen. Ilmassa tapahtuva liikennöinti kuluttaa enemmän resursseja kuin kaapelissa tapahtuva, joten WLAN:ssa kannattaa käyttää nimenomaan

ennakoivaa menettelyä törmäysten välttämiseksi. Tämä tarkoittaa osaltaan kuitenkin pidempiä viiveitä. Kun paketti on lähetetty, odotetaan ACK-kuittauksen saapumista ja mikäli sitä ei tule, lähetetään paketti uudestaan. Huomioitavaa siis on, että langattomassa lähiverkossa on yksi yhteinen siirtomedia, ilmatie, jonka kaikki saman tukiaseman päätelaitteet jakavat. Vain yksi päätelaite voi lähettää kerrallaan dataa ilmatien yli ja MAC huolehtii tästä käyttöoikeuksien jakamisesta eri päätelaitteiden kesken. Siirtoyhteyskerros huolehtii lisäksi pakettien eheydestä CRC (Cyclic Redundancy Check)-tarkistussumman eli virheentarkistusalgoritmin avulla. Lisäksi MAC-osakerros huolehtii mahdollisesta suurien pakettien pilkkomisista pienempiin osiin häiriöisessä verkossa. MAC-osakerros hoitaa myös pakettien uudelleen kokoamisen. Esimerkiksi DCF- ja PCF-protokollia käydään tarkemmin läpi neljännessä kappaleessa käsiteltäessä palvelun laadukkuutta langattomissa lähiverkoissa.

3.5.2 WLAN-verkon rakenne

Verkkotopologian kannalta mahdollisia ratkaisutopologioita on kaksi; ad hoc -verkko, jossa ei erillistä tukiasemaa ole ollenkaan, vaan kaikki langattomat päätelaitteet keskustelevat keskenään. Toinen, käytetympi vaihtoehto on infrastruktuuriverkko, jollaisessa verkossa on aina vähintään yksi tukiasema langattomien päätelaitteiden lisäksi, johon verkon muut päätelaitteet ovat yhteydessä langattomasti. Yleensä tukiasemat ovat langallisesti kiinni muussa lähiverkossa, eli ne ovat langallisia vain yhteen suuntaan. Yhden tukiaseman tapauksessa käytetään nimitystä BSS (Basic Service Set) ja useamman kuin yhden tukiaseman tapauksessa nimitystä ESS (Extended Service Set). Jälkimmäisessä tapauksessa tulee huomioida, että tukiasemille täytyy määritellä jokaiselle erikseen oma kanavansa (taajuusalueensa), jotteivät kaikki tukiasemat toimisi samalla taajuudella ja haittaisi toisiaan. Langattomat verkot erotellaan toisistaan SSID:iden (Service Set IDentifier) avulla. SSID:t ovat eräänlaisia verkon yksilöiviä tunnistenimiä, joiden avulla verkot voidaan jakaa useampaan loogiseen osaan.

Liikkuvuudesta (handover) huolehtiminen langattomien päätelaitteiden osalta on otettava myös huomioon. Mikäli päätelaite liikkuessa havaitsee, että yhteys tukiasemaan alkaa käydä heikoksi, se rupeaa etsimään vaihtoehtoista, paremman kuuluvuuden

tarjoavaa tukiasemaa. Mikäli tällainen löytyy, päätelaite lähettää uuden assosiointipyynnön uudelle tukiasemalle ja mikäli tukiasema hyväksyy pyynnön, päätelaite lisätään kyseisen uuden tukiaseman asiakkaaksi ja poistetaan vanhan tukiaseman asiakkaiden joukosta. Edellä mainittua toimenpidettä varten kehitetty protokolla on nimeltään IAPP (Internet Access Point Protocol) [24].

Käyttäjien liikkuvuuteen liittyvä tukiaseman vaihto aiheuttaa myös palvelunlaadullisia ongelmia, sillä tiettyyn päästä-päähän -laatuun pyrittäessä tukiaseman vaihto tarkoittaa sitä, että myös uuden tukiaseman tulee tukea tiettyjen laatuvaatimusten toteutumista.

3.5.3 802.11-standardit

OFDM-tekniikkaa käyttävä 802.11a-standardi ei ole yleistynyt. Se toimii korkealla 5 GHz:n taajuudella ja mahdollistaa 54 Mbit/s nopeuden. Sen sijaan melkeinpä kaikissa nykypäivän WLAN-ratkaisuissa on käytössä DSSS:ää käyttävä 802.11b-standardi, jossa taajuusalue on 2,4 GHz ja maksiminopeus 11 Mbit/s, tai vaihtoehtoisesti oikeastaan yhdistelmä edellisistä, uudempi 802.11g, jossa nopeus on 802.11a:n kanssa sama, mutta operointitaajuus taas sama kuin 802.11b:ssä. 802.11g-standardi käyttää sekä DSSS:ää että OFDM:ää. 802.11e taas keskittyy parantamaan palvelunlaatua muokkaamalla MAC-kerrosta tuomalla neljä erilaista pääsykategoriaa eri liikenneluokkien suhteen sekä monipuolistamalla palvelunlaadullisia seikkoja ylipäätään. Näitä käydään tarkemmin läpi tutkimuksessa myöhemmin. Edellisten standardien lisäksi kehitteillä on 802.11-standardiin perustuva jatko-osa, 802.11n, jonka lopullisen version on arvioitu julkaistavan vuoden 2009 aikana [55].

Seuraavassa taulukossa on esitetty tärkeimmät 802.11-standardit ja niiden ominaisuudet.

Taulukko 3. 802.11-standardit [40]

STANDARDI	802.11	802.11b	802.11g	802.11a	802.11e	802.11n
Taajuus	2,4 GHz	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz ja 5 GHz
Nopeus	1 Mbit/s ja 2 Mbit/s	11 Mbit/s	54 Mbit/s	54 Mbit/s	54 Mbit/s	Jopa 600 Mbit/s, käytännössä kuitenkin 100–200 Mbit/s (arvio)
Radiotaajuus-tekniikka	Infrapuna, FHSS, DSSS	DSSS	DSSS & OFDM	OFDM	DSSS, OFDM	OFDM
Julkaisuvuosi	1997	1999	2003	1999	2005	2009(arvio)
Yhteensopivat standardit		802.11g, 802.11n, 802.11e	802.11b, 802.11n, 802.11e	802.11n	802.11b, 802.11g, 802.11a 802.11n	802.11b, 802.11g, 802.11a, 802.11e
Toimintasäde sisällä	n. 20 m	n. 38 m	n. 38 m	n. 35 m	Standardista riippuen	n. 70 m
Kanavat ja ei-päällekkäisten kanavien lukumäärä	14 kanavaa, 3 ei-päällekkäistä	14, 3	12, 3	12, 12	Standardista riippuen	Standardista riippuen
Muuta tietoa	Ensimmäinen, maailmanlaajuinen WLAN-standardi	Oli pitkään käytetyin standardi, mutta 802.11g nyt syrjäyttänyt tämän	Käytännössä syrjäyttänyt 802.11b:n tarjoamalla 802.11a:n nopeuden 802.11b:n taajuudella. Yhteensopiva 802.11b:n kanssa	Nopeus hyvä, mutta korkea taajuus heikentää kantamaa. Ei yhteensopiva 802.11g:n tai 802.11b:n kanssa	Parantaa QoS:ää MAC-kerroksen laajennuksella	Kehitteillä oleva standardi, jossa suuret nopeudet ja pitkä kantama

3.6 Yhteenveto langattomien verkkojen erityispiirteistä

WLAN-tekniikalla ei ainakaan vielä tässä vaiheessa voida lähteä kilpailemaan suoraan vaikkapa 3G:n tai WiMAX:n kanssa selvästi lyhyemmän kantomatkan takia. Tuleva

802.11n-standardi nimittäin mahdollistaa maksimissaan noin 70 metrin etäisyyden tukiasemaan, aiemmat standardit eivät sitäkään. WLAN-tekniikka soveltuukin paremmin esimerkiksi yrityksen sisäverkon tietoliikenneratkaisuksi ja toisaalta erilaisten yleisöpaikkojen (lentokentät, kahvilat, keskustat) tietoliikenneyhteyksien mahdollistajaksi. WLAN-päätelaitteiden edullisuus mahdollistaa useidenkin päätelaitteiden hankkimisen taloudellisesti kannattavana edellä mainittuihin sisätiloihin, jolloin esimerkiksi koko yritys saadaan WLAN:in peittoalueelle.

Langattomiin verkkoihin liittyy suorituskyvyllisiä ongelmia verrattuna langallisiin verkkoihin. Langattomissa verkoissa bittivirhetiheys (BER, Bit Error Rate) on huomattavan paljon suurempi kiinteisiin yhteyksiin verrattuna. Lisäksi yhteyden katkeaminen on mahdollista useasta eri syystä. Siirtyminen tukiasemalta toiselle, siirtyminen kokonaan pois tukiaseman kuuluvuusalueelta, väliaikainen katvealueelle joutuminen tai tukiasemaan yhteydessä olevien päätelaitteiden suuri määrä voivat kaikki aiheuttaa yhteyden katkeamisen. Tukiaseman kuuluvuusalueen pienentäminen saattaa parantaa yhteyksien laatua käyttäjämäärien vähentyessä, mutta toisaalta tukiasemien vaihdoksista johtuvat katkokset kasvavat ja kuuluvuusalueen reunoilla saattaa esiintyä uusia katvealueita. Lisäksi samalla taajuusalueella toimivat muut laitteet saattavat häiritä WLAN-signaalin kulkemista.

Varsinkin matkaviestinverkoissa ja esimerkiksi @450-verkossa yleinen verkko-operaattori – palveluoperaattori -malli ei ole yleistynyt samalla lailla WLAN-palveluverkoissa, sillä WLAN-palveluntarjoajat vastaavat yleensä itse myös verkko-operoinnista, eivätkä myy kapasiteettia muille operaattoreille. Uudemmat verkkolaitteet mahdollistavat kuitenkin paremmin kapasiteetin jakamisen ja verkkolaitteiden osittamisen, joten verkko-operaattori – palveluoperaattorimalli on mahdollinen toteutusmalli tulevaisuudessa myös WLAN-ratkaisuissa.

4. Palvelunlaatu langattomissa lähiverkoissa

Kappale yhdistää aiemmissa kappaleissa esille tulleet asiat palvelunlaatu sekä langattomat lähiverkot kuvaamalla ensin SLM:n ulottamista langattomiin verkkoihin ja tarkastelemalla sen jälkeen tarkemmin palvelunlaatua langattomissa lähiverkoissa sekä palvelunlaatua yleisesti tietoturvan kannalta.

Kohdassa 4.2 *QoS langattomissa lähiverkoissa* käydään vielä ensin tarkemmin läpi tekniikkaa päätelaitteiden ilmatielle pääsyn suhteen ja jatketaan sen jälkeen perehtymistä tarkemmin QoS-mekanismeihin langattomissa verkoissa.

Langattomuuden yleistyessä ja liikenteen monipuolistuessa sekä sovellusvaatimusten kasvaessa palvelunlaadun ulottaminen langattomiin lähiverkkoihin on yleisen toiminnallisuuden ja ennen kaikkea esimerkiksi multimedian ja puheen kunnollisen toimivuuden kannalta oleellisen tärkeää. Loppukäyttäjän kokema QoE asettaa suuremmat vaatimukset langattomalle verkolle langalliseen verrattuna. Mikäli halutaan myös puhe- ja videoliikenteen toimivan WLAN-yhteyden takaa, täytyy olla selvillä seikoista, jotka vaikuttavat kyseisten liikennetyyppien toimivuuteen.

4.1 SLM-käytännön ulottaminen langattomiin lähiverkkoihin

Palvelutason hallinta ja jatkuva laadun varmistaminen sekä parantaminen on otettava huomioon langattomissa verkoissa vastaavalla lailla kuin langallisissakin. Päästä-päähän yhteyden toimivuutta mitattaessa ja käytettävyyksien ja sitä myöten sanktioiden raja-arvoja suunniteltaessa myös langattoman verkon osuus tulee ottaa mukaan tarkasteluun.

Langattomia lähiverkkoja hyödyntävien sovellusten automaattinen seuranta ja valvonta ovat vasta yleistymässä samalla kun langattomien verkkojen määrä kasvaa. Aiemmin langattoman verkon yli käytetyn sovelluksen virheilyn on lähes poikkeuksetta uskottu johtuvan nimenomaan langattoman verkon ongelmista. Ulottamalla SLM-käytännön myös langattomiin verkkoihin pystytään tulevaisuudessa selvittämään entistä helpommin, onko vika varmasti langattoman verkon osuudella vai esimerkiksi vasta

langattomasta tukiasemasta runkoverkkoon päin tai vaikka palvelimella. Valvonnan ulottamisella myös WLAN-verkon puolelle saadaan nopeasti tietoa häiriöistä ja ongelmista ja ennen kaikkea paikallistettua ja korjattua ne mahdollisimman kätevästi. Samalla voidaan todentaa SLA-sopimusten mukaisten laatutasojen toteuma eksaktisti.

Täytyy kuitenkin tiedostaa, että radioverkon ollessa alttiimpi häiriöille langalliseen verkkoon verrattuna, ei operaattorikaan suostu samanlaisiin käytettävyysvaatimuksiin kuin langallisessa verkossa. Vaatimukset tulee siis määritellä yhteisymmärryksessä ja realistisina molempien osapuolten kannalta.

4.2 QoS langattomissa lähiverkoissa

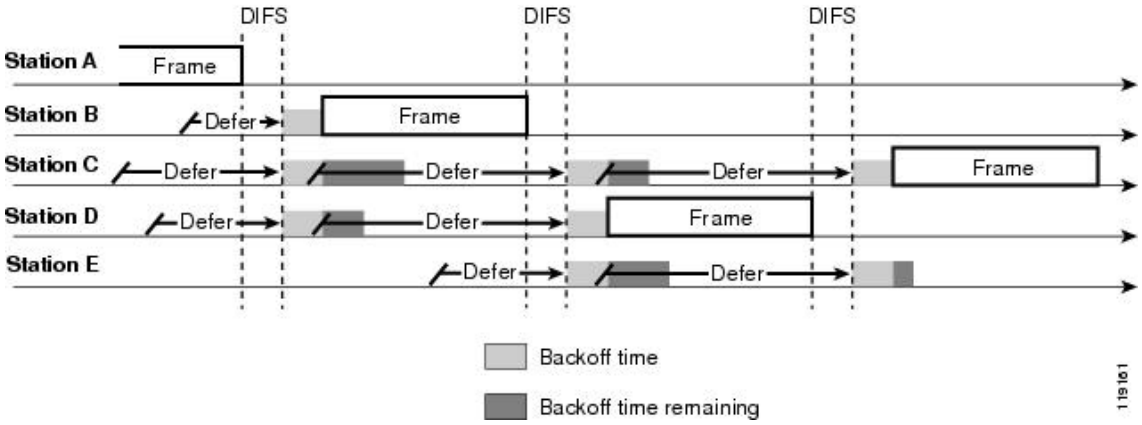
Langattomissa lähiverkoissa ilmatie on varattu siten, että vain yksi käyttäjä voi kerrallaan lähettää dataa. Tästä syystä palvelunlaadun tarjoaminen tapahtuu langattomissa lähiverkoissa helpoimmin priorisoimalla ilmatien käyttöä, eli valitsemalla tiettyjen parametrien mukaan sen käyttäjän, jolle annetaan käyttöoikeus ilmatielle. Alun perin 802.11-standardissa ei oltu huomioitu QoS:ää, mutta standardin kehittämisen myötä uudemmissa versioissa on jo mahdollisuuksia käyttää useampiakin tekniikoita takaamaan eritasoista palvelunlaatua erityyppisille sovelluksille.

MAC-kerros hoitaa WLAN-verkoissa käyttäjädatan lähettämisen hallinnoinnin. Datan pääsystä siirtomedialle vastaavat ja kontrolloivat kaksi MAC-kerroksen koordinointifunktiota; hajautettu koordinointifunktio DCF sekä pistekoordinointifunktio PCF [25].

4.2.1 DCF (Distributed Coordination Function)

DCF tarjoaa vain asynkronista datapalvelua, eli käytännössä best-effort -luokan mukaista palvelua ja se on pakollinen kaikissa WLAN-standardin mukaisissa laitteissa. Se soveltuu vain ei-aikakriittisen liikenteen siirtoon eikä pysty takaamaan reaaliaikasovelluksille niiden vaatimaa palvelutasoa viiveen ja viiveen vaihtelun suhteen.

Kuvassa 4 on kuvattuna DCF-funktion toimintaperiaate.



Kuva 4. DCF:n toimintaperiaate [25],[26]

Kuten aiemmin on kerrottu, DCF perustuu CSMA/CA-tekniikkaan, jossa asema, joka on lähettämässä dataa, kuuntelee ensin kanavaa ja selvittää, onko se vapaa. Mikäli on, voi asema alkaa lähettää dataa. Muussa tapauksessa asema odottaa, että kanava vapautuu. Tällä tavoin pystytään välttämään törmäyksiä mahdollisimman hyvin ja saadaan hyödynnettyä rajallinen siirtotien kapasiteetti mahdollisimman hyvin. Lisäksi on määritelty DIFS-aika (DCF Interframe Space), ja mikäli se on kulunut ilman, että mikään asema lähettää paketteja, pääsee asema siirtotielle välittömästi. DIFS-ajan lisäksi täytyy kuitenkin ottaa huomioon myös ns. backoff-ikkuna (Backoff Window), joka on määritelty aikavälin moninkertana. Backoff-ikkuna kertoo, kuinka monta aikaväliä täytyy vielä odottaa DIFS-ajan lisäksi, ennen kuin asema pääsee siirtotielle lähettämään dataa. Backoff-ikkunan arvo kuvataan kokonaislukuna välillä [0, CW], missä CW (Contention Window) on välillä [CWmin, CWmax]. Kuvassa 4 on kuvattu *Backoff time* -palkilla aikaa, joka odotetaan ennen kuin seuraava asema pääsee siirtotielle. Tummemmalla kuvattu *Backoff time remaining* taas kuvaa muiden kuin siirtotielle päässeen aseman jäljelle jääneitä Backoff-aikoja, jotka huomioidaan seuraavan DIFS-ajan jälkeen valittaessa seuraavaa asemaa siirtotielle [25],[27].

Kun vastaanottaja saa onnistuneesti kehyksen, odottaa vastaanottaja DIFS:tä lyhyemmän ajan SIFS (Short Interframe Space), ennen kuin se lähettää ACK-kuittauksen. Mikäli siirtomedia on kuitenkin tässä vaiheessa varattuna, täytyy taas odottaa, että asema on vapaana ajan DIFS. Tämän jälkeen lähettävän aseman CW:n arvo kaksinkertaistetaan ja yritetään lähettää uudelleen. Mikäli CW nousee maksimiarvoon

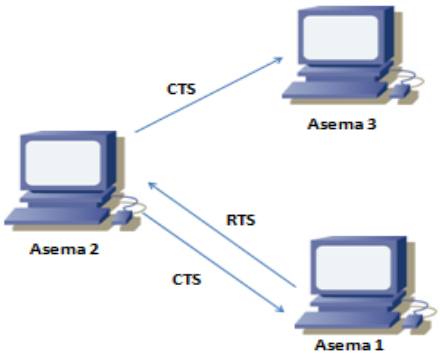
CWmax, sitä ei enää kasvateta vaan lähetystä yritetään uudelleen niin kauan, että onnistutaan lähettämään. Tämän jälkeen CW-arvo tiputetaan takaisin arvoon CWmin [27].

Asema, jolla on lyhyin odotusaika, saa aina oikeuden käyttää kanavaa. Kilpailun hävinneet asemat eivät kuitenkaan valitse tässä vaiheessa uutta CW-arvoa, kun ne yrittävät lähettää uudestaan, vaan ne saavat pitää sen CW-arvon, mikä backoff-laskuriin jäi sillä hetkellä, kun jokin toinen asema sai lähetysoikeuden. Tämän johdosta näillä kyseisillä hävinneillä asemilla on suurempi todennäköisyys päästä seuraavalla kerralla kanavalle lähettämään dataa CW-arvon ollessa pienempi. Näin ollen pisimpään odottanut asema saa parhaan mahdollisuuden päästä lähettämään dataa. Tämä mahdollistaa kohtalaisen oikeudenmukaisen toiminnan.

4.2.2 Piiloaseman tunnistaminen (DCF ja RTS/CTS)

Edellä kuvattu tilanne olettaa, että kaikki saman verkon asemat kuulevat toistensa lähetykset. Verkossa saattaa kuitenkin olla tilanne, jossa kaikki asemat eivät välttämättä kuule toisiaan. Tällöin fyysinen kanavankuuntelumekanismi ei sovellu käytettäväksi, sillä asemat voivat tulkita kanavan vapaaksi, vaikka jollain asemalla olisi lähetys käynnissä. Kyseessä on piiloasemaongelma. DCF:n kanssa voidaan käyttää menetelmää, jolla voidaan välttää piilossa olevan päätelaitteen ongelma [27].

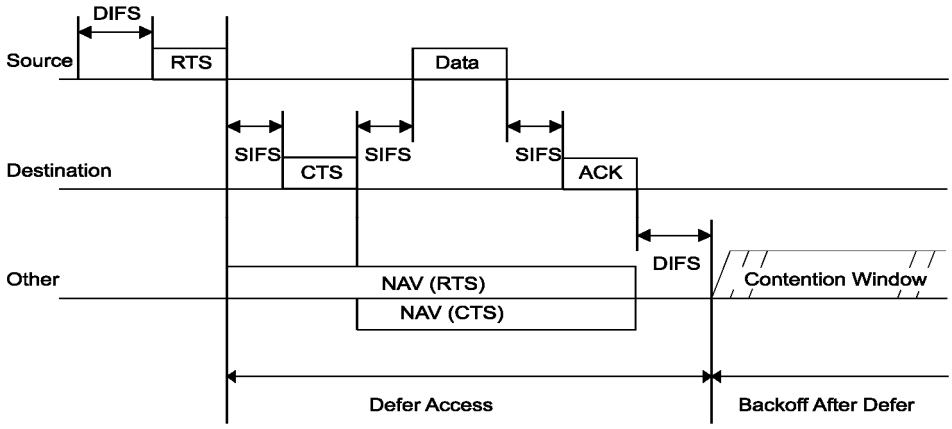
Ongelma voidaan ratkaista kahden kontrolliviestin avulla: RTS (Request To Send) ja CTS (Clear To Send). Yksinkertainen periaate on kuvattu kuvassa 5. RTS/CTS-viesteillä siis estetään asemien 1 ja kolme samanaikainen lähetys asemalle 2.



Kuva 5. RTS/CTS-esimerkkitapaus

Kun siirtotie on ollut vapaana vähintään ajan DIFS, pyytää Asema 1 lupaa datan lähettämiseen RTS-paketilla ja kertoo siinä, miten pitkäksi aikaa se aikoo varata kanavan. Tukiasema 2 vastaa tähän RTS-viestiin SIFS-odotusajan jälkeen CTS-viestillä. Myös CTS sisältää tiedon varauksen kestosta. Mikäli jokin tukiasema (tässä tapauksessa Asema 3) on niin kaukana lähettävästä asemasta, ettei se vastaanota RTS-viestiä, se vastaanottaa kuitenkin voimakkaampana lähetetyn CTS-viestin ja tallentaa verkon varausajan NAV-muuttujaan (Network Allocation Vector). Näin jokainen verkon tukiasema pysyy tietoisena varaustilanteesta. Tällä vältetään se tilanne, että kaksi toistensa kantaman ulkopuolella olevaa asemaa (Asemat 1 ja 3) lähettäisivät samanaikaisesti dataa kolmannelle niiden välissä olevalle asemalle (Asema 2) ja tapahtuisi törmäys.

Kuvassa 6 on vielä kuvattu tarkemmin virtuaalisen kanavankuuntelumekanismin toiminta.



Kuva 6. RTS/CTS-tekniikan toiminta [25],[28]

Kanavankuuntelumekanismi toimii siten, että lähettäjä (Source) ilmoittaa alussa RTS-viestillä vastaanottavalle tukiasemalle (Destination), kuinka pitkäksi aikaa se varaa kanavan. Tukiasema vastaa tähän RTS-viestiin CTS-viestillä. Molemmat viestit sisältävät tiedon verkon varausajan pituudesta. Mikäli jokin asema on liian kaukana lähettävästä asemasta, vastaanottaa se kuitenkin voimakkaampana lähetetyn CTS-viestin ja osaa näin ollen tallentaa oikean varausajan. Data-palkki kuvastaa lähetettävää dataa.

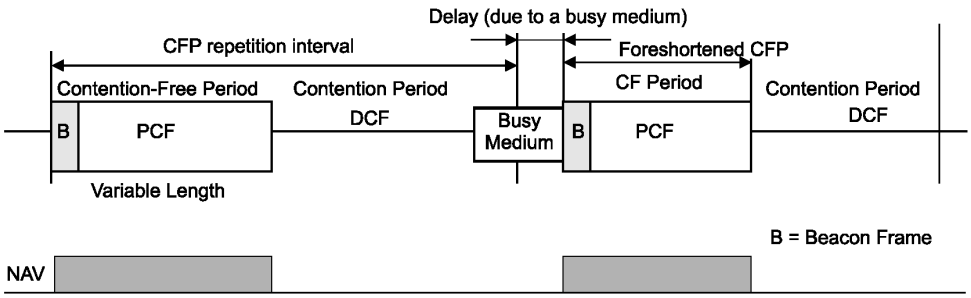
Verkon varausaika tallennetaan aina NAV-muuttujaan ja *Defer Access* eli viivästetty pääsy kuvastaa tilannetta, jossa kolmas tukiasema ei lähetä dataa kyseisen ajanjakson aikana. Piiloaseman tunnistamiseen suunniteltua RTS/CTS-toimintoa voidaan käyttää valikoiden joko aina, ei koskaan tai sitten tietyn pituuden ylittävien pakettien kanssa.

4.2.3 PCF (Point Coordination Function)

PCF tarjoaa aikarajoitettua palvelua infrastruktuurisissa verkoissa, joissa liityntäpiste kontrolloi liikennettä. Kyse on keskitetystä liikenteenhallinnasta. PCF on 802.11-standardissa toinen, ja käytännössä QoS:n kannalta parempi vaihtoehto pelkästään ei-reaaliaikaisen liikenteen tiedonsiirtoon tarkoitetulle DCF:lle [29]. PCF:n avulla liikenne pystytään jakamaan kahteen tasoon, korkean ja alhaisen prioriteetin luokkiin.

PCF:ssä on käytössä kohdistava koordinaattori PC (Point Coordinator), joka toimii tukiasemassa, päättäen mikä työasema kulloinkin on lähetysvuorossa, jolloin kilpailutilannetta ei synny. Osa verkon asemista on PCF-asemia ja osa DCF-asemia. Kohdistava koordinaattori pitää listaa PCF-asemista, joiden liikenne kuuluu prioriteetiltaan korkeampaan luokkaan. Kilpailuttoman jakson aikana (CFP, Contention Free Period) käytetään siis PCF:ää ja tämän jälkeen seuraa kilpailuvaihe, joka käyttäytyy DCF-mekanismin mukaisesti. Jaksot seuraavat toisiaan vuoronperään tietyn ajanjakson mittaisissa sykleissä [28],[29].

Seuraavassa kuvassa 7 on esitetty kilpailuttoman jakson ja kilpailuvaiheen toimintaperiaate, kun PCF on käytössä.



Kuva 7. PCF ja kilpailullinen sekä kilpailuton jakso [25],[29]

Kilpailuton jakso alkaa PC:n lähettämällä merkkikehyksellä (B). Merkkikehyksiä lähetetään tasaisin väliajoin, jotta jokainen asema tietäisi seuraavan merkkikehyksen saapumisajan. Jokaisessa merkkikehyksessä ilmoitetaan kehysten lähetysjakso (TBTT, Target Beacon Transition Time). DCF-aseman vastaanottaessa merkkikehyksen se asettaa NAV-muuttujaan kilpailuttoman jakson ajan. Käytännössä tämä tarkoittaa sitä, että DCF-asema odottaa tuon kyseisen ajanjakson ajan, kunnes jakso on ohi. Kun PCF alkaa, PC pollaa jokaista korkean prioriteetin PCF-asemaa vuorotellen ja nämä asemat vastaavat sille. Pollattu asema voi tässä vaiheessa vuorollaan lähettää vapaasti. Jos jollain PCF-asemalla ei ole vuorollaan dataa lähetettävänä, se lähettää PC:lle takaisin nollakehyksen. Mikäli käy niin, että kilpailuton jakso päättyy ennen kuin PC on ehtinyt käydä läpi (pollata) kaikkia PCF-asemia, saa DCF välillä vuoron ja seuraavan jakson alkaessa jatketaan PC:n pollausta siitä PCF:stä, mihin edellisellä kerralla jäätiin. Jos taas aseman lähetys epäonnistuu, se yrittää lähettää paketin uudestaan, kun PC pollaa kyseistä asemaa seuraavan kerran. PC lopettaa CFP:n lähettämällä CFEnd-kehyksen [29].

DCF-asemat eivät voi lähettää dataa kilpailuttoman jakson aikana, sillä ne ovat asettaneet NAV-muuttujansa juuri CFP:n pituiseksi. Myös PCF:ää käytettäessä datakehysten välinen aika on pienempi (PIFS, PCF Interframe Space) kuin DCF:n tapauksessa käyttämä DIFS-aika. Täytyy kuitenkin huomioida, että DCF-lähetykset eivät saa estyä kokonaan. Kilpailujakson tulee siis olla riittävän pitkä siihen, että asemat ehtivät lähettää ainakin yhden maksimikokoisen kehyksen.

PCF:n käyttöön liittyy kuitenkin myös ongelmatilanteita eikä sitä ole laajalti käytössä. Vaikka PCF on IEEE:n suunnittelema, ei se pysty tarjoamaan riittävää palvelunlaatua kaikille kriittisille sovelluksille. PCF:n pollaus on kompleksista ja epätehokasta [29]. Lisäksi kaikki liikenne kulkee AP:n kautta.

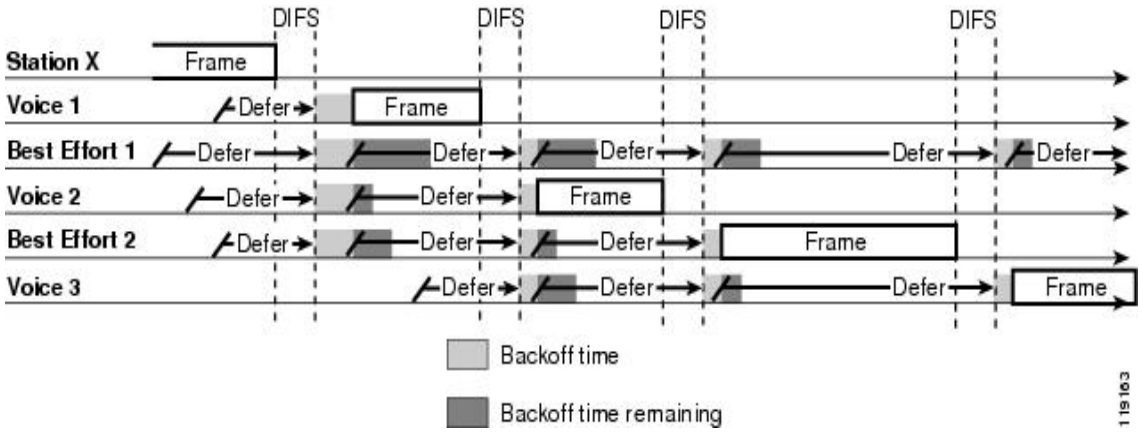
Jokin asema saattaa olla piilossa PCF-asemilta eikä vastaanota merkkikehyksiä. Tällöin se ei havaitse jonkin PCF-aseman lähetystä eikä osaa asettaa NAV-muuttujaan CFP:n kestoa. Tällainen asema jatkaa toimimista DCF-tilassa ja lähettää näin ollen myös

kilpailuttoman jakson aikana häiritseviä kehyksiä. Toinen ongelma on kilpailuttoman jakson aloitukseen liittyvä DCF:n käyttö merkkikehyksen lähetyksessä. Tämä johtaa siihen, että merkkikehyksen lähetys saattaa viivästyä, jos verkko on varattu lähetyshetkellä. Tästä aiheutuu viivettä tiedonsiirtoon.

4.2.4 HCF (Hybrid Coordination Function)

802.11e tuo parannuksen DCF:ään ja PCF:ään tarjoamalla uuden koordinointifunktion, HCF:n. HCF sisältää kaksi erilaista kanavallepääsymetodia; kilpailuttoman jakson HCCA:n (Hybrid Coordination Function Controlled Channel Access) sekä kilpailullisen jakson pääsymekanismin EDCA:n (Enhanced Distributed Channel Access), jotka molemmat jakavat liikenteen eri liikennekategorioihin tai liikenneluokkiin (engl. TC, Traffic Category tai Traffic Class) prioriteetin suhteen riippuen liikennetyypin tai sovelluksen vaatimasta tarpeesta.

EDCA on käytännössä paranneltu ja uudistettu versio DCF:stä. Luokiteltuaan liikenteen useampaan erilaisen prioriteetin kategoriaan se erottelee jokaisen kategorian mahdollisuuden päästä radiokaistalle lähettämään dataa. Kategoriat ovat siis yhden ja saman WLAN-aseman sisällä toimivia eräänlaisia virtuaaliasemia, jotka kilpailevat saman aseman toisten virtuaaliasemien sekä muiden WLAN-asemien kanssa lähetysmahdollisuudesta. Kuvassa 8 näkyy aiemmasta DCF:n toimintaperiaatteesta poikkeava EDCA:n toimintaperiaate.



Kuva 8. EDCA:n toimintaperiaate [25],[26]

EDCA mahdollistaa kahdeksan eri prioriteettikategorian käytön. Nämä kahdeksan prioriteettikategoriaa on mapattu neljään FIFO-jonoon, joita kutsutaan pääsykategorioiksi (AC, Access Categories) ja joiden avulla eri kategorioiden liikenteen jakelu hoidetaan. Jokainen korkean tason datapaketti tietyllä prioriteetilla määritetään tiettyyn AC:hen, joilla on jokaisella omat MAC-parametrit ja jotka toimivat kukin itsenäisesti toisista riippumatta. Neljä AC:ta ovat video-, puhe-, best-effort ja taustaliikenteet (voice, video, best-effort ja background application) ja kyseisen tyyppiset liikenteet voidaan näin ollen jakaa eri pääsykategorioihin ja jokaisella neljällä pääsykategorialla on oma FIFO-jononsa. Jokaisella pääsykategorialla on oma backoff-arvonsa ja korkeimman prioriteetin kategorialla on luonnollisesti pienimmät parametriarvot (pienempi backoff-ikkunan arvo muihin verrattuna) tarkoittaen sitä, että kyseisen luokan paketeilla on todennäköisin mahdollisuus saada lähetysmahdollisuus. Huolimatta useista pääsykategorioista suosituksena on, että liikenne jaetaan prioriteetin puolesta kahteen kategoriaan, tärkeään (puhe, video) ja ei-tärkeään kategoriaan.

EDCA:n neljä parametria (CWmin, CWmax, TXOP (Transmit Opportunity Limit) ja AIFS (Arbitary Interframe Space)) hoitavat erottelun eri pääsykategorioiden välillä. TXOP:lla tarkoitetaan kestoa, jonka aikana asemalla on mahdollisuus lähettää dataa siinä vaiheessa, kun asema on voittanut pääsyn kanavalle. Kun TXOP:in arvo on nolla, aseman on sallittua lähettää yksi kehys. Jos taas TXOP on riittävän suuri usean paketin lähettämiseen, asema laskee miten monta pakettia se pystyy lähettämään, jotta myös ACK-paketti kulkeutuu perille. Myös TXOP:n arvo riippuu prioriteettitasosta. Korkeamman prioriteetin liikenteelle myös TXOP:n arvo on suurempi [23],[27].

HCCA taas toimii hyvin samankaltaisesti PCF:n kanssa. Se on kehittynein koordinointimenetelmä. Kilpailullisen jakson (CP, Contention Period) aikana kaikki asemat toimivat EDCA-muodossa. AP voi pyytää kilpailuvapaata jaksoa (CFP, Contention Free Period) missä tahansa CP:n vaiheessa lähettämällä Control Contention (CC)-kehyksen. CFP:tä kutsutaan 802.11e-standardissa CAP:ksi (Controlled Access Phase). CAP:n aikana verkon tukiasemassa toimii koordinaattori (HC, Hybrid Controller), joka jakaa lähetysoikeuksia.

EDCA on pakollinen 802.11e-standardissa, kun taas HCCA ei. HCCA vaatii keskitettyä pollausta ja ajoitusalgoritmeja resurssien allokointiin eikä sitä ole laajalti käytössä nykyään [30],[31].

HCF:n lisäksi muita 802.11e-standardin tuomia etuja ovat MAC-tason FEC, AP:n liikkuvuuden parantaminen sekä suoran kommunikoinnin mahdollistaminen infrastruktuuriverkoissa.

4.3 Tietoturva langattomissa lähiverkoissa

WLAN-verkkojen tietoturvaan tulee kiinnittää oleellista huomiota, sillä radioteitse tapahtuva liikennöinti on alttiimpi ulkopuolisille häiriötekijöille kuin langallisesti tapahtuva liikennöinti. Tästä syystä tässäkin tutkimuksessa käydään lyhyesti läpi WLAN-verkkojen tietoturvaan liittyviä käsitteitä. Täytyy kuitenkin muistaa, että WLAN-verkkojen tietoturva on vain osa, joskin tärkeä sellainen, koko verkon tietoturvaa.

WLAN:n 802.11-standardiperheen 802.11i-standardi keskittyy nimenomaan tietoturvakysymyksiin. Se tarjoaa aiempia standardeja tehokkaampia salausmenetelmiä ja nykyisissä verkkokorteissa ja -päätteissä olisikin hyvä olla tuki myös 802.11i-standardille.

Langattomiin lähiverkkoihin liittyy uhkia riippumatta siitä, onko kyse koti- vai yrityskäytöstä. Uhat voi jaotella kolmeen osaan seuraavasti:

- Liikenteen salakuuntelu
- Yhteyden luvaton käyttö
- Tunkeutuminen yrityksen sisäisiin järjestelmiin

Liikenteen salakuuntelu on mahdollista langattoman verkon kuuluvuusalueella, mikäli liikenne on salaamatonta. Toisaalta verkkoyhteyden luvaton käyttö langattoman tukiaseman kautta on myös erittäin helppoa silloin, jos suojaus on heikko (WEP-protokolla, Wireless Equivalent Privacy) tai jos autentikoitumista ei ole otettu käyttöön

ollenkaan. Tällöin kuka tahansa pääsee tukiasemaan kiinni ja saa sitä kautta yhteyden eteenpäin. Käytännössä esimerkiksi kerrostalossa naapuri pystyy tällöin käyttämään ilmaiseksi Internet-yhteyttä maksamatta siitä mitään. Usein tällaisissa tapauksissa yhteyttä käytetään vieläpä haittaaviin tarkoituksiin, esimerkiksi roskapostittamiseen. Tunkeutuminen yrityksen sisäisiin järjestelmiin on mahdollista, mikäli salaus on heikko ja langaton verkkopääte on kytketty suoraan yrityksen sisäverkkoon kiinni.

Kaikkiin kolmeen edellä mainittuun torjuntakeinona on jonkin liikenteen salaukseen ja tunnistautumiseen tarkoitetun protokollan käyttö. WEP-protokollan heikkouksia on korjattu uudemmassa WPA-protokollassa (Wi-Fi Protected Access). WPA:sta on myös uudempi WPA2-versio, jossa käytetään vahvaa AES-kryptausta. WPA-protokollan käyttö onkin aina suositeltavaa. Lisäksi yritysten kannattaa huomioida, että WLAN-tukiasemaa ei kannata kytkeä suoraan yrityksen sisäverkkoon kiinni, vaan jonkin palomuurin taakse, jolloin yrityksen sisäverkkoon pääseminen vaikeutuu tunkeutujan kannalta huomattavasti. Poikkeuksena edellä mainituille ovat tarkoituksella avoimet WLAN-verkot esimerkiksi kahviloissa ja lentokentillä.

4.4 Yhteenveto langattomuuden vaikutuksista palvelunlaatuun

Koska langattomassa verkossa käytetään jaettuja resursseja, on palvelunlaadullisia tavoitteita vaikeampi toteuttaa langallisiin verkkoihin verrattuna. Langattoman verkon päätelaitteille ei ole olemassa mitään pelkästään kyseiselle päätelaitteelle dedikoitua kaistaa datan lähettämiseen ja vastaanottamiseen, vaan päätelaitteet kilpailevat radiotielle pääsystä keskenään. Tämä asettaa omat haasteensa palvelunlaadulle ja sen toteutumiselle.

Signaalin kulkeutumiseen radiorajapinnan yli vaikuttavat mahdolliset fyysiset esteet kuten rakennukset. Lisäksi tukiaseman kantoalueen reunoilla kuuluvuuden kanssa saattaa ilmetä ongelmia. Siirtyminen tukiasemalta toiselle asettaa myös omat haasteensa.

Ilmarajapinta on alttiimpi tietoturvallisuusuhille ja ulkoisille häiriötekijöille. Ulkoisia häiriötekijöitä voivat olla esimerkiksi samalla taajuusalueella operoivat järjestelmän ulkopuoliset laitteet, kuten mikroaaltouunit sekä langattomat ohjaimet ja puhelimet.

Edellä kuvattu liikenteen priorisointi mahdollistaa tärkeän liikenteen luokittelun ensisijaiseksi. 802.11e:n myötä liikenne on mahdollista jakaa pakettien priorisoinnin avulla neljään erilliseen luokkaan tärkeysasteen mukaan. Lisäksi kuvatut QoS-menetelmät WLAN-verkoissa pyrkivät estämään pakettien törmäykset ja kasvavat viiveet mahdollisimman hyvin. 802.11n-standardin mahdollistamat suuremmat nopeudet parantavat entisestään langattomien lähiverkkojen yli käytettävien sovellusten ja palveluiden käytettävyyttä ja samalla asiakkaan kokemaa QoE:tä.

On kuitenkin huomioitava, että liikenteen priorisointimääritykset ovat asiakkaan vastuulla, joten väärin konfiguroimalla saattaa esimerkiksi sähköposti päätyä tärkeimpään prioriteettiluokkaan puheliikenteen sijaan. Ongelma on kärjistetty, sillä tällainen varmasti huomataan nopeasti. Konfigurointivaade asettaa kuitenkin asiakkaalle lisää vastuuta. Varsinkin yritysten ollessa kyseessä hallinnan tulisi olla keskitetyillä palvelimilla ja niin sanotulla WLAN-kytkimellä (WLAN-kontrolleri), joka hoitaa lähiverkon hallinnoinnin keskitetysti. WLAN-kytkimet ovat lisääntyneet selvästi yrityskäytössä, sillä ne mahdollistavat laajan ja monimutkaisenkin WLAN-verkon hallinnan keskittämisen yhdelle laitteelle.

Perinteisiin WLAN-verkkoihin verrattuna suurin ero on siinä, että äly siirtyy tukiasemilta WLAN-kytkimelle. Tällöin päästään eroon perinteisten WLAN-verkkojen ongelmasta, jossa laajoissa verkoissa täytyy muutostilanteiden yhteydessä tehdä päivitykset jokaiselle tukiasemalle erikseen.

Hallinnan keskittäminen mahdollistaa entistä laajempien langattomien lähiverkkojen hallinnoimisen helposti ja tehokkaasti. Samalla esimerkiksi haluttu tietoturvapolitiikka on helpompi ottaa käyttöön yhteisesti kaikille tukiasemille. Myös VoWLAN-puheluiden laatu paranee keskitetyn hallinnan avulla. WLAN-kytkin pystyy tarkkailemaan koko

radiotien liikennettä ja se tallentaa keskitetysti tiedot kaikista verkon alueella havaitsemistaan laitteista sekä käyttäjistä. Tunnistautuminen tehdään vain kerran, eikä tukiasemalta toiselle liikkuvaa päätelaitetta tarvitse tunnistaa enää uudestaan. Tällöin esimerkiksi tukiaseman vaihdosta johtuvat viiveet käytännössä poistuvat. WLAN-kytkin pystyy myös vaihtamaan päätelaitteen tukiasemalta toiselle jo ennakoivasti, mikäli se havaitsee, että toinen tukiasema pystyy tarjoamaan paremman yhteyden. Kytkin pystyy myös optimoimaan verkkoa ja siirtämään osan päätelaitteista toiselle tukiasemalle ensimmäisen ruuhkautuessa, mikäli toinen tukiasema pystyy tarjoamaan riittävän palvelutason.

On selvää, että WLAN-kytkimeltä vaaditaan suorituskyvyn ja tehokkuuden suhteen paljon, sillä kaikki liikenne kulkee sen kautta. Kytkimissä on sisäistä välityskykyä kuitenkin yleisesti vähintään 1GB/s, joten välityskyky ei muodostune pullonkaulaksi. WLAN-kytkimet myös mahdollistavat useiden virtuaalisten WLAN:ien määrittelyn SSID:iden avulla ja ainakin jotkin kytkimet pystyvät ruuhkatilanteissakin takaamaan esimerkiksi 10 % kaistan kunkin virtuaalisen WLAN:n käyttöön mahdollistan näin VoWLAN:in toimivuuden.

802.11e-standardissa mukaan otettu DLP (Direct Link Protocol) mahdollistaa datan siirron suoraan kahden eri päätelaitteen välillä sen jälkeen, kun tukiaseman kautta on ensin saatu muodostettua yhteys [32]. Yhteydenmuodostus tapahtuu siten, että päätelaite A lähettää tukiasemalle pyynnön DLP-yhteydestä tukiasemien A ja B kesken. Tukiasema ohjaa tiedon pyynnöstä päätelaitteelle B, mikäli kyseinen päätelaite sijaitsee samassa BSS:ssä eli saman tukiaseman vaikutuspiirissä. Jos B hyväksyy pyynnön, lähettää se vastauskehyksen tukiasemalle, joka ohjaa kyseisen kehyksen edelleen A:lle. Tämän jälkeen A ja B saavat muodostettua suoran yhteyden keskenään. Edellä kuvattu toimenpide vähentää tukiaseman kuormitusta ja edesauttaa paremman palvelunlaadun toteutumista. Suora yhteys kahden eri päätelaitteen välillä pysyy ylhäällä tietyn määrätyn ajan ja yhteys katkeaa, mikäli kehyksiä ei lähetetä kumpaankaan suuntaan tämän määrätyn ajan puitteissa.

5. Puheliikenne ja palvelunlaatu

Kappaleessa käydään läpi laatukriittisen, eli tässä tapauksessa puheliikenteen kuljetusta niin langattomassa kuin langallisessakin IP-verkossa. Ensin käydään läpi signalointiprotokollia ja koodekeita, jonka jälkeen selvitetään käsitteen VoIP taustoja. Tämän jälkeen siirrytään langattoman verkon puolelle tutkimalla ensin pidemmän kantaman verkkoja ja keskittymällä sitten VoWLAN-käsitteeseen.

5.1 Peruskäsitteitä

Puhe- ja dataliikenteen yhdistäminen kulkemaan samassa verkossa (verkkokonvergenssi) on ollut esillä jo pitkään, mutta edelleen se on yksi tämän päivän trendeistä. Asia kiinnostaa myös operaattoreita huolimatta aiemmista tuloksettomiksi osoittautuneista ratkaisuista, sillä kuluja saa karsittua huomattavasti, kun ei tarvitse enää ylläpitää kahta täysin erillistä verkkoa; toista puheliikennettä varten (piirikytkentäinen) ja toista dataliikenteelle (pakettikytkentäinen). Tulevaisuuden suuntaus onkin se, että jatkossa tullaan operoimaan yhä enemmän pelkästään pakettikytkentäisen verkon kanssa ja sovitetaan myös puheliikenne kulkemaan sen läpi.

Puheliikenne asettaa verkolle ja käytettävälle yhteydelle tiukemmat vaatimukset, kuin tavallinen purskeinen dataliikenne. Puheen pitää kulkeutua vastaanottajalle lähes reaaliaikaisesti mahdollisimman pienellä pakettihävikillä, viiveellä ja viiveen vaihtelulla.

H.323

H.323 on ITU-T:n luoma signalointiprotokolla. Käytännössä se on ITU-T:n eräänlainen kattostandardi, joka pitää sisällään useita eri aliprotokollia (esimerkiksi H.225.0 ja H.245). H.323 on luotu mahdollistamaan puheen ja videon sovittaminen pakettiverkkoon. H.323 on suunniteltu nimenomaan monimutkaisiin verkkoihin, kuten Internetiin ja se onkin suosittu videoneuvotteluissa. H.323 on kohtalaisen monipuolinen, mutta myös monimutkainen protokolla, ja juuri joustavuuden puute tekeekin siitä heikomman SIP:iin verrattuna. Protokollaa ei myöskään ole alun perin suunniteltu

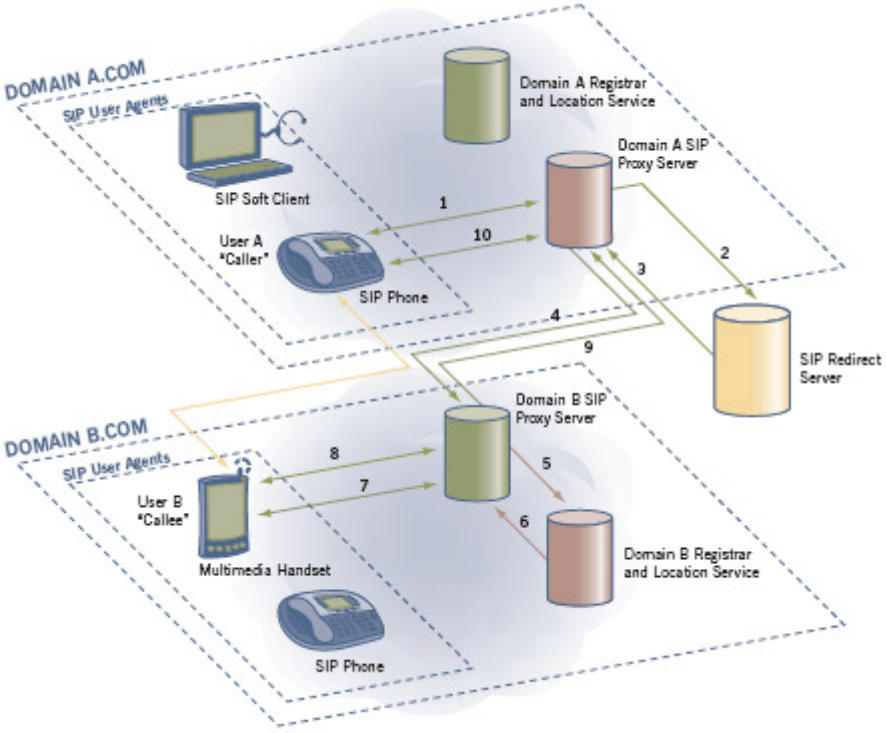
VoIP-käyttöä varten, kuten SIP on, vaan videopuhelustandardiksi. Itse liikenteen kuljetukseen H.323 käyttää IETF:n standardoimaa RTP-protokollaa (Real-Time Transport Protocol). H.323 käyttää viesteissään binäärimuotoa [33], [34].

SIP (Session Initiation Protocol)

IETF:n SIP on signalointiprotokollista käytetympi. Tekstipohjainen ja avoin SIP on yksinkertaisempi protokolla binääripohjaiseen H.323:een verrattuna, mutta myös SIP on monimutkaistunut toimintojen ja käytön lisääntyessä. SIP perustuu HTTP:n (Hypertext Transfer Protocol) sekä SMTP:n (Simple Mail Transfer Protocol) kaltaiseen malliin ja se on näin ollen helposti käytettävissä HTTP:n kanssa yhteensopivien ohjelmien kanssa. SIP on käytössä myös 3G-verkossa IP-puolen signalointiprotokollana. Kuten H.323, myös SIP käyttää RTP-protokollaa pakettien kuljetukseen. Tarkemmin SIP:n määrittelemät tiedot kuvaa SDP-protokolla (Session Description Protocol).

SIP:iin liittyy neljä erillistä osiota; *User Agent, Proxy server, Redirect server, Registrar server* [34]. *User Agent* on loppukäyttäjän päätelaite, puhelin, tietokone tms., joka hoitaa puhelun muodostamisen. *User Agent* voidaan vielä jakaa kahteen osaan; *User Agent Client*iin sekä *User Agent Server*iin. *User Agent Client* muodostaa SIP-pyynnön ja *User Agent Server* ottaa yhteyden käyttäjään SIP-pyynnön saapuessa ja palauttaa vastauksen käyttäjän puolesta. *Proxy server* eli välityspalvelin voi toimia sekä palvelimena että asiakkaana tehden pyyntöjä toisten asiakkaiden puolesta. Samassa toimialueessa oleville kohdepäätelaitteille välityspalvelin ohjaa SIP-pyynnön suoraan, muussa tapauksessa se välittää pyynnön edelleen toiselle välityspalvelimelle, mikäli vastaanottava *User Agent* sijaitsee toisessa toimialueessa. SIP:n *Redirect server*it mahdollistavat välityspalvelimien ohjata SIP-pyynnöt ulkoisille toimialueille. *Registrar server*it eli SIP-rekisterit ovat tietokantoja, jotka sisältävät tiedot kaikista SIP-käyttäjistä ja heidän sijainneistaan toimialueen sisällä ja joilta välityspalvelimet kysyvät sijaintitietoja.

Kuvassa 9 on kuvattu VoIP-puhelun muodostumisprosessi, kun soittaja ja vastaanottaja sijaitsevat eri toimialueissa (engl. *domain*).



Kuva 9. VoIP-puhelun muodostaminen SIP-protokollan avulla kahden eri toimialueen välillä [35]

Soittaja sijaitsee toimialueessa A ja puhelun vastaanottaja toimialueessa B. Keltainen nuoli kuvaa lopussa muodostettua RTP-yhteyttä. Vihreät nuolet ovat SIP-merkinantoon liittyviä ja punaiset nuolet eivät sisällä SIP-signalointia, vaan ovat tietokannasta etsimistä yms.

Puhelunmuodostusprosessi etenee seuraavasti:

1. A haluaa soittaa B:lle ja pyyntö kulkeutuu A-toimialueen *Proxy Server*ille eli välityspalvelimelle.
2. Välityspalvelin toteaa, että B ei sijaitse samassa toimialueessa kuin A ja välittää SIP-pyynnön SIP *Redirect Server*ille ja kysyy, miten saadaan yhteys käyttäjään B toimialueessa B.
3. *Redirect Server* palauttaa A-toimialueen välityspalvelimelle pyynnön ja tiedon B-toimialueen välityspalvelimesta.
4. A-toimialueen välityspalvelin lähettää SIP-kutsun eteenpäin B-toimialueen välityspalvelimelle.

5. B-toimialueen välityspalvelin kysyy omalta *Registrar (and Location) Server*iltä, että missä käyttäjä B sijaitsee.
6. *Registrar Server* palauttaa B:n osoitteen.
7. B-toimialueen välityspalvelin ohjaa SIP-pyynnön käyttäjälle B.
8. B:n hyväksyntä/vastaus samaa polkua pitkin päinvastaiseen suuntaan.
9. B:n hyväksyntä/vastaus samaa polkua pitkin päinvastaiseen suuntaan.
10. B:n hyväksyntä/vastaus samaa polkua pitkin päinvastaiseen suuntaan.

Keltainen nuoli kuvaa edellä mainitun prosessin jälkeen muodostettua RTP-yhteyttä käyttäjien A ja B välillä, jolloin A ja B pystyvät keskustelemaan keskenään.

SIP-viestipyynnön tulee sisältää vähintään seuraavat kentät: *To, From, CSeq, Call-ID, Content Length, Max-Forwards* ja *Via*. Näiden lisäksi jokaisessa SIP-viestissä tulee ensimmäisellä rivillä olla *method, Request-URI* sekä SIP:n versio. Itse sisältökenttä on yleensä SDP-viesti. *To* ja *From* kuvaavat yksiselitteisesti vastaanottajan sekä lähettäjän, *Cseq* on luku joka yksiselitteisesti määrittelee tietyn tapahtuman. *Call-ID* auttaa määrittelemään ja identifioimaan yksittäisen SIP-dialogin tai -rekisteröinnin. *Content Length* kuvaa oktettien määrän viestin dataosiossa. *Max-Forwards* rajoittaa välietappien määrän (välityspalvelimet, yhdyskäytävät) tiettyyn lukemaan matkalla vastaanottajalle. *Via* ilmaisee jo siihen asti kuljetun polun tarkoituksenaan ehkäistä esimerkiksi looppien syntymistä [36].

SIP ei itse tarjoa QoS:ää, vaan tekee yhteistyötä RSVP:n kanssa tähän liittyen. SIP ei myöskään itse määrittele muodostettavan session tyyppiä, vaan ainoastaan sen, miten sessiota tulisi hallita. Tämä SIP:n joustavuus tarkoittaa sitä, että protokollaa voidaan käyttää lukuisien ohjelmien ja sovellusten kanssa [37].

Koodekit

Koodekit (engl. *codecs*) muuntavat analogisen puhesignaalin digitaaliseksi datavirraksi. Koodekkeja on olemassa useita erilaisia, ja esimerkiksi eri enkoodaustekniikoilla voidaan vaikuttaa siihen, mikä on äänisegmentin kesto ja toisaalta lähetysnopeus.

Koodekit siis vaikuttavat digitaaliseksi muutettuun puheeseen kahdella lailla; viiveen ja puheen laadukkuuden kannalta. Koodekit voidaan jakaa kolmeen erilliseen luokkaan; aaltomuotokoodekit, mallinnuskoodekit ja hybridikoodekit. Aaltomuotokoodekit ovat hyvin yksinkertaisia ja ne pyrkivät olemaan ottamatta kantaa puheen sisältöön. Mallinnuskoodekit taas ovat tehokkaampia mallintaen äänilähteen ja pyrkien sitten jäljittelemään alkuperäistä äänilähdettä mahdollisimman tarkasti. Tiedonsiirtokapasiteetti on mallinnuskoodekeilla todella pieni, mutta puheen laatu ei ole kovin hyvä. Puhe kuulostaa metalliselta ja tukkoiselta. Kolmas ryhmä, eli hybridikoodekit, pyrkii yhdistämään kahden edellä mainitun ryhmän ominaisuudet. Käytännössä pyritään siis säilyttämään alkuperäisen puheen tärkeät osat ja syntetisoimaan loput. Lopputulos on laadullisesti mallinnuskoodekin ja aaltomuotokoodekin välillä, mutta toisaalta kaistantarve on myös pienempi kuin aaltomuotokoodekeilla.

Yksi yleisimmin käytettyä puhekoodekkeja ja kaikkein yksinkertaisin varsinaisista koodausmenetelmistä on ITU-T:n standardin G.711-aaltomuotokoodekki, joka perustuu pulssikoodimodulaatioon (PCM, Pulse-code modulation). Toinen yleisesti käytetty koodekki on CELP (Code-excited linear prediction)-koodaukseen perustuva hybridikoodekki G.729, josta on sanottu, että se pärjää vertailussa jopa normaalille PSTN-verkon (Public Switched Telephone Network) puheelle ollen myös kustannustehokkaampi ratkaisu G.711:teen verrattuna, sillä G.711 tarvitsee huomattavan paljon enemmän kaistaa toimiakseen [38], [39]. CELP-pohjaiset koodekit ovat ADPCM-pohjaisia koodekeita heikompia taustamelun suhteen. CELP-koodekeita käytetään video-, matkapuhelin- ja satelliittisovelluksissa. Esimerkiksi CELP-pohjainen koodekki G.728 tarjoaa melkein saman laadun ADPCM-pohjaiseen G.726-koodekkiin verrattuna, mutta vaatii puolet vähemmän kaistaa. Kannattaa kuitenkin huomioida, että kaistantarve pystytään kattamaan hitaimmallakin laajakaistayhteydellä kivuttomasti ja yhden laajakaistaisen yhteyden takaa voidaan muodostaa useampia samanaikaisia VoIP-puheluita.

Taulukkoon mukaan otetut koodekit ovat kaikki ITU-T:n standardoimia. Muitakin toki löytyy, mutta yleisimmin käytetyt standardit ovat ITU-T:n kehittämiä. Viiveiden osalta on taulukkoon kuvattu algoritminen viive. Lisäksi viivettä aiheuttaa paketointi- ja prosessointiviiveet. Näitä ei kuitenkaan ole otettu taulukkoon mukaan, sillä viiveiden arvot vaihtelevat esimerkiksi prosessointitehon mukaan. Viiveet ovat osittain suuntaa-antavia.

Taulukko 4. Yleisimmin käytettyjä koodekeita [40]:

KOODEKKI	G.711	G.722	G.722.1	G.726	G.728	G.729
Kuvaus ja lisätietoa	Perustuu PCM:ään. Kaksi versiota, A-law ja U-law. Ei pakkausta ollenkaan. Käytetään digitaalisissa puhelinverkoissa	Perustuu ADPCM:ään	Perustuu ADPCM:ään	Perustuu ADPCM:ään, korvaa G.721:n ja G.723:n	Perustuu CELP:iin (LD-CELP)	Perustuu CELP:iin (ACELP)
Puheensiirron kaistavaatimus	64 kbit/s	48 / 56 / 64 kbit/s	24 / 32 kbit/s	16 / 24 / 32 / 40 kbit/s	16 kbit/s	8 kbit/s
Näytteen / kehyksen koko	10 ms, näytepohjainen	20 ms, kehyspohjainen	20 ms, kehyspohjainen	10 ms, kehyspohjainen, sis. 80 näytettä	2,5 ms, kehyspohjainen, sis. 20 näytettä	10 ms, kehyspohjainen
Koodekin tyyppi	Aaltomuoto	Mallinnus	Mallinnus	Mallinnus	Hybridi	Hybridi
(Algoritminen) viive	0,75 ms	40 ms	40 ms	2,5 – 10 ms	0,625 ms	10 ms
Näytteenotto-taajuus	8 kHz	16 kHz	16 kHz	8 kHz	8 kHz	8 kHz

MOS (Mean Opinion Score)

MOS on yleisesti käytössä oleva geneerinen tapa mitata IP-verkossa kulkevan puheen laatua loppukäyttäjän kannalta. Alun perin MOS on kehitetty tavallista puhelinpalvelua varten, mutta nykyään sitä käytetään nimenomaan selvitettäessä puheen laatua IP-

verkossa. Siinä on sanallisesti määritelty asteikolle 1-5 ulottuvat puheen laadulliset ominaisuudet ykkösen tarkoittaessa heikointa puheen laatua, jossa tavallinen keskustelu ei enää onnistu ollenkaan, ja viitosen tarkoittaessa vastaavasti erinomaista, parasta mahdollista puheen laatua. Aiemmin pelkästään käyttäjien arvostelun perusteella muodostettu numeerinen keskiarvo kuvaa siten kokonaiskuvaa puheen laadusta. Yleisesti on arvioitu, että asteikolla yli neljän arvossa oleva MOS on vielä puheen laadun kannalta kiitettävällä tasolla ja keskustelu onnistuu hyvin vielä yli kolmen MOS-arvolla. Nykyään MOS saadaan muodostettua useimmiten E-mallin avulla laskemalla.

E-malli

Edellä kuvatun subjektiivisen MOS-mittauksen lisäksi on olemassa objektiivisia laadunmittausmenetelmiä. E-mallia (E-model) käytetään selvitettäessä verkon valmiutta puheliikenteen kuljetukseen. E-malli sisältää yksityiskohtaisen laskentamallin, jonka perusteella pystytään selvittämään puheensiirron laatua IP-verkon ylitse ja toisaalta E-mallin perusteella pystytään myös estimoimaan MOS-arvo: MOS = 1 + 0,035R + R(R-60)(100-R)7*10^-6.

Suorituskykyparametri R saadaan laskettua seuraavalla kaavalla:
R = R0 – Is – Id – Ie + A, missä
R0 = signaali-kohina –suhde
Is = yhtäaikainen heikennystekijä (simultaneous impairment factor)
Id = viiveen aiheuttama heikennystekijä (delay impairment factor)
Ie = laitteistosta aiheutuva heikennystekijä (effective impairment factor)
A = etutekijä (impairment factor)
Käytännössä suorituskykyyn vaikuttavia muuttuvia tekijöitä ovat viive, pakettihävikki ja käytetyn koodekin aiheuttama heikennys.

MOS-arvo ei tällöin tosin voi nousta täyteen viiteen asti. Tämä voidaan perustella esimerkiksi sillä, että käytetään sitten mitä tahansa koodekkia puheen muuntamiseen analogisesti digitaaliseksi ja päinvastoin, laskee tämä toimenpide aina puheen laatua.

E-mallin laskentakaava määritellään ITU-T:n standardissa G.107 [56]. Mallin avulla pystytään määrittelemään puheyhteyden ajan funktiona muuttuva arvo päästä-päähän suorituskyvylle. Suorituskykyä kuvaava arvo on nimeltään R-arvo ja mitä suurempi kyseinen R-arvo on, sitä parempi on puheyhteyden suorituskyky kyseisellä päästä-päähän välillä.

E-mallin lisäksi muita objektiivisia menetelmiä ovat esimerkiksi PSQM (Perceptual Speech Quality Measure) ja käytännössä sen pohjalta tehty uudempi versio PESQ (Perceptual Evaluation of Speech Quality) [41]. PSQM:ssä oli ongelmia vaihtelevien viiveiden osalta ja PESQ:ssa nämä on korjattu. PESQ:n tärkein puheen laadullisen mittauksen tulos on nimenomaan aiemmin kuvattu MOS.

PSQA (Pseudo-Subjective Quality Assessment)

E-malli on alun perin suunniteltu vain kokeilu- ja suunnittelutarkoituksiin, eivätkä sen antamat tulokset välttämättä aina ole täysin käyttäjän kokeman laadun kaltaisia. Vielä totuudenmukaisempi menetelmä on PSQA [42], jota käytetään selvittämään usean eri parametrin vaikutuksia QoE:hen. PSQA ilmoittaa yhden objektiivisen tuloksen, joka on E-mallia paremmin vertailtavissa MOS:iin. Erona MOS:iin on kuitenkin se, että PSQA on helpommin mitattavissa, koska se perustuu todellisiin objektiivisiin arvoihin. PSQA antaa tuloksena lähes MOS:n kaltaisia arvoja, ja sen avulla voidaan reaaliaikaisesti valvoa, miten tietyt parametrien arvot vaikuttavat laatuun.

5.2 VoIP

VoIP tarkoittaa puheen (ja videon) kuljettamista (langallisen) IP-verkon yli. Käytännössä tämä tarkoittaa sitä, että puhe muutetaan digitaaliseksi ja kuljetetaan paketteina IP-verkon yli vastaanottajalle, missä puhe muutetaan takaisin analogiseen muotoon. Usein puhutaan VoIP:sta, vaikka puhe kulkisikin esimerkiksi alkumatkan langattoman verkon yli, mutta tässä tutkimuksessa VoIP:lla käsitetään nimenomaan langallisen IP-verkon yli tapahtuvaa puheen kuljetusta. Puheen muuttamisessa analogisesta digitaalisiksi paketeiksi ja päinvastoin käytetään koodekkeja. Datan paketoimiseen kuluu tietty aika käytetystä koodekista riippuen. Signalointiprotokollana (voidaan puhua myös merkinantoprotokollasta tai yhteydenmuodostusprotokollasta)

käytetään joko H.323:a tai SIP:ä (Session Initiation Protocol). Signaloinnin lisäksi viestinvälitysprotokollana käytetään yleisimmin UDP:tä (User Datagram Protocol), joskus myös TCP:tä (Transmission Control Protocol). UDP on kuitenkin soveltuvampi puheliikenteeseen, sillä sitä käytettäessä vastaanottajan ei tarvitse kuitata jokaista pakettia saaduksi, eikä lähettäjän näin ollen tarvitse lähettää osaa paketeista uudelleen. TCP:n tapa kuitata jokainen paketti vastaanotetuksi johtaa puheliikenteessä helposti kaistan turhaan käyttöön, sillä useinkaan kadonneiden pakettien uudelleenlähetykset eivät ole enää ajallisesti mielekkäitä sallittuun viiveeseen nähden ja liian myöhään saapuneet paketit tiputetaan. Lisäksi VoIP:n yhteydessä käytetään RTP-protokollaa itse datan kuljettamiseen.

VoIP:n edut voidaan yritysmaailmassa jakaa karkeasti kolmeen osaan; käyttökustannussäästöt, paremmat ja monipuolisemmat ominaisuudet sekä liiketoiminnan sovellus- ja yksinkertaistamismahdollisuudet. Verrattuna analogiseen PSTN-linjaan VoIP:n etuina voidaan pitää seuraavia:

- Yhdellä laajakaistaisella yhteydellä pystytään välittämään useita puheluita
- Operaattoreiden normaalisti lisäpalveluina veloittamat ominaisuudet ovat helposti toteutettavissa (puhelunvälitys, automaattinen uudelleenvalinta yms.)
- VoIP-teknologia mahdollistaa verkkokonvergenssin toteutumisen ja viestinnän yhtenäisyyden, sillä sen toimiessa IP-verkossa pystytään se helposti yhdistämään muihin Internet-palveluihin, kuten videoneuvotteluihin [43]

5.3 VoWIP

Erilaisten langattomien laajakaistaisten yhteysratkaisujen lisääntyessä ja yleistyessä (kuten aiemmin kuvatut WiMAX, @450, 3G) myös VoWIP:n käyttö on kasvanut. Kuten edellä on mainittu, puheen kuljetuksesta IP-verkossa käytetään erittäin usein kuitenkin pelkkää VoIP-nimitystä. VoWIP on itse asiassa vielä harvoin käytetty nimitys, jolla tarkoitetaan puheen kuljettamista langattoman pitkän kantaman IP-verkon, eli nimenomaan esimerkiksi WiMAX-verkon tai 3G-verkon yli.

3G-liikenneluokat

Langattomien pitkän kantaman yhteysratkaisujen suurin pullonkaula on radioverkko-osuus. Se asettaa suurimmat rajoitukset kaistanleveyden suhteen ja toisaalta aiheuttaa suurimmat bittivirheet ja viiveet. Niinpä palvelunlaadun kunnollisen toteutumisen vaatimukset ovat eri tasolla kuin langallisissa verkoissa.

3G:n UMTS:ssä verkon mahdollisimman tehokas ja palvelunlaadun kannalta soveltuvin käyttäytyminen on mahdollistettu jakamalla liikenne neljään liikenneluokkaan. Tämä mahdollistaa sovelluskohtaisten ominaisuuksien perusteella tehtävän jaottelun ja edesauttaa siten verkon mahdollisimman tehokasta ja taloudellista käyttöä. Eri palveluluokkien välittämiseen käytetään DiffServ-liikenneluokkia. Määritellyt neljä liikenneluokkaa ovat [23],[44]

- Conversational class
- Streaming class
- Interactive class
- Background class

Suurin erottava tekijä edellä mainittujen liikenneluokkien kesken on se, miten viiveherkkää liikenne on. *Conversational*-luokka on tarkoitettu kaikista viiveherkimmälle liikenteelle ja *Background*-luokka taas päinvastaisesti on vähiten viiveherkälle liikenteelle. Jaottelu voidaan tehdä karkealla tasolla siten, että *Conversational*- ja *Streaming*-luokat on tarkoitettu reaaliaikaiselle liikenteelle, eli esimerkiksi puheelle ja videoneuvotteluille ja muille multimediasovelluksille. Kaksi jälkimmäistä luokkaa, *Interactive* sekä *Background*, ovat taas tarkoitettu lähinnä normaaliin WWW-selailuun, sähköpostikäyttöön yms. *Interactive* sekä *Background*-luokat ovat virheasteeltaan parempia, koska ne käyttävät kanavakoodausta ja uudelleenlähetystä. Ne eivät kuitenkaan sovellu puhe- ja videoliikenteelle, sillä tällöin kyseisten luokkien käyttö on hitaampaa ja viiveen osalta suurempaa, mutta toisaalta pakettien perillemenotodennäköisyys on suurempi edellä mainittujen syiden takia.

WiMAX:in palvelunlaatuluokat

WiMAX sisältää neljä eri QoS-luokkaa ja näiden lisäksi mobiili-WiMAX 802.16e sisältää viidennen QoS-luokan. QoS-luokat ovat [23],[45]

- Unsolicited Grant Service (UGS)
- Real-Time Polling/Packet Service (rtPS)
- Extended Real-Time Packet Service (ErtPS)
- Non-Real-Time Polling/Packet Service (nrtPS)
- best-effort (BE)

Edellä kuvatuista QoS-luokista UGS on tarkoitettu ennen kaikkea reaaliaikaiselle dataliikenteelle, esimerkiksi VoIP:lle. rtPS soveltuu vaihtelevankokoisille, periodeissa lähetetyille paketeille, esimerkiksi MPEG:lle. ErtPS on aiemmin mainittu mobiili-WiMAX:in viides QoS-luokka, joka on myös VoIP-puheliikenteelle tarkoitettu luokka. nrtPS soveltuu liikenteelle, joka tarvitsee kaistaa, mutta ei ole niin viiveherkkää, eli esimerkiksi FTP. Viimeinen luokka eli best-effort soveltuu liikenteelle, jolla ei ole erityisiä vaatimuksia laatumääreiden suhteen.

802.16 ja 802.16e sisältävät siis muutoin samat luokat keskenään, mutta 802.16e:ssä on ylimääräisenä luokkana ErtPS. Lisäksi 802.16e:ssä *polling* on korvattu *packet*-sanalla [46].

Jokaisella luokalla on omat palvelunlaatuparametrit, joten käytettävä luokka tulee valita käytetyn sovelluksen tarpeen mukaan. Tämä mahdollisuus on toteutettu päätelaitteissa, jotka pystyvät halutessaan muodostamaan jokaiselle sovellukselle oman yhteyden käyttäen haluttua QoS-luokkaa [47].

@450 ja QoS

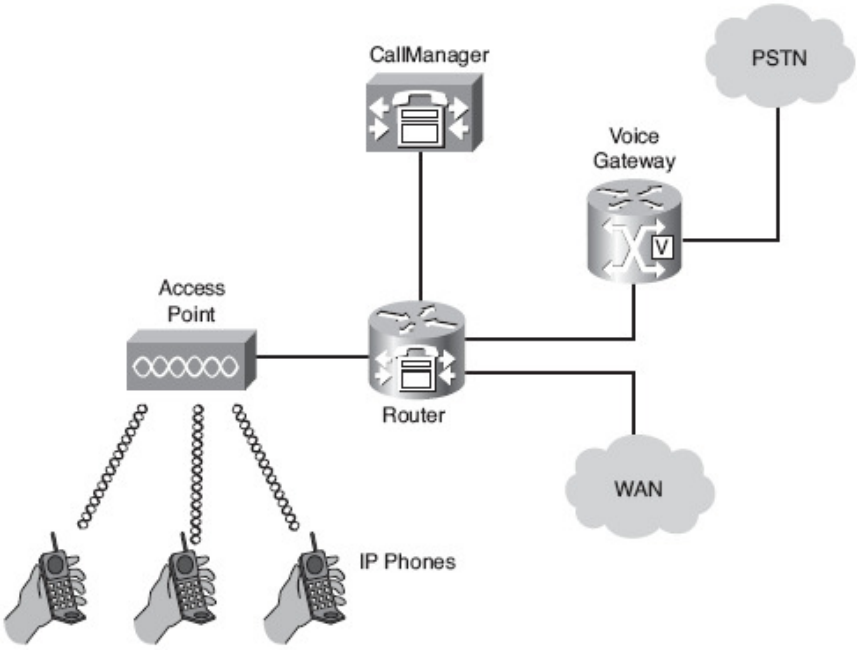
@450-verkon on sanottu mahdollistavan pienet latenssit ja paremman QoS:n käytetyn tekniikan ansiosta. Esimerkkinä tästä on nopea käyttäjän siirto *aktiiviseen* ja *ei-aktiiviseen* tilaan sen mukaan, onko käyttäjä juuri siirtämässä tietoa vai esimerkiksi selailemassa web-sivuja. Flash-OFDM myös tarjoaa korkeaa luotettavuutta käyttämällä

ARQ:ta (Automatic Repeat Request), jota käytetään tarkistamaan siirrettyjen datapakettien virheitä. Mikäli virheitä löydetään, lähetetään paketit nopeasti uudelleen. Kiertoaika on alle 10 millisekuntia, joten latenssi on alhainen ja paketit pystytään lähettämään nopeasti uudelleen. Tämä takaa korkean luotettavuuden ja toisaalta sen sekä pienen latenssin ansiosta erilaisten interaktiivisten sovellusten käyttö @450-verkon yli on mahdollista. Sekä Qualcomm että Digita mainostavat VoIP:n (ja tässä tapauksessa VoWIP:n) toimivan verkossa hyvin viiveiden pysyessä yleisesti alle 50 millisekunnissa. Kuitenkaan liikennettä ei voida priorisoida esimerkiksi erilaisten liikennetyyppien mukaan, vaan ainoa mahdollisuus on priorisoida itse liittymä, jolloin suuremmalla hinnalla kyseisen liittymän liikenne saa verkon ruuhkautuessa etusijan muihin nähden. Kaikki yhden käyttäjän liikenne on siis kuitenkin keskenään samanarvoista [48].

5.4 VoWLAN

Yritysten siirtyessä yhä enemmän langattomuuteen myös lähiverkon osalta, siirrytään puhumaan aiemman VoIP-käsitteen sijaan VoWLAN-käsitteestä. Mikäli yritys käyttää IP-puhelimia langattoman lähiverkon yli, on kyse VoWLAN:ista. VoWLAN onkin hyvä ratkaisu nimenomaan yrityksen sisäverkossa tapahtuviin sisäisiin puheluihin, mutta myös Internetin yli muodostettaviin puheluihin, sillä VoWLAN mahdollistaa toki puhelut myös julkiseen PSTN-verkkoon sekä Internetiin. VoWLAN tuleekin yritykselle pitkällä aikavälillä selvästi edullisimmaksi vaihtoehdoksi. Ensimmäinen VoWLAN:in mukainen 802.11-perheen standardi on 802.11e.

VoWLAN:iin liittyvät komponentit on kuvattu alla olevassa kuvassa 10.



Kuva 10. VoWLAN-komponentit [49]

Kuvassa näkyvät VoWLAN-puhelimet (IP Phones) ovat yhteydessä langattomasti tukiasemaan (Access Point), joka taas on erikseen yhdistetty reitittimeen (Router). Tukiasema saattaa toimia itse myös reitittimenä, jolloin erillistä reititintä ei tarvita. *CallManager* hoitaa perinteisen yksityisen puhelinvaihteen tehtävät eli prosessoi ja hallinnoi puheluita, hoitaa IP-puhelimien rekisteröinnin verkkoon ja hallinnoi reittisuunnitelmia. *Voice Gateway* yhdistää IP-verkon puhelut muunlaisiin verkkoihin, kuten perinteiseen PSTN-verkkoon. Tämä voi olla ensisijainen reitti IP-puhelimien ja PSTN-puhelimien välillä yrityksen verkossa. Vaihtoehtoisesti Voice Gatewayn kautta voidaan muodostaa varareitti, mikäli yhteys WAN (Wide Area Network)-verkkoon katkeaa.

VoWLAN:in käsittely ja katsontakanta riippuvat paljon myös osapuolesta. Samat positiiviset puolet, jotka on kuvattu VoIP:ia koskevassa kappaleessa, pätevät joka tapauksessa myös VoWLAN:issa. Loppukäyttäjää varmasti miellyttää sisäpuheluiden ilmaisuus, mutta mietityttää puhelun laadukkuuden toteutuminen. Operaattorit taas pyrkivät kaikin keinoin saamaan asiakkaita hankkimaan vähintäänkin lisäpalveluita, mikäli itse liikennöinnistä ei pystytä veloittamaan suuria määriä. VoWLAN:in etuna

voidaan pitää sitä, että samaa puhelinta voidaan käyttää toimiston tai kodin lisäksi myös muualla langattomien WLAN-tukiasemien määrän lisääntyessä.

VoWLAN-puhelinta käyttävä yrityksen työntekijä on paremmin tavoitettavissa, kuin perinteisen langallisen puhelinyhteyden päässä oleva työntekijä. Lisäksi työntekijöiden vaihtaessa toimitiloja VoWLAN-puhelin on helppo ottaa mukaan uuteen paikkaan ilman uusia kaapelointeja. Edullisuus ja helppous ovatkin VoWLAN:in suurimpia etuja. On kuitenkin huomioitava, että yrityksen miettiessä VoWLAN:in käyttöönottoa, tulee sen miettiä tarkat suunnitelmat ja laskelmat VoWLAN:in kannattavuudesta ja siitä, miten pitkä takaisinmaksuaika uuteen järjestelmään siirtymisellä olisi. Mikäli työntekijät eivät liiku oman työpisteensä ulkopuolella juurikaan, ei tarvetta mobiilille järjestelmälle ole olemassa, vaan yritys pärjää nykyisellä langallisella ratkaisulla. Jos taas työntekijät ovat paljolti liikkeessä, silloin VoWLAN on harkinnan arvoinen ratkaisu ja voittaa edullisuudessaan 3G-verkon kautta käytettävät matkapuhelinliittymät.

VoWLAN:in haasteita (WLAN:ssa) puheliikenteeseen ja muuhun kriittiseen liikenteeseen liittyen ovat:

- Akkujen kulutus
- Tukiasemasta ja verkosta toiseen siirtyminen
- Kaistan käyttö/kapasiteetti
- Palomuurit ja NAT (Network Address Translation)
- Palvelunlaadun riittävän hyvä toteutuminen
- Erilaisten päätelaitteiden suuri määrä ja yhteensovittaminen
- Laskutuksen sujuvuus (lukuisia toimijoita)

Yksi suurimmista ongelmista VoWLAN:in toiminnallisuuden kannalta on se, että päätelaitteet kuluttavat runsaasti akkua. Hyvä ja tunnettu keino on tiputtaa päätelaitteen virrankulutusta *idle*-tilassa mahdollisimman alhaiseksi ja nostaa sitten takaisin normaalille tasolle siinä vaiheessa, kun päätelaite on taas aikeissa päästä radiotielle ja lähettämässä tai vastaanottamassa dataa.

DTPC:n (Dynamic Transmit Power Control) ottamista käyttöön ei välttämättä suositella langattomissa lähiverkoissa, joissa on tarkoitus välittää puheliikennettä. DTPC kyllä kasvattaa muiden AP:iden virtaa, mikäli jokin AP katoaa kokonaan alueelta ja mahdollistaa siten muiden AP:iden osalta peittoalueen laajenemisen ja siten myös kartalta poistuneen AP:n palvelualueella on mahdollista edelleen päästä johonkin toiseen AP:hen kiinni. Ongelma DTPC:ssä on kuitenkin se, että puheliikenne vaatii tasaista virtatasoa toimiakseen optimaalisesti ja mikäli DTPC:n avulla virtatasoa joissain laitteissa kasvatetaan, ei virtataso ole enää tasainen aiheuttaen näin ongelmia äänenlaadulle [50]. Muut AP:t saattavat lisäksi häiritä samalla kanavalla olevia laitteita, mikäli tehoa kasvatetaan. Tehon kasvattamiseksi vaaditaan usein myös AP:n osalta väliaikaista radiolinkin alasajoa, mikä myös katkaisisi itse yhteyden. Toisaalta, mikäli DTPC ei ole käytössä, yksi alhaalla oleva tukiasema voi estää joidenkin päätelaitteiden pääsyn verkkoon kokonaan, mikäli päätelaite ei löydä riittävän läheltä toista AP:ta. Suositeltavin ratkaisu on kuitenkin välttää DTPC:tä ja mieluumminkin pyrkiä saamaan alhaalla oleva AP mahdollisimman nopeasti takaisin toimintaan.

Puheliikenne kuluttaa kohtalaisen paljon kaistaa, joten yhtenä ongelmana VoWLAN:ssa voidaan nähdä kaistan käyttö ja ennen kaikkea kaistan mahdollinen riittämättömyys. Mikäli puheliikenne vie varsinkin priorisointimääritysten takia suuren osan kaistasta, on muun liikenteen osana jäädä jalkoihin. Tässä yhteydessä palvelunlaadun riittävä toteutuminen puheliikenteen osalta saattaa siis johtaa siihen, että vaikka VoWLAN toimisikin moitteettomasti, aiheuttaisi se liikaa palvelunlaadullisia ongelmia muuhun liikenteeseen. Tämäkään ei ole tavoiteltava tilanne.

Lisäksi puheliikenteeseen ongelmallisesti vaikuttavia tekijöitä ovat palomuurit sekä NAT. Palomuuri saattaa estää UDP-pakettien liikennöinnin molempiin suuntiin estäen näin VoWLAN:in ja ylipäätään puheliikenteen käyttämän UDP-liikenteen etenemisen. Puheliikenteen käyttämät UDP-portit onkin näin ollen asetettava sallittujen listalle, jotta VoWLAN toimisi. STUN-palvelin (Simple Traversal of UDP Through NAT) mahdollistaa NAT:n ja palomuurin takana oleville sisäverkon laitteille VoWLAN-puheluiden muodostamisen paikallisen verkon ulkopuolella sijaitseville palvelimille.

STUN-palvelimen avulla sisäverkon käyttäjä saa tietoonsa julkisen IP-osoitteensa, tietoja siitä, minkälainen NAT sisäverkon ja ulkomaailman välillä on käytössä sekä julkisen verkon puolella käytetyn portin. Edellä mainittujen tietojen avulla saadaan muodostettua yhteys käyttäjän ja VoIP-palvelimen välille. STUN-protokolla on määritetty IETF:n dokumentissa RFC 3489 [51].

STUN-palvelimeen otetaan yhteys UDP-porttiin 3478, mutta palvelin neuvoo kuitenkin asiakkaita suorittamaan testejä myös muihin IP- ja porttinumeroihin (STUN-palvelimilla on kaksi IP-osoitetta). RFC3489:n mukaan portti ja IP-osoite ovat vapaasti valittavissa.

Tukiasemien vaihdosta johtuvat katkokset ovat yksi VoWLAN:in käyttöä haittaava tekijä. 802.11e-standardi on tuonut QoS-aspektin langattomiin lähiverkkoihin, mutta nopeaan tukiaseman vaihtamiseen liikuttaessa paikasta toiseen kyseinen standardi ei tuo apua. Tukiasemalta toisen alueelle siirtyminen tai parempilaatuisen signaalin löytymisestä johtunut tukiaseman vaihto aiheuttaa usein lyhyen katkoksen liikennöintiin. Käyttäjän tunnistaminen tapahtuu useimmiten RADIUS-palvelimen (Remote Authentication Dial In User Service) avulla. Langattomissa verkoissa RADIUS:ta käytetään esimerkiksi käyttäjäkunnan rajaamiseen. RADIUS-palvelimien välisten luottamussuhteiden avulla käyttäjän on mahdollista kirjautua myös vierasverkkoon oman operaattorinsa tarjoamalla autentikointimenetelmällä ja käytännössä omilla tutuilla tunnuksillaan, mikäli operaattorit ovat tehneet keskenään sopimuksen ja sallivat toisten operaattoreiden asiakkaiden käyttävän kyseisen operaattorin verkkopalveluita. Tällaisessa tapauksessa operaattorit ovat keskenään sopineet tulonjaosta ja käyttäjää laskutetaan hänen oman operaattorinsa toimesta myös vierasverkon käytön osalta.

RADIUS-palvelimien käyttö on yleistynyt viime vuosina. Haasteena on se, että tukiaseman vaihtuessa myös liikennöintiin tulee katkos, kun RADIUS-palvelimen kanssa tulee autentikoitua uudestaan. RADIUS:n kanssa voidaan käyttää esiautentikointia, jolloin osa autentikointitoimenpiteistä suoritetaan jo ennen tukiaseman

vaihtoa. Tämä lyhentää katkoksen kestoa. Toisena haasteena on se, että käyttäjän kokema palvelu on vierasverkon operaattorin tarjoama ja edellyttää esimerkiksi kyseisen verkon asetusten käyttöönottoa. Lisäksi palvelunlaadulliset seikat saattavat poiketa toisistaan eri verkkojen kesken.

Uudempi Diameter-protokolla on nykyään hyvä vaihtoehto ennen kaikkea mobiililiikenteelle tunnistamismenetelmäksi, sillä siinä on määritelty RADIUS:ta paremmin esimerkiksi virhetilanteista toipuminen. Myös konfiguroinnin tarve vähenee Diameter-protokollan myötä.

802.11e-standardissa, eli käytännössä ensimmäisessä QoS:n huomioivassa 802.11-standardissa oli mukana EDCA, joka jo mahdollisti liikenteen erottelun kriittistä liikennettä varten. Standardi ei kuitenkaan vielä huomioinut tukiaseman vaihdon nopeuttamista, johon on kehitetty erillinen, nimenomaan IP-puheluiden entistä parempaa toteutumista WLAN-verkon yli varten suunniteltu kesällä 2008 julkaistu IEEE standardi 802.11r. Standardista käytetään myös nimeä Fast Basic Service Set Transition (FBSST) ja IEEE hyväksyi sen kesällä 2008 [57].

802.11r pyrkii entisestään lyhentämään katkosaikaa päätelaitteen siirtyessä tukiasemalta toisen tukiaseman alaisuuteen tai langattomasta verkosta toiseen käyttämällä ennakoivaa autentikointia mahdollisimman pitkälle. Käytännössä tämä tarkoittaa sitä, että katkosajan tulee rajoittua maksimissaan 50 millisekuntiin IP-puheen kunnollisen toimivuuden takaamiseksi. 802.11r tuo ratkaisun myös aiemmin mainittuun QoS-ongelmaan, jossa kaikki tukiasemat eivät välttämättä tue samoja palvelunlaatuvaatimuksia keskenään. Standardissa uusi tukiasema lähettää sen hetkisen tukiaseman kautta päätelaitteelle tiedon siitä, pystyykö uusi tukiasema tukemaan sen hetkisiä laatuvaatimuksia IP-puheen kannalta.

Uuden 802.11r-standardin uskotaan lisäävän ennen kaikkea yritysten kiinnostusta langatonta IP-puhetta kohtaan. Standardin mahdollisesta tulosta markkinoilla oleviin laitteisiin asti ei ole vielä tarkempaa tietoa, mutta optimistisimpien arvioiden mukaan

laitteita olisi tulossa markkinoille jo vuoden 2009 aikana. Vielä ei tiedetä myöskään sitä, tarvitaanko standardin käyttöönottamiseksi erillistä laitteistopäivitystä, vai selvitäänkö nykyisiin laitteisiin tehtävillä ohjelmistopäivityksillä [57].

Palvelunlaadun riittävän hyvän toteutumisen kannalta aiemmissa kappaleissa kuvatut menetelmät ovat oleellisia. Lisäksi kannattaa luoda erillinen SSID tai VLAN (Virtual Local Area Network) VoWLAN-liikennettä varten ja erotella kyseinen liikenne näin muusta liikenteestä selkeästi erilliseksi osaksi. Tukiasemien antennien oikeanlainen suuntaaminen kuuluu myös olennaisena osana laadullisesti hyvän lopputuloksen edellytyksiin.

5.5 VoWLAN vs. VoIP palvelunlaadun ja QoE:n suhteen

IP-puheluiden palvelunlaadusta puhuttaessa viitataan yleensä ennen kaikkea reaaliaikavaatimukseen. Tutkimuksessa on aiemmin kuvattu erilaisia tapoja liikenteen priorisoimiseksi, jolloin tärkeät liikennepaketit saavat mahdollisesti etuoikeuden tai enemmän kaistaa muihin paketteihin verrattuna. Viive, viiveen vaihtelu sekä pakettihävikki tulee saada mahdollisimman pieniksi puheen toimivuuden varmistamiseksi.

Vertailtaessa VoWLAN:ia ja VoIP:ia keskenään QoE:n kannalta voidaan todeta, että useimmissa tapauksissa käyttäjä kokee VoIP:n laadullisesti paremmaksi tai vähintään yhtä hyväksi VoWLAN:n kanssa. Tämä voidaan perustella yksinkertaisesti sillä toteamuksella, että VoWLAN käyttää samaa verkkoinfrastruktuuria kuin VoIP, mutta VoWLAN:ssa on lisäksi langattoman lähiverkon osuus, mikä on kaikista altein häiriöille.

Kärjistettynä tilanne on se, että mikäli järjestelmän kapasiteettia, eli yleisimmin kaistaa, on käytössä riittävästi, ei QoS:ää tarvita ollenkaan. Tilanne on kuvatun kaltainen esimerkiksi silloin, kun muodostetaan VoIP-puheluita pelkästään LAN-verkon sisäisesti 100 Mbit/s tai Gigabit Ethernet -yhteydellä. Myös esimerkiksi runkoverkossa viiveet ja pakettihävikit ovat yleensä minimaalisia, eikä runkoverkon osuudella näin ollen tapahdukaan merkittäviä seikkoja, jotka vaikuttaisivat IP-puheluiden laadukkuuden tai

toimivuuden heikkenemiseen. Sen sijaan päästä-päähän -laatuun tulee kiinnittää huomiota myös VoIP:n tapauksessa, sillä vastapuolen käyttämä yhteys ei välttämättä ole yhtä suurikapasiteettinen kuin soittajan.

5.5.1 VoWLAN:n toteuttaminen WLAN:n yli

QoS:n on VoIP:n yhteydessä ajateltu yleisesti koskevan OSI-mallin 3. kerrosta eli verkkokerrosta (ja ylempiä kerroksia). Lisäksi monet VoIP-sovellukset käsittelevät sovellusta erillään alla olevasta verkosta, eivätkä VoIP-sovellukset näin ollen useinkaan tiedä, mitä teknologiaa OSI-mallin 2. tasolla eli siirtoyhteyskerroksella käytetään. VoWLAN:issa taas ollaan tietoisia siirtoyhteyskerroksesta, jolloin palvelunlaatu tulee relevantiksi myös OSI:n 2. kerroksella. VoWLAN-puheluissa palvelunlaatuun tuleekin kiinnittää oleellista huomiota, vaikka puhelut kulkisivat pelkästään yrityksen sisäverkossa. VoWLAN:in käyttöön liittyy se perustavaa laatua oleva ongelma, että 802.11-standardi suunniteltiin alun perin täysin dataliikenteelle, eikä puheliikenteen vaatimuksia otettu millään lailla huomioon. 802.11-standardi on kuitenkin kehittynyt vuosien mittaan, ja nykyään QoS huomioidaan paremmin myös WLAN-yhteyden osalta.

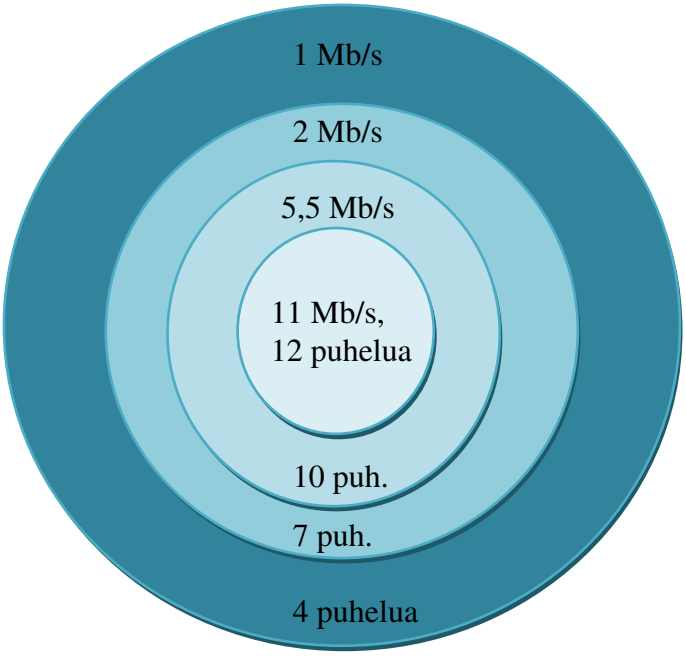
Yksinkertaisesti ajateltuna WLAN-verkon läpäisykyky saadaan mahdollisimman suureksi kasvattamalla pakettikokoa isommaksi. VoWLAN:in tapauksessa tämä ei kuitenkaan ole toimiva ratkaisu, sillä pakettien pitää olla kooltaan riittävän pieniä, jotta päästä-päähän -viive ei kasva liian suureksi. VoWLAN:in keskimääräinen paketointijakso on 10 – 40 ms ja keskimääräinen pakettikoko on noin 100 – 300 tavua. Tämän johdosta tehokas kaista VoWLAN:ille on noin 1 – 2 Mbit/s yhden tukiaseman tapauksessa. Suuremmat nopeudet auttavat kasvattamaan järjestelmän kapasiteettia, mutta muutos on tällöin suurin isoilla paketeilla. VoWLAN:in käyttämillä pienillä paketeilla muutos ei ole suuri.

Järjestelmän kapasiteetti on joka tapauksessa tärkein mittari. 802.11-standardin MAC-osakerros ei ota huomioon eri päätelaitteiden liikennöintiaikaa, kun kilpaillaan siirtotielle pääsystä. Sen sijaan MAC pyrkii luomaan eri päätelaitteiden siirtomahdollisuudet tasavertaisiksi. Toisin sanoen, kun asema on päässyt vuorollaan

siirtotielle ja lähettänyt paketin, joutuu se sen jälkeen taas kilpailemaan siirtotielle pääsystä muiden asemien kanssa. Kun tietty asema on siirtotiellä, ei MAC ota huomioon paketin kokoa. Asema voi siis lähettää 10 tavun kokoisen paketin tai vaihtoehtoisesti vaikka 2500 tavun paketin, jolloin isomman paketin lähettävä asema pystyy kerrallaan lähettämään huomattavan paljon suuremman määrän dataa. Tästä syystä VoWLAN-järjestelmissä (pienet pakettikoot) pieniä datamääriä lähettävät VoWLAN-päätelaitteet joutuvat odottamaan suhteessa pidempään asemalle pääsyä, mikäli jokin asema lähettää välillä suuria paketteja. Mitä kauemmin ison paketin lähetys kestää, sitä enemmän VoWLAN-liikenne kärsii.

Toinen ongelmallinen tekijä VoWLAN-liikenteessä on pakettien suuret otsikkokentät. Hyötymäärä paketissa saattaa jäädä jopa reiluun kymmenesosaan koko paketin koosta. Verrattuna VoIP-paketteihin MAC lisää WLAN:ssa vielä oman otsikkokentän VoWLAN-pakettiin, mikä lisää paketin kokoa. Lisäksi fyysinen kerros luo vielä oman otsikkokenttänsä. Vaikka sen koko ei ole kovin suuri, vaikuttavat nämä kaikki yhdessä WLAN:in 1 – 2 Mbit/s nopeuksisella linjalla.

Alla on kuvattu samanaikaisten puheluiden määrä yhtä tukiasemaa kohden. Järjestelmän kapasiteetti on suurimmillaan nopeilla yhteyksillä, mutta kantoalue on tällöin pieni. Nopeuden laskiessa myös yhtäaikaisten puheluiden määrä laskee, mutta kantoalue laajenee samalla.



Kuva 11. Etäisyyden vaikutus järjestelmän kapasiteettiin. Osittain muokattu alkuperäisestä kuvasta [52]

Kuva selventää hyvin sen, että signaalin voimakkuus heikkenee kauemmaksi mentäessä. Etäisyyden kasvaessa siis nopeus ja mahdollisten yhtäaikaisten puheluiden määrä laskevat. Mitä lyhyemmän kantaman päässä ollaan, sitä nopeampaan yhteyteen päästään. Tällöin yhden paketin välittäminen vie lyhyemmän aikaa ja media on vapaana pidempään. Samalla järjestelmän kapasiteetti siis kasvaa. On kuitenkin huomioitava, että lyhyellä etäisyydellä tapahtuva suuremmalla nopeudella operoiminen vaatii kompleksisempaa modulointia. Tämä johtaa hitaampaa yhteyttä suurempaan kohinaan ja saattaa osaltaan johtaa bittivirhetodennäköisyyden kasvuun sekä sen myötä suurempaan pakettihävikkiin. Tällöin paketteja täytyy lähettää uudestaan, jolloin järjestelmän kapasiteetti laskee. Nopeuden ja yhtäaikaisten puheluiden määrän oikeanlaisen suhteen löytäminen onkin tärkeää toiminnallisuuden maksimoimiseksi. Nopeuden muokkaaminen on yksi keino päästä parhaaseen mahdolliseen lopputulokseen. Optimaalisen nopeuden valitseminen eli nopeuden sovitus (*rate adaptation*) aina vallitsevien kanavaolosuhteiden mukaan on mahdollista toteuttaa joko automaattisesti tai manuaalisesti muutamasta eri nopeusvaihtoehdosta valitsemalla [53]. 802.11-standardissa ei alun perin ollut määritelty nopeuden sovitusta ollenkaan, mutta

nykyään se on oleellinen osa toimivia WLAN-yhteyksiä ja tähän tarkoitukseen on kehitetty useita erilaisia algoritmeja.

Puheeseen ja muuhun reaaliaikaisuutta vaativaan liikenteeseen nopeuden sovitus ei kuitenkaan sovellu parhaalla mahdollisella tavalla. Syynä on se, että puheliikenne on herkkää viiveelle ja viiveen vaihtelulle. Nopeuden sovitus taas pyrkii löytämään optimaalisen nopeuden, jotta läpäisykyky saataisiin mahdollisimman suureksi. Tällöin pakettihävikki kuitenkin kasvaa ja kehyksiä joudutaan lähettämään uudestaan. Kuten edellä on todettu, tämä on dataliikenteelle optimaalinen ratkaisu, mutta ei sovellu suoraan reaaliaikaisen liikenteen tarpeisiin.

5.5.2 Sallitut laatuparametrien arvot puheliikenteelle

Viive ja viiveen vaihtelu ovat puheliikenteeseen eniten vaikuttavia palvelunlaatuparametreja. Viiveen pysyessä alle 150 millisekunnissa, ei IP-puheessa ole havaittavaa ongelmaa. Mikäli viive nousee 150 – 250 ms välille, on puhe vielä täysin toimivaa, mutta pientä viivettä ja häiriötä on jo havaittavissa. Mikäli viive edelleen kasvaa yli 250 millisekunnin, alkaa se häiritä jo niin paljon, että puhuminen ei ole mielekästä. Yli 400 millisekunnin viiveen voidaan sanoa aiheuttavan puhelun mahdottomaksi [54].

Kun viiveen vaihtelu pysyy alle 40 millisekunnissa, ei puheessa ole havaittavaa häiriötä. Viiveen vaihtelun kasvaessa 40 – 75 ms välille alkaa häiriöitä ilmetä, mutta laatu on edelleen täysin kelvollinen. Yli 75 ms viiveen vaihtelu ei ole enää hyväksyttävä [53]. Pakettihävikin tulisi pysyä ainakin alle 3 prosentissa, mutta mielellään vielä pienempänä.

5.5.3 Puheliikenteen tietoturva

Tietoturvallisuustekijät ovat oleellisessa asemassa IP-puheessa. Perinteiseen analogiseen puhelinverkkoon liittyvien ongelmien lisäksi mukana ovat IP-verkon tietoturvariskit. Lisäksi VoWLAN:n osalta mukaan tulee vielä langattoman verkon osuus. Kappaleessa 4.3 on kuitenkin käyty jo tarkemmin läpi WLAN-verkon tietoturvaa, joten sitä ei käsitellä tässä yhteydessä enää.

IP-verkossa mahdollisia uhkatekijöitä puheliikenteen kannalta perinteisen analogisen puhelinverkon uhkien lisäksi ovat esimerkiksi

- Palvelunestohyökkäykset. Kaapattuja koneita hyväksikäyttäen voidaan estää IP-puheen käyttö ruuhkauttamalla palvelu, palvelin tai verkkolinkki
- Puheluiden salakuuntelu IP-verkon yli
- Virukset, troijalaiset ja muut haittaohjelmat ovat ongelma myös puheliikenteen osalta ja voivat levitä nopeasti myös VoIP-sovelluksissa ja niiden kautta

Edellä mainittujen toteutumisen estämiseksi on olemassa useita keinoja. Erilaiset IP-verkoissa yleisesti käytössä olevat ja tässäkin dokumentissa kuvatut salauskeinot ovat sovellettavissa myös IP-puheeseen. Lisäksi on mahdollista käyttää listaa luotetuista numeroista, jolloin ainoastaan kyseisistä numeroista tulevat puhelut päästetään läpi.

6. Tapaustutkimus

Kappaleessa kuusi käydään läpi tapaustutkimus, jossa on mitattu langattoman lähiverkon palvelunlaatua Salon kaupungin verkossa. Alun Noval Networksin yleiskuvauksen jälkeen on kuvattu asiakkaan ympäristö ja mittausjärjestelyt, sekä näiden jälkeen raportoitu itse mittaustulokset. Kappaleessa seitsemän on analysoitu mittaustuloksia tarkemmin.

6.1 Noval Networks ja sen toimintatapa

6.1.1 Noval Networksin kuvaus

Tämä diplomityö on tehty Noval Networks Oy:lle. Noval Networks on vantaalainen, vuonna 2000 perustettu riippumaton, velaton ja AAA-luokiteltu suomalainen konsultointi- ja innovaatioyritys, joka on keskittynyt palvelutasonhallintaan [58]. Yritys työllistää tällä hetkellä noin 20 henkeä.

Noval Networksin liikeideana on auttaa asiakasta liiketoimintakriittisten ICT-palveluiden palvelutasonhallinnassa. Yrityksen ydinosaamisalueisiin kuuluvat:

- ICT-palveluiden laadun määrittely, seuranta ja jatkuva parantaminen sekä kilpailuttaminen
- Toimintavarmuuden takaamisessa tarvittavat teknologiat ja toimintatavat
- Tietoliikennetekniikat

Noval Networksin asiakaskuntaan kuuluvat pääasiassa suuret ja keskisuuret yritykset sekä julkishallinnon organisaatiot.

6.1.2 NetEye-työkalu & SLM

Noval Networksin palvelut voidaan jakaa kolmeen osa-alueeseen:

- Noval NetCare: Konsultointi- ja asiantuntijapalvelut
- Noval NetEye: ICT-palveluiden laadun valvonta, seuranta ja mittaaminen
- Noval TopCare: Palvelutasonhallinta (SLM), ”Easy ITIL”

Yksinkertaistettuna palvelukonseptia voidaan tarjota aikasyklisesti siten, että ensin asiakas tilaa jonkin toimeksiannon, esimerkiksi tietoliikennekilpailutuksen. Tämä palvelu toteutetaan Noval NetCare -palvelukonseptin alla sisältäen asiakasympäristöön tutustumisen, tarvittavat palaverit ja workshopit, tarjouspyynnön ja vaatimusmäärittelyn työstön sekä sopimusneuvottelut. Kilpailutuksen ja toimittajan sen pohjalta toteuttaman tietoliikenneverkkoratkaisun käyttöönoton jälkeen asiakas tilaa Noval Networksiltä NetEye-valvontajärjestelmän, jolla asiakkaan tietoliikenneverkko sekä kriittiset palvelimet ja järjestelmät otetaan valvonnan piiriin. Jatkuvaan palvelutasonhallintaan päästään, kun asiakas tekee sopimuksen Noval TopCare -palvelusta ja NetEye-järjestelmän tuloksia pystytään käsittelemään kuukausittaisissa laatu- ja seurantapalavereissa. Näin päästään parhaiten palvelutasonhallintaan oleellisesti liittyvään jatkuvan parantamisen menetelmään.

Palvelut voidaan edelleen jakaa useampiin alakokonaisuuksiin. Noval NetCare pitää sisällään esimerkiksi erilaiset auditoinnit, kilpailutukset, SLA-määrittelyt ja suunnittelutoimeksiannot. Noval NetEye taas on Noval Networksin kehittämä mittausjärjestelmä, jolla voidaan helposti valvoa organisaation omaa tietoliikenneverkkoa, ulkoisia yhteyksiä, palvelimia, palomuureja sekä tulostimia ja muuta kriittistä IT-infrastruktuuria sekä IT-palveluita. NetEye-tuoteperheeseen kuuluu seitsemän tuotetta:

- NetEye Base (perusvalvonta, ylläpitäjän työkalu)
- Business Application Monitor, BAM (kriittisen IT-palvelun päästä-päähän -käytettävyyden seuranta)
- Analyze Engine (protokollatason analysointi ja vasteaikojen mittaus passiivimittauksen keinoin)
- Traffic Engine (toimivuuden ja suorituskyvyn analysointi aktiivimittauksen keinoin)
- Report Engine (määrämuotoinen vakioraportointi)
- Network Device Backup Engine (verkkolaitteiden konfiguraatioiden varmistukset ja hallinta)
- Backup Monitor (varmistusten valvonta)

Lisäksi NetEye-tuoteperheeseen kuuluu www.neteye.fi-palvelusta toteutettavat sähköpostin ja verkkopalvelun valvonta.

Tässä työssä NetEye-palvelin sijoitettiin Salon kaupungin konesaliin. Lisäksi pääterveyskeskukseen vietiin NetEye-probe -mittalaitteita, joiden avulla pystyttiin mittaamaan ja valvomaan aiemmissa kappaleissa kuvattuja palvelunlaatuparametreja. Tarkempi mittauskokoonpano ja asiakkaan ympäristö on kuvattu kappaleessa 6.2.

Noval TopCare-palvelu keskittyy SLM-käytännön mukaisiin toimenpiteisiin. Ennen kaikkea palvelu keskittyy ICT-palveluiden palvelutasonhallintaan ja palveluiden jatkuvaan parantamiseen. Käytännön perustana ovat säännöllisesti pidettävät seuranta- ja kehityspalaverit, joita pidetään yleensä kerran kuukaudessa ja joissa käydään läpi esimerkiksi NetEye-järjestelmän keräämät tiedot, käyttäjien palautteet ja ylläpitäjien huomiot edellisen kuun aikana tapahtuneista poikkeamista ja niiden korjausajoista sekä poikkeamien syistä. Palaverissa sovitaan korjaavista toimenpiteistä, joilla parannetaan IT-palvelun laatua. TopCare-palvelu räätälöidään aina asiakaskohtaisesti ja sovitetaan kulloisenkin asiakkaan tarpeiden mukaiseksi. TopCare-käytäntö muokkautuu kuukausien ja vuosien saatossa jatkuvasti asiakkaan kanssa yhteistyötä tekemällä ja asiakkaan mielipiteitä kuuntelemalla.

6.2 **Asiakasprojekti**

Tässä diplomityössä käsiteltävä projekti keskittyy Salon kaupungin pääterveyskeskuksen WLAN-verkon laatumittauksiin. Laatumittaukset perustuvat käytössä havaittuihin ongelmiin palvelunlaadussa ja käytettävyydessä ja mittausten tarkoituksena onkin paikantaa syyt ongelmien taustalla.

Salon kaupungilla on pääterveyskeskuksessa käytössään TietoEnatorin (nykyinen Tieto) tarjoama Effica-sovellusratkaisu. Effica on käytössä kannettavissa PC:issä ja lääkärit käyttävät sovellusta päivittäin hoivaosastolla suoritettavilla muutaman tunnin mittaisilla lääkärikierroilla WLAN-verkon yli. PC:ihin on kytketty myös EKG- eli sydänfilmilaitteet ja kyseisessä langattomassa käytössä on havaittu ongelmia Effica-sovelluksen käytettävyydessä sekä palvelunlaadussa. Ongelmat ilmenevät WLAN-

verkkoa käytettäessä. Langallisen verkon puolella ei vastaavaa vikaa ole havaittu ollenkaan. Etukäteen arveltiin, että syy ongelmiin lienee tietokantayhteyden katkeaminen Effica-palvelimeen, sillä Effica ei salli katkosta tietoliikenneyhteydessä ja WLAN-verkon ominaisuuksiin kuuluvat lyhyet katkokset varsinkin tukiaseman vaihdon yhteydessä ovat siten todennäköisin syy havaittuihin Effica-ongelmiin. Ongelmien ilmaantuessa Effica-sovellus vaatii kantayhteyden muodostamisen uudelleen toimiakseen jälleen. Effica on asiakkaan liiketoiminnan kannalta kriittinen IT-järjestelmä ja verrattavissa esimerkiksi kriittiseen IP-puheeseen. Mittausten tarkoituksena olikin löytää syyt ilmenneille ongelmille ja kehittää ratkaisu- ja korjausehdotukset kyseisten ongelmien mahdollisimman kattavaksi eliminoimiseksi.

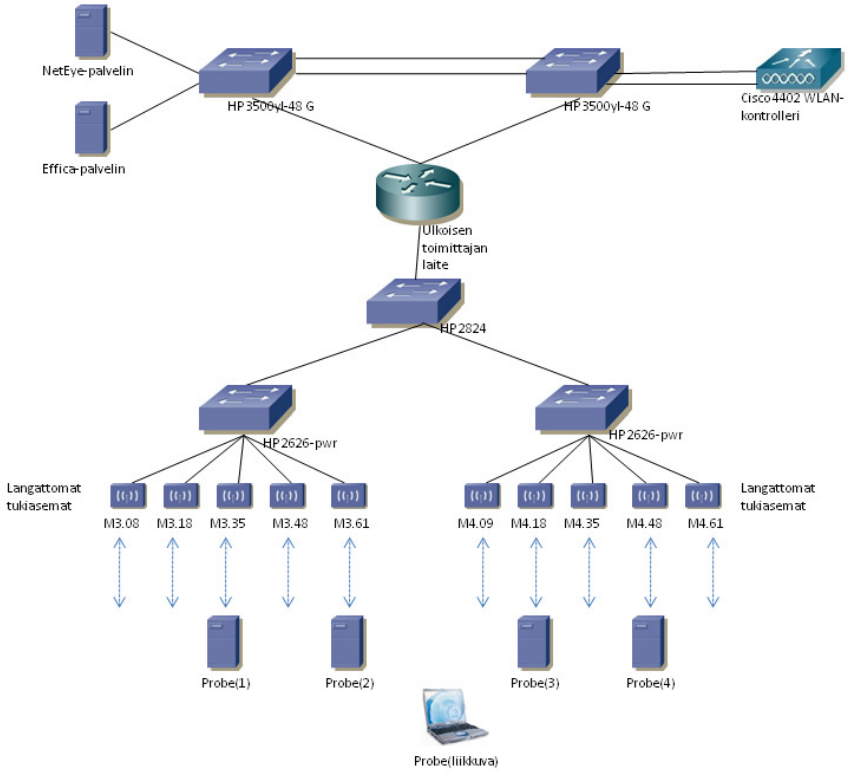
Projekti aloitettiin laatimalla mittaussuunnitelma, jonka pohjalta mittauksia oli tarkoitus toteuttaa. Mittaussuunnitelmaan kuvattiin projektin tausta ja tavoitteet, kuvaus verkkoympäristöstä sekä itse mittauksista ja niiden toteutuksesta. Lisäksi projektin lopuksi asiakkaalle laaditaan mittausprojektin kattava loppuraportti, jossa kuvataan mittausten kulku sekä kehitysehdotukset ongelmien eliminoimiseksi.

6.2.1 Testiympäristö

Mittausten kohteeksi valitulla Salon pääterveysasemalla suoritetaan lääkärikiertoa hoivaosaston kahdessa eri kerroksessa. Asiakas on itse rakentanut verkon ja hoitaa sen ylläpidon. Effican palvelinylläpito on vuokrattu ulkoiselta toimittajalta. Itse verkkoyhteydet ovat toisen ulkopuolisen palveluntarjoajan toimittamia.

Pääterveysaseman liikenne kulkee toisessa asiakkaan toimipisteessä 2 sijaitsevan Ciscon 4402 WLAN-kontrollerin kautta eteenpäin. Seuraavassa kuvassa 12 kuvatun ulkoisen toimittajan laite toimii siltana ja kuljettaa liikenteen läpi sellaisenaan. Kaikki reititys tapahtuu toimipisteen 2 HP 3500 -kytkimillä. Kaikki mittauksiin liittyvät verkkolaitteet ja tukiasemat ovat samassa aliverkossa, jolloin erillisiä palomuuriavauksia ei tarvittu valvontaliikennettä varten.

Alla olevassa kuvassa 12 on kuvattu tarkemmin mittauksiin liittyvä verkkoympäristö. Ulkoisen toimittajan laitteen alapuolinen osio kuvaa pääterveysaseman verkkoa ja yläpuolinen osio fyysisesti Salon kaupungin toimipisteessä 2 sijaitsevaa verkkoa.



Kuva 12. Salon kaupungin verkkoympäristö

WLAN-tukiasemia on kahdessa kerroksessa yhteensä kymmenen kappaletta (viisi molemmissa kerroksissa). Verkkoon on määritelty vain yksi SSID kaikille tukiasemille, joten kun päätelaitteelle on määritelty oikeanlaiset asetukset, pystyy päätelaite liikkumaan verkon alueella ilman, että yhteyttä jouduttaisiin muodostamaan uudestaan tukiasemaa vaihdettaessa. Päätelaite pystyy kuuntelemaan signaalitasoja ja valitsemaan parhaan signaalitason antavan tukiaseman.

Tukiasemat on yhdistetty kahteen HP 2626-kytkimeen (viisi tukiasemaa kumpaankin kytkimeen). HP 2626-kytkimet on puolestaan yhdistetty yhteiseen HP 2824-kytkimeen. Käytössä on lisäksi Cisco 4402 WLAN-kontrolleri (WLAN-kytkin), joka hallinnoi

tukiasemia niin pääterveysaseman kuin toimipisteen 2 tukiasemien osalta. Pääterveysaseman langattomat WLAN-tukiasemat on asennettu tiettyjen huoneiden eteen välikaton alapuolelle. Katvealueita kahden kerroksen tilat kattavassa WLAN-verkossa ei ole tiedossa lainkaan. Kuvassa tukiasemien jälkeen kuvatut Probe-mittalaitteet ovat Noval Networksin mittauksia varten toimittamia laitteita, joihin palataan myöhemmin tarkemmin.

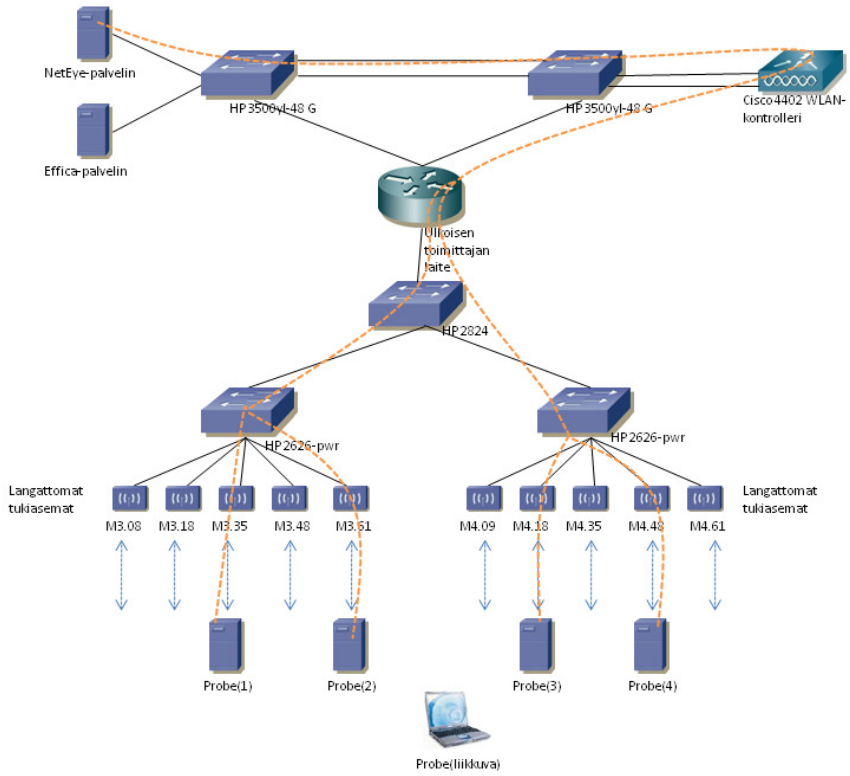
6.2.2 Mittaustopologia

Noin neljä viikkoa kestäneiden mittausten tarkoituksena oli selvittää langattoman lähiverkon laadukkuus ja mahdolliset ongelmakohdat. Mittaustuloksista pystytään analysoimaan viivettä, viiveen vaihtelua sekä pakettihävikkiä ja nähdään osaltaan, miten kriittinen liikenne tulisi kulkemaan verkon läpi. Koska nykyisillä 802.11-standardin tarjoamilla keinoilla ei pystytä saamaan täyttä selvyyttä radiotaajuusspektristä ja esimerkiksi ulkoisista saman taajuusalueen laitteista, käytettiin mittausten apuna Ciscon Spectrum Expert -nimistä tuotetta. Mittaukset aloitettiinkin pääterveysaseman hoivaosastolla toteutettavilla kuuluvuusmittauksilla (SiteSurvey), joissa käytettiin kyseistä Cisco Spectrum Expertiä. Spectrum Expert oli käytössä Noval Networksin kannettavassa tietokoneessa, jonka PCMCIA (Personal Computer Memory Card International Association)-korttipaikkaan oli kytketty Spectrum Expertin käyttämä sensorikortti sekä siihen kytketty ulkoinen antenni. Kannettavan kanssa käveltiin hitaasti pääterveyskeskuksen hoivaosaston tiloissa ja samalla Spectrum Expert tallensi noin sekunnin välein havaitsemansa tiedot signaalitasoista ja taajuusalueella operoivista langattomista laitteista.

Tuotteen avulla selvitettiin pääterveysaseman signaalitasoja mahdollisimman hyvää tukiasemien sijoittelua silmälläpitäen sekä pyrittiin löytämään mahdolliset samalla taajuusalueella toimivat häiritsevät laitteet ja eliminoimaan ne mahdollisuuksien mukaan. Spectrum Expert listaa havaitsemansa langattomat 2.4 GHz – 2.5 GHz taajuusalueella toimivat laitteet ja piirtää myös reaaliaikaista kuvaa esimerkiksi signaalin voimakkuudesta kullakin kanavalla (1-11). Spectrum Expertin tuloksia on käsitelty tarkemmin kappaleessa 7.

SiteSurveyn lisäksi toteutettiin mittauksia Noval Networksin NetEye-verkonvalvontajärjestelmän ja erillisten Probe-mittalaitteiden avulla. NetEye-palvelin asennettiin Salon kaupungin toimipisteeseen 2 samaan paikkaan, jossa Effica-palvelin jo sijaitsee. Näin mittaukset WLAN:n yli Probe-mittalaitteelta NetEye-palvelimelle vastasivat hyvin todellista käyttötilannetta, jossa lääkärit käyttävät Efficaa WLAN:n yli.

Kuvaan 13 on lisätty edellisen kuvan verkkoympäristöön alkuperäinen suunnitelma mittausten kulusta Probe-mittalaitteiden sekä NetEye-palvelimen välillä. Tarkoituksena oli, että lääkärikierrolla käytetään kannettavaa tietokonetta, johon oli etukäteen asennettu Probe-ohjelmisto (Probe(liikkuva)). Tämän lisäksi alkuperäisenä suunnitelmana oli käyttää neljää Probe-mittalaitetta (Probe(1) - Probe(4)) Linksysin WET54G WLAN-siltojen (ei ole piirretty kuvaan, sillä vain ohjaavat liikenteen eteenpäin) kanssa, jolloin Probet olisivat olleet kytketty kyseisiin WLAN-siltoihin, joista taas olisi ollut langaton yhteys tukiasemaan. Tämä siitä syystä, että Probeissa ei ole korttipaikkaa WLAN-kortille. Molempiin kerroksiin oli tarkoituksena sijoittaa kaksi Probea paikalleen mittaamaan verkon laatua Probejen ja NetEye-palvelimen välillä.



Kuva 13. Salon kaupungin verkkoympäristön mittaukset

Mittausten käynnistyksen yhteydessä kohtasimme kuitenkin haasteita Linksysin WLAN-siltojen osalta. Probe-mittalaitteet saatiin kyllä yhteyteen asiakkaan toimipisteen WLAN-tukiasemien kanssa, mutta WLAN-sillat eivät suostuneet pysymään yhteydessä tukiasemaan kuin puolesta minuutista kahteen minuuttiin. Tämän jälkeen yhteys tippui ja silta muodosti yhteyden automaattisesti uudestaan. Mittausten kannalta laitteiden pitäisi kuitenkin ehdottomasti pysyä linjalla jatkuvasti, joten tämä asetti uusia haasteita mittauksia kohtaan.

Tietoturvallisuussyistä tässä työssä ei kuvata tarkemmin asiakkaan langattoman verkon salaus- ja autentikointimenetelmiä. Näistä WLAN-siltojen ongelmat eivät kuitenkaan jääneet kiinni, sillä mittauksia käynnistettäessä kokeiltiin erilaisia salausmenetelmiä sekä erillistä SSID:tä mittalaitteita varten. Laitteet myös saivat yhteyden langattomaan verkkoon muodostettua, mutta jostain syystä silta aina tiputti yhteyden hetken päästä ja aloitti yhteyden muodostuksen uudelleen. Ciscon WLAN-kontrolleri ei omassa

logissaan kertonut tarkkaa syytä siltojen tippumiseen ja toisaalta sillat oli todettu toimiviksi Noval Networksin toimistolla, missä ne pysyivät langattomassa verkossa kiinni yhtäjaksoisesti tutkitun vuorokauden mittaisen ajan. Ongelma lieneekin jonkinlainen Linksys WET54G:n ja Ciscon 4402 WLAN-kontrollerin välinen yhteensopivuusongelma tai mahdollisesti WET54G:n laiteohjelmistoversion ongelmat.

Projektin puitteissa ei ollut kuitenkaan mahdollisuutta lähteä selvittämään asiaa WLAN-kontrollerin tai WLAN-siltojen puolelta enempää. Lääkärikiertoa varten suunniteltu Probe-ohjelmistolla ja WLAN-kortilla varustettu Noval Networksin kannettava tietokone (Probe(liikkuva)) saatiin joka tapauksessa pysymään langattomassa verkossa tasaisesti, joten asiakasta ohjeistettiin ottamaan kyseinen kannettava mukaan seuraaville lääkärikierrolle alkuperäisen suunnitelman mukaisesti. Kannettava oli määritelty asetusten suhteen siten, että lääkärikiertoa suorittavien henkilöiden ei tarvinnut kuin laittaa kannettava päälle ja kirjautua tietyillä tunnuksilla sisään, jolloin Probe-prosessi käynnistyi automaattisesti ilman asiakkaalta erikseen vaadittavia toimenpiteitä. Tällä pyrittiin mahdollisimman pieneen ylimääräiseen häiriöön lääkärikiertoa suorittavien henkilöiden osalta, jotta he pystyivät keskittymään omiin toimiinsa. Kannettavan tietokoneen avulla pystyttiin selvittämään yhteyden toimivuutta liikkeessä lääkärikierron ulottuessa kahdessa hoivaosaston kerroksessa vuorollaan jokaisen tukiaseman alueelle. Kannettava tietokone käytti omaa akkuaan lääkärikierron aikana, sillä liikkuvassa lääkärikierron kärryssä ei ollut erillistä sähkönsyöttöä kannettavaa varten. Lääkärikierron jälkeen kannettava laitettiin latautumaan seuraavaa kierrosta varten.

Kyseisten kierrosten jälkeen kannettava sijoitettiin yhden pääterveysasemalla sijaitsevan WLAN-tukiaseman läheisyyteen toimimaan yhtenä kiinteänä Probe-mittapisteenä. Asiakkaan tiloihin toimitettiin lisäksi vielä toinen Probe-ohjelmistolla varustettu kannettavaa lisää, ja nämä kaksi laitetta toimivat mittauksissa korvaavina Probe-mittalaitteina aiemmin suunniteltujen Probe(1) – Probe(4) sijaan. Kannettavien paikkaa vaihdettiin asiakkaan toimesta muutaman päivän välein, jotta kahden kerroksen tilat

saatiin lopulta katettua mittauksilla kattavasti ja liikenteen kulkua saatiin selvitettyä jokaisen WLAN-tukiaseman kautta.

Mittaustuloksiin alkuperäisestä suunnitelmasta poikenneet muutokset eivät vaikuttaneet millään lailla, sillä Probe-ohjelmistolla varustetut kannettavat mahdollistivat täysin alkuperäisen suunnitelman mukaiset mittaukset ainoana erona se, että nyt laitteita oli vähemmän, jolloin asiakas joutui vaihtamaan niiden paikkaa hieman useammin, jotta mittauksia saatiin tehtyä käyttämällä jokaista kymmentä WLAN-tukiasemaa vuorollaan.

6.2.3 Perusvalvonta

NetEye suorittaa verkon perusvalvontaa ja tarjoaa lisäksi raportointinäkymät tulosten tarkasteluun. Perusvalvonta perustuu SNMP (Simple Network Management Protocol)- ja ICMP (Internet Control Message Protocol)-protokollien käytölle. Lisäksi yhteysvälien laitteilta voidaan kerätä Syslog-viestejä.

SNMP-protokollalla valvotaan yhteysvälien kuormituksia, Syslog-viesteillä nähdään laitteiden tilatiedoissa tapahtuvia muutoksia ja ICMP-viesteillä mitataan verkkolaitteiden päälläoloa. ICMP-ping -kyselyillä pystytään selvittämään jonkin laitteen päälläolo, mutta myös SNMP-kyselyiden avulla pystytään toteamaan aktiivilaitteiden päälläolo. SNMP:llä pystytään lisäksi selvittämään tarkemmin myös laitteiden kuormituksia, virheilyä ja pakettihävikkiä.

Asiakas salli verkon aktiivilaitteissa lukuoikeudet NetEye-palvelimen IP-osoitteesta SNMP-valvonnan mahdollistamiseksi. Laitteiden Syslog-viestit ohjattiin NetEye-palvelimelle, josta ne olivat luettavissa NetEyen Event Monitor -osiosta. Itse tulosten tarkastelu ja mittausten käynnistykset ja muokkaukset pystyttiin hoitamaan etäyhteyden avulla Noval Networksin toimistolta käsin sen jälkeen, kun kaikki mittalaitteet oli konfiguroitu kuntoon ja viety oikeille paikoilleen.

6.2.4 Aktiivimittaukset

Edellä kuvatut verkon perusvalvontamenetelmät ovat oleellisia työvälineitä Probe-mittalaitteiden ja NetEyen välillä suoritettavien aktiivimittausten tukena, kun

analysoidaan verkon laadussa tapahtuvia muutoksia ja rajataan vikojen sijaintia ja aiheuttajaa.

Tässä projektissa tärkeässä roolissa olleet aktiivimittaukset toteutettiin NetEyen Traffic Engine -osion avulla, joka mahdollistaa testiliikenteen luomisen verkkoon ja yhteyden laadukkuuden toteamisen kyseisen testiliikenteen avulla. UDP-testiliikenteen käyttö mittauksissa soveltui hyvin kriittisen liikenteen (tässä tapauksessa Effican käytön, mutta myös esim. VoWLAN:n) laadukkuuden selvittämiseen. Mittauksiin määriteltiin reitinlaatutesti (Route Quality, UDP) sekä optiona toteutettava läpäisykykytesti (Throughput, TCP). Noin kerran sekunnissa lähetettävien UDP-pakettien käyttö reitinlaatutestissä on perusteltua, sillä UDP ei lähetä pudonneita paketteja uudelleen, jolloin tulokseksi saadaan todellinen pakettihävikki ja edestakainen kiertoaikaviive. Testit ovat kevyitä eivätkä kuormita tuotantoliikennettä haittaavasti. Sen sijaan TCP-paketeilla suoritettavat lyhyet läpäisykykytestit, joilla voidaan selvittää maksimaalinen läpäisykyky, pystytään suorittamaan vain yöaikaan suuren hetkellisen kuormituksen takia. Asiakas ei tässä vaiheessa halunnut TCP-läpäisykykytestejä ajettavan ollenkaan suuren kuormituksen vuoksi.

Aktiivimittaukset toteutettiin molempiin suuntiin, eli Probe-mittalaitteilta NetEye-palvelimelle ja päinvastoin. Probe-laitteiden välisiä mittauksia ei tehty.

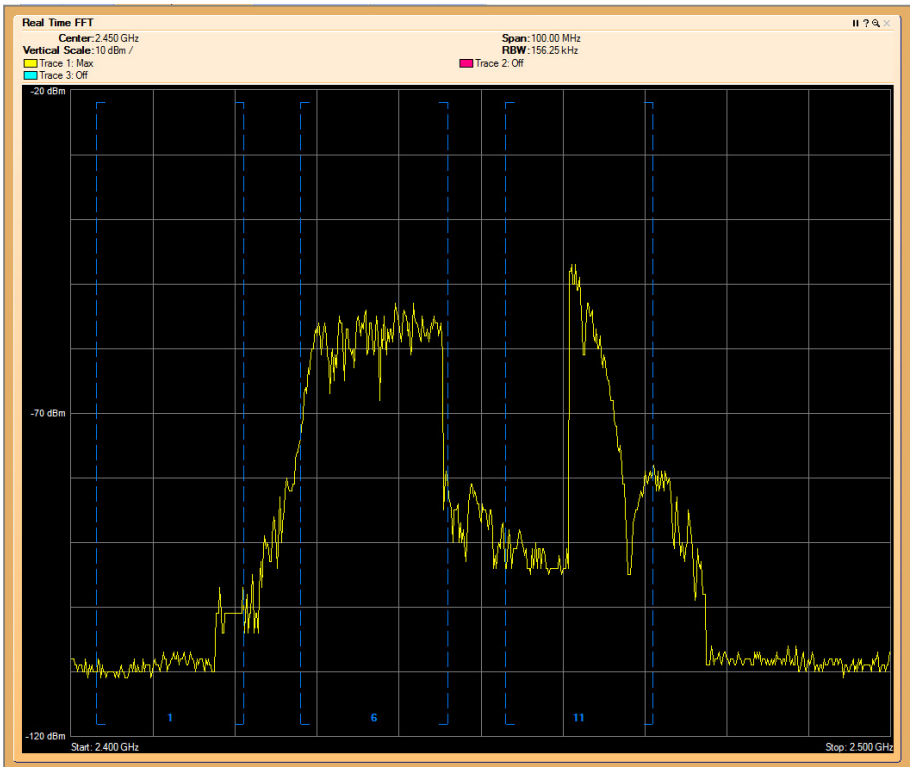
7. Tulokset

7.1 Kuuluvuusaluemittaukset

Kuuluvuusaluemittaukset tehtiin suorittamalla kaksi kierrosta eri päivinä pääterveysaseman tiloissa kahdessa eri kerroksessa. Molemmat kerrokset kuljettiin jalkaisin ympäri ja yhteen kaksi kerrosta käsittävään kierrokseen käytettiin aikaa noin 30 minuuttia. Potilashuoneisiin ei menty, vaan mittaukset toteutettiin käytävillä kävellen hitaasti eteenpäin ja pysähtyen toisinaan noin 30 sekunnin ajaksi paikalleen.

Parhaimmillaan Spectrum Expert löysi kolmannessa kerroksessa yli 20 tukiasemaa samanaikaisesti. Osa kyseisistä tukiasemista on seinien takaa säteileviä toisten tilojen laitteita. Neljännessä kerroksessa tukiasemia havaittiin hieman vähemmän, keskimäärin Spectrum Expert havaitsi siellä noin 10 – 15 tukiasemaa.

Alla olevassa kuvassa 14 on kuvattu Ciscon Spectrum Expertin mittaama reaaliaikainen FFT(Fast Fourier Transform), eli nopea Fourier-muunnos kolmannen kerroksen eteläkäytävältä huoneen 42 lähettyviltä. Kuvassa on x-akselilla kuvattu taajuusalue 2,4 GHz – 2,5 GHz ja y-akselilla radiotaajuusspektrin voimakkuus noin sekunnin mittaisen mittausjakson aikana. Kanavien 1, 6 ja 11 taajuusalueet ovat näkyvillä sinisellä ja muut kanavat menevät näiden suhteen lomittain.



Kuva 14. Cisco Spectrum Expertin FFT-kuvaaja 3. kerroksen eteläkäytävältä

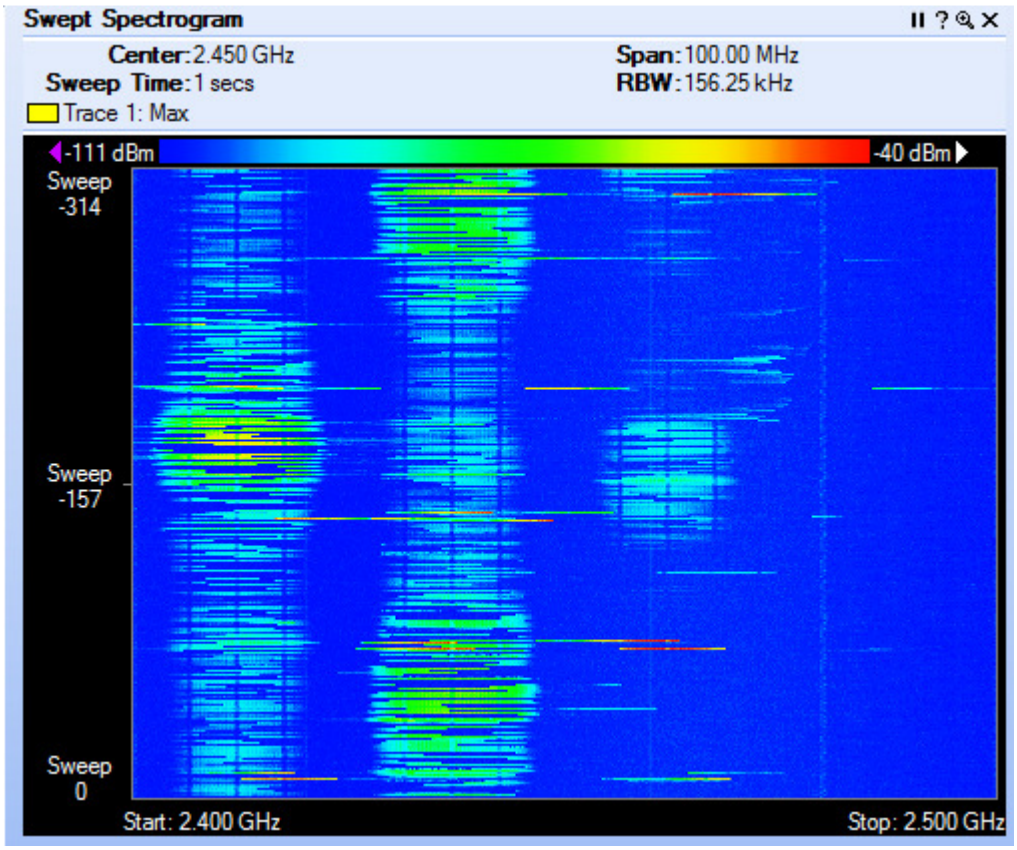
Kuvasta huomataan, että kyseisellä sekunnin mittaisella ajanhetkellä huoneen 42 lähettyvillä vahvin radiotaajuusspektrin voimakkuus on ollut kanavan 6 sekä kanavan 11 ympäristössä. On kuitenkin huomioitavaa, että Spectrum Expertin piirtämä mittausdata päivittyi sekunnin välein, ja radiotaajuusspektrin voimakkuudessa tapahtui suuria vaihteluita jatkuvasti.

Selvemmin signaalin laadukkuutta kuvaakin Spectrum Expertin piirtämä toinen kuvaaja, *Swept Spectrogram*, joka on käytännössä vain erilainen esitystapa aiemmin esitetylle FFT-kuvaajalle. Swept Spectrogram näyttää radiotaajuusspektrin voimakkuuden pidemmällä aikavälillä kuin käytännössä jatkuvasti päivittyvä FFT-kuvaaja. Tällöin yksittäisenä kuvana Swept Spectrogram kertoo totuudenmukaisemman tuloksen spektristä.

Swept Spectrogram -kuvaajassa jokainen horisontaalinen rivi kuvaa radiotaajuus-spektrin voimakkuutta taajuuden funktiona noin sekunnin mittaisen mittausjakson aikana, eli täsmälleen edeltävän FFT-kuvaajan esittämän asian. Koska

radiotaajuussignaalin voimakkuus vaihtelee ajan kuluessa, on Swept Spectrogramissa kuvattu jokainen horisontaalinen ajanhetki eri väreillä. Kuva päivittyy sekunnin välein siten, että alhaalle tulee sekunnin välein uusi horisontaalinen rivi ja ylhäältä poistuu samalla ylin rivi näkyvistä. Yhteen näkymään mahtuu noin 314 sekuntia, eli hieman yli viisi minuuttia dataa. Kuvasta on FFT-kuvaajaa helpompi nähdä signaalin voimakkuuksia ajan kuluessa.

Alla olevassa kuvassa 15 on kuvattu Cisco Spectrum Expertin Swept Spectrogram kolmannen kerroksen pohjoiskäytävältä. Kuvasta huomataan, että kanavien 1 ja 6 taajuusalueiden ympärillä radiotaajuussignaalin voimakkuus on selvästi kanavan 11 taajuusalueen ympäristöä suurempaa.



Kuva 15. Cisco Spectrum Expertin Swept Spectrogam 3.krs pohjoiskäytävältä

Tulosten perusteella vahvin signaalinvoimakkuus kolmannen kerroksen eteläkäytävällä oli kanavan 11 taajuusalueen lähettyvillä. Kerroksen päässä kanavan 6 taajuusalueen ympäristö nousi voimakkuudeltaan kanavan 11 taajuusalueen ohi signaalin voimakkuudessa ja pohjoiskäytävää kuljettaessa kanavien 1 ja 6 voimakkuus oli kanavan 11 aluetta vahvempaa, kuten kuvasta 15 näkyy. Pohjoiskäytävän osalta myös havaittujen tukiasemien määrä tippui verrattuna aiempaan. Kuuluvuutta oli kuitenkin riittävästi edelleen ja aiemmat tukiasemat, joita havaittiin kolmannessa kerroksessa, mutta ei enää neljännessä, olivat seinien takaa säteileviä toisten tilojen laitteita.

Kokeiluluontoisessa testissä hissillä kerrosten kolme ja neljä välillä kuljettaessa tukiasemien määrässä ei tapahtunut merkittävää muutosta, mutta signaalin voimakkuus laski koko taajuusalueella merkittävästi. Neljännessä kerroksessa tilanne oli aika lailla kolmannen kerroksen kaltainen, eli eteläkäytävällä kanavan 11 taajuusalue oli korkein signaalinvoimakkuudeltaan. Kerroksen päädyssä taajuusalueet kanavien 1 ja 6 läheisyydessä olivat voimakkaampia signaalitasoltaan, mutta pohjoiskäytävällä kanavan 11 taajuusalueen ympäristön signaalitaso oli taas vahvin. Kuten edellä on mainittu, havaittujen langattomien tukiasemien määrä oli noin 25 % alempi kuin kolmannessa kerroksessa.

Lisäksi Spectrum Expert -ohjelmaa käytettäessä on mahdollista tarkastella esimerkiksi eri kanavien käyttöasteita, mutta mittausajankohtana langattoman lähiverkon käyttö oli sen verran vähäistä, että erillistä kuvaa ei tässä yhteydessä näytetä.

Kuvaajien lisäksi Ciscon Spectrum Expert listaa havaitsemansa langattomat 2,4 GHz – 2,5 GHz taajuusalueella toimivat laitteet ja päivittää listaa sekunnin välein. Ohjelma kertoo esimerkiksi laitteen fyysisen osoitteen, signaalin voimakkuuden, laitteen käyttämät kanavat ja laitteen päälläoloajan.

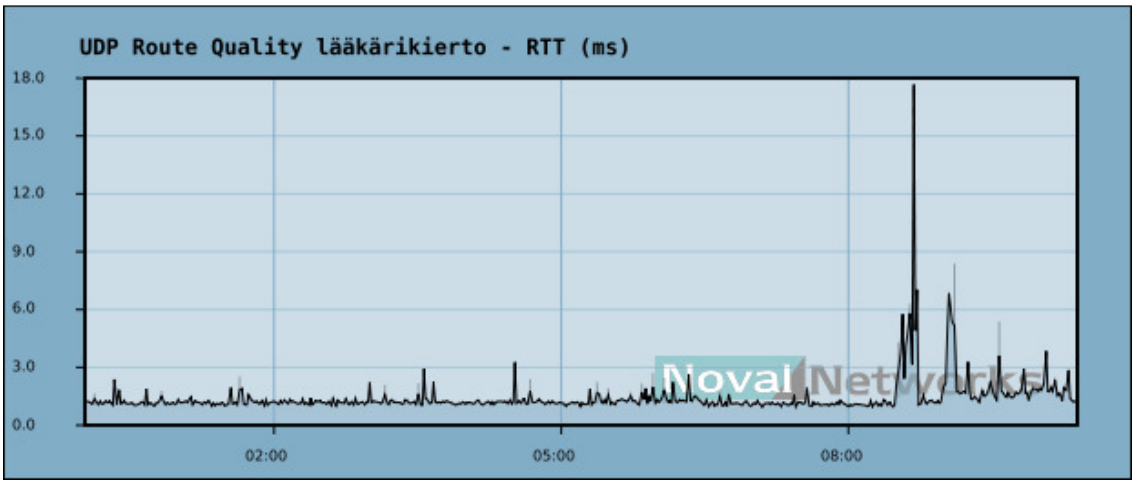
7.2 **Aktiivimittaukset**

NetEyen perusvalvontaan liittyen seurattiin lähinnä verkkolaitteiden päälläoloa ja mahdollisia virhetilanteita. Tärkeämmässä roolissa tässä projektissa olivat kuitenkin aktiivimittaukset NetEyen ja Probe-mittalaitteiden välillä.

Traffic Enginen avulla ja UDP-paketeilla toteutettujen aktiivimittausten tuloksia pystyttiin tarkastelemaan Noval Networksin toimistosta käsin NetEyen keräämien tietojen perusteella.

Esimerkkitapaukseksi on otettu lääkärikiertokannettava ja sen ja NetEyen väliltä kerätty mittausdata keskiviikolta 18.3, koska tulokset kuvaavat hyvin verkon yleistä tilaa ja toimivuutta. Lääkärikiertokannettava oli sijoitettu paikalleen lääkärikiertokärryyn edellisen päivän lääkärikierron päätyttyä. Lääkärikiertokärryä säilytetään paikallaan neljännen kerroksen keskivaiheilla sijaitsevassa kansliassa kierrosten välillä ja samalla kärryssä olevia laitteita pystytään lataamaan yön yli, jotta niiden akut riittävät taas seuraavan päivän lääkärikierron suorittamiseen.

Alla olevissa mittauskuvissa on ensin kuvattu edestakainen kiertoaikaviive NetEye-palvelimen ja lääkärikiertokannettavan välillä kuvassa 16.

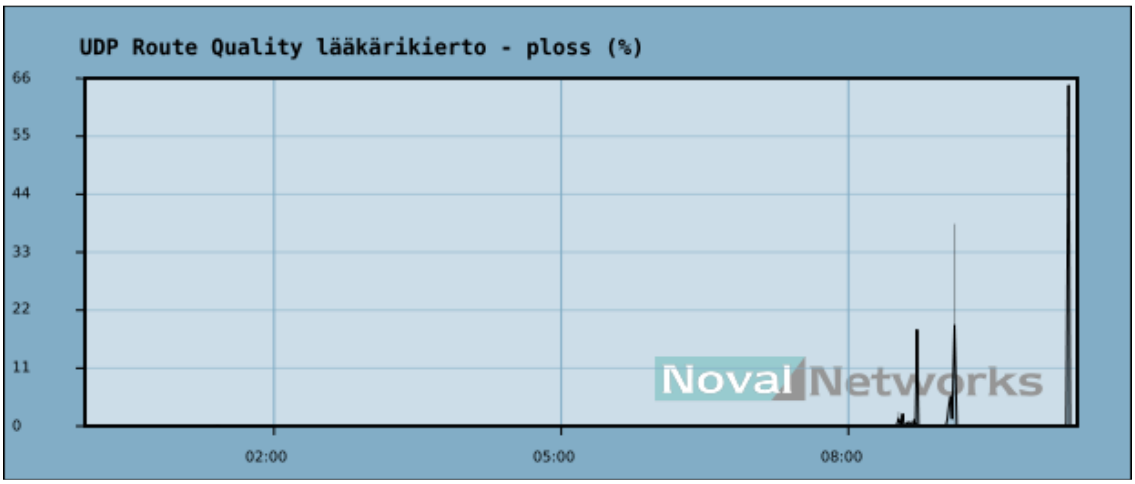


Kuva 16. Edestakainen kiertoaikaviive välillä NetEye – lääkärikiertokannettava – NetEye. Ke 18.3. klo 00:00 – 10:30

Kuvassa näkyy selvästi, että viiveet ovat erittäin pieniä WLAN-verkon yli mitatessa, kun mittalaite on paikallaan kanslian lääkärikiertokärryssä. Lääkärikierto on aloitettu noin klo 8:30 aikoihin, jolloin mittalaite on siis lähtenyt lääkärikiertokärryn mukana liikkeelle. Heti alussa on havaittavissa viiveiden kasvamista ennen kaikkea muutaman yksittäisen piikin osalta. Keskimäärin viive on hieman korkeampaa kuin paikallaan

oltaessa, mutta muutamaa piikkiä lukuun ottamatta viive pysyy kuitenkin vielä erittäin alhaisena.

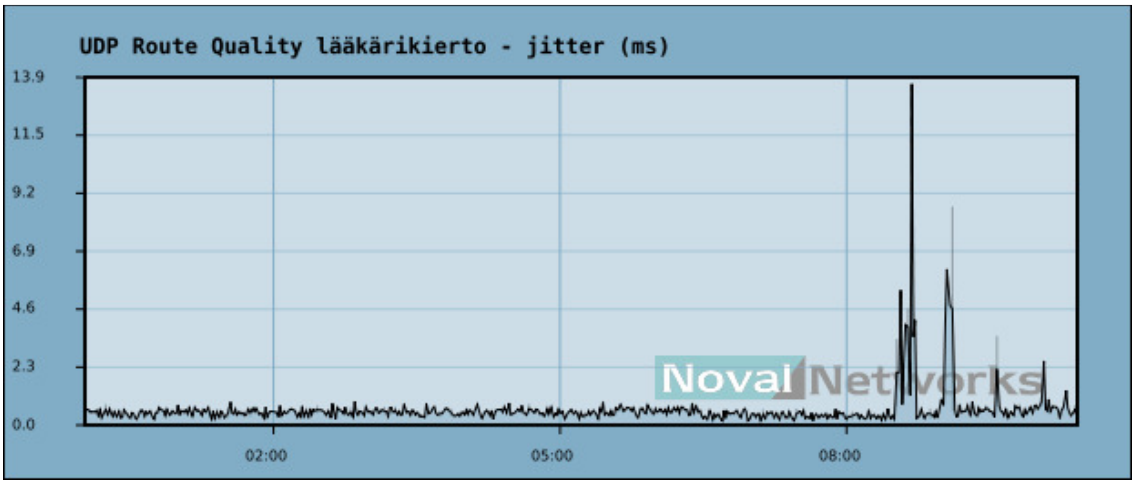
Kuvassa 17 on tarkasteltu samalta aikajaksolta (keskiviikko 18.3 klo 00:00 – 10:30) pakettihävikkiä NetEyen ja lääkärikiertokannettavan välillä.



Kuva 17. Pakettihävikki välillä Neteye - lääkärikiertokannettava. Ke 18.3. klo 00:00 - 10:30

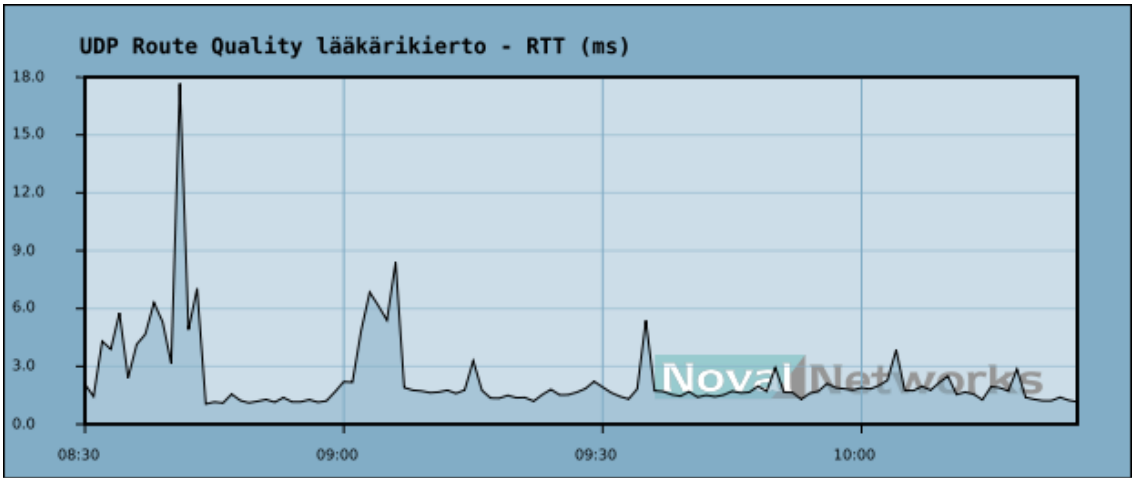
Kuten kuvasta havaitaan, kansliassa yön yli paikallaan oltaessa ei verkossa ilmene pakettihävikkiä ollenkaan. Lääkärikierron ajalta kuvassa näkyy kaksi isompaa piikkiä, jotka ovat voineet aiheutua esimerkiksi tukiaseman vaihtamisesta. Muuten tällöinkään ei pakettihävikkiä liiemmälti ole.

Kuvassa 18 on kuvattu vielä viiveen vaihtelu samalta aikaväliltä. Viiveen vaihtelu noudattelee viiveen kuvaajaa vaihtelun ollessa alle 1 millisekunnin paikallaan pysyttäessä. Liikuttaessa viiveen vaihtelussakin näkyy muutama piikki, mutta yleinen taso pysyy edelleen alle yhdessä millisekunnissa.



Kuva 18. Viiveen vaihtelu välillä NetEye – lääkärikiertokannettava - NetEye. Ke 18.3. klo 00:00 - 10:30

Seuraavassa kuvassa 19 on tarkasteltu vielä tarkemmin viivettä lääkärikierron jo alettua. Aikaväliksi on siis otettu keskiviikko 18.3. klo 08:30 – 10:30.

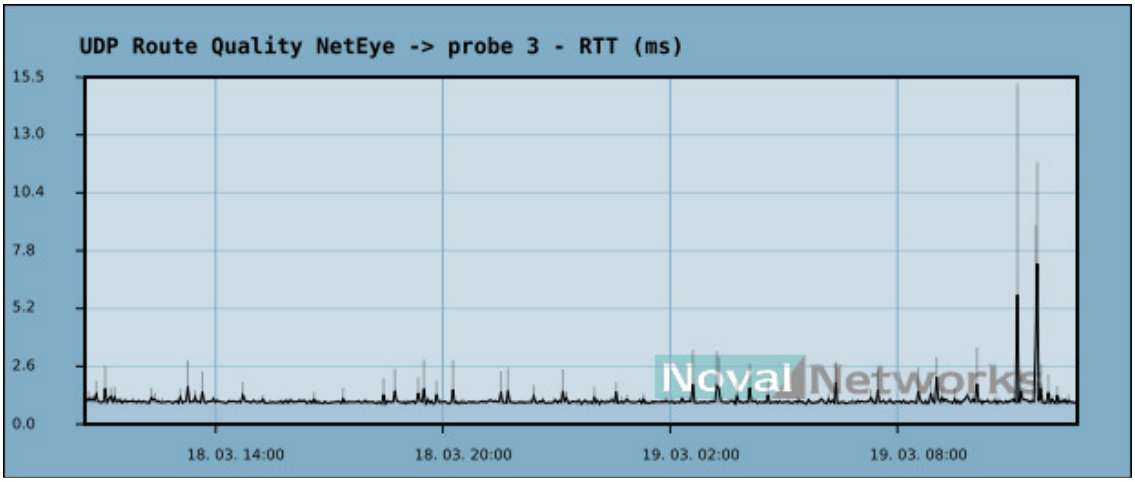


Kuva 19. Edestakainen kiertoaikaviive välillä NetEye - lääkärikiertokannettava - NetEye. Ke 18.3. klo 08:30 - 10:30

Kuten y-akselin arvoista näkee, viive pysyy kierroksella pääasiassa noin kahden millisekunnin paikkeilla suurimman osan ajasta. Lääkärikierron alkupuolella on havaittavissa kaksi viivepiikkiä, joissa viive on ollut 6 millisekunnin luokkaa sekä yksittäinen 18 millisekunnin piikki. Tämän jälkeen viive on pysytellyt hyvin alhaisena koko mittausjakson ajan.

Lääkärikiertokannettavan lisäksi pääterveyskeskuksen hoivaosaston tiloihin asennettiin toinen Noval Networksin kannettava tietokone, johon oli asennettu Probe-mittaohjelmisto sekä määritelty langattoman verkon osalta asetukset kuntoon.

Kyseinen kannettava mittalaite, josta seuraavassa kuvassa 20 käytetään nimeä ”probe 3”, pysyi paikallaan hoivaosaston tiloissa, eli sitä ei otettu lääkärikierroille mukaan. Alla on kuvattu kiertoaikaviive NetEye-palvelimen ja probe 3:n välillä ke 18.3 noin puolesta päivästä torstaihin 19.3 noin puoleen päivään asti.



Kuva 20. Edestakainen kiertoaikaviive NetEye - probe 3 - NetEye. Ke 18.3. klo 11:00 - to 19.3. klo 13:00

Taulukon alin sininen poikkiviiva on 2,6 millisekunnin kohdalla, joten kuvan osoittaman mittausjakson alusta aina torstaiaamupäivään asti viive on ollut todella pientä, noin yhden millisekunnin luokkaa suurimpien piikkien ollessa juuri 2,6 millisekunnin mittaisia. Torstaina aamupäivällä on kaksi korkeampaa piikkiä, mutta näissäkään viive ei ole noussut kuin kaksi yksittäistä kertaa yli kymmenen millisekunnin.

8. Johtopäätökset

8.1 Tulosten analysointi

8.1.1 Kuuluvuusaluemittaukset

Ciscon Spectrum Expertillä tehdyt kuuluvuusaluemittaukset osoittivat, että nykyisellä tukiasemamäärällä (kymmenen kappaletta) saadaan katettua koko kahden kerroksen pääterveysaseman tilat. Tukiasemat on sijoitettu oikeisiin paikkoihin, sillä katvealueita ei löytynyt kummassakaan kerroksessa. Tässä yhteydessä täytyy kuitenkin huomioida, että mittauksia ei ulotettu itse potilashuoneisiin asti. Lääkärikierron aikana lääkärikiertokärry viedään kuitenkin aina myös potilashuoneeseen asti, joten on mahdollista, että huoneissa verkon kantavuus ei ole ainakaan käytävän veroista varsinkin, kun tukiasemat on pääsääntöisesti sijoitettu käytävälle katonrajaan. Toisaalta WLAN-verkko ei kadonnut kokonaan edes hississä kolmannen ja neljännen kerroksen välillä ja seinien takaa havaittiin myös ulkopuolisia WLAN-tukiasemia, joten suurella todennäköisyydellä verkko kattaa mainiosti myös potilashuoneet. Lisäksi WLAN-verkon toimivuutta saatiin tutkittua potilashuoneista asti lääkärikiertokärryyn asennetusta kannettavasta mittalaitteesta käsin suoritettaessa aktiivimittauksia NetEye-palvelimen ja lääkärikiertokannettavan välillä.

Signaalitasot vaihtelivat voimakkuudeltaan kahden kerroksen alueella, mutta tilanne oli pääasiassa se, että mikäli kanavan 11 taajuusalueen signaalinvoimakkuus oli alhainen, oli kanavien 1 ja 6 taajuusalueiden osalta voimakkuus suurempi.

Myöskään häiritseviä ulkoisia laitteita ei havaittu muutamaa satunnaista WLAN:n kanssa samalla taajuudella toimivaa langatonta puhelinta ja kuuloketta lukuun ottamatta. Näiden käyttö on kuitenkin toisaalta välttämätöntä ja toisaalta satunnaista, eikä Spectrum Expert joka tilanteessa edes havainnut kyseisiä laitteita, joten laitteiden eliminointiin tai muihin vastaaviin toimenpiteisiin ei tarvitse missään tapauksessa ryhtyä. Laitteet eivät myöskään aiheuta WLAN-tuotantoliikenteelle merkittävää haittaa laitteiden hyvin pienten liikennemäärien vuoksi.

Kuuluvuusmittaukset toteutettiin kahtena peräkkäisenä viikkona. Aikataulullisesti mittaukset ajoittuivat iltapäivään, jolloin lääkärikierto oli kyseisten päivien osalta jo päättynyt. Kuten olettaa saattaa, WLAN-liikenteen määrä oli hyvin pientä mittausten aikana. WLAN-verkon tärkein päämäärä onkin toimia lääkärikierron aikana mahdollistamassa yhteydet ulkomaailmaan ja esimerkiksi Effican potilastietokantaan.

Kaksi Ciscon Spectrum Expertin tärkeintä tehtävää oli katvealueiden etsintä ja mahdollisten häiritsevien ulkoisten laitteiden etsiminen. Katvealueita ei havaittu ja ulkoisten laitteiden osalta ainoa merkittävä seikka on seinän takaa naapurista säteilevät WLAN-tukiasemat varsinkin kolmannessa kerroksessa. Pääterveyskeskuksen kymmenen omaa tukiasemaa ovat kuitenkin voimakkuudeltaan vahvempia ja hoivaosaston tiloissa käytettävät päätelaitteet pystyvät onnistuneesti muodostamaan yhteyden kyseisiin tukiasemiin. Tämä vaatii kuitenkin luonnollisesti oikeanlaisten salausasetusten käytön ja erillisen sertifikaatin päätelaitteeseen, joten kuka tahansa vierailija ei pääse langattomaan verkkoon ja sitä kautta asiakkaan sisäverkkoon kiinni.

8.1.2 Aktiivimittaukset

Aktiivimittaukset toteutettiin loppujen lopuksi kahdella mittalaitteella, lääkärikiertokannettavalla ja toisella, useamman päivän yhtäjaksoisesti samassa paikassa pidetyllä kannettavalla.

Tuloksista käy yllättävänkin selvästi ilmi, että Salon kaupungin pääterveyskeskuksen hoivaosaston langaton lähiverkko toimii erittäin hyvin. Kuten kappaleen 7 mittaustuloksissa on kuvattu, viiveet ovat erittäin alhaisia ja pakettihävikkiä ei käytännössä ilmene lainkaan varsinkaan paikalla oltaessa.

Sekä lääkärikiertokannettava että toinen mittalaitekannettava vahvistavat mittausten osalta sen, että mittalaitteen pysyessä paikallaan viiveet ovat yhden millisekunnin luokkaa ja liikuttaessakin normaalitaso viiveelle on noin 1,5 - 2 millisekuntia. Liikuttaessa voidaan havaita muutama korkeampi viivepiikki, mutta nämä ja samalla pakettihävikkipiikit johtuvat mitä ilmeisimmin tukiasemavaihdoksista. WLAN-

verkoissa lyhyitä pakettien katoamisia syntyy väistämättä välillä. Tunnistautumista ei tarvitse WLAN-kontrolleria käyttävässä langattomassa lähiverkossa tehdä uudestaan, mutta tukiaseman vaihdosta aiheutuu joka tapauksessa lyhyt katkos, joka näkyy pakettihävikkipiikkinä ja sen johdosta viiveen kasvuna kuvaajissa.

Pienenä ongelmana mittausten osalta voidaan nähdä se, että lääkärikiertokannettava jäi toisinaan käynnistämättä akun loppumisen jälkeen. Tarkoituksena oli, että kannettava kytkettäisiin virtalähteeseen ja se käynnistettäisiin lääkärikierron loputtua ja lääkärikiertokärryn saapuessa kansliaan odottamaan seuraavaa päivää. Kannettava laitettiinkin tässä yhteydessä latautumaan, mutta itse koneen käynnistys jäi lääkäreiltä tosinaan tekemättä, jolloin myöskään mittaustuloksia ei ollut saatavilla siltä osin. Mittauksista saatiin kuitenkin riittävän kattavat myös liikkuvuuden osalta, sillä kannettava oli mukana useammalla lääkärikierrolla.

Salon kaupungin pääterveyskeskuksen WLAN-verkko soveltuu palvelunlaatuparametrien osalta todella hyvin myös kriittiselle liikenteelle. Mikäli verkossa haluttaisiin ottaa käyttöön esimerkiksi VoWLAN-puhelimia, nämä tulisivat toimimaan verkossa hyvin. Myös Effican käytön tulisi onnistua nykyisessä verkossa mainiosti, mutta ongelma lieneekin siinä, että Effica ei mitä ilmeisimmin salli käytännössä minkäänlaista katkosta verkkoyhteydessä.

8.2 Tärkeimmät suositukset

8.2.1 Suositukset Salon kaupungille

Salon kaupunki on panostanut WLAN-verkon keskitettyyn hallintaan ja ottanut jo aiemmin käyttöön Ciscon WLAN-kontrollerin, jolla se hallinnoi keskitetysti kaikkia WLAN-tukiasemia IETF:n määrittelemään LWAPP (LightWeight Access Point Protocol) tekniikkaan perustuen. Tukiasemien paikat on alun perin valittu itse tehdyn SiteSurveyn perusteella, eikä toteutettujen kuuluvuusmittausten perusteella ole tarpeen tehdä muutoksia tukiasemien sijoittelun tai kappalemäärän suhteen.

Mittaustulosten perusteella Salon kaupungin pääterveyskeskuksen toimipisteen langattoman lähiverkon toimivuus on kriittiselle liikenteelle soveltuvaa varsinkin paikalla pysyttäessä. Viiveet olivat tällöin hyvin alhaisia ja pakettihävikkiä ei mittauksissa havaittu ollenkaan. Liikuttaessa viiveet kasvoivat hieman ja mittaustuloksista näkyy myös muutama pakettihävikkipiikki, mutta palvelunlaatuparametrien arvot ovat edelleen todella hyvällä tasolla myös kriittisen liikenteen kuljettamiseksi. Lisäksi langattoman verkon alueella tukiasemaa vaihdettaessa lyhyet katkot ovat kuitenkin ennemmin sääntö kuin poikkeus, eikä niitä nykyisillä järjestelmillä ja laitteilla pystytä täysin estämään.

WLAN-verkoissa toisinaan tapahtuvat pienet katkokset ovat siten syy ongelmiin Effica-järjestelmässä. Lyhyisiin, esimerkiksi tukiasemaa vaihdettaessa tapahtuviin katkoksiin ei WLAN-verkon osalta pystytä vaikuttamaan, vaan on mukauduttava siihen ajatukseen, että WLAN-verkon osalta lyhyitä katkoja tapahtuu toisinaan. Tästä syystä asiakkaan tulisikin käydä ongelmatilannetta jatkossa läpi Effica-ohjelmistotoimittajan kanssa. Ohjelmistotoimittajan tulisi pyrkiä jatkuvan SLM-käytännön mukaisesti parantamaan Effica-tuotteen toimivuutta ja tässä tapauksessa pyrkiä estämään Effican vaatima uusi kirjautuminen lyhyen verkossa tapahtuvan katkon yhteydessä. Asiakkaan tuleekin mainita Toimittajalle langattomaan lähiverkkoonsa tehdystä laatu- ja toimivuusselvityksestä ja kertoa, että itse WLAN-verkon laatu toteuttaa myös kriittisen liikenteen tarpeet ja mahdollistaa myös reaaliaikaisen liikenteen sujuvan toimimisen riippumatta päätelaitteen sijainnista hoivaosaston tiloissa tai kellonajasta, jona liikennettä siirtyy langattoman verkon yli.

Asiakkaan mukaan viime aikoina lääkäreiltä ei kuitenkaan ole tullut aiempaan verrattavissa olevaa määrää vikailmoituksia Effican toimimattomuudesta. Lisäksi Effica kestää asiakkaan mukaan nykyään erittäin lyhyen katkon ja pysyy silti ylhäällä, joten tilannetta tulee seurata ja ohjelmistotoimittajaan olla yhteydessä, mikäli ongelmat edelleen jatkuvat.

8.2.2 Noval Networksin palvelukokonaisuus ja langattomat verkot

Langattomien verkkojen käytön lisääntyessä tulevaisuudessa, täytyy Noval Networksin keskittyä jatkossa yhä enemmän myös langattoman verkon laatumittauksiin tuotteistamalla palvelukonseptiaan tarkemmaksi myös langattoman verkon osalta. Langattoman verkon mittauksista tulisi saada mahdollisimman pitkälle tuotteistettuja siten, että pienin projekti- ja asiakaskohtaisin muutoksin pystytään helposti mittaamaan niin WLAN-verkkoa kuin muitakin langattomia verkkotekniikoita ja ennen kaikkea ulottamaan SLM-käytäntö helposti ja kätevästi myös langattomiin verkkoihin mahdollistamalla esimerkiksi mittausten ja valvonnan toteutus riittävän yksinkertaisesti. Mikäli tämä toteutuu, pystytään jatkossa laatimaan paremmin kattavia SLA-sopimuksia, joissa on huomioitu päästä-päähän laatu myös WLAN-verkon osalta.

Ennen kaikkea Noval Networksissa tulee kiinnittää huomiota langattoman verkon mittalaitteisiin ja miettiä jatkossa, minkälaisella laitteistolla mittauksia on kannattavinta toteuttaa. Noval Networksin langallisessa verkossa käyttämät Probe-mittalaitteet eivät sovellu langattoman verkon mittauksiin sellaisenaan Probe-mittalaitteista puuttuvan WLAN-korttipaikan vuoksi. Tässä yhteydessä tulisikin miettiä, käytetäänkö jatkossakin langallisen verkon puolella nykyisiä Probe-mittalaitteita ja mietitään langattoman verkon puolelle erillinen mittalaite, vai lähdetäänkö miettimään kokonaan uuden mittalaitteen mahdollisuutta, joka pystyisi hoitamaan myös langattoman verkon mittaukset ja jota voitaisiin jatkossa käyttää myös langattoman verkon mittauksissa. Mittalaitteiston tulisi joka tapauksessa olla helposti muokattavissa kulloisenkin asiakkaan verkkoympäristön sekä tarpeiden mukaan. Tässä projektissa toteutetuissa mittauksissa Probe-mittalaitteiden kanssa käytettäväksi suunniteltuja WLAN-siltoja ei saatu kunnolla toimimaan Ciscon WLAN-kontrollerin kanssa ja tilalle otetut kannettavat tietokoneet ovat vain väliaikainen ratkaisu niiden kalliin hinnan ja ison tilantarpeen vuoksi.

8.2.3 Muut suositukset

Ongelmana WLAN-verkkojen laadunvalvonnan suhteen yleisellä tasolla on ollut tähän asti sopivien valvontajärjestelmien puute. Nykyiset laadunhallintajärjestelmät pystyvät valvomaan langallista verkkoa, mutta eivät langatonta. Toisaalta WLAN-kontrollerit

pystyvät kyllä hallitsemaan WLAN-verkkoa, mutta verkon tarjoamasta palvelunlaadusta ei niidenkään avulla saada tietoa. Nyt markkinoille on tullut ennen kaikkea WLAN-verkon laadunhallintaan ja valvontaan erikoistuneita yrityksiä ja tuotteita, joten asiaan on jo kiinnitetty huomiota. Noval Networksin tulee myös edelleen kehittää valvontajärjestelmäänsä, jotta se saa kasvatettua markkina-asemaansa myös langattomien verkkojen valvonnan osalta.

Nykyisissä SLA-sopimuksissa on hyvin harvoin puututtu käytettävyyteen WLAN:n osalta yksinkertaisesti siitä syystä, että WLAN:n osuutta ei ole aiemmin voitu kunnolla edes mitata. Asiakkaan ja toimittajan välisiin palvelutasosopimuksiin tuleekin saada jatkossa kuvattua ja sovittua päästä-päähän -käytettävyydestä myös WLAN-verkon osalta ja palvelun toimittaja tulee sitouttaa valvomaan ja mittaamaan myös WLAN-verkon toimivuutta. Päästä-päähän -käytettävyys on tärkeä varsinkin kriittisen liikenteen tapauksessa. Ylipäätään SLA-sopimuksiin tulee kirjata riittävän tarkasti yhdessä sovitut laatutasot ja toimenpiteet sekä sanktiointimallit poikkeustapauksissa. Nämä edesauttavat kasvattamaan myös toimittajan kiinnostusta ja panostusta langattoman verkon toimintavarmuuden parantamiseen ja tuovat WLAN-verkkojen seuraamisen ja valvonnan osaksi toimittajien arkea.

Ainakin ajatustasolla yksi mielenkiintoinen, mutta erittäin haasteellinen vaihtoehto on yhdistää eri palvelunlaatuparametrit tulevaisuudessa yhdeksi parametriksi, jota olisi huomattavasti helpompi käsitellä ja hallita. Tulevaisuudessa yksi yhteinen palvelunlaatuparametri olisi sovellettavissa käytettäväksi minkä tahansa teknologian kanssa. Haasteena tässä on kuitenkin esimerkiksi se, että kaikki tärkeät palvelutasotavoitteet tulee saada huomioitua. Tulevaisuudessa ollaan joka tapauksessa menossa enemmän ja enemmän siihen suuntaan, että Internetistä tulee enenevissä määrin monipalveluverkko, jossa voidaan käyttää mitä tahansa päätelaitetta ja erilaisia verkkoteknologioita päätelaitteen valitessa aina soveltuvimman tekniikan käytettäväksi. Päätelaitteista on siis tulossa monipuolisempia ja soveltuvampia useiden eri tekniikoiden käyttöön. Myös käyttäjäkeskeisyys ja käyttäjälähtöinen ajattelutapa on vallalla. Siinä käyttäjä valitsee palvelut mielensä mukaan ja palvelut toteuttava

tekniikka on vain taustalla toimiva kokonaisuus, josta palvelun käyttäjän ei tarvitse tietää mitään. Tällöin yksi yhteinen palvelunlaatuparametri mahdollistaisi laaduntarkkailun yksinkertaistamisen ja palvelutasosopimusten selkeyttämisen ja yleisen palvelunlaatukehyksen luomisen.

Operaattoreiden tulee jatkossa miettiä, miten monipalveluverkosta ja käyttäjien personalisoinnista saadaan operaattoreille ja palveluntarjoajille taloudellisesti kannattavampia. Heidän tulee pitää mielessä kolmimallin toteutuminen: Teknisesti mahdollinen, taloudellisesti kannattava ja asiakasta kiinnostava [23]. Palvelunlaatu tulee suunnitella siten, että jokaiselle sovellukselle ei ole määritelty omia laatumääreitä, vaan voidaan käyttää soveltaen yleistä palvelunlaatukehystä kautta koko palvelutasosopimuksen.

9. Tutkimuksen arviointi ja jatkotutkimus

9.1 Tutkimuksen arviointi

Tutkimus pyrki selvittämään palvelunlaadun toteutumista nykyisissä langattomissa lähiverkoissa ja langattomien verkkojen sidottavuutta palvelutasonhallinnan käytäntöihin. Kirjallisuustutkimuksen pohjalta oli tarkoitus todentaa asiakasprojektin mittausten avulla Salon kaupungin langattoman lähiverkon laatua ja soveltuvuutta kriittisen liikenteen välittämiseen.

Tutkimuksessa onnistuttiin toteuttamaan kirjallisuustutkimuksen pohjalta ja laaditun asiakaskohtaisen mittaussuunnitelman avulla asiakasverkon laatumittaukset, joiden tuloksia analysoitiin ja joiden perusteella pohdittiin suosituksia niin Salon kaupungille, Noval Networksille kuin yleisestikin. Itse mittauksissa kohdattiin haasteita mittalaitteiden langattomassa verkossa pysymisen sekä liikkuvan mittalaitteen akun keston suhteen. Lisäksi haasteena oli saada lääkärikiertoa suorittaville lääkäreille iskostettua oikeanlainen toimintatapa Noval Networksin mittalaitteen käsittelyn osalta. Lopulta mittaukset saatiin kuitenkin toteutettua onnistuneesti ja kattavasti tulosten tarjotessa mahdollisuuden verkon toimivuuden analysointiin.

Laatumittausten tulosten perusteella selvitettiin Salon kaupungin langattoman lähiverkon soveltuvuutta Effica-potilastietojärjestelmän käyttöön ja kriittisen liikenteen kuljetukseen. Verkko osoittautui laadullisesti erittäin hyväksi ja sen todettiin soveltuvan nykyisellään laatukriittisen liikenteen kuljetukseen niin viiveiden kuin pakettihävikinkin arvojen osalta. Työn perusteella todettiin, että Salon kaupungin tuleekin jatkossa neuvotella Effica-ohjelmistotoimittajan kanssa sovelluksen kehitysmahdollisuuksista, jotta Effican herkästi tapahtuvaan tietokantayhteyden katkeamiseen saataisiin parannusta. Ohjelmistotoimittajan kanssa keskustellessaan asiakas voi viitata tässä projektissa tehtyihin mittauksiin ja mittaustuloksiin havainnollistaen näin toimittajalle langattoman lähiverkon erittäin hyvän toimivuuden.

Lisäksi diplomityössä selvitettiin kehitysmahdollisuuksia Noval Networksin toimintaan ja palveluihin liittyen sekä pohdittiin SLM-käytännön ulottamista langattomiin lähiverkkoihin asti. Tutkimuksen teoriaosuudessa korostettiin kokonaiskäytettävyyden ja QoE:n, eli käyttäjän kokeman laadun tärkeyttä. Aiemmin lähinnä langallisen verkon puolella mahdollisena ollut kokonaiskäytettävyyden päästä-päähän -mittaaminen tulee jatkossa ulottaa myös WLAN-verkon puolelle, jolloin SLA-sopimuksista saadaan aiempaa kattavampia ja todenmukaisempia. Tämä mahdollistaa tarkkojen palvelutasojen sekä laatuluokitteluiden määrittelyn toimittajan ja asiakkaan välisiin sopimuksiin sekä ennen kaikkea selventää asiakkaalle odotettavissa olevan palvelutason, jolloin asiakkaan odotukset eivät kasva turhan korkeiksi. Samalla toimittaja saadaan käytännössä automaattisesti kiinnostumaan myös QoE:n parantamisesta.

Noval Networksin palvelukokonaisuuden kannalta tärkeää on mittalaitteiston tarkempi määrittely ja yhtenäistäminen siten, että myös langattoman verkon mittaukset saadaan jatkossa toteutettua yhtenäisellä laitteistolla vain pienin asiakas- tai projektikohtaisin muutoksin. Tällöin WLAN-verkon yli ulotettava päästä-päähän -käytettävyyden mittaaminen saadaan tuotteistettua riittävän tarkalla tasolla ja otettua helposti käyttöön asiakasprojektista riippumatta.

Johtuen työhön liittyvä aiheen alati päivittyvästä ja muuttuvasta aihealueesta, työn lähdemateriaali on pitkälti Internetistä haettua, mutta myös lähdekirjallisuutta on pyritty käyttämään ja käymään aktiivisesti läpi työtä tehdessä johtuen painetun kirjallisuuden paremmasta luotettavuudesta ainakin julkaisuhetkellä. Internet-lähteitä on pyritty käymään kriittisesti läpi, mutta on kuitenkin huomioitava, että myös kyseiset lähteet saattavat menettää tietoarvonsa nopeastikin.

Diplomityö täytti asetetut tavoitteet ja työn pohjalta on mahdollista lähteä tekemään jatkotutkimusta.

9.2 Jatkotutkimus

Nopeasti muuttuvalla tietoliikennetekniikan alueella uusia tekniikoita ja standardeja ilmestyy nopeaan tahtiin. Langattomien lähiverkkojen osalta ollaan entistä enemmän

keskittymässä palvelun laadukkaaseen tuottamiseen ja erilaisten sovellusten vaatimien tarpeiden täyttämiseen. Taustana kaikelle tälle on ajatus aiempaa asiakaslähtöisemmästä periaatteesta.

Tämän diplomityön pohjalta voidaan lähteä tutkimaan tarkemmin palvelunlaadun toteutumista esimerkiksi suunnitelluissa neljännen sukupolven matkaviestintäverkoissa, jossa ajatuksena on yhdistää erilaiset langattomat laajakaistaiset verkkoratkaisut yhdeksi kokonaisuudeksi. Palvelunlaadun toteutumista tällaisissa usean eri tekniikan yhdistelmäverkoissa tulee selvittää hyvissä ajoin, sillä kuten tämänkin työn pohjalta on huomattu, jo yhden teknologian palvelunlaadun kunnollinen toteutuminen on suuri haaste. Lisäksi tulevaisuuden verkkoihin ehdottamani yhteinen palvelunlaatuparametri vaatii tarkempaa selvitystä toteuttamiskelpoisuuden osalta ja tarjoaa mielenkiintoisen jatkotutkimuskohteen.

Muita mahdollisia jatkotutkimuskohteita ovat UMA (Unlicensed Mobile Access) ja 802.11u-standardi, jonka on arveltu julkaistavan vuoden 2010 alkupuolella.

10. Viitteet

[1] Macfarlane Ivor & Rudd Colin: The IT Service Management Forum: IT Palvelunhallinta – ITIL Käsikirja. ISBN 0-9551245-2-2.

[2] Kilkki, Kalevi: Quality of Experience in Communications Ecosystem. Journal of Universal Computer Science, vol. 14, no. 5 (2008), s. 615-624. Viitattu 22.9.2008. Saatavilla: http://www.jucs.org/jucs_14_5/quality_of_experience_in/jucs_14_05_0615_0624_kilkki.pdf

[3] Orasaari, Sami: IMS – IP Multimedia Subsystem. Tietotekniikan kandidaatintutkielma (3.4.2006), Jyväskylä: Jyväskylän Yliopisto, Tietotekniikan laitos. 22 s. Viitattu 22.9.2008. Saatavilla: http://www.ad.jyu.fi/palhala/imsfinal.pdf

[4] Karila, Arto. Karila A. & E. Oy: Internet-puhelut (VoIP). Selvitys. Liikenne- ja viestintäministeriön julkaisuja 16/2005. Helsinki: Liikenne- ja viestintäministeriö. 71 s. Viitattu 15.9.2008. Saatavilla: http://www.mintc.fi/fileserver/Julkaisuja%2016_2005.pdf

[5] Petcher, Adam: QoS in Wireless Data Networks. Washington University in St.Louis. Department of Computer Science & Engineering. Esitelmä (27.2.2006 & 1.3.2006) kurssilla CSE574S: Advanced Topics in Networking: Wireless and Mobile Networking (Spring 2006). 18 s. Viitattu 21.5.2008. Saatavilla: http://www.cse.wustl.edu/~jain//cse574-06/ftp/wireless_qos.pdf

[6] Luoma, Marko: S-38.3180: Quality of Service in Internet. Espoo: Teknillinen Korkeakoulu, Networking laboratory. S-38.3180 Quality of Service in Internet: Lecture I: Egress Traffic Processing (8.11.2007). Kurssin luentokalvot. Viitattu 19.6.2008. Saatavilla: http://www.netlab.tkk.fi/opetus/s383180/2007/luentokalvot/L3.pdf

[7] Hicks, Mike: Optimizing Applications on Cisco Networks. Cisco Press. 2004.

[8] Rosen, et. al.: RFC 3031 - Multiprotocol Label Switching Architecture. Internet Engineering Task Force. January 2001. 61 s. Viitattu 5.3.2009. Saatavilla: http://tools.ietf.org/rfc/rfc3031.txt

[9] Hämäläinen Matti & Ristiniemi Jukka: MPLS-verkkoteknologia. Ti5316800 Lähiverkot –erikoistyökurssi. Seminaari, kevät 2006 (28.2.2006). Lappeenranta: Lappeenrannan Teknillinen Yliopisto, Tietotekniikan osasto, Tietoliikennetekniikan laitos. 22 s. Viitattu 4.3.2009. Saatavilla: http://www.it.lut.fi/kurssit/05-06/Ti5316800/seminaarit/MPLS-verkkoteknologia_Matti_Hamalainen_Jukka_Ristiniemi_seminaari.pdf

[10] Braden R, Clark D & Shenker S: RFC 1633: Integrated Services in the Internet Architecture: an Overview. Internet Engineering Task Force. June 1994. 33 s. Viitattu 6.3.2009. Saatavilla: http://www.ietf.org/rfc/rfc1633.txt

[11] Blake, et. al.: RFC 2475: An Architecture for Differentiated Services. Internet Engineering Task Force. December 1998. 36 s. Viitattu 6.3.2009. Saatavilla: http://www.ietf.org/rfc/rfc2475.txt

[12] Kilkki, Kalevi: Differentiated Services for the Internet. Macmillan Technical Publishing, Indianapolis, IN, USA. 1999. Viitattu 5.3.2009. Saatavilla: http://kilkki.net/3

[13] Luoma, Marko: S-38.3180: Quality of Service in Internet. Espoo: Teknillinen Korkeakoulu, Networking laboratory. S-38.3180 Quality of Service in Internet: Lecture I: Quality and/or Differentiation (1.11.2006). Kurssin luentokalvot. Viitattu 21.5.2008. Saatavilla: http://www.netlab.tkk.fi/opetus/s383180/2007/luentokalvot/L1.pdf

[14] Roimola, Taneli: Laajakaistayhteyksien vertailua käyttäjän ja rakennuttajan näkökulmasta. Diplomityö (31.5.2007). Lappeenranta: Lappeenrannan Teknillinen Yliopisto, Digitaalisen viestintätekniikan / Tietotekniikan osasto. 61 s. Viitattu 27.6.2008. Saatavilla: https://oa.doria.fi/bitstream/handle/10024/30327/TMP.objres.730.pdf?sequence=1

[15] WiMAX Forum: IEEE 802.16a Standard and WiMAX Igniting Broadband Wireless Access. 7 s. Viitattu 10.6.2008. Saatavilla: http://admin.npu.ac.th/media/WiMAXWhitepaper.pdf

[16] Binchul Ihm, Ronny Kim & Wookbong Lee: IEEE 802.16m Requirements (12.1.2007). IEEE C802.16m-07/007. Institute of Electrical and Electronics Engineers. 6 s. Viitattu 25.6.2008. Saatavilla: http://www.ieee802.org/16/tgm/contrib/C80216m-07_007.pdf

[17] @450 Langaton laajakaista. Digitan tuottama infosivusto [WWW]. Viitattu 11.7.2008. Saatavilla: http://www.450laajakaista.fi/9023/9046

[18] ITU-T: All about the technology (3G). International Telecommunication Union (14.5.2003). Viitattu 6.3.2009. Saatavilla: http://www.itu.int/osg/spu/ni/3G/technology/index.html

[19] Lehto, Tero: Entistä nopeammat 3g-verkot yleistyvät. Tietokonelehti, Uutiset-osio, artikkeli 14.1.2008. Viitattu 11.7.2008. Saatavilla: http://www.tietokone.fi/uutta/uutinen.asp?news_id=32444

[20] Syrjälä, Marko: WLAN – Langaton lähiverkko. Essee (7.3.2001). Espoo: Teknillinen Korkeakoulu, Tietotekniikan osasto. Viitattu 27.6.2008. Saatavilla: http://users.tkk.fi/~mjsyrjal/wlan.html

[21] Ahvenainen, Marko: Langattomien Lähiverkkojen Turvallisuus. Diplomityö (30.9.2003). Espoo: Teknillinen Korkeakoulu, Sähkö- ja tietoliikennetekniikan osasto. 80 s. Viitattu 27.6.2008. Saatavilla: http://www.netlab.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf

[22] Leskinen, Petri: Suljettu WLAN tietoliikennelaboratorioon. Tutkintotyö (2.5.2007). Tampere: Tampereen Ammattikorkeakoulu, Tietotekniikan koulutusohjelma, Tietoliikennetekniikan suuntautumisvaihtoehto. 38 s. Viitattu 14.7.2008. Saatavilla: https://oa.doria.fi/bitstream/handle/10024/5460/Leskinen.Petri.pdf?sequence=1

[23] Ma Maode, Denko K. Mieso & Zhang Yan: Wireless Quality of Service. CRC Press. 2008.

[24] Vesanen, Ari: Langattomien lähiverkkojen tietoturva. Oulu: Oulun Yliopisto, Tietojenkäsittelytieteiden laitos. Langattoman tietoliikenteen tietoturva, 81540S, kurssin luentomateriaali. Viitattu 14.7.2008. Saatavilla: http://www.tol.oulu.fi/~avesanen/Langaton_TT/20012002/Wlan.html

[25] IEEE: IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (12.6.2007). IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999). Institute of Electrical and Electronics Engineers. 1184 s. Viitattu 17.7.2008. Saatavilla: http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[26] Cisco Systems: Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide (October 2005). Cisco Systems. 208 s. Viitattu 13.10.2008. Saatavilla: http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/wrlsddg.pdf

[27] Nihtilä, Timo: Palvelunlaatu langattomissa tietoliikenneverkoissa. Pro Gradu – tutkielma (3.6.2003). Jyväskylä: Jyväskylän yliopisto, Tietotekniikan laitos.

[28] Open Simulation Architecture: MAC Layer [WWW]. Viitattu 13.10.2008. Saatavilla: http://osa.inria.fr/wiki/Developments/MACLayer

[29] Landweber Lawrence & Murai Jun: Wireless LAN - IEEE802.11: Chapter 27: DCF and PCF. Wisconsin: University of Wisconsin, Introduction to Computer Networks (CS640) -kurssin luentokalvot (10.4.1999). Viitattu 13.10.2008. Saatavilla: www.soi.wide.ad.jp/class/99007/slides/09/27.html

[30] Harihar Dheeraj, Prasad Bora Revoti & Sehrawat Saurabh: Performance Analysis of QoS supported by Enhanced Distributed Channel Access (EDCA) mechanism in IEEE 802.11e. International Association of Engineers, vol 33, issue 1 (13.2.2007): IAENG International Journal of Computer Science, 33:1, IJCS_33_1_6. 6 s. Viitattu 5.8.2008. Saatavilla: http://www.iaeng.org/IJCS/issues_v33/issue_1/IJCS_33_1_6.pdf

[31] Frederic, Merle: WLAN QoS: 802.11e. Tampere: Tampereen Teknillinen Korkeakoulu, Langattomat lähiverkot TLT-6556-kurssin luentokalvot (29.3.2007). Viitattu 6.8.2008. Saatavilla: http://www.cs.tut.fi/kurssit/TLT-6556/Slides/1-802.11e.pdf

[32] Kandala, et. al.: IEEE P802.11 Wireless LANs: Direct Link Protocol Specification, July 2002. 4 s. Viitattu 3.12.2008. Saatavilla: https://mentor.ieee.org/802.11/file/02/11-02-0438-01-000e-direct-link-protocol.doc

[33] Jones, Paul E.: Overview of H.323. Packetizer, April 2007. Viitattu 8.7.2008. Saatavilla: http://hive.packetizer.com/users/packetizer/papers/h323/overview_of_h323.pdf

[34] Ohrtman, Frank: Voice over 802.11, Artech House, Inc. 2004.

[35] Ubiquity Software Corporation: Understanding SIP, 2003. 6 s. Viitattu 10.7.2008. Saatavilla: http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,16/Itemid,75/

[36] Kantola, Raimo: S-38.3115: Signaling protocols. Espoo: Teknillinen Korkeakoulu, Networking laboratory. S-38.3115-kurssin luentokalvot: Session Initiation Protocol (14, 15 & 17.2.2006). Viitattu 10.7.2008. Saatavilla: http://www.netlab.tkk.fi/opetus/s383115/2006/kalvot/lecture13.pdf

[37] Rosenberg, et. al.: RFC 3261: SIP: Session Initiation Protocol. Internet Engineering Task Force. June 2002. 269 s. Viitattu 10.7.2008. Saatavilla: http://www.ietf.org/rfc/rfc3261.txt

[38] Hardy, William C., VoIP Service Quality: Measuring and Evaluating Packet-Switched Voice, McGraw-Hill Networking. 2003.

[39] ITU-T: G.711. Pulse Code Modulation (PCM) of Voice Frequencies, Appendix I: A high quality low-complexity algorithm for packet loss concealment with G.711. International Telecommunication Union – The Telecommunication Standardization Sector. (09/99). 26 s. Viitattu 8.7.2008. Saatavilla: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.711-199909-I!AppI!PDF-E&type=items

[40] Karhula, Tuomas: Langattoman Internet-puhelupalvelun tarjoaminen. Diplomityö (16.11.2007). Lappeenranta: Lappeenrannan Teknillinen Yliopisto, Tietotekniikan osasto, Tietoliikennetekniikan laitos. 90 s. Viitattu 22.9.2008. Saatavilla: https://oa.doria.fi/bitstream/handle/10024/29914/TMP.objres.749.pdf?sequence=1

[41] Ixia: Assessing VoIP Call Quality Using the E-model [WWW]. 2005. 8 s. Viitattu 16.7.2008. Saatavilla: http://www.ixiacom.com/elqNow/elqRedir.htm?ref=http://www.ixiacom.com/pdfs/library/white_papers/voip_quality.pdf

[42] Couto Da Silva, Varela, de Souza e Silva, Leao & Rubino: Quality Assessment of Interactive Voice Applications (15.1.2008). Elsevier, Computer Networks 52 (2008) 1179 – 1192. Viitattu 3.12.2008. Saatavilla: https://www.land.ufrj.br/laboratory/repository/upfiles/article/version-published-ComNet-2008.pdf

[43] Hersent Olivier, Petit Jean-Pierre & Gurle David: IP Telephony: Deploying Voice-over-IP Protocols, John Wiley & Sons, Ltd. 2005.

[44] Hämäläinen, et. al.: TeraBitti: QoS:n toteutus GPRS- ja UMTS-järjestelmissä. Jyväskylä: University of Jyväskylä, Department of Mathematical Information Technology, Telecommunication laboratory (21.11.2001). 43 s. Viitattu 15.7.2008. Saatavilla: http://tisu.it.jyu.fi/terabitti/Documents/QoSUMTS.pdf

[45] WiMAX.com: What Every Company Needs To Know About Mobile WiMAX and QoS [WWW]. Viitattu 25.6.2008. Saatavilla: http://www.wimax.com/commentary/spotlight/what-every-company-needs-to-know-about-mobile-wimax-and-qos

[46] Sipilä, Markku: Communications Technologies, VTT's Research Programme 2002-2006, Final Report. VTT Publications 629. Espoo: VTT. Edita Prima Oy, 2007. 359 s. Viitattu 23.9.2008. Saatavilla: http://www.vtt.fi/inf/pdf/publications/2007/P629.pdf

[47] Alanen, Olli: WiMAX (Worldwide Interoperability for Microwave Access). Jyväskylä: University of Jyväskylä, TIES422 Langattomat järjestelmät -kurssin

luentomateriaalia (8.10.2008). Viitattu 9.6.2008. Saatavilla: http://users.jyu.fi/~arjuvi/opetus/ties422/wimax_2008.ppt

[48] Qualcomm: Flash-OFDM Technology Overview [WWW]. Viitattu 8.8.2008. Saatavilla: http://www.qualcomm.com/products_services/networks/flash-ofdm/overview.html

[49] Geier, Jim: Deploying Voice over Wireless LANs (Networking Technology). Cisco Press. 2007.

[50] Wexler, Joanie, Network World: Dynamic Wi-Fi power can stymie VoIP (5.12.2006). Techworld [WWW]. Viitattu 17.10.2008. Saatavilla: http://www.techworld.com/mobility/features/index.cfm?featureID=2990&pagtype=all

[51] Rosenberg, et. al.: RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Internet Engineering Task Force. March 2003. 47 s. Viitattu 17.10.2008. Saatavilla: http://www.ietf.org/rfc/rfc3489.txt

[52] Chandra Praphul, Lide David: Wi-Fi Telephony: Challenges and Solutions for Voice over WLANs. Paperback. 2006.

[53] Lagace Mathieu, Manshaei Mohammad Hossein & Turletti Thierry: IEEE 802.11 Rate Adaptation: A Practical Approach. 9 s. Viitattu 6.3.2009. Saatavilla: http://www.marlow.dk/tech/madwifi/lacage04.pdf

[54] Miras, Dimitrios: Network QoS Needs of Advanced Internet Applications – A Survey. Internet2 QoS Working Group. November 2002. 67 s. Viitattu 9.6.2008. Saatavilla: http://qos.internet2.edu/wg/apps/fellowship/Docs/Internet2AppsQoSNeeds.pdf

[55] IEEE 802.11: Wireless Local Area Networks. Institute of Electrical and Electronics Engineers [WWW]. Viitattu 6.3.2009. Saatavilla: http://grouper.ieee.org/groups/802/11/

[56] ITU-T: G.107. The E-model, a computational model for use in transmission planning. International Telecommunication Union – The Telecommunication Standardization Sector. (05/2000). 20 s. Viitattu 6.3.2009. Saatavilla: http://eu.sabotage.org/www/ITU/G/G107.doc

[57] Electronista: New 802.11r Wi-Fi standard allows quick roaming (29.8.2008) [WWW]. Viitattu 12.3.2009. Saatavilla: http://www.electronista.com/articles/08/08/29/ieee.approves.802.11r.wifi/

[58] Noval Networks Oy: Yritysesittely [WWW]. Viitattu 25.3.2009. Saatavilla: http://www.novalnetworks.com