



# **3G-YHTEYDET YRITYKSEN PÄÄ- JA VARAYHTEYKSINÄ**

Martti Moskari

Opinnäytetyö  
Huhtikuu 2012  
Tietotekniikka  
Tietoliikennetekniikka ja tie-  
toverkot

TAMPEREEN AMMATTIKORKEAKOULU  
Tampere University of Applied Sciences

## TIIVISTELMÄ

Tampereen ammattikorkeakoulu  
Tietotekniikan koulutusohjelma  
Tietoliikennetekniikka ja tietoverkot

Martti Moskari:  
3G-yhteydet yrityksen pää- ja varayhteyksinä

Opinnäytetyö 51 sivua, josta liitteitä 12 sivua  
Huhtikuu 2012

---

Tämä opinnäytetyö tehtiin Ruovedellä toimivalle Pohjois-Hämeen Puhelin Oy:lle, joka tuottaa asiakkailleen kiinteitä-, mobiili- ja kaapelitelevisioverkkoja hyödyntäviä tehokkaita ja monipuolisia tietoliikennepalveluita. Yhtiö toimii Kuoreveden, Mänttä-Vilppulan, Ruoveden ja Virtain alueella. Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa Mänttä-Vilppulan Vesihuollolle 3G-yhteyksiä ja VPN-tekniikkaa hyödyntävä verkko. Suunnitellun verkon tarkoituksena oli korvata vanhat kiinteällä puhelinyhteydellä toimivat hallintayhteydet 3G-yhteyksillä. Verkon toteuttamiseen käytettiin Ciscon 819 3G-reititintä ja Ciscon ASA 5505 palomuuria.

Tässä opinnäytetyössä käytiin läpi kolmannen sukupolven matkapuhelinjärjestelmän teknisiä perusteita ja tulevaisuuden neljännen sukupolven matkapuhelinjärjestelmien tuomia muutoksia. Työssä keskityttiin erityisesti Euroopassa yleisimmin käytettyyn UMTS-tekniikkaan (Universal Mobile Telecommunications System). Työssä käytiin myös läpi kolmannen ja neljännen sukupolven järjestelmien välisiä nopeuseroja käytännön esimerkkien avulla.

Työn tuloksena saatiin suunniteltua ja toteutettua Mänttä-Vilppulan Vesihuollolle verkko, jonka olisi mahdollista korvata tällä hetkellä käytössä oleva verkko. Uusi 3G-tekniikkaa hyödyntävä verkko mahdollistaisi helpomman vikojen paikallistamisen ja uuden verkon ansiosta verkon ylläpitokustannuksetkin saataisiin pienemmään.

## ABSTRACT

Tampereen ammattikorkeakoulu  
Tampere University of Applied Sciences  
Degree Programme in ICT Engineering  
Telecommunications Engineering and Networks

Martti Moskari:  
3G-connections as companys primary- and back up connections

Bachelor's thesis 51 pages, appendices 12 pages  
April 2012

---

This Bachelor's thesis was made for Pohjois-Hämeen Puhelin Oy, a Ruovesi-based company, which provides mobile and fixed telecommunication services to its customers. The company operates in the areas of Kuorevesi, Mänttä-Vilppula, Ruovesi and Virrat. The goal of this thesis was to design and implement a network for Mänttä-Vilppulan Vesihuolto Oy. The networks main goal was to replace the old fixed land lines with 3G-connections including VPN (Virtual Private Network). The devices that were used in this thesis were Cisco 819 3G-router and Cisco ASA 5505 firewall.

This thesis focuses on the basics of 3<sup>rd</sup> generation UMTS-network (Universal Mobile Telecommunications System) and on the upcoming changes of the 4<sup>th</sup> generation LTE-networks (Long Term Evolution). There is also a practical example of the speeds of 3<sup>rd</sup> generation and 4<sup>th</sup> generation connections in this thesis.

As a result of this thesis, it is now possible for the Mänttä-Vilppula's Vesihuolto to update their old network to the new one which uses 3G-connections. By the use of this new network it is easier to troubleshoot the connections and as a result of this the maintenance costs of the network will go down also.

---

Key words: 3G, UMTS, VPN, HSPA, LTE.

## SISÄLLYS

1	JOHDANTO.....	11
2	3G-TEKNOLOGIA.....	12
2.1	UMTS – kolmannen sukupolven matkapuhelinjärjestelmä.....	12
2.2	UMTS-verkko.....	13
2.3	UTRAN-arkkitehtuuri.....	15
2.3.1	Radorajapinnan tekniikka.....	15
2.4	UMTS-verkon solut.....	16
2.5	UMTS-verkko ja käyttäjä.....	17
2.6	HSPA-standardit.....	18
2.6.1	HSDPA -tekniikka.....	19
2.6.2	HSUPA -tekniikka.....	21
2.6.3	Evolved HSPA -tekniikka.....	23
2.6.4	DC-HSPA –tekniikka.....	24
3	TULEVAISUUDEN TEKNIIKAT.....	25
3.1	LTE-tekniikka.....	25
3.1.1	LTE-järjestelmän tavoitteet.....	25
3.1.2	LTE-verkon arkkitehtuuri.....	26
3.2	3G ja 4G – Nopeudet käytännön testeissä.....	27
4	VESIHUOLLON VERKON TOTEUTTAMINEN.....	31
4.1	Työn lähtökohdat ja tavoitteet.....	31
4.2	Työssä käytetyt laitteet.....	32
4.2.1	Cisco 819 reititin.....	32
4.2.2	Cisco ASA 5505 palomuri.....	33
4.2.3	Schneider Electric AtmosWare iC1000 ala-asema.....	34
4.3	Yleiskuvaus yhteydestä.....	36
5	POHDINTA.....	37
	LÄHTEET.....	38
	LIITTEET.....	39
	Liite 1. Cisco 819 reitittimen konfiguraatiot.....	39
	Liite 2. Cisco ASA 5505 palomuurin konfiguraatiot.....	45

**LYHENTEET JA TERMIT**

3G	(eng. Third Generation). Kolmannen sukupolven matkapuhelinteknologiat.
3GPP	(eng. 3rd Generation Partnership Project). Usean standardointijärjestön yhteistyöorganisaatio, joka pyrkii luomaan kolmannen sukupolven matkapuhelinjärjestelmille eli 3G-järjestelmille maailmanlaajuisia teknisiä määrittelyjä.
CAD	(eng. Computer-aided Design). Tietokoneen käyttöä apuvälineenä etenkin insinöörien ja arkkitehtien harjoittamassa suunnittelutyössä.
CBS	(eng. Cell Broadcast Service) Solukohtaisten levitysviestien käsittely.
CDMA	(eng. Code Division Multiple Access). Koodijakokanavointi. Yksi radiotien kanavanvaraustekniikoista.
CPE	(eng. Customer-Premises Equipment). Kuluttajan omistamat laitteet.
DC-HSDPA	(eng. Dual Carrier High Speed Downlink Packet Access). HSPA:han kehitetty versio, joka käyttää tiedonsiirtoon kahden kantaallon tekniikkaa. Alavirran liikenne.
DC-HSPA	(eng. Dual Carrier High Speed Packet Access). HSPA:han kehitetty versio, joka käyttää tiedonsiirtoon kahden kantaallon tekniikkaa.
DC-HSUPA	(eng. Dual Carrier High Speed Uplink Packet Access). HSPA:han kehitetty versio, joka käyttää tiedonsiirtoon kahden kantaallon tekniikkaa. Ylävirran liikenne.

E-AGCH	(eng. Enhanced – Absolute Grant Channel). Kanava jolla tukiasema säätelee päätelaitteiden käyttämää tehoa.
E-DCH	(eng. Enhanced – Data Channel). HSUPA:n datan siirtoon käyttämä kanava.
E-DPCCH	(eng. Enhanced – Dedicated Control Data Channel). Merkinantokanava, joka kuvaa datakanavalla siirtyvän tiedon ominaisuudet.
E-DPDCH	(eng. Enhanced – Dedicated Physical Data Channel). E-DCH-kanavan käyttämä fyysinen kanava datan siirtoon.
E-RGCH	(eng. Enhanced – Relative Grant Channel). Kanava jolla tukiasema säätelee päätelaitteiden käyttämää tehoa suhteellisesti.
E-UTRA	(eng. Evolved UMTS Terrestrial Radio). LTE-verkon radiorajapinta.
EDGE	(eng. Enhanced Data rates for GSM Evolution). Pakettikytkentäiseen tiedonsiirtoon suunniteltu tekniikka.
ERC	(eng. European Radiocommunications Committee). Vastaa radio- ja televiestinnän asioista. Nykyään osa ECC:tä (Electronic Communications Committee).
ETSI	(eng. European Telecommunications Standards Institute). Riippumaton, voittoa tavoittelematon eurooppalainen telealan standardisointijärjestö. ETSI luo standardeja niin laitevalmistajien kuin verkko-operaattoreidenkin tarpeisiin muun muassa telekommunikaation, mediajakelun sekä lääkinnällisten laitteistojen aloilla.

Evolved HSPA	(eng. Evolved High Speed Packet Access). HSPA-järjestelmän kehittyneempi versio. Tunnetaan myös nimellä HSPA+.
FDD	(eng. Frequency Division Duplex). Taajuuskanavoitu liikenne.
FPLMETS	(eng. Future Public Land Mobile Telephony System). UMTS-projektin ensimmäinen nimi.
GPRS	(eng. General Packet Radio Service). GSM-verkossa toimiva pakettikytkentäinen tiedonsiirtopalvelu.
GSM	(eng. Global System for Mobile Communications). Matkapuhelinjärjestelmä jota käytetään maailmanlaajuisesti.
H-ARQ	(eng. Hybrid – Automatic Repeat Request). Toipuminen, jonka avulla pystytään välttämään langattoman TCP-liikenteen ongelmat.
HS-DSCH	(eng. High Speed – Downlink Shared Channel). HSDPA-tekniikan alavirtaan kulkevan datan siirton tarkoitettu kanava.
HSDPA	(eng. High Speed Downlink Packet Access). Matkaviestinten yhteyskäytäntö, joka nopeuttaa UMTS-pohjaista 3G-matkapuhelinverkkoa. Nopeutus koskee pääasiassa vain liikennettä verkosta päätelaitteelle.
HSPA	(eng. High Speed Packet Access). Matkapuhelinviestintäprotokollien kokoelma, joka laajentaa ja parantaa olemassa olevien UMTS-protokollien suorituskykyä.

HSUPA	(eng. High Speed Uplink Packet Access). Matkaviestinten yhteyskäytäntö, joka nopeuttaa UMTS-pohjaista 3G-matkapuhelinverkkoa. Nopeutus koskee pääasiassa vain liikennettä päätelaitteesta verkkoon.
IC	(eng. Integrated Circuit). Elektroniikan puolijohdekomponentti, johon on integroitu suuri määrä aktiivisia ja usein myös passiivisia elektronisia komponentteja.
IMT-2000	(eng. International Mobile Telecommunications 2000). Projekti, jonka tavoitteena oli laatia suositukset maailmanlaajuisista kolmannen sukupolven matkapuhelinjärjestelmää varten. Tunnettiin aikaisemmin nimellä FPLMTS.
IOS	(eng. Internetwork Operating System). Ciscon laitteiden käyttämä käyttöjärjestelmä.
Ipssec	(eng. IP Security Architecture). joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia Internet-yhteyksien turvaamiseen.
ITU	(eng. International Telecommunications Union). Kansainvälinen televiestintäliitto.
LCS	(eng. LoCation Service). Sijaintipalvelu.
LTE	(eng. Long Term Evolution). Edistynyt 3G-tekniikka josta käytetään myös nimeä 4G.
M2M	(eng. Machine-to-Machine). Teknologia joka mahdollistaa langallisten ja langattomien laitteiden välisen keskustelun.
MIB	(eng. Management Information Base). Virtuaalinen tietokanta, joka hallitsee verkon käyttöä.



MIMO	(eng. Multiple Input Multiple Output). Tekniikka, jossa sekä lähetykseen että vastaanottoon käytetään samanaikaisesti useampaa kuin yhtä antennia.
MSS	(eng. Mobile Satellite Spectrum). Mobiilien satelliittien spektri.
OFDM	(eng. Orthogonal Frequency Division Multiplexing). Eli DMT-modulointi (Discrete Multitone) perustuu tiedon siirtoon lukuisilla toisiaan häiritsemättömillä taajuuskanavilla yhtä aikaa.
QAM	(eng. Quadrature Amplitude Modulation). Modulointitekniikka, joka yhdistää vaihemodulaation ja amplitudimodulaation.
QPSK	(eng. Quadrature Phase Shift Keying). Neljää kanta-aallon vaihetta käyttävä nelivaiheinen vaiheavainnus.
RAN	(eng. Radio Access Network). Tukiasemaohjaimen ja tukiaseman välinen verkko.
RNC	(eng. Radio Network Controller). Tukiasemaohjain.
RNS	(eng. Radio Network Subsystem). Tukiasema alijärjestelmä.
SH	(eng. Soft Handover). CDMA- ja W-CDMA-tekniikkojen ominaisuus, jossa matkapuhelin on samanaikaisesti yhteydessä yli kahteen soluun.
SSL	(eng. Secure Sockets Layer). Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.

TCP	(eng. Transmission Control Protocol). Tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille, joilla on pääsy Internetiin.
TDD	(eng. Time Division Duplex). Aikajakokanavoitu liikenne.
TTI	(eng. Transmission Time Interval). Menetelmä, jonka avulla järjestelmä pystyy reagoimaan nopeammin käyttäjien pyyntöihin ja kapasiteettin varauksiin HSDPA-tekniikassa.
UE	(eng. User Equipment). Mobiililaitteen käyttäjä.
UMTS	(eng. Universal Mobile Telecommunications System). Kolmannen sukupolven matkapuhelinteknologia.
USIM	(eng. Universal Subscriber Identity Module). Käyttäjäkohdainen matkapuhelinliittymän älykortti UMTS-järjestelmässä.
UTRA	(eng. UMTS Terrestrial Radio Access). UMTS-järjestelmän radioverkon pääsy.
UTRAN	(eng. UMTS Terrestrial Radio Access Network). UMTS radioliityntäverkko.
VPN	(eng. Virtual Private Network). Internetin yli muodostettava virtuaalinen yksityinen verkko.
WCDMA	(eng. Wideband Code Division Multiple Access). UMTS-verkossa käytettävä laajakaistainen koodijakokanavointitekniikka.

## 1 JOHDANTO

Kolmannen sukupolven matkapuhelinjärjestelmät ovat alkaneet yleistymään huimaa vauhtia. Monet yrityksetkin ovat alkaneet enemmässä määrin siirtämään verkkojaan kolmannen sukupolven matkapuhelinjärjestelmien varaan. Tämä opinnäytetyö tehdään Ruovedellä toimivalle Pohjois-Hämeen Puhelin Oy:lle, joka tuottaa asiakkailleen kiinteitä-, mobiili- ja kaapelitelevisioverkkoja hyödyntäviä tehokkaita ja monipuolisia tietoliikennepalveluita. Yhtiö toimii Kuoreveden, Mänttä-Vilppulan, Ruoveden ja Virtain alueella.

Tässä opinnäytetyössä käydään läpi kolmannen sukupolven matkapuhelinjärjestelmän tekniikan perusteita ja tulevaisuuden neljännen sukupolven matkapuhelinjärjestelmien tuomia muutoksia.

Työn alussa käydään läpi kolmannen sukupolven UMTS-tekniikan historiaa, teknisiä perusteita ja selvitetään UMTS-verkon rakennetta. Tämän jälkeen käydään läpi tulevaisuuden neljännen sukupolven verkkojen tuomia muutoksia ja tarkastellaan 3G- ja 4G-yhteyksien nopeuksia käytännön testeissä.

Työn lopussa käydään läpi käytännön esimerkin avulla 3G:llä toteutetun verkon toteuttaminen. Kyseinen verkko rakennettiin Mänttä-Vilppulan Vesihuollon käyttöön. Verkon tarkoituksena oli korvata vanhat kiinteät puhelinyhteydet tietoturvaisilla VPN-tunneleita (Virtual Private Network) hyödyntävillä 3G-yhteyksillä.

## 2 3G-TEKNOLOGIA

### 2.1 UMTS – kolmannen sukupolven matkapuhelinjärjestelmä

ITU (International Telecommunications Union) aloitti 1990-luvulla Future Public Land Mobile Telephony System (FPLMTS) nimisen projektin. Myöhemmin projektin nimeksi muutettiin IMT-2000 (International Mobile Telecommunications - 2000). Projektin tavoitteena oli laatia suositukset maailmanlaajuisista kolmannen sukupolven matkapuhelinjärjestelmää varten, ja tavoitteena oli järjestelmä, joka kattaisi koko maapallon samalla laitteella ja samoilla toiminnoilla. Tämän avulla päästäisiin eroon siitä teknologian kirjavuudesta, jonka toisen sukupolven järjestelmät ovat luoneet, ja satelliittien avulla saataisiin samat palvelut käyttöön kaikkialla (Granlund 2001, 202).

Maailmalla käynnistyi monia toisistaan riippumattomia kehityshankkeita. Japani päätyi WCDMA-tekniikkaan (Wideband Code Division Multiple Access) vuonna 1997, ja European Telecommunications Standards Institute (ETSI) päätti omalta osaltaan käytettävästä tekniikasta vuonna 1998. Tällöin ETSI valitsi WCDMA-tekniikan UMTS-verkon radiotien ratkaisuksi. Suositustyö käynnistyi ETSI-yhtymän sisällä, ja vuoden 1999 lopulla perustettiin 3GPP-työryhmä (3rd Generation Partnership Project), jonka tehtäväksi annettiin UMTS-verkon radiorajapinta UTRA:n (UMTS Terrestrial Radio Access) kehittäminen. 3GPP lähti liikkeelle Euroopasta ja siihen ovat liittyneet muun muassa seuraavat standardointiyhteisöt:

- T1P1 Yhdysvalloista
- TTC, ARIB Japanista
- TTA, Koreasta
- ETSI, Euroopasta (Granlund 2001, 203)

## 2.2 UMTS-verkko

ITU:n (International Telecommunications Union) IMT-2000 projektin avulla lähdettiin hakemaan ratkaisuja 3G-matkapuhelinjärjestelmää varten. Järjestelmän käyttöön piti saada kaikki palvelut perinteisestä puhelinliikenteestä multimediaan asti. UMTS-verkon palvelukirjoista voimme poimia muutaman tavoitteen:

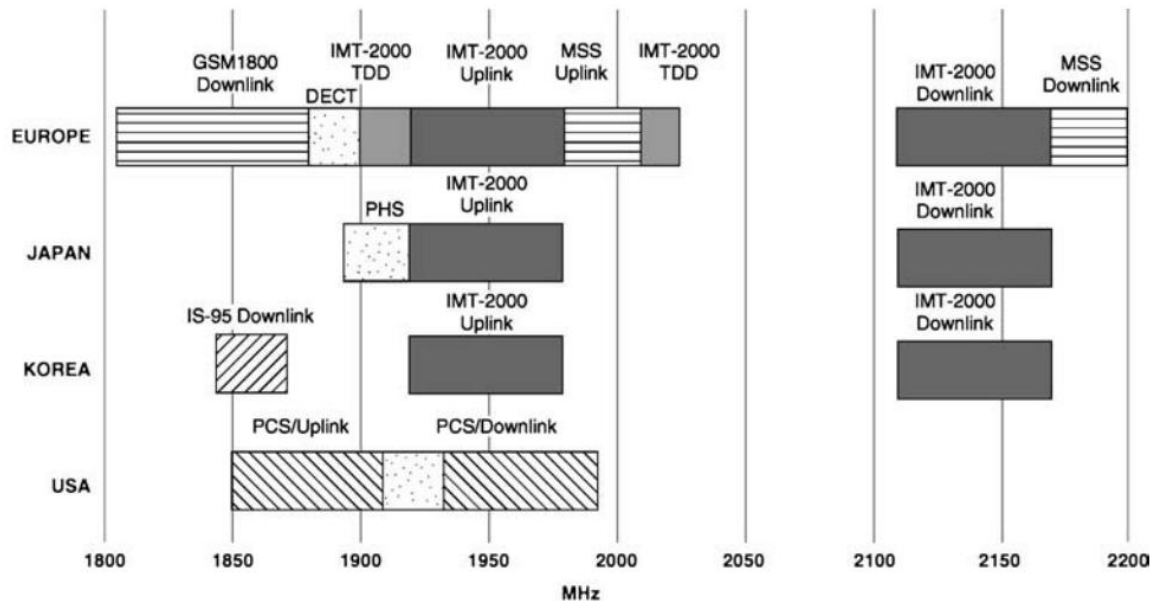
- Äänen laatu samalle tasolle kiinteän verkon kanssa. Tässä on huomattavaa, että kiinteän verkon tasoon ei nykyisessä GSM-verkossa päästä, vaan koodekki on erikoistunut puheäänien välittämiseen.
- Datanopeus liikkuvasta autosta tulisi olla vähintään 144 kbit/s.
- Jalankulkijalle ja paikallaan olevalle käyttäjälle tarjotaan siirtonopeutta 384 kbit/s.
- Paikallaan oleva kiinteä laite voisi käyttää jopa 2 Mbit/s siirtonopeutta pakettikytkentäisellä liikenteellä.
- Tuki sekä piirikytkentäiselle että pakettikytkentäiselle liikenteelle.
- Radiokaistan mahdollisimman tehokas käyttö.

UMTS-käsitteen alle sijoittuu myös Japanissa ja Yhdysvalloissa käytetty CDMA 2000 – tekniikka. Tässä työssä kyseinen tekniikka on jätetty vähemmälle huomiolle (Granlund 2007, 417).

ERC (European Radio communications Committee) hyväksyi kesällä 1997 päätöksen, joka osoittaa UMTS:n maanpäällisille komponenteille seuraavat taajuusalueet:

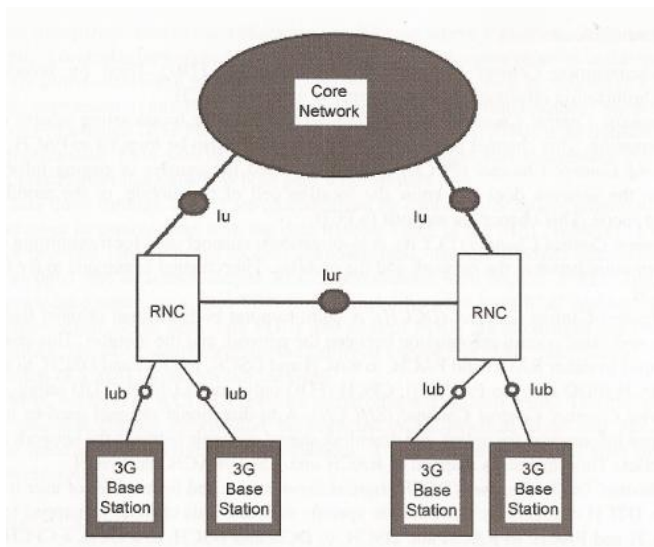
- 1900-1920 MHz, UMTS TDD –tekniikka
- 1920-1980 MHz, UMTS FDD –tekniikka ylävirtaan
- 2010-2020 MHz, lisensseistä vapaat TDD-sovellukset
- 2020-2025 MHz, UMTS TDD –tekniikka
- 2110-2170 MHz, UMTS TDD –tekniikka alavirtaan
- 2170-2200 MHz, satelliittiliikenne

Myöhemmin UMTS-järjestelmään on lisätty myös 900 MHz:n taajuusalue. UMTS-verkon taajuuskanavoidun liikenteen (FDD) käytössä on vajaat 120 MHz, ja aikajako-kanavoidussa liikenteessä (TDD) vajaat 20 MHz (Granlund 2007, 418). Kuvassa 1 on esitetty 2 GHz taajuuskaistan jako Euroopassa, Japanissa, Koreassa ja Yhdysvalloissa. (MSS = Mobile Satellite Spectrum).



KUVA 1. 2 GHz taajuuskaistan jako (Holma, H., Toskala, A. 2004, 34)

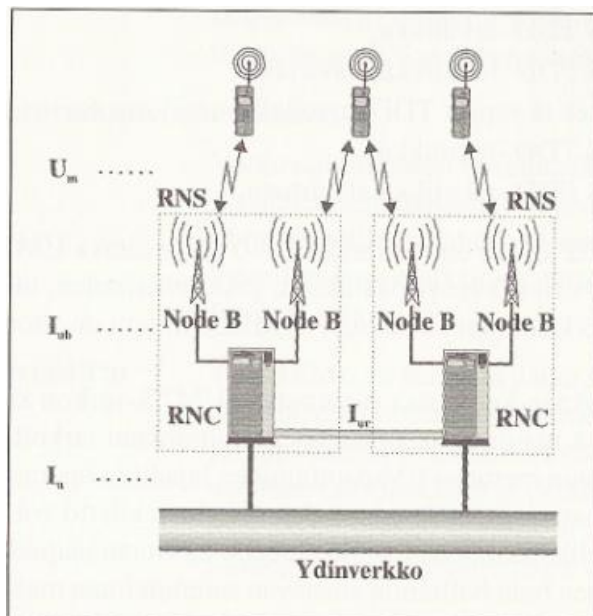
UMTS-verkko koostuu 3G-tekniologiaa käyttävistä tukiasemista (BS), alijärjestelmää ohjaavasta tukiasemaohjaimesta (RNC) ja runkoverkosta (Core Network). RNC:n ja tukiaseman välinen yhteys muodostetaan Iub-rajapinnan välityksellä. Iur-rajapinnan välityksellä muodostetaan yhteys toisiin RNC:hin. RNC:n tehtävänä on kontrolloida 3G-tukiasemien toimintoja. RNC:n ja tukiaseman välistä verkkoa kutsutaan nimellä RAN (Radio Access Network), jota yleensä kutsutaan nimellä UMTS Terrestrial RAN (UTRAN). RNC:n ja runkoverkon välinen yhteys muodostetaan Iu-rajapinnan välityksellä. Kuvassa 2 on esitetty UMTS-verkon rakenne. (Nicopolitidis, P., Obaidat, M. S., Papadimitriou, G. I., Pomportsis, A. S. 2003, 182).



KUVA 2. UMTS-verkon rakenne (Nicopolitidis, P., Obaidat, M. S., Papadimitriou, G. I., Pomportsis, A. S. 2003, 182)

## 2.3 UTRAN-arkkitehtuuri

UMTS-verkon radio-osasta käytetään nimitystä UTRAN (UMTS Terrestrial Radio Access Network). UTRAN osa toteutetaan GSM-ydinverkon päälle. Tähän kytkeytyvät GSM-verkon tukiasema-alijärjestelmää vastaava RNS (Radio Network Subsystem)  $I_{ub}$ -rajapintaa käyttämällä. Alijärjestelmää ohjaa tukiasemaohjain RNC (Radio Network Controller), johon tukiasemat kytkeytyvät  $I_{ub}$ -rajapinnan välityksellä. UTRAN-arkkitehtuurissa tukiasemista käytetään nimitystä Node B. Mobiililaitteen käyttäjää kuvaavat kolme puhelinta, joista käytetään nimitystä UE (User Equipment). Kuvassa 3 on esitetty UTRAN-verkon rakenne (Granlund 2001, 210).



KUVA 3. UTRAN-arkkitehtuuri (Granlund 2001, 210)

### 2.3.1 Radiorajapinnan tekniikka

UMTS-verkossa radiorajapinnan tekniikka perustuu WCDMA-tekniikkaan (Wideband CDMA). WCDMA-tekniikka pohjautuu CDMA-tekniikkaan. CDMA-tekniikka voidaan jakaa kolmeen ryhmään, CDMA (Code Division Multiple Access), WCDMA (Wideband CDMA) ja BCDMA (Broadband CDMA). WCDMA-tekniikkaan perustuvat järjestelmät käyttävät vähintään 5 MHz kaistaa ja BCDMA-tekniikkaan perustuvat taas 8 MHz kaistaa.

WCDMA-tekniikan käyttö tuo mukanaan paljon uusia ominaisuuksia, joita vanhemman sukupolvien järjestelmissä ei ole. Uusista ominaisuuksista voidaan mainita seuraavat:

- Teoreettisesti jopa 2 Mbps bittinopeus.
- Joustava tiedonsiirtokapasiteetti (Bandwidth On Demand)
- Parempi taajuuksien uudelleenkäyttö (Frequency Reuse), koska kaikki saman operaattorin solut käyttävät samoja radiotaajuuksia (Granlund 2001, 211).

UMTS-verkon WCDMA-tekniikassa käytetään nopeutena 3 840 000 lastua/sekunti. Tästä käytetään merkintää 3,84 Mcps (chip per second). Hajautushyöty (Processing Gain) saadaan määriteltyä jakamalla lastunopeus bittinopeudella. Tämä tarkoittaa sitä, että hajautushyöty on suoraan riippuvainen bittinopeudesta – mitä suurempi nopeus, sitä huonompi hajautushyöty. Toisaalta mitä parempi hajautushyöty, sitä paremmin signaali on tunnistettavissa vastaanottajalla. Tästä voidaan tulkita, että 2 Mbps siirtonopeus on mahdollista lähinnä tukiaseman välittömässä läheisyydessä.

Kapeakaistaisen signaalin muuttaminen laajakaistaiseksi WCDMA-tekniikan avulla ei suoraan paranna signaalin laatua, vaan suurin hyöty saadaan paremmasta taajuuksien uusiokäytöstä ja häiriön keskiarvoitumisesta (Granlund 2001, 211).

## 2.4 UMTS-verkon solut

UMTS-verkko on rakenteeltaan hierarkkinen tai monitasoinen, ja se jakautuu moneen eri osaan. Nämä osat ovat kotisolu, pikosolu, mikrosolu, makrosolu ja globaali satelliittijärjestelmä.

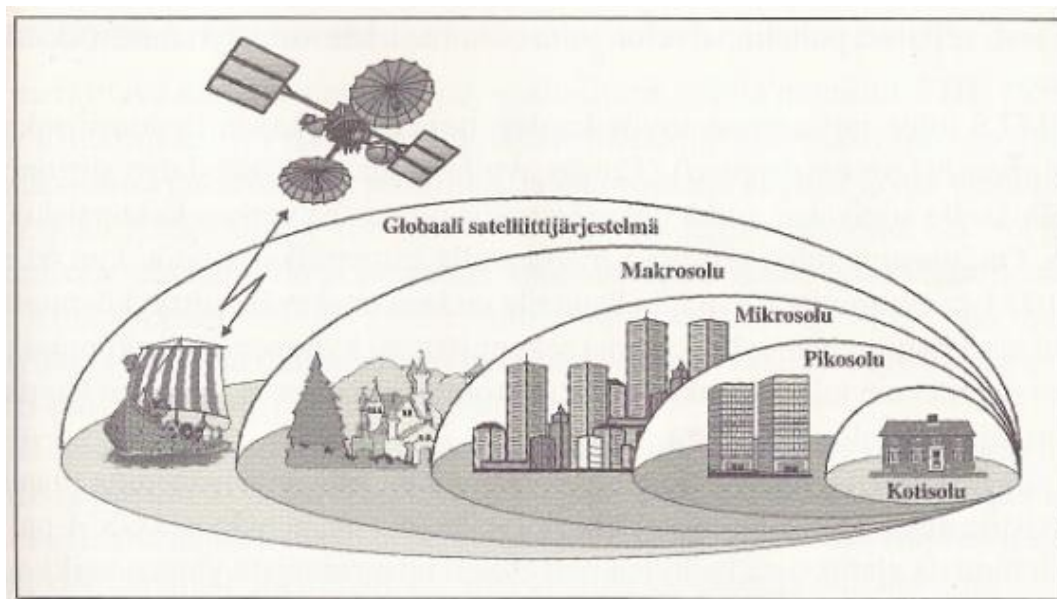
Alinta tasoa UMTS-verkossa edustaa pikosolu, joka yleensä kattaa rakennuksen tai jonkin rakennuksen osan. Pikosolua voidaan verrata langattomaan lähiverkkoon tai Bluetooth-verkkoon. Pikosolun halkaisija on yleensä muutaman kymmenen metrin kokoinen. Hierarkian seuraava taso on mikrosolu, joka kattaa muutaman korttelin kokoisen alueen.

Hierarkian seuraava taso on makrosolu. Makrosolu voi suurimmillaan kattaa jopa tuhansia neliökilometrejä. UMTS-verkon suurista käyttötaajuuksista johtuen tällaisia peittoalueita ei UMTS-verkossa tulla käytännössä saavuttamaan, vaan solukoot ovat huo-



mattavasti pienempiä. WCDMA-tekniikka vaikuttaa myös solujen kokoon, koska GSM-verkossa solujen koko määräytyy taloudellisten ja maantieteellisten seikkojen perusteella, mutta UMTS-verkossa solujen koko määräytyy aktiivisten käyttäjien lukumäärän mukaan.

Hierarkian ylintä tasoa edustaa globaali satelliittijärjestelmä. UMTS-verkko vaatii yläpuolelleen satelliittijärjestelmän täydellisen kattavuusalueen saavuttamiseksi. Satelliiteilla voidaan tavoittaa sellaisia alueita, joihin tavallisten tukiasemien verkot eivät yltä (Granlund 2001, 205). Kuvassa 4 on esitetty UMTS-verkon hierarkia.



KUVA 4. UMTS-verkon hierarkia (Granlund 2001, 205)

## 2.5 UMTS-verkko ja käyttäjä

UMTS-verkossa päätelaitteesta käytetään nimitystä UE (User Equipment). Nimitys laajentaa käytettävän laitteen käyttöaluetta liikkuvasta asemasta tai puhelimesta sellaiseen, joka pystyy liittymään UMTS-verkkoon ottamatta kantaa laitteen muihin ominaisuuksiin tai käyttötapoihin. Suositus ETSI TR 121 904 kuvaa päätelaitteen toiminnot, ja näistä voidaan mainita seuraavat:

- Puheen siirto
- Häätäpuhelut
- Lyhytsanomapalvelu
- Solukohtaisten levitysviestien käsittely (CBS, Cell Broadcast Service)

- Piirikytkentäinen datan siirto
- Pakettikytkentäinen datan siirto
- UMTS-verkon lisäpalveluiden tuki
- Sijaintipalvelut (LCS, LoCation Service)
- GSM-verkon palvelut (Granlund 2007, 419)

UMTS-järjestelmässä SIM-kortista käytetään nimitystä USIM (Universal Subscriber Identity Module). USIM sijoitetaan integroidulle piirille (IC, Integrated Circuit), josta käytetään nimitystä UICC (UMTS IC Card). Teknisesti kyseisen piirin rajapinta perustuu suositukseen ISO 7816, joten kyseessä on sama ratkaisu kuin GSM-maailmassa (Granlund 2007, 419).

USIM-kortti yksilöi käyttäjän ja se pitää olla käytettävässä laitteessa aina, kun laitetta käytetään, poislukien hätäpuhelut. UMTS-laite toimii hyvin pitkälle samalla periaatteella kuin GSM-puhelin. USIM-kortille tallennetaan myös tietoturvaan liittyvät osat, kuten algoritmit ja salausavain K, joka on liittymäkohtainen.

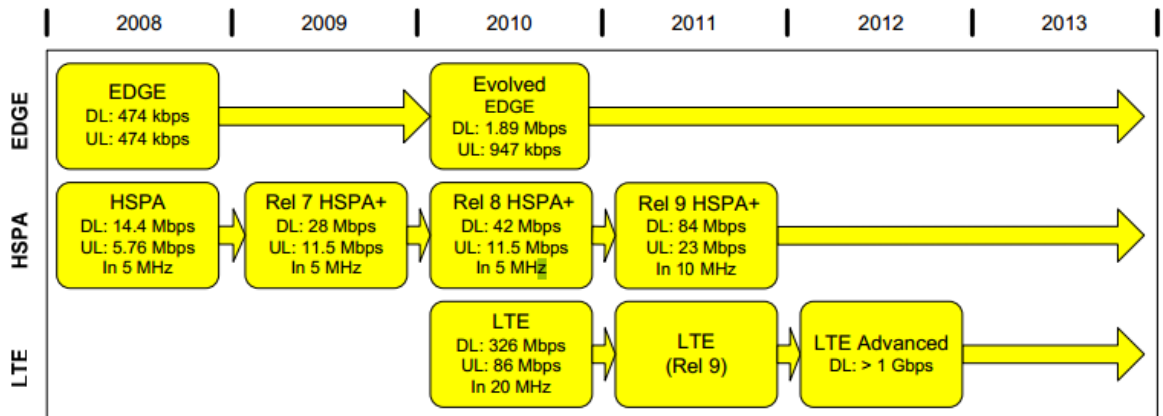
USIM käyttää SIM-kortin tavoin PIN-koodiin perustuvaa autentikointia käyttäjän tunnistamiseksi. PIN-koodin minimipituus on 4 merkkiä ja maksimipituus on 8 merkkiä. PIN-koodi on syötettävä, jotta USIM-kortin palvelut saadaan käyttöön. PIN-koodin lisäksi rinnalla on myös 8 merkkiä pitkä Unblock PIN, jolla voidaan palauttaa toimintaan sellainen USIM-kortti, johon on annettu virheellinen PIN-koodi kolme kertaa. Unblock PIN-koodia käyttäjä ei pysty itse muuttamaan, ja kolme kertaa väärin syötetty Unblock PIN lukitsee USIM-kortin (Granlund 2007, 419).

## **2.6 HSPA-standardit**

HSDPA (High Speed Downlink Packet Access) julkaistiin 3GPP Release 5:n mukana. HSDPA nostaa siirtonopeuksia sekä alavirtaan että ylävirtaan. Alavirtaan kulkevasta tiedosta käytetään nimitystä HSDPA. 3GPP Release 6:n mukana julkaistiin E-DCH (Enhanced – Data Channel), josta käytetään nimitystä HSUPA (High Speed Uplink Packet Access). Yhdessä näistä käytetään nimitystä HSPA (High Speed Packet Access).

HSPA-standardit eivät aiheuta muutoksia olemassa oleviin päätelaitteisiin, vaan laitteiden toiminta perustuu käytettävien kanavien osalta edelleen 3GPP Release 99:n laatiimiin suosituksiin. Uudet päätelaitteet tulevat perustumaan HSPA-tekniikkaan (Granlund 2007, 430).

Kuvassa 5 on esitetty EDGE-, HSPA- ja LTE teknologioiden eri kehitysskeleett sekä tekniikalla saavutettavat tiedonsiirtonopeudet.



KUVA 5. Teknologioiden kehitysskeleett sekä tiedonsiirtonopeudet (HSPA to LTE-Advanced, 2009)

### 2.6.1 HSDPA -tekniikka

HSPA:n mukana tuli radiotielle sekä uusia kuljetuskanavia että uusia fyysisiä kanavia. Seuraavaksi käymme läpi kuljetukanavat ja niihin liittyvät fyysiset kanavat.

HS-DSCH-kanava (High Speed – Downlink Shared Channel) on alavirtaan kulkeva datan siirton tarkoitettu kanava. Kanavan ominaisuudet poikkeavat 3GPP Release 99:n DCH –kanavasta. Seuraavaksi on lueteltu uudet ominaisuudet:

- Kanava on jaettu käyttäjien kesken. Käyttäjien käyttämä data siirtyy samalla aikajakokanavoidulla kanavalla.
- TTI (Transmission Time Interval), joka Release 99:ssä on 10-80 ms, lyhennettiin 2 ms:iin. Tämän avulla järjestelmä pystyy reagoimaan nopeammin käyttäjien pyyntöihin ja kapasiteettin varauksiin.
- Lyhyempi TTI vaatii nopeampaa dataliikenteen ohjausta. Tämän avulla verkko pystyy reagoimaan nopeammin olosuhteiden muutoksiin.

- 2 ms:n aikavälissä voidaan käyttää 15 rinnakkaista kanavaa, jotka levitetään SF-16-hajautusavaimella. Jokainen aikaväli voi siis kuljettaa 2 ms:n aikana 15 eri käyttäjän dataa, tai yhden käyttäjän dataa, joka on hajautettu 15 osaan. Käyttäjä voi siis olosuhteiden salliessa saada käyttöönsä koko siirtotien kapasiteetin.
- Järjestelmään ei sisälly nopeaa tehonsäätöä. Datan sovitus siirtotielle tapahtuu valitsemalla tilanteeseen sopiva modulointi, koodaus ja hajautus.
- Soft Handover –tyyppinen tukiaseman vaihto ei ole mahdollista. Päätelaitte liikkenei vain yhden tukiaseman kanssa.
- Release 99:ssä käytetyn QPSK –tekniikan (Quadrature Phase Shift Keying) sijaan voidaan käyttää 16-QAM-modulaatiota (Quadrature Amplitude Modulation). QPSK käyttää neljää tilaa per symboli, joilla voidaan kuvata 2 bittiä. 16-QAM käyttää 16 tilaa per symboli, jolloin siirrettävien bittien lukumäärä on 4 per symboli. 16-QAM-modulaation on siis kaksi kertaa nopeampi kuin QPSK.
- ARQ-perustaisen H-ARQ toipumisen (Hybrid – Automatic Repeat Request) avulla pystytään välttämään langattoman TCP-liikenteen (Transmission Control Protocol) ongelmat. Negatiivinen ja positiivinen kuittaus palautetaan käyttäjälle 10 ms:n viiveellä viheellisen sanoman saapumisesta.
- Data suojataan käyttämällä turbokoodausta sen tehokkuuden takia. H-ARQ mahdollistaa esilaisten turbokoodien muodostamisen uudelleenlähetyksissä. Tällöin vastaanottaja tallentaa virheellisen sanoman, ja jos myös uudelleenlähetyksessä sisältää virheitä, vastaanottaja voi yhdistää näiden turbokoodien käisttelyn, ja löytää oikean datan (Granlund 2007, 431 – 433).

Taulukossa 1 on luokiteltu HSDPA:n suorituskyky eri luokkiin moduloinnin, koodauksen ja rinnakkaisten kanavien lukumäärän mukaan. Taulukon arvot perustuvat puhtaasti teoreettisiin laskelmiin. Käytännössä siirtonopeudet riippuvat olemassa olevista päätelaitteista, operaattoreiden panostuksista verkkoon sekä radiotien ominaisuuksista.

TAULUKKO 1. HSDPA:n suorituskyky (Granlund 2007, 432)

HS-DSCH-luokka	SF-16 kanavien lukumäärä	TTI-väli	Modulointi	Huippunopeus Mbit/s
Category 1	5	3	QPSK & 16-QAM	1,2
Category 2	5	3	QPSK & 16-QAM	1,2
Category 3	5	2	QPSK & 16-QAM	1,8
Category 4	5	2	QPSK & 16-QAM	1,8
Category 5	5	1	QPSK & 16-QAM	3,6
Category 6	5	1	QPSK & 16-QAM	3,6
Category 7	10	1	QPSK & 16-QAM	7,3
Category 8	10	1	QPSK & 16-QAM	7,3
Category 9	15	1	QPSK & 16-QAM	10,2
Category 10	15	1	QPSK & 16-QAM	14,4
Category 11	5	2	QPSK	0,9
Category 12	5	1	QPSK	1,8

### 2.6.2 HSUPA -tekniikka

3GPP Release 6:n mukana julkaistiin E-DCH (Enhanced – Data Channel), josta käytetään nimitystä HSUPA (High Speed Uplink Packet Access). HSUPA on kehitetty siirtoviiveiden pienentämiseksi ja ylävirran siirtonopeuksien nostamiseksi. HSUPA:ssa tietoliikenteen hallinta on HSDPA:n tavoin tukiaseman tehtävä. HSUPA kuitenkin eroaa HSDPA:sta siten, että HSDPA on vapaa ohjaamaan verkon päätelaitteille siirtyvää dataa, jolloin siirtien kapasiteetti voidaan käyttää statistisen aikajakokanavoinnin periaatteilla.

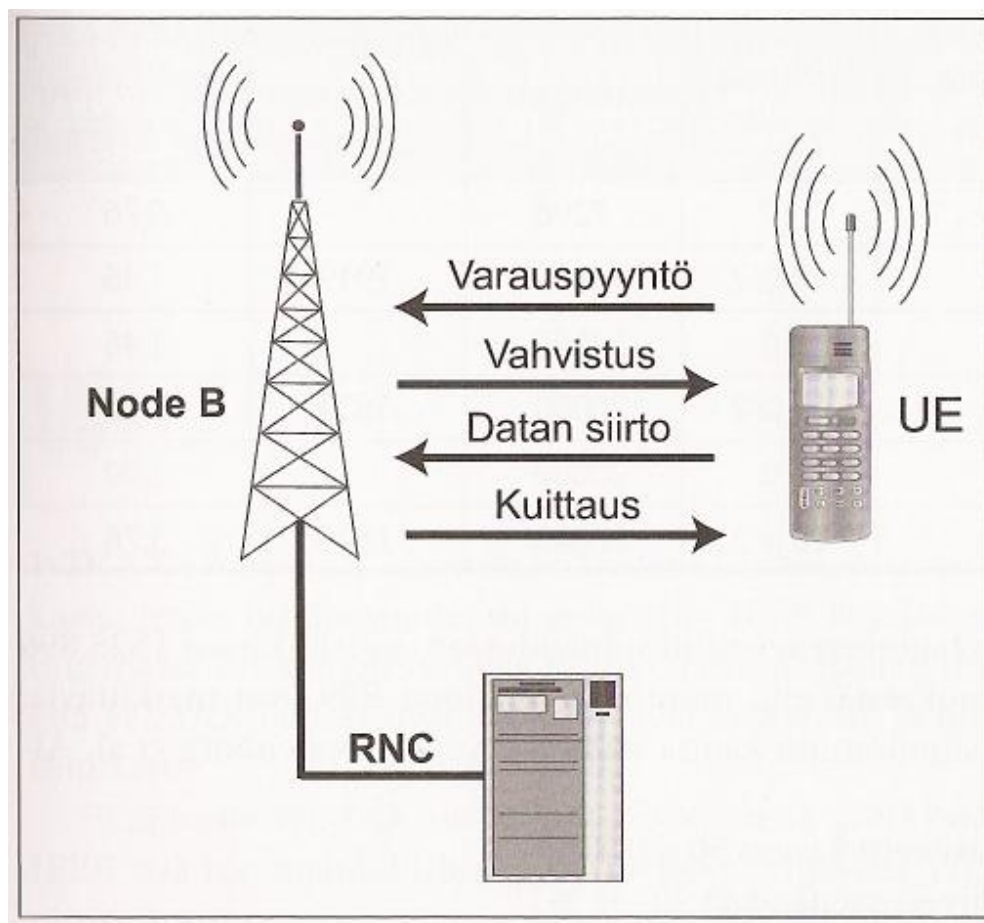
Päätelaitteen kirjautuessa verkkoon, se saa itselleen hajautusavaimen perustuvan onistettun datakanavan, jolla liikennöidään tukiasemalle. Ylävirran tietoliikenne ei siis tarvitse erillisiä kanavanvarausmenettelyjä. Yhteys on siis jatkuvasti käytettävissä Release 99:n mukaisen verkon tavoin.

Tukiaseman tehtävänä on päätelaitteiden tehojen säätäminen ja siirtokapasiteetin jakaminen. Tukiasema voi E-AGCH-kanavalla (Enhanced – Absolute Grant Channel) käs-

keä päätelaitteet käyttämään määrättyä tehoa lähetetyllä viestillä, tai muuttamaan tehojaan suhteellisesti E-RGCH (Enhanced – Relative Grant Channel) lähetetyllä viestillä. Lähtökohtana on, että kaikilla päätelaitteilla on tiedossaan enimmäisnopeus, jolla ne voivat lähettää. Mikäli maksinopeutta ei käytetä kokonaan, päätelaitteiden määrä solun sisällä kasvaa tai solun kokonaiskuorma ylävirtaan kasvaa, voi tukiasema edellämainittuja kanavia käyttäen alentaa päätelaitteiden tehoja (Granlund 2007, 433).

HSUPA käyttää datan siirtoon E-DCH-kuljetuskanavaa (Enhanced – Data Channel). E-DCH-kanavan data puolestaan siirretään fyysisellä E-DPDCH-kanavalla (Enhanced – Dedicated Physical Data Channel). Tämän kanavan kanssa siirretään rinnakkain merkinantokanava E-DPCCH (Enhanced – Dedicated Control Data Channel), joka kuvaa datakanavalla siirtyvän tiedon ominaisuudet (Granlund 2007, 434).

HSUPA:ssa käytetään päätelaitteelle omistettuja kanavia datan siirtoon. Tästä johtuen päätelaitteen on suoritettava tarvitsemiensa resurssien varaus ennen kuin se voi siirtää dataa verkkoon päin. Kuvassa 5 on esitetty HSUPA:n kanavanvaraus.



KUVA 6. HSUPA:n kanavanvaraus (Granlund 2007, 435)

Taulukossa 2 on esitetty HSUPA:n kuusi esi-kategoriaa ja niitä vastaavat suoritusarvot. Siirtonopeudet ovat tekniikan mahdollistamia suurimpia nopeuksia.

TAULUKKO 2. HSUPA:n suorituskyky (Granlund 2007, 436)

E-DCH luokka	E-DCH hajautus-koodien lkm	TTI ms	Bitit/jakso TTI = 10	Bitit/jakso TTI = 2	Siirtonopeus Mbit/s
Category 1	1	10	7296	-	0,76
Category 2	2	10 ja 2	14592	2919	1,46
Category 3	2	10	14592	-	1,46
Category 4	2	10 ja 2	20000	5837	2,92
Category 5	2	10	20000	-	2,00
Category 6	4	10 ja 2	20000	11520	5,76

### 2.6.3 Evolved HSPA -tekniikka

Evolved HSPA-tekniikka (Evolved High Speed Packet Access) tunnetaan myöskin nimellä HSPA+. Evolved HSPA otettiin käyttöön 3GPP:n Release 7:n mukana. Evolved HSPA:n tarkoituksena on parantaa HSPA:n käsittämien HSDPA:n ja HSUPA:n siirtonopeuksia. Evolved HSPA-tekniikkaa aloitettiin kehittämään kasvavan mobiilidataliikenteen tarpeen takia. Nykyään monet ihmiset haluavatkin mobiiliyhteyksiensä olevan yhtä nopeita kuin heidän kiinteät yhteytensä kotona.

Evolved HSPA:ssa on monia uusia ominaisuuksia ja parannuksia HSPA-tekniikkaan nähden. Suurin uudistus Evolved HSPA-tekniikassa on MIMO-tekniikan (Multiple Input Multiple Output) käyttöön ottaminen. MIMO-teknologia mahdollistaa usean lähetys- vastaanottoantennin samanaikaisen käytön. Toisena suurena uudistuksena on korkeamman asteen modulointien käyttäminen. Evolved HSPA-tekniikassa voidaan käyttää 64-QAM-modulaatiota, mikäli signaalitaso on riittävän korkea. 64-QAM-modulaatiota voidaan siis käyttää myös ilman MIMO-tekniikka (Evolved HSPA / HSPA+ 2012).

3GPP on määritellyt muutamia tavoitteita Evolved HSPA-tekniikalle. Tavoitteista tärkeimmiksi voidaan sanoa seuraavat:

- CDMA-tekniikasta (Code Division Multiple Access) tulisi ottaa kaikki hyöty irti ennen kuin siirrytään LTE-teknologian (Long Term Evolution) käyttämään OFDM-tekniikkaan (Orthogonal Frequency Division Multiplexing).
- Saavuttaa sama suorituskky kuin LTE-verkoissa käyttäen 5 MHz:n spektriä.
- Saada Evolved HSPA-tekniikka ja LTE-tekniikka toimimaan yhteen saumattomasti, jotta tekniikasta toiseen siirtyminen olisi mahdollisimman helppoa.
- Käyttää pakettikytkentäistä verkkoa sekä datan että äänen kuljettamiseen
- Yhteensopivuus vanhempien järjestelmien kanssa.
- Taata sama suorituskky vanhoille sekä uusille laitteille.
- Helpottaa siirtymistä vanhemmasta HSPA-tekniikasta Evolved HSPA-tekniikkaan (Ryvasy 2006, 35).

#### **2.6.4 DC-HSPA –tekniikka**

DC-HSPA (Dual Carrier High Speed Packet Access) on HSPA:han kehitetty versio, joka käyttää tiedonsiirtoon kahden kantoaallon tekniikkaa. 3GPP:n Release 8:n mukana otettiin käyttöön DC-HSDPA (Dual Carrier High Speed Downlink Packet Access), joka on kahta kantoaaltoa käyttävä HSDPA-tekniikka. DC-HSDPA:n avulla saavutetaan entistä suurempia tiedonsiirtonopeuksia. Release 9:n mukana tulee myös mahdollisuus käyttää MIMO-tekniikkaa DC-HSDPA:n kanssa. Release 9:ssä aloitettiin hyödyntämään myös DC-HSUPA-tekniikkaa (Dual Carrier High Speed Uplink Packet Access), jonka avulla saadaan nostettua tiedonsiirtonopeuksia ylävirtaan (Dual carrier – DC-HSPA 2012).



## 3 TULEVAISUUDEN TEKNIIKAT

### 3.1 LTE-tekniikka

3GPP Long Term Evolution (LTE) on viimeisin standardi mobiiliverkkojen teknologi-  
oissa. LTE-tekniikan kehitykseen johtivat GSM- , EDGE- ja UMTS-verkkojen eri kehi-  
tysvaiheet. LTE-tekniikan kehityksestä ja teknisistä vaatimuksista vastaa 3rd Generation  
Partnership Project (3GPP) yhteistyössä European Telecommunications Standards Insti-  
tuten kanssa (LTE Encyclopedia 2012).

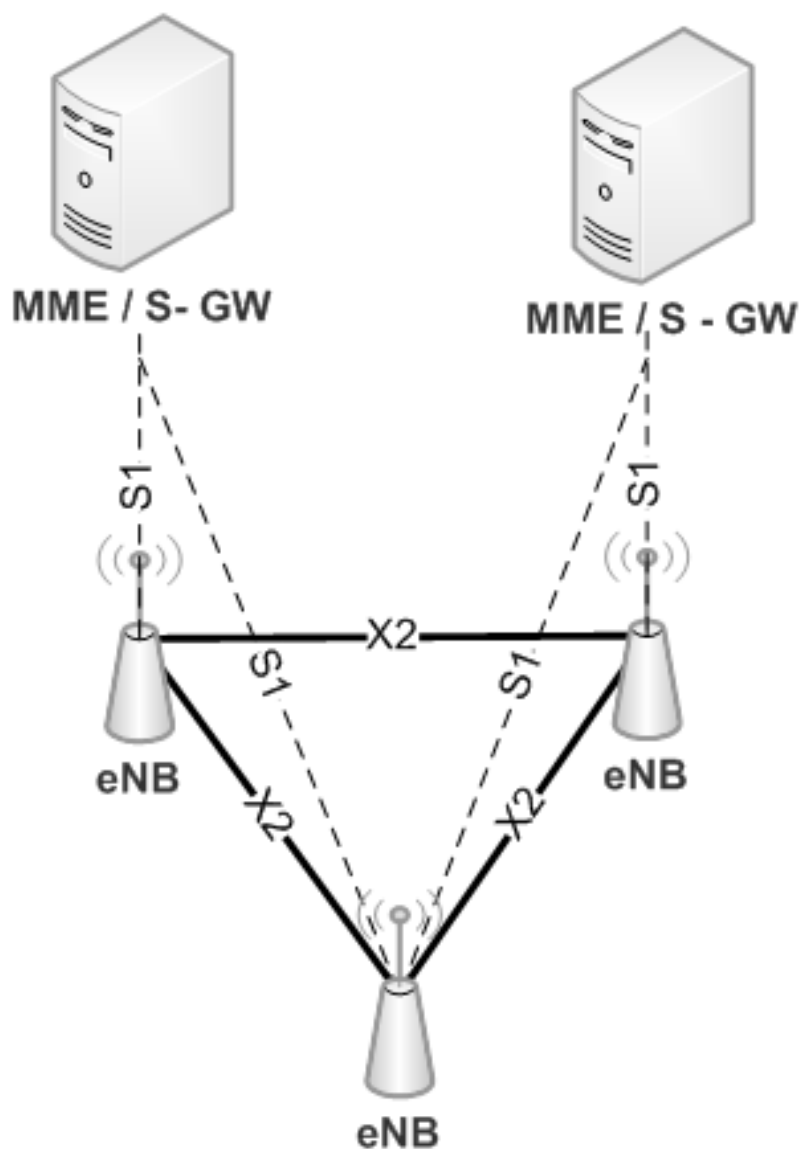
#### 3.1.1 LTE-järjestelmän tavoitteet

Long Term Evolution on seuraava kehitysaskel kolmannen sukupolven verkkojen kehi-  
tyksessä. LTE-tekniikasta käytetään myöskin nimitystä Evolved UMTS Terrestrial Radio  
Access (E-UTRA) sekä Evolved UMTS Terrestrial Radio Access (E-UTRAN). LTE-  
tekniikka tuo mukanaan monia uudistuksia verrattuna vanhempiin kolmannen sukupol-  
ven järjestelmiin. LTE-tekniikan tärkeimmiksi tavoitteiksi voidaan luetella seuraavat:

- Korkeammat tiedonsiirtonopeudet sekä ylävirtaan että alavirtaan. 100 Mbps ala-  
virran liikenteelle. 50 Mbps ylävirran liikenteelle.
- Viiveen pienentäminen.
- Skaalautuva kaistanleveys.
- Tehokkaampi spektrin hyödyntäminen.
- Verkko perustuu kokonaan IP-tekniikkaan.
- Yhteensopivuus vanhempien teknologioiden kanssa.
- Yhteensopivuus monien eri laitteiden kanssa.
- Saavuttaa samat siirtonopeudet kuin kiinteillä yhteyksillä.
- Pienentää operaattoreiden kustannuksia.
- Saavuttaa parempi toimivuus solujen reuna-alueilla.
- Järjestelmän käyttäjäkapasiteetin kasvattaminen (LTE Encyclopedia 2012).

### 3.1.2 LTE-verkon arkkitehtuuri

E-UTRAN käyttää yksinkertaistettua yhden noodin arkkitehtuuria koostuen monesta eNB:stä (E-UTRAN Node B). eNB kommunikoi Evolved Packet Coren (EPC) kanssa käyttäen S1-rajapintaa. S1-rajapinta koostuu MME:stä (Mobile Management Entity) ja UPE:stä (User Plane Entity). UPE:stä käytetään myöskin nimitystä Service Gateway (S-GW). MME ja UPE toteutetaan yleensä yksittäisinä noodeina skaalautuvuuden parantamiseksi. Tukiasemat, eli eNB:t keskustelevat toistensa kanssa käyttäen X2-rajapintaa (LTE Encyclopedia 2012). Kuvassa 7 on esitetty LTE-verkon arkkitehtuuri.

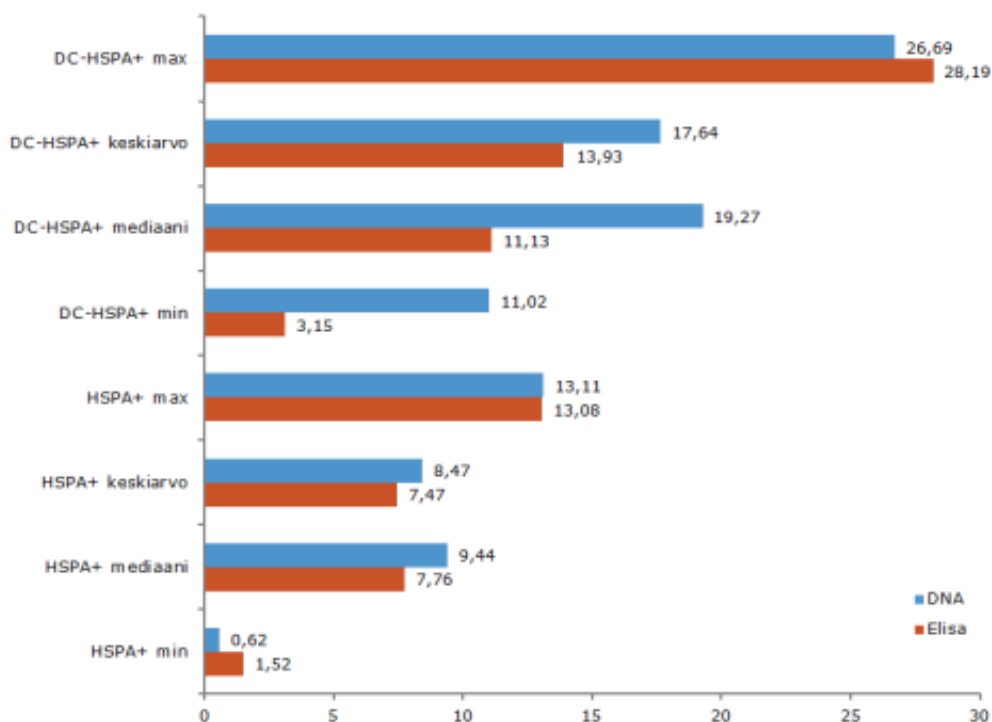


KUVA 7. LTE-verkon arkkitehtuuri (LTE Encyclopedia 2012)

### 3.2 3G ja 4G – Nopeudet käytännön testeissä

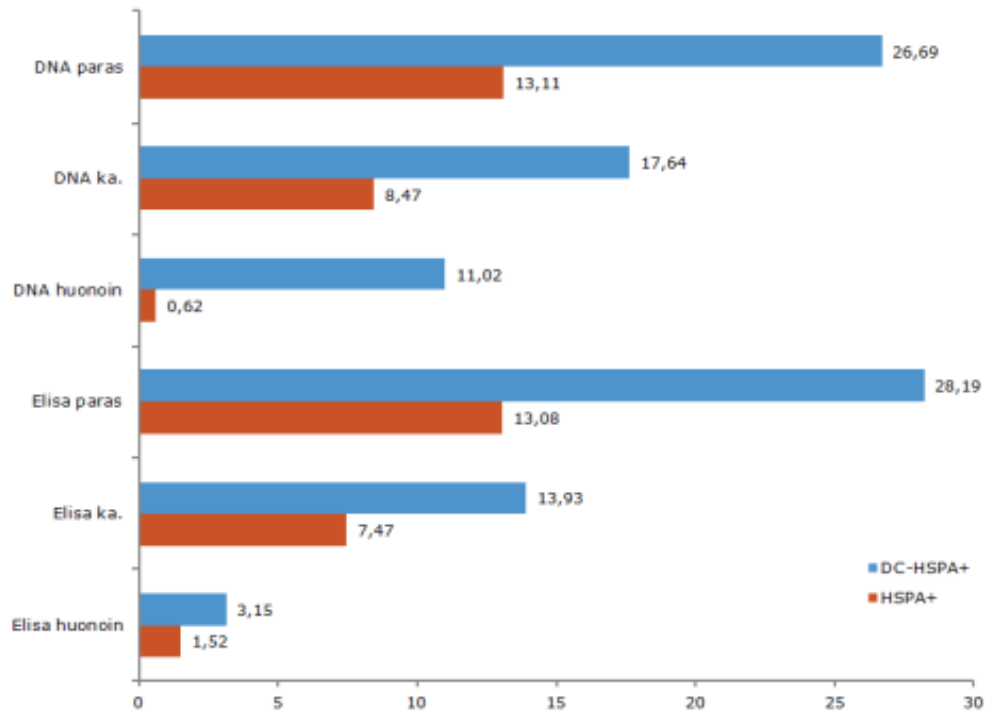
3G- ja 4G-datayhteyksiä testattiin matkamikroon liitetyn nettitikun avulla 12 eri paikkakunnalla yhteensä 32 mittauspisteessä. Mittauspistettä oli valittu kaupunkien keskuksista, lentoasemilta, asuntoalueilta tai urheilukeskuksista, joissa verkkojen voi odottaa tarjoavan parasta yhteyden laatua. Testauspaikkakuntina käytettiin Helsinkiä, Turku, Tampere, Oulua ja Jyväskylää. Kullakin paikkakunnalla käytettiin vähintään neljää mittauspistettä. Lisäksi mittauksia tehtiin Lappeenrannassa, Jämsässä, Hyvinkäällä, Kouvolassa ja Lahdessa. Siirtonopeudet mitattiin käyttäen Speedtest.net-palvelua. Testattavina olivat valtakunnalliset operaattorit DNA, Elisa ja Sonera. Mittaukset suoritti Tietokone-lehden toimitus (Tietokone 2012).

Ensimmäisessä mittauksessa tutkittiin eri operaattoreiden 3G-tekniikoiden nopeuksia. Kuviossa 1 on esitetty Elisan ja DNA:n eri 3G-tekniikoiden nopeudet.



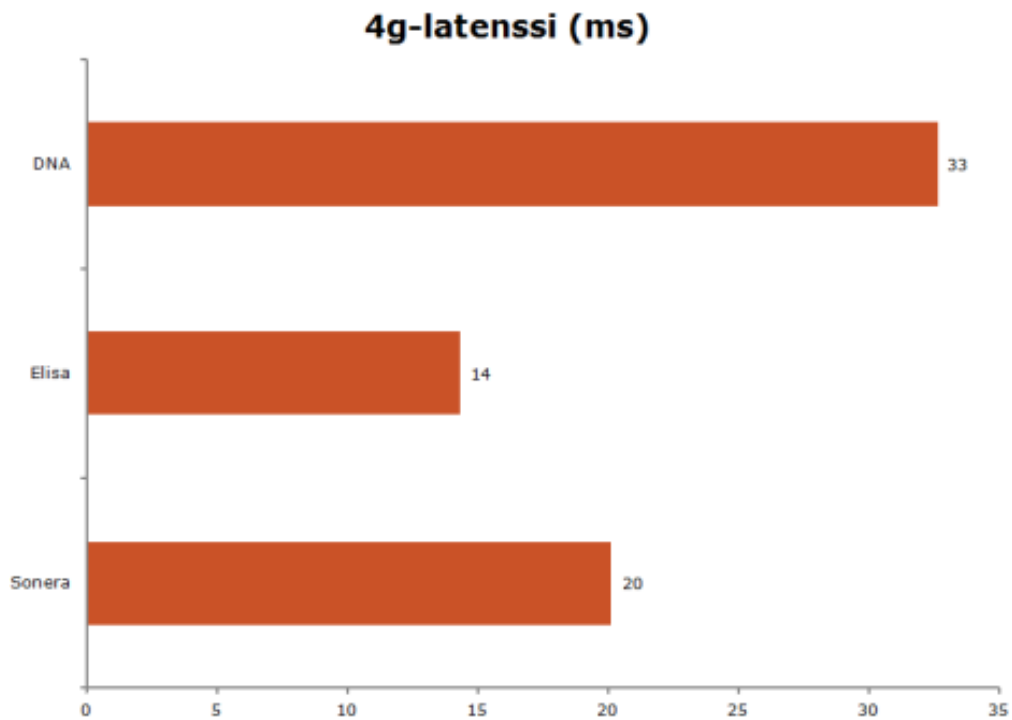
KUVIO 1. 3G-tekniikoiden latausnopeudet, Mbps (Tietokone 2012)

Seuraavassa mittauksessa tutkittiin DNA:n ja Elisan DC-HSPA+ -yhteyksien (Dual Carrier - High Speed Packet Access) nopeuksia. Kuviossa 2 on esitetty DNA:n ja Elisan DC-HSPA+ -yhteyksien latausnopeudet.



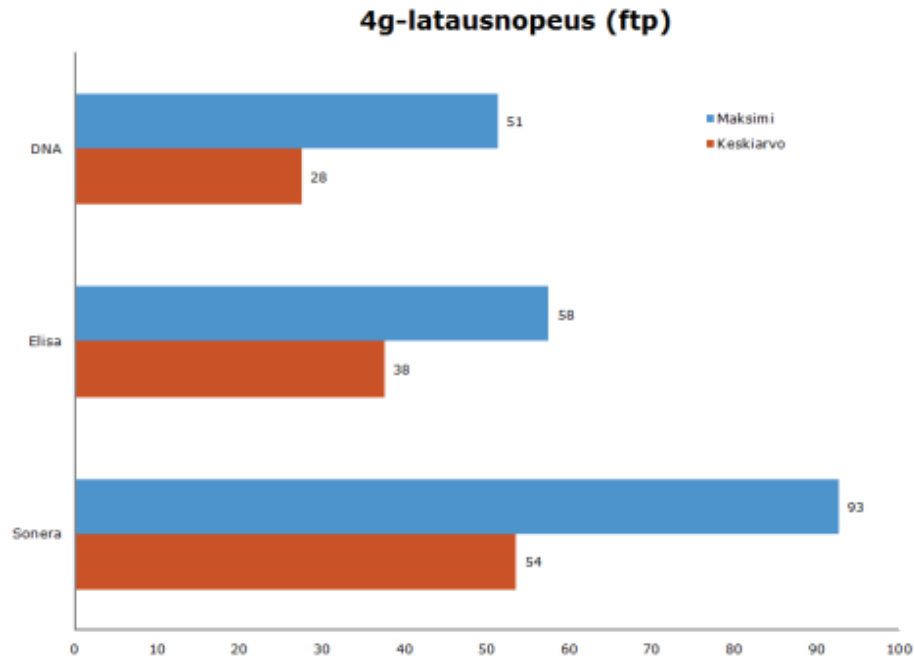
KUVIO 2. DC-HSPA+ -tekniikan latausnopeudet, Mbps (Tietokone 2012)

Seuraavassa mittauksessa tutkittiin LTE-yhteyksien (4G) viivettä Ficixin palvelimeen. Kuviossa 3 on esitetty DNA:n, Elisan ja Soneran yhteyksien viiveet käyttäen LTE-tekniikkaa.



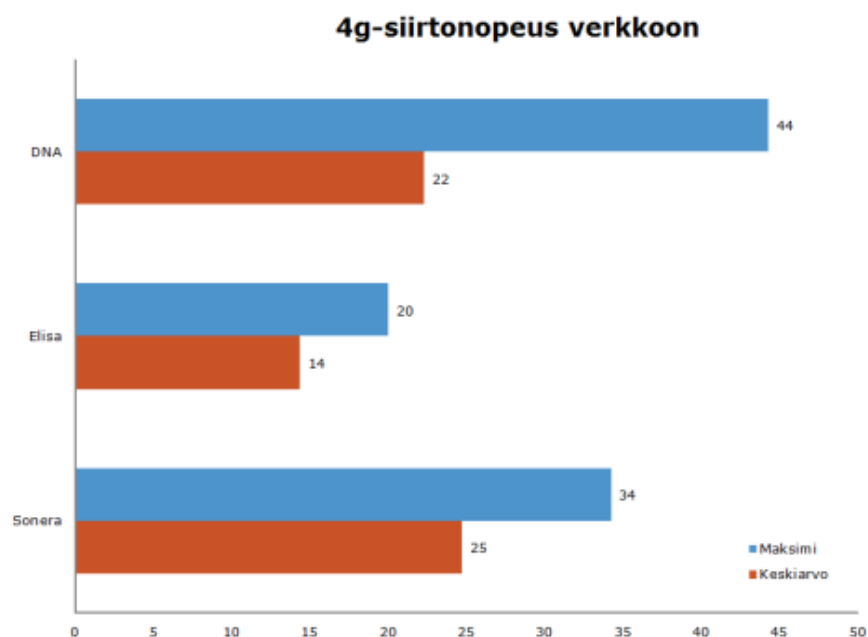
KUVIO 3. LTE-yhteyksien viiveet (Tietokone 2012)

Seuraavassa mittauksessa tarkasteltiin LTE-yhteyksien latausnopeuksia käyttäen FTP:tä. Kuviossa 4 on esitetty DNA:n, Elisan ja Soneran yhteyksien latausnopeudet käyttäen LTE-tekniikkaa.



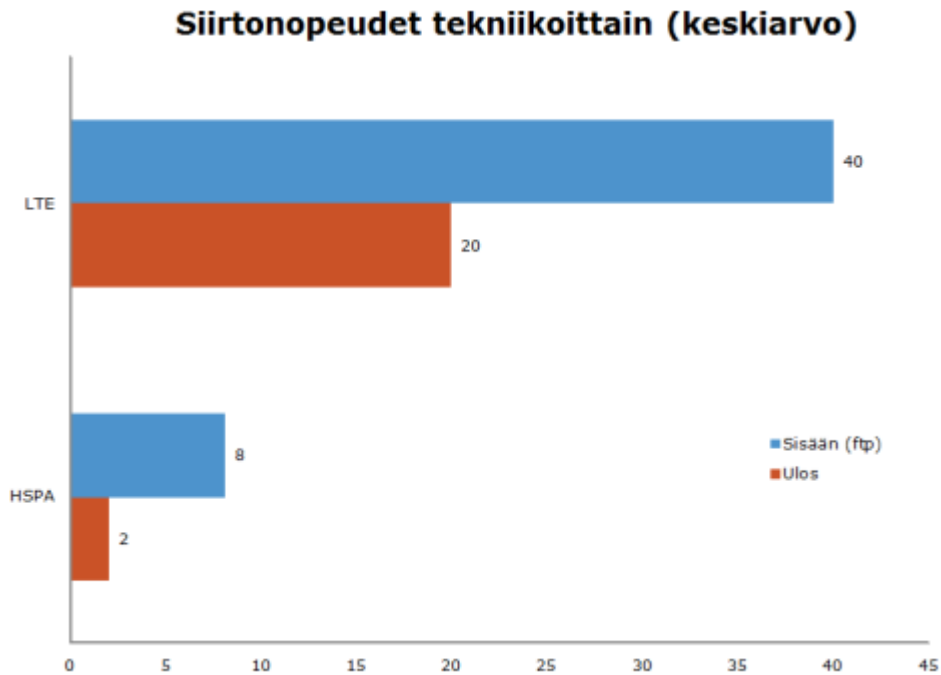
KUVIO 4. LTE-yhteyksien latausnopeudet (Tietokone 2012)

Seuraavassa mittauksessa tarkasteltiin LTE-yhteyksien siirtonopeuksia verkkoon päin. Kuviossa 5 on esitetty DNA:n, Elisan ja Soneran yhteyksien siirtonopeudet verkkoon päin käyttäen LTE-tekniikkaa.



KUVIO 5. LTE-yhteyksien siirtonopeudet verkkoon (Tietokone 2012)

Viimeisessä mittauksessa tutkittiin eri tekniikoiden siirtonopeuksien keskiarvoja. Kuviossa 6 on esitetty siirtonopeuksien keskiarvot eri tekniikoita käyttäen.



KUVIO 6. Siirtonopeudet tekniikoittain, Mbps (Tietokone 2012)

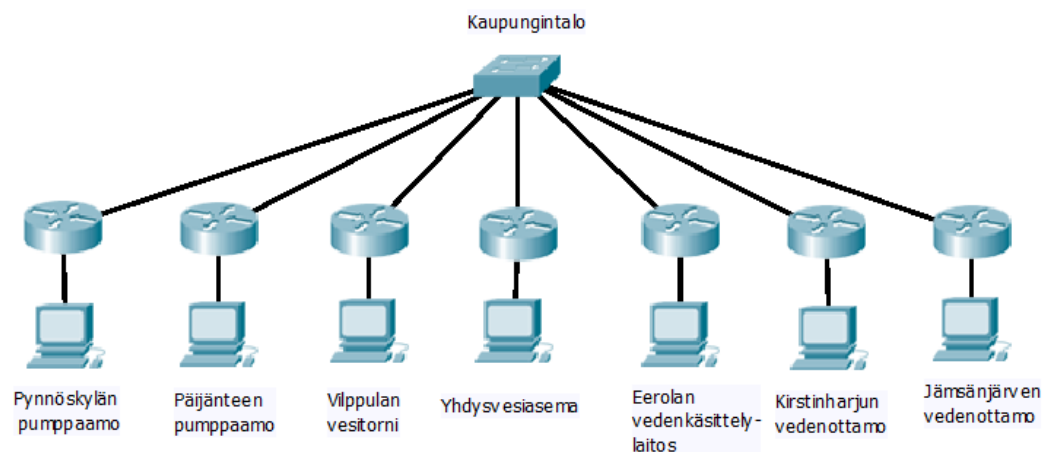
Tietokone-lehden tekemien mittausten perusteella voidaan päätellä, että neljännen sukupolven LTE-yhteydet tulevat nostamaan tiedonsiirtonopeudet aivan uudelle tasolle. Mittaustuloksista voi myös huomata sen, että 4G-yhteyksissä viiveen suuruus on melko pieni verrattuna vanhempiin kolmannen sukupolven yhteyksiin. Juurikin tämä viiveen pieneneminen vaikuttaa eniten käyttäjän kokemuksiin verkkoa käyttäessä. Mitä pienempi viive, sitä parempi käyttökokemus. Mittaustuloksista tulee toki huomioida se, että 4G-verkko on vielä suurimmaksi osaksi voimakkaassa kehitysvaiheessa.

## 4 VESIHUOLLON VERKON TOTEUTTAMINEN

### 4.1 Työn lähtökohdat ja tavoitteet

Työn tarkoituksena oli korvata Mänttä-Vilppulan Vesihuollon kiinteillä puhelin-yhteyksillä toimivat hallintayhteydet tietoturvalisillä VPN-tunneilla (Virtual Private Network) hyödyntävillä 3G-yhteyksillä.

Vesihuollon verkko koostuu yhteensä seitsemästä eri ala-asemasta. Kaikille ala-asemille menee oma kiinteä puhelin-yhteys hallintayhteyttä varten. Kaikilta ala-asemilta on yhteys Kaupungintalolla olevaan hallinta-PC:seen. Hallinta-PC:n kautta pystytään tarkkailemaan veden virtausta kaikkien ala-asemien läpi. Kuvassa 8 on esitetty Vesihuollon verkon rakenne.



KUVA 8. Vesihuollon verkko

Työn tavoitteena oli päivittää verkko nykyaikaiseen tekniikkaan. 3G-tekniikkaan siirtymisen ansiosta vian paikallistaminen verkossa helpottuu ja 3G-yhteyksiin siirtyminen myös vähentää asentajien työtä. Tätä kautta verkon huoltamisen kustannuksetkin saadaan pienemmäksi.

## 4.2 Työssä käytetyt laitteet

### 4.2.1 Cisco 819 reititin

Työssä käytettiin 3G-yhteyden muodostamiseen Ciscon 819 reititintä. Kuvassa 9 on esitetty Ciscon 819 reititin.



KUVA 9. Cisco 819 reititin (Cisco 819 2012)

Ciscon 819 reititin on kompakti laite 3G-yhteyksien muodostamiseen. Laitetta pystytään käyttämään ulko- ja sisätiloissa sekä mobiileissa ympäristöissä. Laitteen käyttöjärjestelmänä toimii Ciscon IOS (Internetwork Operating System). Reititin tukee viimeisintä HSPA+ (High Speed Packet Access Plus) –standardia. Laite on myös yhteensopiva vanhempien HSPA- (High Speed Packet Access), UMTS- (Universal Mobile Telecommunications), EDGE- (Enhanced Data Rates for Global Evolution) ja GPRS-standardien (General Packet Radio Service) kanssa. 3G-yhteyttä voidaan käyttää laitteen pääasiallisena datayhteytenä. Tässä työssä laitteessa hyödynnettiin pelkästään laitteen 3G-yhteyksien mahdollistamia ominaisuuksia. Reitittimessä on neljä 10/100 Mbps Fast Ethernet porttia jotka mahdollistavat verkon luomisen. Laitteessa on myös yksi 1000 Mbps liitäntä nopeampia tiedonsiirtoyhteyksiä varten. Laite sopii parhaiten pienten toimistojen käyttöön.

Laitteella saavutetaan monia hyötyjä verrattuna reitittämiin, joissa ei ole 3G-ominaisuuksia. Seuraavaksi lueteltuina tärkeimmät:

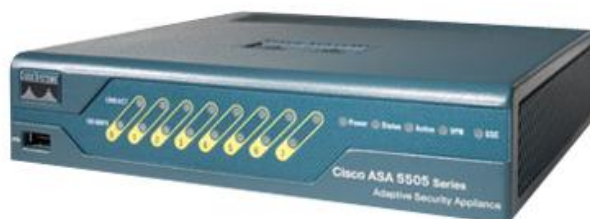


- Tarjoaa M2M (Machine-to-Machine) sovelluksia ja palveluita.
- Tarjoaa CPE-pohjaisia (Customer-Premises Equipment) MIB (Management Information Base) 3G-yhteyksiä.
- Mahdollistaa kahden SIM-kortin samanaikaisen käytön. Tämä mahdollistaa kahden palveluntarjoajan samanaikaisen hyödyntämisen.
- Sisältää täyden tuen Ciscon IOS-käyttöjärjestelmälle (Internetwork Operating System).
- Mahdollistaa 3G- ja 4G-yhteyksien hyödyntämisen. Täten saadaan yhteys myös syrjäisempiin paikkoihin, joihin ei ole kiinteitä linjoja.
- Laitteessa on mahdollista käyttää ulkoista lisäantennia, joka parantaa kuuluvuutta.
- Mahdollistaa verkon luomisen liikkuviin kohteisiin.
- Tukee GPS-tekniikkaa (Global Positioning System).
- Tarjoaa monia tietoturvallisia yhteysratkaisuita (Cisco 819 2012).

Liittessä 1 on esitetty laitteeseen tehdyt konfiguraatiot. Liittessä 1 käydään läpi vaadittavat konfiguraatiot 3G-yhteyden aikaansaamiseksi, sekä VPN-yhteyden muodostamiseksi Ciscon ASA 5505 palomuurin kanssa.

#### 4.2.2 Cisco ASA 5505 palomuri

Työssä käytettiin 3G-yhteyksien terminointiin Ciscon ASA 5505 palomuuria. Kuvassa 10 on esitetty Cisco ASA 5505 palomuri.



KUVA 10. Cisco ASA 5505 palomuri

Ciscon ASA 5505 on monipuolinen palomuri pienten ja keskisuurten toimistojen käyttöön. ASA 5505 perusmalli tukee kymmentä samanaikaista käyttäjää lähiverkossa ja toimii ja samalla kahdeksan porttisenä kytkimenä. Laitteessa on myös monia tietoturvaan liittyviä ominaisuuksia. Näistä tärkeimpinä tuki kymmenelle samanaikaiselle Isec VPN-yhteydelle (IP Security Architecture) ja kahdelle SSL VPN-yhteydelle (Secure Sockets Layer). Tässä työssä käytettiin pelkästään Isec VPN-yhteyksiä.

Liitteessä 2 on esitetty laitteeseen tehdyt konfiguraatiot. Liitteessä 2 käydään läpi vaadittavat konfiguraatiot VPN-yhteyden aikaansaamiseksi Ciscon 819 reitittimen kanssa, sekä tietoturvallisen lähiverkon luomiseksi kaupungintalon hallinta PC:lle.

#### **4.2.3 Schneider Electric AtmosWare iC1000 ala-asema**

Työssä käytettiin ala-asema –yhteyksien terminointiin Schneiderin AtmosWare iC1000 ala-asemaa. Kuvassa 11 on esitetty AtmosWare iC1000 ala-asema.



KUVA 11. AtmosWare iC1000 (T.A.C ATMOSTECH 2012)

AtmosWare iC1000 on uudistettu malli vanhemmasta Atmos-88 –alakeskuksesta. Uusi iC1000 sisältää markkinoiden nykyaikaisinta tekniikkaa ja sen ohjelmistotuki sekä yhteensopivuus aiempiin versioihin on erinomainen. Järjestelmän suurin etu on sen vaihtovan yhdistäminen Ethernet-verkkoon. iC1000 tarjoaa nopeaa tiedonsiirtoa ja mahdollistaa nopean etäkäytön, joka taas lisää turvallisuutta ja parantaa taloudellisuutta.

iC1000 mahdollistaa nykyaikaisen tekniikkansa ansiosta kiinteistön seurannan internetin välityksellä. Uusi alakeskus tuo joustavuutta kiinteistön hallintaan monella saralla: hälytykset ja tarkkailu hoituvat etänä, eikä paikan päälle tarvitse mennä kuin hätätapa-uksissa. Uudessa alakeskuksessa on myös tuki CAD-kuville (Computer-aided Design) ja paikantamistasoille.

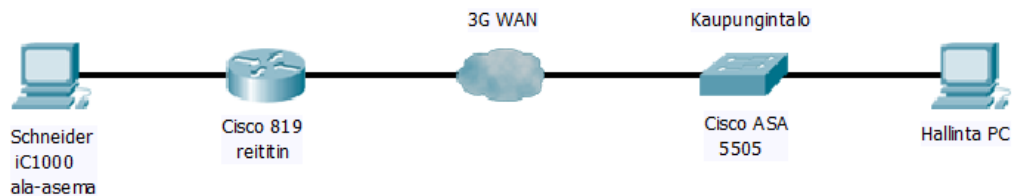
iC1000 on erittäin yhteensopiva vanhojen järjestelmien kanssa. Vanhat laitteet voidaan hyödyntää uusissa järjestelmissä halutulla tavalla. iC1000:iin sopii niin uudet kuin vanhatkin I/O-modulit. Järjestelmä on myös helppo asentaa, koska se ei vaadi uudelleen- koodausta vanhojen järjestelmien takia. iC1000 psaa hyödyntää jo olemassaolevat tietokannat suoraan.

Helppokäyttöisyys on yksi iC1000:n parhaista ominaisuuksista. Se on täysin suomen-kielinen järjestelmä. Järjestelmää on yksinkertaista käyttää ja se on helposti omaksuttavissa ilman suuria määriä koulutusta. iC1000:ssa on myös helppokäyttöinen näyttö paikanpäältä käytettäessä.

iC1000:sta voidaan web-selaimella tarkastella sisältöä, johon päivittyy dynaamiset pistetiedot, trendit, arvot ja hälytyslistaukset, niin aktiiviset, poistuneet kuin kuitaamattomatkin. Keskukseen on saatavissa kiinteistöstä noin 1000 I/O-pisteen tiedot, mikä on huomattavasti enemmän kuin vanhemmassa Atmos-88 –versiossa. Uusien I/O-modulien käyttö tarjoaa paremman hajautettavuuden eikä niissä tarvita erillistä virtalähdettä, vaan ne saavat virtansa suoraan laitteelta. Parempi hajauttaminen tuo mukanaan taloudellisia säästöjä, koska kohteessa selvittää vähemmällä keskusyksiköillä. 2-3 vanhan yksikön sijaan riittää yksi iC1000 ja muissa paikoissa selvittää pelkillä modulikeskuksilla. iC1000:ssa on runsaasti teknisiä laajennusmahdollisuuksia, mikä tekee siitä kannattavan investoinnin pitkälle tulevaisuuteen (T.A.C ATMOSTECH 2012).

### 4.3 Yleiskuvaus yhteydestä

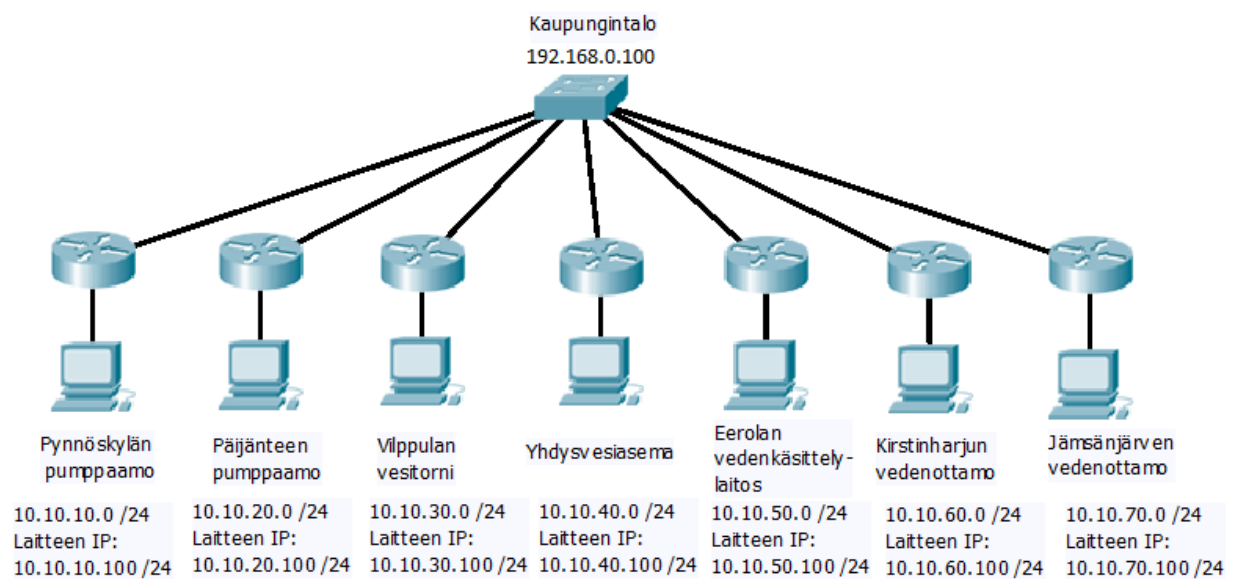
Yhteys koostuu kaiken kaikkiaan Schneider iC1000 ala-asemasta, Ciscon 819 reitittimestä, Ciscon ASA 5505 palomuurista ja kaupungintalolla olevasta hallinta PC:stä. Kuvassa 12 on esitetty yleiskuvaus yhteydestä.



KUVA 12. Yleiskuvaus yhteydestä

Ciscon 819 reititin muodostaa yhteyden internetiin 3G-yhteyden kautta. Tässä työssä käytettiin palveluntarjoajana Elisaa. Ciscon 819 reitittimen ja Ciscon ASA 5505:n välille muodostetaan VPN-yhteys internetin välityksellä. Hallinta PC pääsee VPN-yhteyden välityksellä yhteyteen halutun ala-aseman kanssa.

Kyseinen yhteysratkaisu toteutettiin yhteensä seitsemään eri ala-asemaan. Tätä verkkoa varten luotiin oma ip-suunnitelma. Ip-osoitteina käytettiin yksityisen verkon ip-osoitteita. Ip-suunnitelma on esitetty kuvassa 13.



KUVA 13. IP-suunnitelma

## 5 POHDINTA

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa Mänttä-Vilppulan Vesihuollolle 3G- ja VPN-tekniologiaa hyödyntävä nykyaikainen verkko vanhan kiinteillä puhelinyhteyksillä toimivan verkon tilalle. Suunnitellun verkon tavoitteena oli saada vian paikallistaminen verkossa helpottumaan ja tätä kautta saada verkon ylläpitokustannukset laskemaan.

Verkon suunnittelussa ja toteuttamisessa sain apua Pohjois-Hämeen Puhelin Oy:n työntekijöiltä. Kaikki tarvittavat laitteet työn tekemistä varten sain myöskin Pohjois-Hämeen Puhelin Oy:n kautta. Verkon toteuttaminen ja suunnittelu aloitettiin Pohjois-Hämeen Puhelin Oy:n tiloissa tämän vuoden alkupuolella luomalla testiympäristö verkkoa varten. Tämän avulla sain työn alkuun melko mutkattomasti ja verkko olikin pian valmis oikeata testausta varten Mänttä-Vilppulan Vesihuollon tiloissa.

Suunnitellusta verkosta on varmasti hyötyä myöskin tulevaisuutta ajatellen. Kyseistä verkkoratkaisua voidaan kehittää vielä eteenpäin ja se varmasti sopii myöskin muihin käyttökohteisiin. 3G-tekniologian yleistyminen tekee tästä verkkoratkaisusta myöskin vartenotettavan vaihtoehdon, kun aloitetaan rakentamaan uutta verkkoa esimerkiksi hieman syrjäisemmälle alueelle johon ei ole mahdollista saada kiinteää laajakaistayhteyttä.

Työn kaikissa tavoitteissa onnistuttiin ja Mänttä-Vilppulan Vesihuollolle onnistuttiin suunnittelemaan ja toteuttamaan uusi verkko. Mänttä-Vilppulan Vesihuollon on nyt siis mahdollista päivittää verkkonsa uuteen 3G-tekniologiaa hyödyntävään tietoturvalliseen verkkoon.

## LÄHTEET

- Granlund, K. 2001. Langaton tiedonsiirto. Jyväskylä: Docendo Finland Oy.
- Granlund, K. 2007. Tietoliikenne. Jyväskylä: WSOYpro/Docendo-tuotteet.
- Holma, H., Toskala, A. 2004. WCDMA for UMTS. Radio Access for Third Generation Mobile Communications. John Wiley & Sons LTD.
- Nicopolitidis, P., Obaidat, M. S., Papadimitriou, G. I., Pomportsis, A. S. 2003. Wireless Networks. John Wiley & Sons LTD.
- Evolved HSPA / HSPA+. A tutorial or overview of the basics of 3G HSPA+ also called Evolved HSPA or HSPA Evolution. Viitattu 20.3.2012. <http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/evolved-high-speed-packet-access-evolution.php>
- Ryvasy, P. 2006. Mobile Broadband: EDGE, HSPA & LTE. Ryvasy Research.
- Dual carrier – DC-HSPA, DCHSDPA. Tutorial of the basics of Dual carrier HSPA. Viitattu 20.3.2012. <http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/dc-dual-carrier-hspa-hsdpa.php>
- HSPA to LTE-Advanced: 3GPP Broadband Evolution to IMT-Advanced (4G). 2009. Viitattu 20.3.2012. [http://www.3gamericas.org/documents/3G\\_Americas\\_RysavyResearch\\_HSPA-LTE\\_Advanced\\_Sept2009.pdf](http://www.3gamericas.org/documents/3G_Americas_RysavyResearch_HSPA-LTE_Advanced_Sept2009.pdf)
- LTE Encyclopedia. LTE. 2012. Viitattu 28.3.2012. <https://sites.google.com/site/lteencyclopedia/home>
- Tietokone: Tietotekniikan asiantuntija. Tietokone mittasi mobiilinetin nopeudet. 2/2012. Viitattu 28.3.2012. <http://blogit.tietokone.fi/tietojakoneesta/2012/03/tietokone-mittasi-mobiilinetin-nopeudet/>
- Cisco. Cisco 819 Integrated Services Router. 2012. Viitattu 4.4.2012. <http://www.cisco.com/en/US/products/ps11615/index.html>
- T.A.C ATMOSTECH. AtmosWare – iC1000 ala-asema. 2012. Viitattu 5.4.2012. <http://www.tac.com/fi/data/internal/data/08/39/1247744979739/iC1000+esite.pdf>
- Verkkokauppa.com. Cisco ASA 5505. 2012. Viitattu 5.4.2012. <http://www.verkkokauppa.com/fi/product/25415/xkdm>

## LIITTEET

Liite 1. Cisco 819 reitittimen konfiguraatiot.

1(6)

Aluksi käydään läpi olennaisimmat konfiguraatiot 3G-yhteyden ja VPN-yhteyden muodostamista varten. Lopussa on esitetty konfiguraatiot kokonaisuudessaan. Kaikki konfiguraation on syötetty IOS-käyttöjärjestelmään console-portin välityksellä.

1. Luodaan yhteysprofiili 3G-yhteyden muodostamista varten ja liitetään tämä profiili line 3 interfaceen, joka muodostaa yhteyden skriptin avulla. Konfiguraatiot on seuraavat.

```
cellular 0 gsm profile create 1 internet chap **username** **password**
chat-script elisa "" "ATDT*99*1#" TIMEOUT 30 "CONNECT"
line 3
  script dialer elisa
  no exec
```

2. Konfiguroidaan Cellular 0 interface 3G-yhteyden muodostamista varten. Konfiguraatiot ovat seuraavat.

```
interface Cellular0
  no ip address
  ip virtual-reassembly
  encapsulation ppp
  dialer in-band
  dialer pool-member 2
  dialer-group 2
  async mode interactive
```

3. Konfiguroidaan Dialer 2 interface 3G-yhteyden muodostamista varten. Konfiguraatiot ovat seuraavat.

```
interface Dialer2
  ip address negotiated
```

```
encapsulation ppp 2(6)
dialer pool 2
dialer idle-timeout 0
dialer string elisa
dialer persistent
dialer-group 2
ppp chap hostname username
ppp chap password 0 password
ppp ipcp dns request
```

4. Luodaan reitittimelle lähiverkko porttiin Fast Ethernet 0. Konfiguraatiot ovat seuraavat.

```
interface Vlan1
description LANI
ip address 10.10.10.1 255.255.255.0
no ip redirects
no ip proxy-arp
crypto ipsec client ezvpn ASA inside
```

```
interface FastEthernet 0
switchport access Vlan 1
```

5. Konfiguroidaan laitteen VPN—asetukset yhteyden muodostamista varten. Konfiguraatiot ovat seuraavat.

```
crypto ipsec client ezvpn ASA
connect auto
group "GROUPNAME" key key
mode network-extension
peer 192.168.0.100
username "username" password "password"
xauth userid mode local
```



Interface Dialer 2

3(6)

```
crypto ipsec client ezvpn ASA outside
```

Interface Vlan 1

```
crypto ipsec client ezvpn ASA inside
```

6. Kongiroidaan laite reitittämään kaikki data Dialer 2 interfacen kautta. Konfiguraatiot ovat seuraavat.

```
ip route 0.0.0.0 0.0.0.0 dialer2
```

---

Seuraavaksi on esitetty laitteen kaikki konfiguraatiot.

```
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
memory-size iomem 10
!
ip source-route
!
ip cef
no ipv6 cef
!
```

```
multilink bundle-name authenticated
chat-script elisa "" "ATDT*99*1#" TIMEOUT 30 "CONNECT"
license
!
username "username" password "password"
!
controller Cellular 0
!
crypto ipsec client ezvpn ASA
connect auto
group "GROUPNAME" key key
mode network-extension
peer 192.168.0.100
username "username" password "password"
xauth userid mode local
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
no ip address
shutdown
duplex auto
speed auto
!
interface Cellular0
no ip address
ip virtual-reassembly
encapsulation ppp
dialer in-band
```

4(6)

5(6)

```
dialer pool-member 2
dialer-group 2
async mode interactive
!
interface Vlan1
description LANI
ip address 10.10.10.1 255.255.255.0
no ip redirects
no ip proxy-arp
crypto ipsec client ezvpn ASA inside
!
interface Dialer2
ip address negotiated
encapsulation ppp
dialer pool 2
dialer idle-timeout 0
dialer string elisa
dialer persistent
dialer-group 2
ppp chap hostname username
ppp chap password 0 password
ppp ipcp dns request
crypto ipsec client ezvpn ASA
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Dialer2
!
dialer-list 2 protocol ip permit
!
control-plane
!
line con 0
```

```
no modem enable
line aux 0
line 3
script dialer elisa
no exec
rxspeed 7200000
txspeed 5760000
line vty 0 4
login
transport input all
!
end
```

6(6)

Liite 2. Cisco ASA 5505 palomuurin konfiguraatiot.

1(7)

Aluksi käydään läpi olennaisimmat konfiguraatiot VPN-yhteyden muodostamista varten. Lopussa on esitetty konfiguraatiot kokonaisuudessaan. Kaikki konfiguraation on syötetty IOS-käyttöjärjestelmään console-portin välityksellä.

1. Luodaan staattinen reitti ulkoreunalla olevasta verkosta sisäverkkoon. Konfiguraatiot ovat seuraavat.

```
route outside 10.10.10.0 255.255.255.0 192.168.0.1 1
```

2. Konfiguroidaan palomuurin salausasetukset. Konfiguraatiot ovat seuraavat.

```
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set DES esp-3des esp-sha-hmac
```

3. Luodaan dynaaminen mappaus valituille salausasetuksille. Konfiguraatiot ovat seuraavat.

```
crypto dynamic-map def-dyn-map 65535 set transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-
AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
```

4. Konfiguroidaan IPsecin salausasetukset. Konfiguraatiot ovat seuraavat. 2(7)

```
crypto map outside_map 65535 ipsec-isakmp dynamic def-dyn-map  
crypto map outside_map interface outside
```

5. Luodaan vaiheen 1 autentikaatioprofiili. Konfiguraatiot ovat seuraavat.

```
crypto isakmp enable outside  
crypto isakmp policy 1  
authentication pre-share  
encryption 3des  
hash sha  
group 2  
lifetime 86400
```

```
crypto isakmp policy 20  
authentication pre-share  
encryption 3des  
hash md5  
group 2  
lifetime 86400
```

6. Konfiguroidaan group-policyt, tunnel-groupit ja pre-shared keyt yhteyden muodostamista varten. Konfiguraatiot ovat seuraavat.

```
group-policy GROUPNAME attributes  
vpn-tunnel-protocol IPSec  
password-storage enable  
nem enable
```

```
tunnel-group GROUPNAME type remote-access  
tunnel-group GROUPNAME general-attributes  
authorization-server-group LOCAL  
default-group-policy 3GPolicy  
tunnel-group GROUPNAME ipsec-attributes
```

```
pre-shared-key                               3(7)
!  
username cisco password cisco
```

---

Seuraavaksi on esitetty laitteen kaikki konfiguraatiot.

```
hostname cisco  
enable password "password"  
!  
interface Vlan1  
 nameif inside  
 security-level 100  
 ip address 192.168.0.1 255.255.255.0  
!  
interface Vlan2  
 nameif outside  
 security-level 0  
 ip address 192.168.0.100 255.255.255.0  
!  
interface Ethernet0/0  
 switchport access vlan 2  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
 shutdown  
!  
interface Ethernet0/3  
 shutdown  
!  
interface Ethernet0/4  
 shutdown  
!
```

```
interface Ethernet0/5
shutdown
!
interface Ethernet0/6
shutdown
!
interface Ethernet0/7
shutdown
!
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 192.168.0.100 1
route outside 10.10.10.0 255.255.255.0 192.168.0.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
```



```
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac      5(7)
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set DES esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map def-dyn-map 65535 set transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-
AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic def-dyn-map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 1
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
crypto isakmp policy 20
  authentication pre-share
  encryption 3des
  hash md5
  group 2
  lifetime 86400
crypto isakmp policy 65535
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

threat-detection basic-threat
```

```
threat-detection statistics access-list 6(7)
no threat-detection statistics tcp-intercept
group-policy 3GPolicy internal
group-policy 3GPolicy attributes
  vpn-tunnel-protocol IPSec
  password-storage enable
  nem enable
username phpoy password eVL/8tFbqw8EVqy5 encrypted
tunnel-group GROUPNAME type remote-access
tunnel-group GROUPNAME general-attributes
  authorization-server-group LOCAL
  default-group-policy 3GPolicy
tunnel-group GROUPNAME ipsec-attributes
  pre-shared-key
!
class-map inspection_default
  match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
```

inspect sip

7(7)

inspect xdmcp

!

service-policy global\_policy global