Kimmo Liikonen

IPv6:n käyttöönotto matkaviestinverkossa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

19.5.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Kimmo Liikonen IPv6:n käyttöönotto matkaviestinverkossa 51 sivua 19.5.2014
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	suunnittelupäällikkö Ville Virtanen yliopettaja Janne Salonen

Insinöörityössä tutkittiin internetprotokollaversio kuuden (IPv6) käyttöönottoa DNA:n matkaviestinverkossa. Internetprotokollaversio neljän (IPv4) osoiteavaruus ei riitä yksilöimään jokaista internetissä olevaa laitetta. Osoitteiden riittämättömyys oli pääsyy IPv6:n kehittämiseen. Tulevaisuudessa internetin osoitteistus tulee siirtymään IPv6:een.

Tämän työn tilaajana oli DNA Oy. DNA haluaa ottaa käyttöön IPv6:n mobiililaajakaistaliittymiinsä. Insinöörityö keskittyi tutkimaan IPv6-protokollan käyttöönottoa loppukäyttäjien liittymiin. IPv6-protokolla mahdollistaa kaikkien kodin laitteiden kytkemisen Internetiin omalla IP-osoitteella. Työn tavoitteena oli tutkia, missä kaikissa matkaviestinverkon elementeissä tarvitaan muutoksia, jotta IPv6 saadaan käyttöön loppukäyttäjille. Lisäksi tavoitteena oli tutkia IPv6:n käyttöönottoa testi- ja tuotantoverkossa, sekä suunnitella käyttöönotto mahdollisimman huolellisesti.

Teoriaosuudessa perehdyttiin aluksi internetin perusperiaatteisiin, sitten IPv4- ja IPv6-protokolliin ja matkaviestinverkkoon IP-protokollan näkökulmasta. Käytännönosuudessa selvitettiin mihin matkaviestinverkon elementteihin tarvitaan IPv6:lle muutoksia, otettiin käyttöön IPv4v6 dual-stack DNA:n matkaviestinverkon pakettirunkoverkkoon ja tehtiin erilaisia testejä loppukäyttäjän näkökulmasta.

Kevyen suorituskykytestin perusteella IPv4-protokolla oli tiedonsiirtonopeudessa kahdeksan prosenttia nopeampi kuin IPv6-protokolla. Web-sivujen latausnopeudessa IPv4-protokolla oli 21 prosenttia nopeampi kuin IPv6-protokolla. Käytännön ero oli kuitenkin niin pieni, että loppukäyttäjät eivät todennäköisesti tule eroa huomaamaan. Erot tulevat vieläkin pienenemän, kun IPv6-reititys kehittyy IPv4-reitityksen tasolle. Huawein B593S reitittimestä löytyi myös ohjelmointivirhe, joka viivästytti IPv6 DNS-kyselyiden vastauksia.

IPv6:n käyttöönotto aiheuttaa muutoksia moneen matkaviestinverkon elementtiin. Tehtyjen testien perusteella voidaan kuitenkin sanoa, että IPv6:n käyttöönotto mobiililaajakaistaliittymille on mahdollista ilman merkittäviä ongelmia.

Avainsanat	IPv6, IPv4, dual-stack, matkaviestinverkko, PDN, PDP

Author(s) Title Number of Pages Date	Kimmo Liikonen Implementing IPv6 in mobile network 51 pages 19 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Ville Virtanen, Planning Chief Janne Salonen, Principal Lecturer

The objective of this Barchelor's Thesis was to explore the Internet Protocol version six (IPv6) in mobile networks. In future addressing of internet will move to IPv6 protocol. This study was carried out on assignment by DNA Oy. DNA Oy wants to enable IPv6 protocol for its mobile broadband customers.

This study was divided into two parts. The theory part focuses on internet principles, IPv4 and IPv6 protocols and mobile networks. The practical part of the work focuses first on exploring which mobile network elements need changes. Then it describes implementing of IPv4v6 dual-stack to user-plane of DNA's mobile packet core network. In the end it presents various tests from end user perspective.

According to performance tests, in file transfer IPv6 protocol was eight percent slower than IPv4 protocol. In web page load time test dual-stack enabled host was 21 percent slower than IPv4 protocol host. It was also found that Huawei B593S mobile broadband router had a software bug, which slows down IPv6 DNS answers.

Enabling IPv6 for DNA's mobile broadband customers causes changes to many mobile elements. According to end user tests, it will be possible to enable IPv6 to end users without significant problems.

Keywords	IPv6, IPv4, dual-stack, mobile network, PDN, PDP

1 Johdanto 1

2 Internet 1

2.1 Historia 2
2.2 Perusperiaatteet 2
2.2.1 Pakettikytkentäinen verkko 3
2.2.2 Päästä päähän periaate 3
2.2.3 Koostuu erilaisista kerroksista 3
2.2.4 Postelin laki 4
2.2.5 Luova anarkia 4
2.3 Standardisointi, protokolla ja kehysrakenne 5
2.4 Tärkeimmät siirtokerroksen protokollat 5
2.5 Osoitejärjestelmä 6
2.6 IPv6-protokolla 7
2.6.1 Kehysrakenne 7
2.6.2 Laajennetut kehykset 8
2.6.3 Internet Control Message Protocol v6 ja Neighbor Discovery Protocol 10
2.6.4 Stateless Address Configuration 12

3 Matkaviestinverkko 13

3.1 Matkaviestinverkkojen eri sukupolvet 13
3.2 Standardisointi 15
3.3 Verkkoarkkitehtuuri 16
3.3.1 GSM-järjestelmä 17
3.3.2 2G General Packet Radio Service (GPRS) 18
3.3.3 2G GPRS -protokollat 19
3.3.4 UMTS ja 3G GPRS 21
3.3.5 3G GPRS-protokollat 22
3.3.6 Evolved Packet System (EPS) 24
3.3.7 EPS-arkkitehtuurin protokollapinot 27

4 IPv4- ja IPv6-protokollat 3GPP-matkaviestinverkoissa 28

4.1 Pakettidataverkon (PDN) yhteyspalvelu 28
4.1.1 EPS bearer ja PDP-konteksti 30
4.1.2 PDP-kontekstin luontiproseduuri GPRS-arkkitehtuurissa 33
4.1.3 PDN-yhteyden muodostusproseduuri EPS-arkkitehtuurissa 34

4.1.4 User-plane, control-plane ja transport plane 35
4.1.5 PDN- ja PDP-yhteystyypit 36
4.1.6 IPv4-osoitteen tai IPv6-prefiksin allokointi PDN-yhteydelle 37
4.1.7 DNS-nimipalvelintiedot 37
4.1.8 IPv6-pakettien välitys 3GPP-matkaviestinverkossa 37

5 IPv6:n käyttöönotto DNA:n matkaviestinverkossa 38

5.1 Lyhyt esittely DNA:n matkaviestinverkosta 38
5.2 DNA:n mobiilipakettirunkoverkon nykyinen tilanne 39
5.3 IPv6:n käyttöönotto DNA:lla 40
5.4 Loppukäytäjän IPv4v6 PDN/PDP-yhteyden vaikutus DNA:n matkaviestinverkon elemetteihin 40
5.4.1 Tilaajarekisterit HLR ja HSS 40
5.4.2 Provisiointijärjestelmä 41
5.4.3 GGSN, PGW ja niiden tukijärjestelmät 41
5.4.4 SGSN, MME ja SGW 43
5.4.5 Radioverkko 43
5.4.6 Päätelaite 43
5.5 IPv6:n tarvitsemat tukipalvelut 44
5.5.1 Domain Name Service (DNS) -kääntäjänimipalvelu 44
5.5.2 DNS forward ja reverseille tietueet käytössä oleville IPv6-osoitteille 44
5.5.3 Content Delivery Network (CDN) -toimijoiden välimuistit 45
5.6 Yhteenveto tarvittavista muutoksista 45

6 IPv6-protokollan testaus DNA:n tuotantoverkossa 46

6.1.1 IPv4v6-yhteyden muodostus 46
6.1.2 FTP-siirtonopeus 49
6.1.3 Web-sivujen vasteaikojen mittaus 49

7 Johtopäätökset 51

Lähteet 52

Lyhenteet

1G	Matkaviestinverkon ensimmäinen sukupolvi, johon kuuluu analogiset matkapuhelinjärjestelmät.
2G	Matkaviestinverkon toinen sukupolvi, johon kuuluu ensimmäiset digitaaliset matkapuhelinjärjestelmät, kuten Global System for Mobile Communications (GSM) –järjestelmä.
3G	Matkaviestinverkon kolmas sukupolvi, johon kuuluu Universal Mobile Telecommunications Systems (UMTS) -järjestelmä ja Code Division Multiple Access (CDMA) –järjestelmä.
4G	Matkaviestinverkon neljäs sukupolvi. IMT Advanced -ohjelman mukaan LTE Advanced ja Wimax release 2 täyttävät vasta 4G-vaatimukset. Vaatimusten mukaan myötäsuuntanopeuden pitäisi olla 1 Gbps paikalla oltaessa ja 100 Mbps liikkeessä. Usein kuitenkin LTE-yhteyksiä markkinoidaan jo 4G-nimellä.
AH	Autentication Header on osa Internet Protocol Security (IPSEC) -protokollaa. AH-protokolla mahdollistaa todennuksen ja takaa viestien eheyden, mutta ei mahdollista luottamuksellisuutta.
AMPS	Advanced Mobile Phone System on Yhdysvalloissa käytetty ensimmäisen sukupolven matkapuhelinjärjestelmä.
APN	Access Point Name on sidos mobiilipakettiverkon ja ulkoisen IP-verkon välillä. APN-nimessä on kaksi osaa: verkko-osa ja operaattoriosa. APN-nimen struktuuri noudattaa samoja sääntöjä kuin Fully Qualified Domain Name (FQDN), joka lopulta käännettään Gateway GPRS Supporting Node (GGSN) tai Packet Data Network Gatewayn (PGW) IP-osoitteeksi. Operaattorin tunnusosa ei ole yleensä näkyvä loppukäyttäjälle, vaan Serving GRPS Supporting Node (SGSN) tai Mobility Management Entity (MME) voi täydentää loppuosan.
ARP	Address Resolution Protocol kuuluu internetprotokolla perheeseen ja sitä käytetään ratkaisemaan verkkotason IP-osoitteita linkkitason osoitteisiin.

BSC Base Station Controller on 2G-matkaviestinverkon tukiasemaohjain. Se voi hallita satoja tai tuhansia 2G-tukiasemia. Se koordinoi mm. tilaajan mobiliteetin tukiasemien välillä, niin ettei esim. puhelu katkea, kun tilaaja liikkuu tukiasemasta toiseen.

BTS Base Transceiver Station on 2G-matkaviestinverkon tukiasema. Se lähettää radioverkon signaalin loppukäyttäjälle. Käyttäjä on suoraan yhteydessä siihen radiorajapinnan (Um) avulla.

CDMA Code Division Multiple Access on Yhdysvalloissa käytetty 2G-matkapuhelinjärjestelmä. CDMA:ta kutsutaan joskus myös Interim Standard 95 (IS-95) –järjestelmäksi.

CDMA2000 Code Division Multiple Access 2000 on Yhdysvalloissa ja Etelä-Koreassa käytetty 3G-matkapuhelinjärjestelmä.

CIDR Classless Inter-Domain Routing, eli luokaton reititys. CIDR korvasi luokallisen reitityksen. Sen avulla IPv4-osoitejärjestelmä saatiin tehokkaammin käyttöön.

CSFB Circuit Switched Fall Back on 4G LTE-matkaviestinverkossa käytetty ominaisuus, jolla päätelaite ohjataan 4G LTE-verkosta piirikytkennäiseen 2G- tai 3G-verkkoon vastaanottamaan tai soittamaan puhelu.

DHCP Dynamic Host Configuration Protocolin tehtävänä on jakaa IP-osoitteita verkkoon kytketyille laitteille.

DNS Domain Name System on hierarkinen ja skaalautuva internetin nimipalvelujärjestelmä. Sen avulla helpommin muistettavat verkkotunnukset käännetään IP-osoitteiksi ja toisinpäin.

DSCP Differentiated Service Code Point on IPv4-paketissa oleva 6-bittinen kenttä, joka oli alun perin nimetty Type Of Service (TOS) -kentäksi, tämä kenttä on määritelty uudestaan RFC2474:ssa. DSCP:tä voidaan käyttää Quality of Service (QoS) -luokan määrittämiseen.

EDGE	Enhanced Data rates for Global Evolution tai Enhanced GPRS:ksi kutsuttu EDGE-teknologia mahdollisti 384 Kbps myötäsuunnan ja 384 Kbps paluusuunnan siirtonopeuden 2G-matkaviestinverkoissa.
ENodeB	Evolved Node B on 4G LTE-matkaviestinverkon tukiasema. ENodeB kuuluu EPS-arkkitehtuurin. Osa tukiasemaohjaimen toiminteista on siirretty LTE-tukiasemaan.
EPC	Evolved Packet Core on osa Evolved Packet Systemiä (EPS), julkaistiin samaan aikaan LTE:n kanssa. EPC:n elementit ovat HSS, MME, SGW ja PGW.
EPS	Evolved Packet System koostuu kahdesta osasta: radioliityntäverkosta (LTE) ja Evolved Packet Core:sta (EPC), eli pakettirunkoverkosta. EPS on yksinkertaisempi kuin aikaisempi GPRS-arkkitehtuuri.
ESP	Encapsulating Security Payload on osa Internet Protocol Security (IPSEC) -protokollaa. ESP mahdollistaa pakettivirran salauksen.
E-UTRAN	Evolved Universal Terrestial Access Network, joka tunnetaan paremmin “LTE” -termillä. Tarkoittaa neljännen sukupolven matkapuhelintekniikkaa.
FDD	Frequency-Division Duplexing tarkoittaa että vastaanottaja ja lähettäjä käyttävät eri taajuuksia.
FQDN	Fully Qualified Domain Name on verkkotunnusnimi, joka koostuu isäntäosasta ja verkkotunnusosasta. Esimerkiksi data.dna.fi on FQDN.
GGSN	Gateway GPRS Supporting Node on 2G- ja 3G-matkaviestinverkon elementti. GGSN on topologinen ankkurointipiste mobiliteetin hallinnalle GPRS-verkossa. Tilaajan liikkuessa kaikki muut matkaviestinverkon elemetit saattavat vaihtua, mutta GGSN pysyy samana koko yhteyden ajan. Se on yhdyskäytävä GPRS-verkon ja ulkoisen verkon välillä (kuten esim. Internet). Kuten SGSN, myös GGSN hoitaa tilaajan signalointia sekä välittää niiden liikennettä.

GPRS General Packet Radio Service on 2G- ja 3G-matkaviestintekniikan pakettipohjainen tiedonsiirtopalvelu.

GTP-C GPRS Tunnel Protocol Control Plane on matkaviestinverkon pakettiverkossa käytettävä signalointiprotokolla. Versio 2:sta käytetään EPS-arkkitehtuurissa.

GTP-U GPRS Tunnel Protocol User Plane on matkaviestinverkon pakettiverkossa käytettävä user-plane protokolla. Se on vastuussa tilaajan IP-pakettien tunneloinnista ja kuljetuksesta. GTP:n perusidea on tunnistaa mihin PDP-kontekstiin mikäkin paketti kuuluu Tunnel Endpoint ID:n (TEID):n avulla.

GSM Global System for Mobile Communications on Eurooppalainen toisen sukupolven matkapuhelinjärjestelmä.

HLR Home Location Register on 2G- ja 3G-matkaviestinverkon tilaajarekisteri. HLR on tietokanta, jossa tilaajatiedot sijaitsevat. Tilaajatiedot sisältävät autentikointidatan ja mihin palveluihin tilaajalla on oikeuksia.

HSDPA High Speed Download Packet Access:n myötä 3G-matkaviestinverkkojen pakettidatan myötäsuunnan nopeus kasvoi merkittävästi.

HSS Home Subscriber Server on 4G LTE -matkaviestinverkon tilaajarekisteri. Sieltä löytyy tilaajatiedot, kuten autentikointi- ja valtuutustiedot.

HSUPA High Speed Upload Packet Access:n myötä 3G-maktaviestinverkkojen pakettidatan paluusuunnan nopeus kasvoi merkittävästi.

ICMP Internet Control Message Protocol on IPv4-protokollan kontrolliprotokolla, jolla verkkolaitteet kuten reitittimet voivat indikoida erilaisista virhetilanteista.

IS-95 Interim Standard 95 on Yhdysvalloissa ja Etelä-Koreassa käytetty toisen sukupolven matkapuhelinjärjestelmä. IS-95:sta kutsutaan joskus myös Code Division Multiple Access (CDMA) -järjestelmäksi.

LTE Long Term Evolution on globaali melkein neljännen sukupolven matkaviestinjärjestelmä. IMT advanced -ohjelman mukaan vasta LTE advanced on oikea neljännen sukupolven matkaviestinjärjestelmä.

LTE A Long Term Evolution Advanced on globaali neljännen sukupolven matkaviestinjärjestelmä.

MIMO Multiple-Input and Multiple-Output:n avulla lähettäjä ja vastaanottaja voi käyttää usempaa kuin yhtä antennia. MIMOn avulla voidaan saavuttaa huomattavasti suurempi tiedonsiirtokapasiteetti kuin yhdellä antennilla. LTE hyödyntää MIMO-tekniikkaa myötäsuunnassa.

MME Mobility Management Entity on 4G LTE -matkaviestinverkon signalointielementti. MME on vastuussa päätelaitteen mobiliteetin hallinnasta, autentikoinnista ja valtuutuksesta. MME on toiminnallisuudeltaan paljon vastaava kuin GPRS-arkkitehtuurin SGSN. MME ei välitä user-plane liikennettä, kuten GPRS-arkkitehtuurin SGSN.

MPLS Multiprotocol Label Switching tekniikka kehitettiin alun perin yksinkertaistamaan reititystä. Sen avulla paketit leimataan. Leimojen avulla paketti voidaan toimittaa kohdelaitteelle. Pakettiin voidaan lisätä useampia leimoja. Useamman leiman avulla voidaan tehdä monia palveluita kuten L2 VPN ja L3 VPN.

MS Mobile Station eli päätelaite, kuten puhelin tai mokkula.

MSC Mobile Switching Center kuuluu 2G- ja 3G-matkaviestinverkkojen piirikytkennäiseen runkoverkkoon (CS Core). On vastuussa tilaajien autentikoinnista, mobiliteetin hallinnasta ja puheluiden kytkennästä.

MSS Maximum Segment Size on TCP-protokollan parametri, joka neuvotellaan aina TCP-yhteyden avauksessa. Se määrittelee TCP-segmentin maksimipakettikoon. Siihen ei lasketa IP- tai TCP-otsikkotietoja. Sen avulla yritetään välttää turhaa paketin pirstalointia IP-tasolla.

NAPT Network Address Port Translation on menetelmä, jolla IPv4-osoitejärjestelmä on saatu riittämään pidempään. Yhden julkisen IPv4-osoitteen takana voi olla useampi laite.

NAS Non-Access-Stratum on UMTS- ja LTE-mobiiliverkoissa päätelaitteen ja MME:n välillä oleva signalointiprotokolla. Se on vastuussa muun muassa EPS bearerien hallinnasta, autentikoinnista ja tietoturvahallinnasta.

NDP Neighbor Discovery Protocol kuuluu IPv6-protokollaperheeseen. Se toimii linkkitasolla ja on vastuussa muun muassa laitteiden automaattisesta osoitteistuksesta, duplikaattiosoitteiden tunnistuksesta ja oletusyhdyskäytävän asetttamisesta.

NMT Nordic Mobile Telephone on Pohjoismaissa käytetty ensimmäisen sukupolven analoginen matkapuhelinjärjestelmä.

NodeB 3G-matkaviestinverkon tukiasema.

OCS Online Charging System on matkaviestinverkon elementti, jonka avulla voidaan toteuttaa reaaliaikainen laskutus. Yleensä prepaid-liittymien raportionti ja laskutus on tehty OCS:n avulla.

OFDMA Orthogonal Frequency Division Multiple Access on 4G LTE-matkaviestinverkossa käytetty myötäsuunnan modulaatio.

OSI Open System Interconnect kuvaa tiedonsiirtoprotokollien yhdistelmän seitemässä kerroksessa.

PCO Protocol Configuration Optionia käytetään väittämään parametreja päätelaitteen ja GGSN- tai PGW-laitteen välillä. Sen avulla neuvotellaan mitä IP-protokollaa PDN- tai PDP-yhteydessä käytetään. GGSN- tai PGW-laite voi kertoa myös päätelaitteelle IPv4-osoitteen tai IPv6-prefiksin sen avulla. PCO-viestissä kulkee lukuisia muita loppukäyttäjän IP-protokollaan liittyviä parametreja kuten DNS-palvelimien tiedot.

PCRF Policy and Charging Rules Function on elementti, jonka kautta voidaan ajaa dynaamisia sääntöjä verkkoon. PCRF on yhteydessä EPS/GPRS-

verkkoon PGW:n tai GGSN:n kautta. Elementti voi laskea muun muassa laskea tilaajan käyttämää datamäärää.

PDCP Packet Data Convergence Protocol on kolmannen sukupolven matkaviestinverkossa käytty user-plane-protokolla. Sitä käytetään tukiaseman ja päätelaitteen välissä. Sen tehtävänä on siirtää paketit radiorajapinnan yli, pakata otsikkotiedot, segmentoida ja koota uudelleen paketteja.

PDP Packet Data Protocol on GPRS-arkkitehtuurissa esitelty yhteyspalvelu, jonka avulla voidaan muodostaa pakettidatayhteys esimerkiksi internetiin. EPS-arkkitehtuurin PDN-yhteyspalvelu on hyvin samanlainen kuin GPRS-arkkitehtuurin PDP-konteksti.

PDN Packet Data Network on EPS-arkkitehtuurin yhteyspalvelu, joka tarjoaa internetprotokollan kautta yhteyden päätelaitteelta matkaviestinverkon yli ulkoiseen IP-verkkoon. Se on päätelaitteen ja liityntäpisteen (APN) välinen assosiaatio. Jokaisella PDN-yhteydellä on IPv4-osoite ja/tai IPv6-prefiksi. GPRS-arkkitehtuurin PDP-konteksti on hyvin samanlainen kuin EPS-arkkitehtuurin PDN-yhteyspalvelu.

PGW Packet Data Network Gateway on yhdyskäytävä EPS:n ja ulkoisten IP-verkkojen välillä sekä on tilaajan IP-liikenteen terminointipiste. PGW ei vaihdu koskaan yhteyden aikana.

QoS Quality of Service kuvastaa verkon palvelun laatua, joka on tärkeä osa pakettipohjaisen IP-verkon toimintaa. Esimerkiksi erilaiset pakettien jonotusmenetelmät voidaan määritellä QoS-termin alle.

RAB Radio Access Bearer on päätelaitteelta pakettirunkoverkon laitteeseen kuten SGW tai GGSN ulottuva user-plane-liikenneputki.

RANAP Radio Access Network Application Part on 3G-matkaviestinverkon control-plane-protokolla.

RCC Roaming Cost Control on DNA:n verkossa oleva matkaviestinverkonelementti, jonka avulla toteutetaan EU:n verkkovierailuasetuksen mukainen saldorajapalvelu tilaajille.

RLC Radio Link Control on kolmannen sukupolven matkaviestinverkossa käytetty user-plane-protokolla. Sitä käytetään tukiaseman ja päätelaitteen välissä. Sen tehtävänä on yhdistää PDP-kontekstitaso Radio Access Beareriin (RAB).

RNC Radio Network Controller on 3G-matkaviestinverkon tukiasemaohjain.

RRC Radio Resource Control on 3G-matkaviestinverkon control-plane-protokolla. Sitä käytetään signalointiin päätelaitteen ja radioverkon välillä.

SC-FDMA Single Carrier - Frequency Division Multiple Access on neljännen sukuplven matkaviestinverkossa käytetty paluusuunnan modulaatio.

SGSN Serving GPRS Supporting Node on 2G- ja 3G-matkaviestinverkon elementti. SGSN hoitaa pääasiallisesti tilaajan autentikoinnin, valtuuttamisen ja mobiliteetin hallinnoimisen. SGSN vastaa pääosin mobiilipakettiverkon signaloinnista (control-plane), mutta se välittää myös loppukäyttäjän (user-plane) liikennettä.

SGW Serving Gateway kuuluu EPS-arkkitehtuuriin ja toimii mobiiliteetin ankkurina kun tilaaja siirtyy LTE-tukiasemasta toiseen LTE-tukiasemaan.

SLAAC Stateless Address Configuration on yksi IPv6:ssa käytetty tilatiedoton proseduuri, jolla voidaan osoitteistaa linkkejä. Se perustuu NDP-protokollaan.

SNDCP Sub Network Dependent Convergence Protocol on GSM-radioverkon user-plane protokolla, joka kuljettaa IP-paketteja. SNDCP multipleksaa useamman Packet Data Protocol (PDP) -konteksti päätelaitteen ja SGSN:n välillä. SNDCP voi kuljettaa IPv4-, IPv6- ja PPP-paketteja.

SS7 Signaling System no. 7 on kokoelma puhelinverkossa toimivia signalointiprotokollia.

TDD Time-Division Duplexing on aikajakoinen multipleksaus, jolla saadaan eriteltyä lähettäjän ja vastaanottajan signaalit. Tällöin lähettäjä ja vastaanottaja voi käyttää samaa taajuutta.

TCP	Transmission Control Protocol on tilatietoinen ja yksi merkittävimmistä Internetin protokollista. TCP mahdollistaa luotettavan ja tietyssä järjestyksessä toimivan tiedonsiirron.
TOS	Type Of Service, IPv4-paketissa oleva 6-bittinen kenttä, jota kutsutaan nykyään DSCP:ksi.
UDP	User Datagram Protocol on yksinkertainen tilatiedoton protokolla, joka ei tarkista että paketit tulisivat perille oikeassa järjestyksessä. Protokollassa ei ole myöskään uudelleenlähetysmekanismia, mikäli paketti on hukkunut matkalle.
UE	User Equipment eli matkaviestinverkkoon yhteydessä oleva päätelaite, kuten puhelin tai mokkula.
UMTS	Universal Mobile Telecommunications System on muun muassa Euroopassa, Japanissa ja Kiinassa käytetty kolmannen sukupolven matkapuhelinjärjestelmä. 3GPP:n määrittelemä nimi on UMTS Terrestial Radio Network (UTRAN).
UTRAN	UMTS Terrestial Radio Network on 3GPP:n määrittelemä nimi kolmannen sukupolven UMTS-järjestelmälle.
VPN	Virtual Private Network on virtuaalinen erillisverkko, jolla voidaan yhdistää useampi fyysinen verkko näennäisesti yhteen. Siirtoprotokollana voi käyttää esimerkiksi MPLS-verkkoa tai IPSEC-tunnelia.
WCDMA	Wideband Code Division Multiple Access on 3G-matkaviestinverkoissa käytetty radiorajapinta.
WIMAX R2	Worldwide Interoperability for Microwave Access on neljännen sukupolven langaton tietoliikennestandardi.

1 Johdanto

Tässä insinöörityössä tutkitaan internetprotokollaversio kuuden (IPv6) käyttöönottoa DNA:n matkaviestinverkossa. Internetprotokollaversio neljän (IPv4) osoiteavaruus ei riitä enää yksilöimään jokaista internetissä olevaa laitetta. Osoitteiden riittämättömyys oli pääsyy IPv6:n kehittämiseen.

Tutkimuksen on tilannut DNA Oy. DNA Oy on suomalainen tietoliikennekonserni, joka tarjoaa yksityishenkilöille ja yrityksille laadukkaita, viimeisintä teknologiaa hyödyntäviä puhe-, data- ja tv-palveluita. Tutkimuksen tekijä työskentelee DNA Oy:llä mobiililaajakaistasuunnittelijana.

Viestintäviraston tavoitteena on, että IPv6:n julkistamispäivä Suomessa on kesäkuussa 2015. Viestintävirasto on tiedustellut operaattoreiden halukkuutta osallistua lanseeraukseen. DNA on mukana IPv6:n käynnistämispäivässä.

Insinöörityö keskittyy tutkimaan IPv6-protokollan käyttöönottoa loppukäyttäjien liittymiin. IPv6-protokolla mahdollistaa kaikkien kodin laitteiden kytkemisen Internetiin omalla IP-osoitteella. Työn tavoitteena on tutkia, missä kaikissa matkaviestinverkon elementeissä tarvitaan muutoksia, jotta IPv6 saadaan loppukäyttäjille. Lisäksi tavoitteena on tutkia IPv6:n käyttöönottoa testi- ja tuotantoverkossa, sekä suunnitella käyttöönotto mahdollisimman huolellisesti.

Käytännössä työn aikana IPv6-protokolla otettiin käyttöön DNA:n matkaviestinverkon pakettirunkoverkkoon. Lisäksi IPv6-protokollaa testattiin loppukäyttäjän näkökulmasta. Loppukäyttäjien internetliikenteeseen ei saa aiheutua ongelmia käyttöönotosta..

2 Internet

Tässä luvussa käydään läpi ensin internetin historia ja perusperiaatteet. Seuraavaksi tarkastellaan IPv4-protokollaa ja tärkeimpiä siirtokerroksen protokollia kuten Transmission Control Protocol (TCP) ja User Datagram Protocol (UDP). Sen jälkeen käydään läpi osoitejärjestelmä ja lopuksi tutustutaan IPv6-protokollaan.

2.1 Historia

Internetin ja internetprotokollan on kehittänyt Defense Advanced Research Agency (DARPA) Yhdysvalloissa. Nykyään internetistä on tullut globaali verkko, joka yhdistää virtuaalisesti kaikki maat. Käyttäjiä verkossa on yli 2 miljardia. [1, s. 2.]

Kasvu pienestä tutkimusprojektista globaaliksi verkoksi on ollut nopeaa. DARPA-projekti aloitettiin 1960-luvun lopulla. Nykyisen Internetprotokollan versio 4 esiteltiin 1980-luvulla ja ensimmäiset internetpalveluntarjoajat aloittivat 1980-luvun lopulla. [1, s. 2.]

Internet on yhä merkittävämpi ja olennaisempi osa ihmisten jokapäiväistä arkea. Olemme koko ajan enemmän riippuvaisia Internetistä ja oletamme sen olevan käytettävissä kaikkialla. Internetistä on tullut osa kriittistä infrastruktuuria, kuten sähköstä ja vedestä.

2.2 Perusperiaatteet

Internet pohjautuu tiettyihin perusperiaatteisiin, jotka ovat mahdollistaneet sen suosion. Nämä perusperiaatteet ovat [1, s. 2]

- pakettikytkentäinen verkko
- päästä päähän periaate
- koostuu erilaisista kerroksista
- postelin laki
- luovaa anarkiaa.

2.2.1 Pakettikytkentäinen verkko

Aikaisemmin puheeseen keskittyneet verkot käyttivät piirikytkentäistä verkkoa, jossa puheelle varattiin aina oma yhteys (kapasiteetti) soittajalta toiselle riippumatta siitä, kuinka paljon puhetta yhteydessä siirrettiin. [1, s. 2-3.]

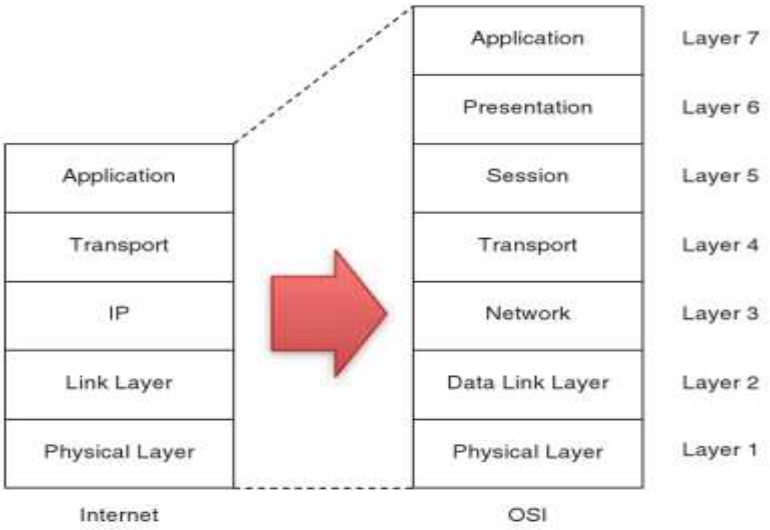
Nykyaikaiset pakettipohjaiset verkot pilkkovat datan pienempiin paketteihin, jotka matkustavat itsenäisesti niiden kohteisiin. Jokainen paketti lähetetään sillä hetkellä parasta reittiä pitkin kohteeseen. [1, s. 3.] Pakettiverkossa useampi yhteys voi jakaa saman kapasiteetin. Yksittäinen yhteys käyttää kapasiteettia vain siirtäessä tietoa. Pakettiverkossa onkin huolehdittava riittävästä palvelun laadusta tai kapasiteetista, tai muuten paketteja voi tippua, ja tiedonsiirto hidastuu tai voi jopa keskeytyä kokonaan.

2.2.2 Päästä päähän periaate

Päästä päähän -periaate on yksi tärkeimmistä internetin perusperiaatteista. Sen mukaan verkon ei pitäisi koskea verkkotasoa ylempiin kerroksiin. Verkon pitää keskittyä siirtämään tietoa lähteeltä kohteelle. Yhteyden aloitus- ja loppupään vastuulla on ymmärtää liikenne ja se kuinka sitä käytetään. Tämä periaate mahdollistaa uusien palveluiden tuomisen verkkoon ilman, että verkkoa täytyy muuttaa. [1, s. 3.]

2.2.3 Koostuu erilaisista kerroksista

Kerrosajattelun periaate on, että erilaiset protokollat voivat jutella toistensa kanssa samalla tasolla. Pääidea periaatteen takana on, että jokainen kerros tekee oman työnsä: ei enempää, ei vähempää. Tarkka erottelu kerrosten kesken mahdollistaa kerrosten muuttamisen ilman, että muita kerroksia tarvitsee muuttaa. Open System Interconnect (OSI) -malli määrittelee 7 kerrosta, mutta Internetin malli määrittelee vain viisi kerrosta. [1, s. 3.] Kuvassa 1 on kuvattuna, kuinka internetin 5 kerroksen malli eroaa OSI-mallista.



Kuva 1. Internet koostuu kerroksista. [1, s. 4.]

2.2.4 Postelin laki

Postelin laki, joka tunnetaan myös nimellä Postelin robustisuus-periaate, tarkoittaa, että ”ole liberaali siinä mitä sallit, mutta ole konservatiivinen siitä mitä lähetät” [2.]. Tämä tarkoittaa että kannattaa olla hyvin konservatiivinen ja tarkka mitä lähettää verkkoon, kun taas vastaanottajan pitäisi pystyä vastaanottamaan kaikki, mikä ei välttämättä olisikaan standardin mukaista. Tämä on hyvin tärkeä periaate, jotta tulevaisuuden laajennukset ja parannukset saadaan tehtyä. [1, s. 4.]

2.2.5 Luova anarkia

Viimeinen periaate, luova anarkia, on jotain, joka voi kuulostaa oudolta tietoliikenteessä. Tämä periaate tarkoittaa, että yksittäinen henkilö tai yritys pystyy luomaan ja levittämään uusia palveluita ja sovelluksia. Tämä periaate on ehkä muiden periaatteiden summa, mutta ilman tätä periaatetta internetpalvelut kuten Google tai Facebook eivät olisi voineet syntyä. [1, s. 4.]

2.3 Standardisointi, protokolla ja kehysrakenne

Internet Engineering Task Force (IETF) kehittää ja edistää Internetstandardeja. IETF on avoin standardointiorganisaatio, johon ei ole jäsenvaatimuksia. Kaikki osallistujat ovat vapaaehtoisia, ja yleensä heidän työnsä kustantaa työnantaja. [3.]

Nykyään laajasti käytössä oleva IPv4-protokolla perustuu vuonna 1981 uusittuun RFC791:een [4]. IPv4-kehys on normaalisti 20 oktettia pitkä, ja se koostuu 14 eri kentästä. Kuvassa 2 on esitetty IPv4-paketin kehysrakenne.

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Kuva 2. IPv4-paketin kehysrakenne. [5.]

2.4 Tärkeimmät siirtokerroksen protokollat

Transmission Control Protocol (TCP) [6] mahdollistaa luotettavan ja tietyssä järjestyksessä toimivan tiedonsiirron. TCP mahdollistaa myös palveluiden ja yhteyksien multipleksauksen sekä ruuhkanhallinnan. Multipleksaus tehdään lähde- ja kohdeportin avulla TCP-otsikkotiedoissa. Luotettavuus saavutetaan sillä, että vastaanottaja kuittaa paketteja, joita se on vastaanottanut. Tämän avulla lähettäjä saa tiedon, mitkä paketit puuttuvat vastaanottajalta. Tämän jälkeen lähettäjä lähettää puuttuvat paketit uudestaan. TCP:n ruuhkanhallinta-algoritmit seuraavat pakettien häviötä. TCP aina olettaa että pakettihäviö aiheutuu ruuhkasta ja tiputtaa yhteyden nopeutta. Tämän toiminnalisuuden takia TCP:tä on pidetty huonona protokollana langattomiin verkkoihin. Langattomissa verkoissa paketti voi hävitä muistakin syistä kuin ruuhkasta. Nykyään TCP:n ruuhkanhallinta-algoritmejä on kehitetty myös langattomien verkkojen näkökulmasta, joten tilanne on parantunut. Useat internetin sovellukset vaativat luotettavan tiedonsiir-

ron. TCP:tä käyttäviä sovelluksia on tiedoston siirto, videon suoratoisto ja nettiselaus. [1, s. 13.]

User Datagram Protocol (UDP) [7] on yksinkertainen protokolla. Se mahdollistaa palvelun ja yhteyden multipleksauksen sekä tarkistesumman vastaanottavaan päähän. Tarkistesummalla voidaan varmistua, ettei bittivirheitä ole tullut siirron aikana. Multipleksaus tehdään porttinumeroiden avulla UDP-kehyksessä. Kehyksessä on määritelty lähde- ja kohdeporteille omat kentät. UDP-protokolla ei takaa, että paketit on vastaanotettu oikeassa järjestyksessä, tai että ne ovat edes tulleet perille. UDP:ta käytetään yleensä latenssikriittisissä sovelluksissa, jossa pakettien häviäminen ei ole kriittistä. Sovelluksissa kuten Voice over IP (VoIP) voi olla parempi unohtaa paketti, kuin toimittaa se uudestaan liian myöhään. [1, s. 13.]

2.5 Osoitejärjestelmä

IPv4-protokolla käyttää 32-bittistä IP-osoiteavaruutta, joka tarkoittaa, että osoitteita on noin 4,3 miljardia (2^{32}). Erilaisia tekniikoita on kehitetty, jotta IPv4-osoitteet riittäisivät pidempään.

IETF julkaisi 1993 Classless Inter-Domain Routing (CIDR) [8] korvaamaan luokallisen reitityksen, jotta IP-osoiteavaruutta saataisiin pilkottua mahdollisimman tehokkaasti ja joustavasti käyttöön. IPv4-osoitetta voidaan ilmaista CIDR-notaatiolla, esim. 192.168.0.0/24, jossa viimeinen 24 luku kertoo merkitsevien bittien lukumäärän vasemmalta alkaen. Samaan osoitelohkoon kuuluvat siis 192.168.0.0 – 192.168.0.255 väliltä olevat osoitteet.

NAPT (Network Address Port Translation) [9] on toinen menetelmä, jonka avulla IPv4-osoiteavaruus on saatu riittämään pidempään. NAPT:ssa multipleksataan monta laitetta käyttämään samaa julkista IP-osoitetta. Yleensä NAPT:ssa käytetään RFC1918 IP-osoitteita sisäpuolella, ja sitten tilatietoisessa laitteessa käännetään monta RFC1918-osoitetta vastaamaan yhtä julkista IP-osoitetta. Menetelmän avulla säästyy julkisia IP-osoitteita. IP-osoitteiden lisäksi NAPT:ssa muutetaan myös porttitiedot siirtokerroksen protokollista kuten TCP ja UDP. NAPT kuitenkin rikkoo internetin päästä päähän -

periaattetta, koska yhden julkisen IP-osoitteen takana voi olla useampi laite. Jokainen internetiin liitetty laite pitäisi pystyä yksilöimään IP-osoitteen avulla.

2.6 IPv6-protokolla

IPv6-protokolla perustuu 1998 julkaistuun RFC2460 [10] määrittelyyn. Protokolla kehitettiin IPv4-osoitteiden riittämättömyyden takia. Siinä on 128-bittinen osoiteavaruus, jossa on noin $3,4 * 10^{38}$ uniikkia osoitetta. Osoitteet voidaan jakaa kolmeen eri pääkategoriaan, joita ovat unicast, anycast, ja multicast. Unicast-tyyppinen osoite identifioi yksittäisen rajapinnan yksittäisestä laitteesta. Anycast-osoite identifioi usean rajapinnan jotka ovat tyypillisesti eri rajapinnoissa. IPv6-paketti, joka lähetetään anycast-osoitteseen, toimitetaan verkon lähimpään anycast-osoitteen rajapintaan. Multicast-osoite identifioi yleensä joukon vastaanottajia. IPv6-paketti, joka lähetetään multicast-osoitteeseen, lähetetään kaikille multicast-ryhmään liittyneille vastaanottajille. [1, s. 81.]

Suositeltava tapa esittää IPv6-osoitetta on x:x:x:x:x:x:x:x, jossa jokainen x esittää 16-bittistä arvoa heksadesimaalimuodossa käyttäen pieniä kirjaimia. 16-bittinen arvo, joka esittää x:ää, voidaan esittää ilman alkavia nollia. Esimerkiksi 2001:14bb:0000:0000:0000:0000:0000:00a0 voidaan esittää lyhyemmässä muodossa 2001:14bb::a0. [1, s. 86.]

2.6.1 Kehysrakenne

IPv6:n kehystä on yksinkertaistettu IPv4:sta, jotta lähde ja kohdeosoitteille jäisi mahdollisimman paljon tilaa. Pääkehys on aina 40 tavun mittainen, joka eroaa IPv4:sta.

IPv6:n kehyksestä on jätetty pois otsikkotiedon koko, tunniste, liput, pirstaleen aloituskohta ja otsikkotiedon tarkistesumma. Optiot on siirretty laajennettuihin kehyksiin. Kuvassa 3 on esitelty IPv4:n ja IPv6:n kehysmallien erot.

Kuva 3. IPv4- ja IPv6-kehysten erot. [11]

IPv6-pakettien pilkkominen tapahtuu aina alkupäässä ja kasaaminen loppupäässä [1, s. 92]. Reitittimet eivät siis pirstaloi IPv6-paketteja, eli tämä eroaa IPv4-protokollasta, jossa reititinkin voi pirstaloida paketin. Mikäli pakettivuon varrella on yhteysväli, joka ei tue tarpeeksi suurta pakettikokoa, niin paketti tiputetaan ja lähettäjälle lähetetään ”paketti liian suuri”, ICMPv6-tyypin 2 viesti, jonka jälkeen lähettäjä saa tiedon, että yritti lähettää liian suurta pakettia ja pienentää pakettikokoa.

Alku- ja loppupään vastuulla on polun maksimipakettikoon tunnistaminen. IPv6-protokolla vaatii, että vähintään 1280 tavun kokoinen paketti pystytään lähettämään ilman pirstalointia. [1, s. 93.]

2.6.2 Laajennetut kehykset

IPv4-protokollasta tutut optiot ovat siirretty erillisiin kehyksiin, joita kutsutaan laajennetuiksi kehyksiksi. Laajennettuja kehyksiä voi ketjuttaa monta peräkkäin.

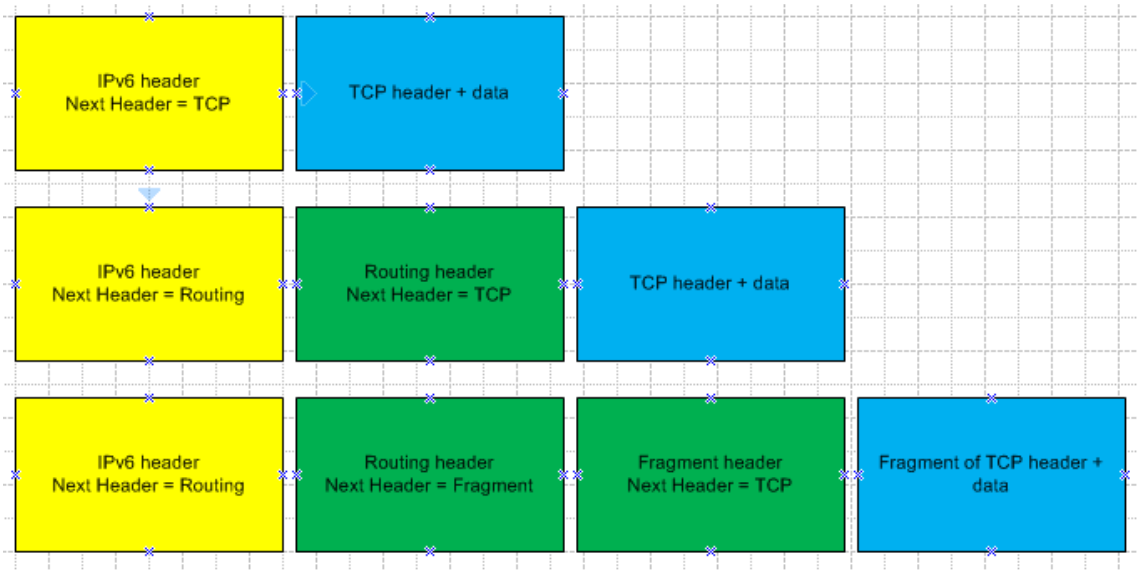
RFC2640 [10] määrittelee, että seuraavia laajennettuja kehyksiä kaikkien laitteiden on tuettava

- hop by hop -optiot
- destination-optioiden kehys
- reitityskehys
- pirstalointikehys

- authentication header (AH)
- encapsulating security payload (ESP).

Laajennettuja kehyksiä prosessoidaan eri paikoissa, riippuen tyypistä ja ne on asetettava tietyssä järjestyksessä. Esimerkiksi hop by hop -optio pitää olla heti IPv6-kehyksen jälkeen, koska se on prosessoitava kaikissa reitittimissä.

Kuva 4 havainnollistaa, kuinka erilaisia kehyksiä voi ketjuttaa.



Kuva 4. Esimerkki kuinka laajennettuja kehyksiä voidaan ketjuttaa. Laajennetut kehykset ovat merkitty vihreällä värillä.

Yksittäistä laajennettua kehystyyppiä saa olla vain yksi lukuun ottamatta Destination optiot kehystä, joka saa esiintyä kaksi kertaa (ennen reitityskehystä ja juuri ennen ylemmän tason kehystä).

Reitityskehyksen idea oli, että lähettäjä voisi vaikuttaa minkä laitteiden kautta paketti kiertää. Reitityskehyksen tyyppi 0 poistettiin IETF:n toimesta käytöstä, koska siitä löytyi haavoittuvuus, jonka kautta pystyi luomaan palvelunestohyökkäyksiä. Reitityskehyksen tyyppi 0 odotetaan poistuvan IPv6-pinoista ja sitä myös tiputetaan joissain verkoissa, jotta hyökkäykset voidaan pysäyttää. [1,s. 92.]

Pirstalointikehystä käytetään, kun IPv6-paketteja lähettävä laite lähettää suuremman paketin kuin lähteen ja kohteen välisen polun maksimipakettikoko (MTU) on. Lähettävä laite aina lisää kehyksen, koska pirstalointia ei tapahdu polun varrella. Pirstalointikehyksestä löytyy tunnistetieto, jolla identifioidaan, mihin pakettiin se kuuluu. Pirstaleen osoittimella indikoidaan mikä kohta alkuperäisestä paketista löytyy. [1, s. 92.]

2.6.3 Internet Control Message Protocol v6 ja Neighbor Discovery Protocol

Yksi tärkeä IPv6-protokollaperheestä on ICMPv6 [29]. ICMPv6 voidaan tuntea parhaiten ”pingauksesta”. Sen avulla voidaan tunnistaa toisen laitteen tavoitettavuus ICMPv6 Echo Request ja Echo Reply -viestien avulla. ICMPv6-viestit voidaan jakaa kahteen eri luokkaan: virheviesteihin ja informatiivisiin viesteihin. Virheviestejä ovat muun muassa: Destination unreachable, Packet Too Big, Time Exceeded ja Parameter Problem. Informatiivisia viestejä ovat Echo Request ja Echo Reply -viestit. [1, s. 97-98.]

Reititin tai kohdejärjestelmä lähettää Destination Unreachable -virheviestin paketin lähettäjälle, jos esimerkiksi sillä ei ole reititystaulussa kohdeverkkoa tai yhteys kohdeosoitteen kanssa ei ole sallittu. Reititin lähettää Packet Too Big -virheviestin paketin lähettäjälle, mikäli sillä on käsiteltävänä liian iso paketti, joka ei enää mahdu seuraavalle linkille. Tiedon avulla lähettäjä pienentää pakettikokoa. Time Exceeded -virheviesti lähetetään paketin lähettäjälle kun paketin Hop Limit piennetään nollaan. Se voi tapahtua muun muassa väärästä määrittelystä tai reitityssilmukasta. Traceroute on yksi sovellus, joka hyödyntää Time Exceeded -virheviestejä. Reititin voi lähettää Time Exceeded -virheviestin myös jos pirstalointipaketin kokoaminen epäonnistuu. Parameter Problem -virheviesti lähetetään paketin lähettäjälle mikäli reititin tai kohdejärjestelmä ei pysty prosessoimaan kehystä tai laajennettuja kehystä. [1, s. 98-100.]

IPv6-protokollan ICMPv6 on huomattavasti merkittävämmässä roolissa kuin IPv4:n ICMPv4. Tämä johtuu siitä että IPv6:n Network Discovery Protocol perustuu ICMPv6:een. ICMPv6:ssa ei ole uudelleenlähetysmekanismia hävinneille paketeille, joten esimerkiksi ICMPv6 virheviestit eivät välttämättä tule perille, vaikka niitä olisi lähetetty. Protokolliin jotka hyödyntävät ICMPv6:sta, on monesti implementoitu uudelleenlähetykset, kuten Neighbor Discovery Protocollaan (NDP). [1, s. 97-98.]

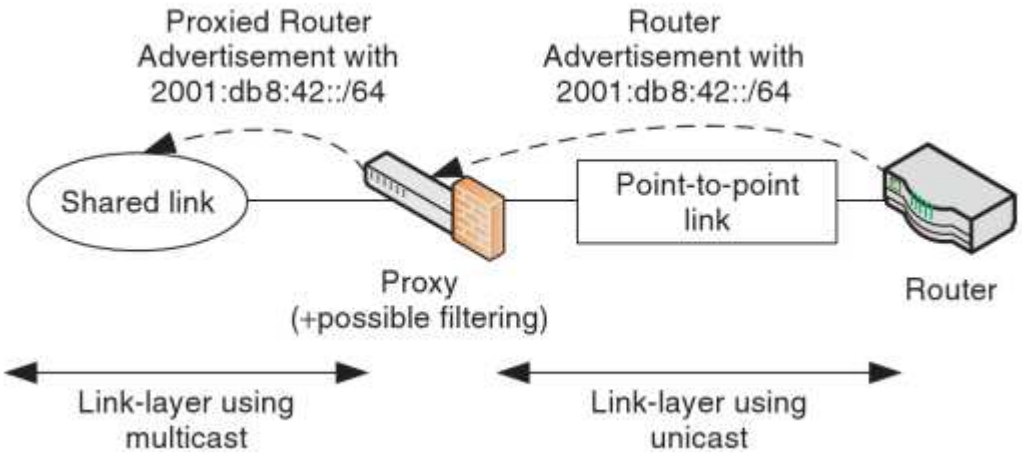
IPv6 Neighbor Discovery Protocollaa (NDP) käytetään löytämään toisia laitteita ja reitittimiä, jotka ovat samalla linkillä. IPv4:ssa käytetyn Address Resolution Protocollan (ARP) tehtävät on siirretty IPv6:ssa NDP:n. Sen avulla voidaan selvittää IPv6-osoitteen linkkitason osoite. NDP:tä hyödyntäen isäntäkone voi saada tiedon oletusyhdyskäytävästä ja mahdollisesti DNS-kääntönimipalvelimista. NDP käyttää viittä erilaista pakettityyppiä. [1, s. 101.]

- Router solicitation: Laite voi lähettää multicastin avulla ”Router Solicitation” -viestin linkille, indikoidakseen reitittimille, että lähettäkää ”Router Advertisement” -viesti nopeammin [1, s. 101].
- Router advertisement: Reititin lähettää ”Router Advertisement” -viestin tietyn ajan jakoissa, tai sen jälkeen kun se on vastaanottanut ”Router Solicitation” -viestin. Viesti sisältää useita IPv6:een liittyviä parametreja kuten oletusyhdyskäytävä ja IPv6-osoite laitteelle itselleen. [1, s. 101.]
- Neighbor solicitation: Laite käyttää ”Neighbor Solicitation” -viestiä löytääkseen naapurin linkkitason (L2-tason) osoitteen [1, s. 101].
- Neighbor advertisement: Laite lähettää “Neighbor Advertisement” -viestin vastauksena “Neighbor Solicitation” -viestiin tai kertoakseen muutoksista linkkitason (L2-tason) osoitteisiin [1, s. 101].
- Redirect: Reititin voi lähettää ”Redirect” -viestin kun parempi reititin on saatavilla kun tällä hetkellä käytetty reititin [1, s. 101].

IPv6-laitteet tarkkailevat naapuruuksien tavoitettavuutta. Tavoitettavuuden tilatieto voidaan päivittää mikäli IPv6-kommunikointi onnistuu, mutta jos IPv6-kommunikointi ei onnistu, niin laite voi käyttää Neighbor Unreachability Detection (NUD) proseduuria tarkistaakseen onko naapuri vielä tavoitettavissa. Toinen NDP-protokollan proseduuri on Duplicate Address Detection (DAD), jonka avulla estetään osoitekolarit. [1, s. 105-106.]

On havaittu että hyökkääjät voivat käyttää Neighbor Discovery (ND) -proseduuria palvelunestohyökkäyksien muodostamiseen. Hyökkääjä voi yrittää saada verkkolaitteen naapuripuskuria täyteen tai aiheuttaa häiriöitä ND-proseduuriin. Hyökkäys perustuu siihen, että verkkolaitteella on 64-bittinen prefiksi ja hyökkääjä lähettää paketteja useisiin kohdeosoitteisiin ja reititin yrittää löytää kohdeosoitteille linkkitason osoitteita ennen kuin voisi lähettää paketteja niihin. Koska kohdeosoitteita ei ole olemassa, niin reitittimen naapuripuskuri voi tulla täyteen. [1, s. 105.]

Voi olla verkkotopologioita, joissa IPv6-laitteet ovat samalla loogisella linkillä, mutta eivät ole fyysisesti samalla linkillä. Hyvä esimerkki tästä on että keskuslaite on kahden erilaisen linkkityypin välissä, kuten jaetun linkin ja point-to-point-linkin. Tällöin laitteet jaetulla linkillä kyllä kuulevat toisensa, mutta eivät point-to-point linkin takana olevaa laitetta. Tavallinen siltaus kahden erityyppisen linkkityypin välillä ei onnistu. Jotta saadaan helpotettua kommunikointia laitteiden välillä, jotka eivät suoraan kuule toisiaan, on kehitetty NDP-välityspalvelu (proxy) -toiminne. NDP-välityspalvelutoiminne tarkoittaa että laite kuuntelee multicast-liikennettä ja valikoidusti uudelleen lähettää sitä toiselle linkille. Uudelleen lähetettäviä viestejä on neljä: ICMPv6 Router Advertisement, Redirects, Neighbor Advertisement, ja Neighbor Solicitation. Neljä uudelleen lähetettävää viestiä sisältää myös linkkitason osoitteita, joten ne on myös muutettava jotta liikenne toimii. NDP-välityspalvelun suuri hyöty on siinä, ettei tarvitse tehdä IPv6 Network Address Translationia (NAT) tai tukea Dynamic Host Configuration Protocol v6 prefiksin delegointia (DHCPv6-PD). [1, s. 108-109.] Kuvassa 5 on havainnollistettu NDP-välityspalvelun toiminta.

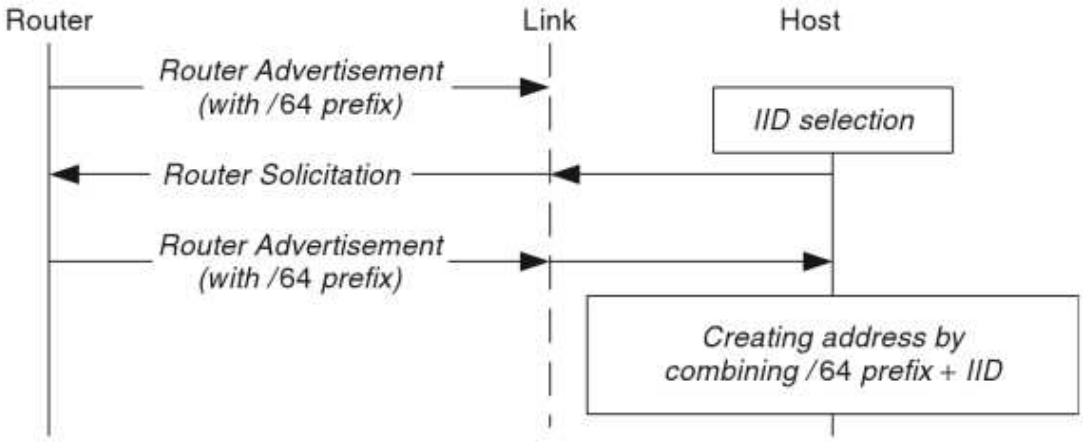


Kuva 5. NDP-välityspalvelun toimintaperiaate. [1, s. 108.]

2.6.4 Stateless Address Configuration

Stateless Address Configuration (SLAAC) perustuu IPv6 Neighbor Discovery Protokollaan. IPv6:n päämekanismi numeroimaan laitteet onkin SLAAC. Tilatiedoton lähestyminen on aina vaadittu link local -osoitteiden määrittelyyn, ja se on kevyempi proseduuri kuin Dynamic Host Configuration Protocol v6 (DHCPv6). SLAAC täytyy olla tuet-

tuna kaikissa IPv6 isäntäkoneissa. Kun isäntäkone yhdistää verkkoon, se ensin valitsee Interface ID:n (IID), sitten se tekee Duplicate Address Detetection (DAD) -proseduurin, jonka jälkeen isäntäkone lähettää Router Solicitation -viestin, jotta se nopeuttaa reitittimen lähettämää Router Advertisement -viestiä. Kun isäntäkone vastaanottaa Router Advertisement -viestin, jossa on IPv6-prefiksi, se yhdistää aikaisemmin luodun IID:n siihen, josta tulee isäntäkoneen IPv6-osoite. Tämän jälkeen isäntäkone voi määrittää /128 IPv6-osoitteen itselleen ja käyttää sitä kommunikointiin. [1, s. 110.] Kuvassa 6 on havainnollistettu SLAAC-proseduuri.



Kuva 6. SLAAC-proseduurin toimintaperiaate. [1, s. 110.]

3 Matkaviestinverkko

Tässä luvussa esitellään aluksi matkaviestinverkkojen eri sukupolvet, sitten standardisointi ja lopuksi verkkoarkkitehtuuri. Tarkoituksena on kuvata matkaviestinverkkojen toiminnan perusperiaatteet.

3.1 Matkaviestinverkkojen eri sukupolvet

Matkaviestinverkko on langaton verkko, joka on hajautettu eri soluihin. Tukiasema lähettää ja vastaanottaa radiosignaaleja päätelaitteilta. Matkapuhelinverkon avulla voi-

daan tuottaa loppuasiakkaille palveluita kuten puhepalvelu, tekstiviestipalvelu, mobiilidatapalvelu (internet-yhteys) ja MMS-kuvapalvelu.

Matkaviestinverkkojen tekniikat voidaan jakaa neljään eri sukupolveen.

- 1G - Ensimmäinen sukupolvi. Analogiset matkapuhelintekniikat kuten Pohjoismaissa käytetty Nordic Mobile Telephone (NMT) -järjestelmä ja Yhdysvalloissa käytetty Advanced Mobile Phone System (AMPS) -järjestelmä [15].

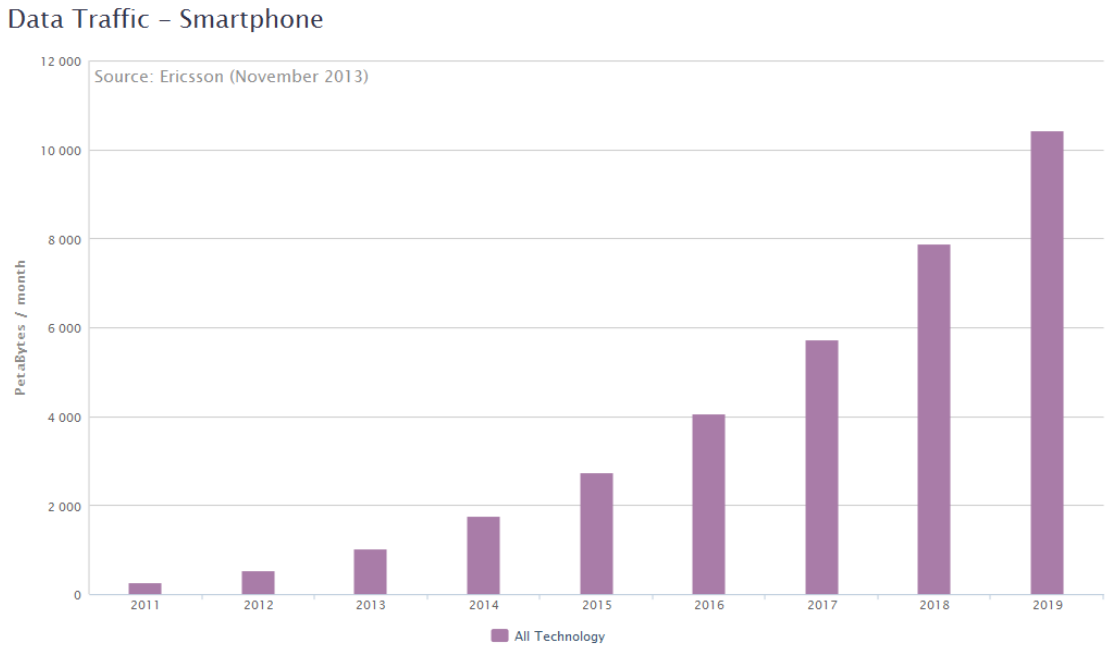
- 2G – Toinen sukupolvi. Ensimmäiset digitaaliset matkapuhelintekniikat kuten eurooppalainen Global System for Mobile Communications (GSM) -järjestelmä ja Yhdysvalloissa käytetty Code Division Multiple Access (CDMA) pohjainen Interim Standard 95 (IS-95) -järjestelmä [16].

- 3G – Kolmas sukupolvi. Euroopassa, Japanissa ja Kiinassa käytetty Universal Mobile Telecommunications System (UMTS) -järjestelmä sekä Yhdysvalloissa ja Etelä-Koreassa käytetty Code Division Multiple Access 2000 (CDMA2000) -järjestelmä [17].

- 4G – Neljäs sukupolvi. Long Term Evolution (LTE) ei vielä täytä IMT Advanced -ohjelman vaatimuksia, vaikka sitä markkinoidaan 4G-tekniikkana. LTE Advanced ja WiMAX Release 2 täyttävät vaatimukset. Vaatimuksissa on määritelty, että siirtonopeus verkosta päätelaitteelle täytyy olla 1 Gbit/s paikallaan ja 100 Mbps liikkuessa [18].

Ensimmäinen pakettipohjainen tiedonsiirtopalvelu esiteltiin toisen sukupolven matkaviestiverkkotekniikassa. Tiedonsiirtopalvelua kutsutaan General Packet Radio Serviceksi (GPRS).

Ericsson on ennustanut, että matkapuhelimien käyttämä mobiilidataliikenne kuusinkertaistuu vuodesta 2014 vuoteen 2019 mennessä. Kuvassa 7 on pylväsdiagrammi matkapuhelinten mobiilidatan kasvun ennusteesta.



Kuva 7. Ericssonin ennuste matkapuhelimien mobiilidatan kasvusta. [12.]

3.2 Standardisointi

3rd Generation Partnership project (3GPP) yhdistää kuusi eri telekommunikaatiostandardisointiorganisaatiosta, joita kutsutaan organisaatiollisiksi partnereiksi. 3GPP:n tehtävänä on toimittaa jäsenilleen stabiilin ympäristön tuottaa korkealaatuisia spesifikaatioita, jotka määrittelevät 3GPP-teknologiat. [13.]

Alun perin 3GPP perustettiin määrittelemään globaali 3G-matkapuhelinverkkostandardi, mutta sen laajuutta on myöhemmin lisätty kattamaan myös mm. GSM-järjestelmä ja LTE-järjestelmä.

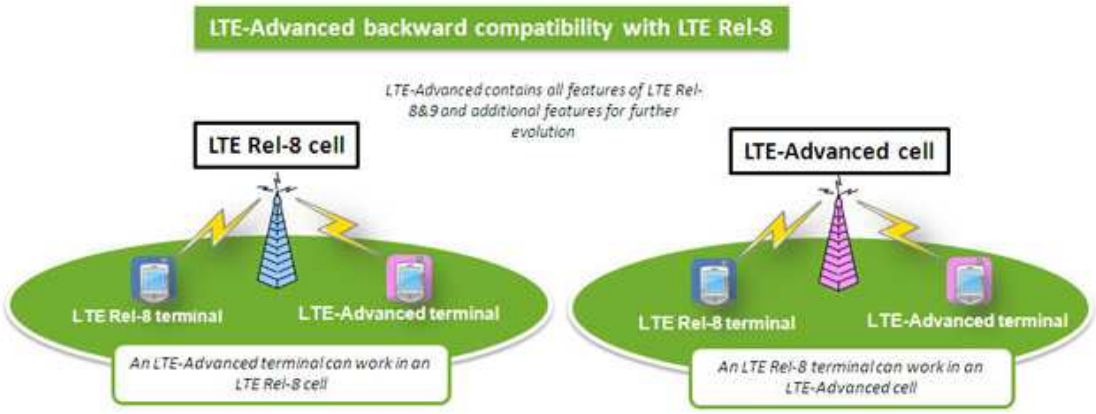
Standardisointitoiminta on jaettu neljään tekniseen määrittelyryhmään (Technical Specification Group). [13.]

- Radio Access Networks (RAN)
  - Kehittää 3G- ja siitä ylöspäin olevia radioverkkostandardeja.
- GSM EDGE Radio Access Networks (GERAN).

- Kehittää GSM ja Enhanced Data rates for Global Evolution (EDGE) – radioverkkostandardeja.

- Service & System Aspects (SA)
  - On vastuussa kokonaisarkkitehtuurista ja palveluista.
- Core Network & Terminals (CT)
  - Kehittää runkoverkkostandardeja ja terminaalien standardeja.

Päämääränä kaikille 3GPP-julkaisuille on tuottaa taaksepäin ja eteenpäin yhteensopivia standardeita aina, kun mahdollista, jotta loppukäyttäjän päätelaitteet toimivat mahdollisimman hyvin. Hyvä esimerkki tästä periaatteesta on, että LTE advanced terminaalit toimivat LTE-verkossa ja toisinpäin, kuten kuva 8 osoittaa [11].



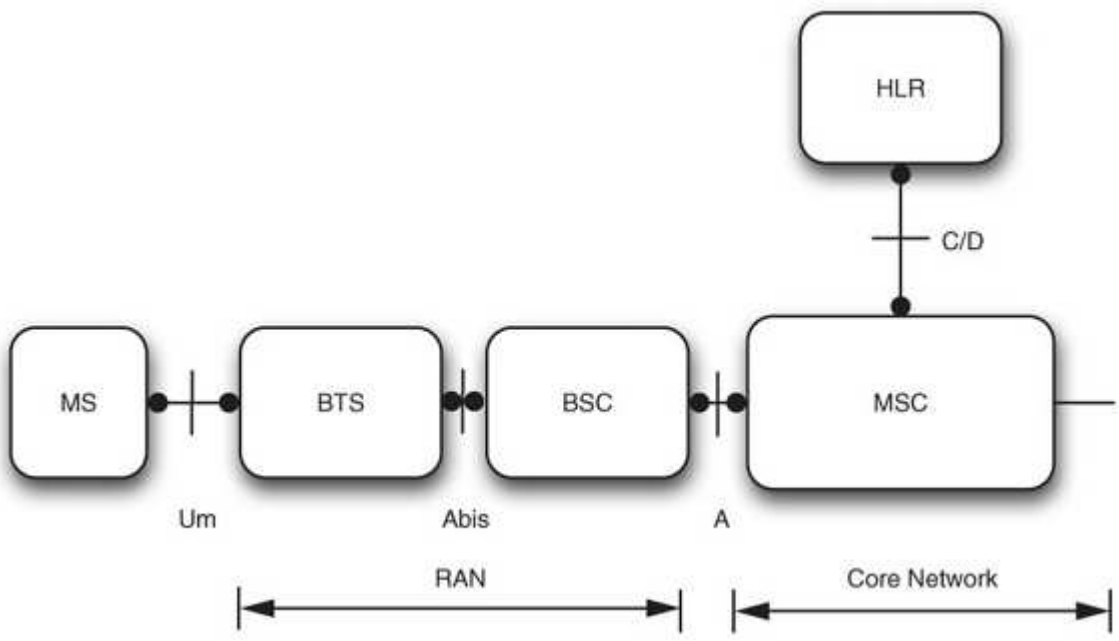
Kuva 8. Kuva osoittaa, että LTE advanced terminaali toimii myös LTE Rel-8 verkossa. [11.]

3.3 Verkkoarkkitehtuuri

Seuraavissa luvuissa esitellään ensin GSM-järjestelmä, sitten GPRS-arkkitehtuuri ja GPRS-arkkituuri 3G-verkossa. Sen jälkeen esitellään Evolved Packet System (EPS) -arkkitehtuuri.

3.3.1 GSM-järjestelmä

GSM-järjestelmä, joka esiteltiin 90-luvun alussa, oli ensimmäinen digitaalinen matkapuhelinjärjestelmä ja jota käytettiin laajasti. GSM:ssä käytetään Time Division Multiple Access (TDMA) pohjaista radioteknologiaa [1, s. 34]. 90-luvun alussa matkapuhelinverkon datan siirto oli vielä piirikytkentäistä. Kuvassa 9 on esitelty GSM-järjestelmän elementit ja niiden rajapinnat.



Kuva 9. Piirikytkennäisen GSM-järjestelmän verkkoarkkitehtuuri. [1, s. 35.]

GSM-verkkoarkkitehtuurin elementit listattuna [1, s. 35]

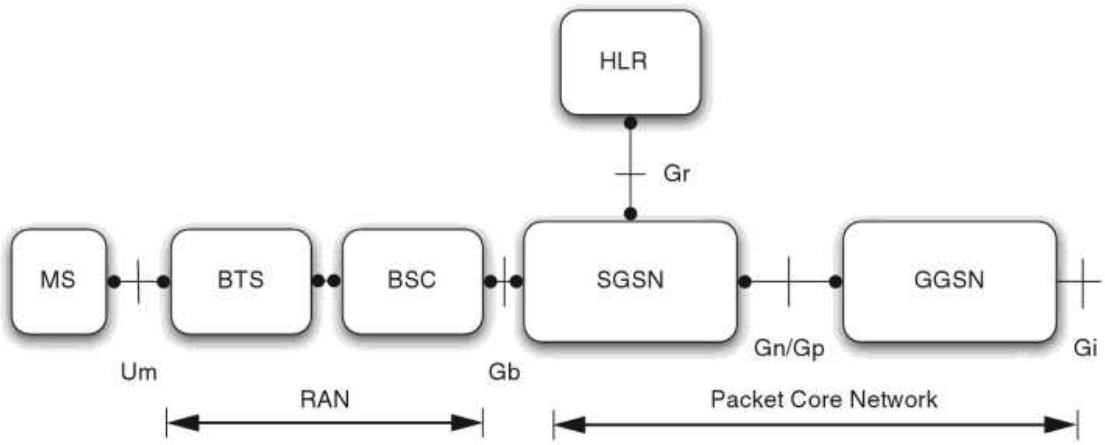
- Mobile Station (MS), eli puhelin tai joku muu laite, joka on kytketty verkkoon.
- Base Transceiver Station (BTS), eli 2G-tukiasema. Radioverkon elementti joka on suoraan yhteydessä MS:ään radiorajapinnan avulla.
- Base Station Controller (BSC), eli 2G-tukiasemaohjain voi hallita satoja tai tuhansia 2G-tukiasemia. Se koordinoi mm. tilaajan mobiliteetin tukiasemien välillä, niin ettei esim. puhelu katkea, kun tilaaja liikkuu tukiasemasta toiseen.

- Mobile Switching Center (MSC), hoitaa tilaajien autentikoinin, mobiliteettin hallinnan ja puheluiden kytkennän.
- Home Location Register (HLR) on tietokanta, jossa tilaajatiedot sijaitsevat. Tilaajatiedot sisältävät autentikointidatan, jota vasten tilaaja autentikoidaan. Tilaajatieto sisältää myös, mihin palveluihin tilaajalla on oikeudet ja paikkatiedon, missä tilaaja on.

3.3.2 2G General Packet Radio Service (GPRS)

Pakettipohjainen tiedonsiirtopalvelu (GPRS) esiteltiin aluksi GSM-verkkoihin vuonna 1997. Release 97:ssa julkaistu GPRS-tiedonsiirtopalvelun siirtonopeus oli tyypillisesti 40 Kbps verkosta tilaajalle päin ja 14 Kbps tilaajalta verkkoon päin [19].

Enhanced Data rates for Global Evolution tai Enhanced GPRS:ksi kutsuttu EDGE-teknologia mahdollisti 384 Kbps siirtonopeuden verkosta tilaajalle päin ja 384 Kbps tilaajalta verkkoon päin [19]. Kuvassa 10 on esitetty 2G GPRS -verkon arkkitehtuuri.



Kuva 10. 2G GPRS-verkkoarkkitehtuuri. [1, s. 36.]

GPRS käyttää pääosin samoja radioverkon elementtejä, joita GSM-järjestelmäkin, mutta runkoverkossa on MSC:n tilalla Serving GPRS Supporting Node (SGSN) ja Gateway GPRS Supporting Node (GGSN).

SGSN hoitaa pääasiallisesti tilaajan autentikoinnin, valtuuttamisen ja mobiliteetin hallinnoimisen. SGSN vastaa pääosin mobiilipakettiverkon signaloinnista (control-plane), mutta se välittää myös loppukäyttäjän (user-plane) liikennettä. Loppukäyttäjän lähettä-

mässä liikenteessä SGSN on ensimmäinen laite, joka näkee MS:n lähettämän IP-paketin. SGSN on myös yhteydessä Roaming-kumppaneiden GGSN:iin Gp-rajapinnalla [1, s. 36].

GGSN on topologinen ankkurointipiste mobiliteetin hallinnalle GPRS-verkossa. Tilaajan liikkuessa kaikki muut matkaviestinverkon elemetit saattavat vaihtua, mutta GGSN pysyy samana koko yhteyden ajan. Se on yhdyskäytävä GPRS-verkon ja ulkoisen verkon välillä (kuten esim. Internet). Kuten SGSN, myös GGSN hoitaa tilaajan signalointia sekä välittää loppukäyttäjän liikennettä. Tilaaja saa IP-osoitteen GGSN:stä, ja se generoi myös laskutustietoja [1, s. 37].

Tärkeimmät rajapinnat ja niiden kuvaukset

- Gb-rajapinta on rajapinta BSC:n ja SGSN:n välillä. Rajapinnassa kulkee sekä control-plane että user-plane liikennettä.
- Gn/Gp-rajapinta on SGSN:n ja GGSN välillä. Gn-rajapintaa käytetään, kun käyttäjä on kotiverkossa (käyttää kotiverkon SGSN:ää). Gp-rajapintaa käytetään kun käyttäjä on toisen operaattorin verkossa (käyttää toisen operaattorin SGSN:ää), mutta kotiverkon GGSN:ää.
- Gr-rajapinta on SGSN:n ja HLR:n välillä. Tilaajatiedot haetaan tätä rajapintaa pitkin.
- Gi-rajapinta yhdistää GPRS-verkon ulkoisiin IP-verkkoihin.

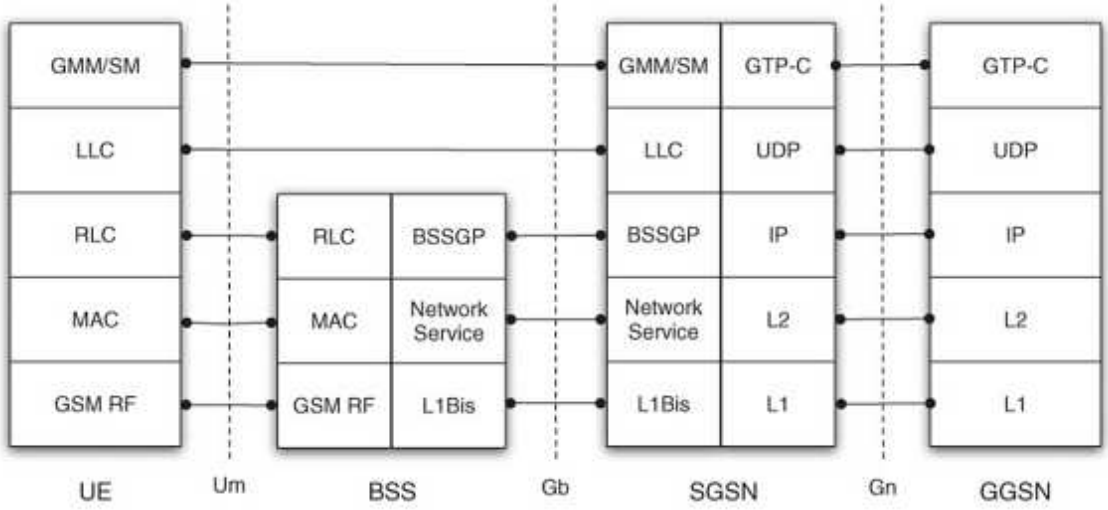
3.3.3 2G GPRS -protokollat

IP:n kannalta tärkeimmät user-plane-protokollat ovat Sub Network Dependent Convergence Protocol (SNDCP) ja GPRS Tunnel Protocol (GTP).

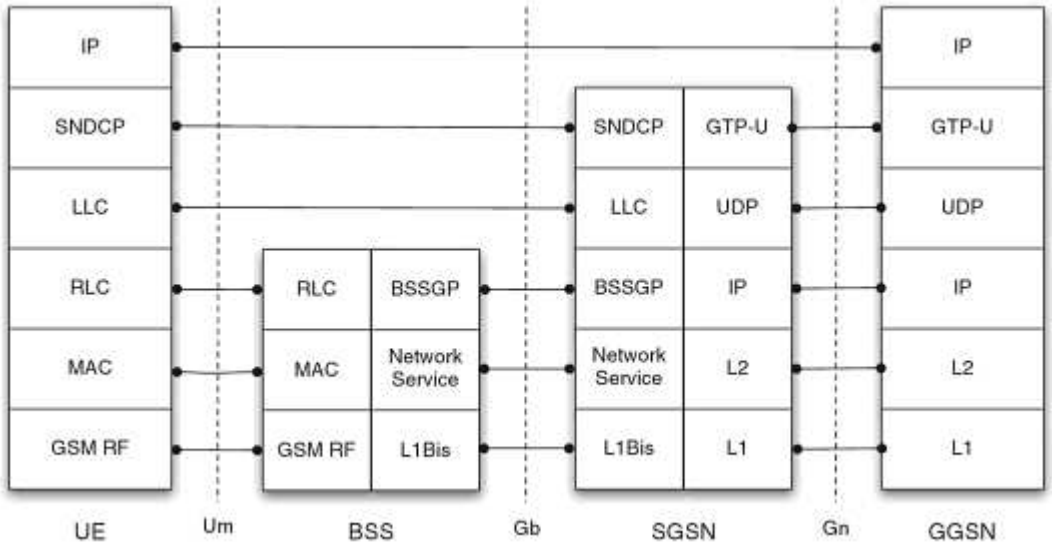
SNDCP on protokolla, joka kuljettaa IP-paketit GSM-radioverkon ylitse. SNDCP:n vastuulla on multipleksata useampi Packet Data Protocol (PDP) -konteksti päätelaitteen ja SGSN:n välillä. Se hoitaa otsikkotietojen pakkauksen, pakettien segmentoinnin, uudelleenkokoamisen sekä sisällön pakkauksen. SNDCP-protokolla voi kuljettaa IPv4-, IPv6- ja PPP-paketteja [1, s. 38].

GPRS Tunnel Protocol User Plane (GTP-U) on vastuussa IP-pakettien kuljetuksesta GPRS core -verkon sisällä. GTP:n perusidea on tunnistaa Tunnel Endpoint ID:n (TEID) perusteella, mihin PDP-kontekstiin paketit kuuluvat [1, s. 38].

GPRS Tunnel Protocol Control Plane (GTP-C) on signalointiprotokolla SGSN:n ja GGSN:n välissä. PDP-kontekstin avauspyynnöt, muutospyynnöt ja lopetuspyynnöt kulkevat GTP-C protokollan avulla SGSN:n ja GGSN:n välillä. Kuvassa 11 on esitelty 2G GPRS control-plane-protokollapino. Kuvassa 12 on esitelty 2G user-plane-protokollapino.



Kuva 11. 2G GPRS control-plane-protokollat. [1, s. 103.]



Kuva 12. 2G GPRS user-plane-protokollat. [1, s. 102.]

3.3.4 UMTS ja 3G GPRS

UMTS julkaistiin 3GPP release 99:ssä vuonna 2000 [20]. UMTS perustuu uudempaan radioteknologiaan, jota kutsutaan Wideband Code Division Multiple Access (WCDMA):ksi. 3GPP määritteli sen nimeksi UMTS Terrestial Radio Network (UTRAN) [21].

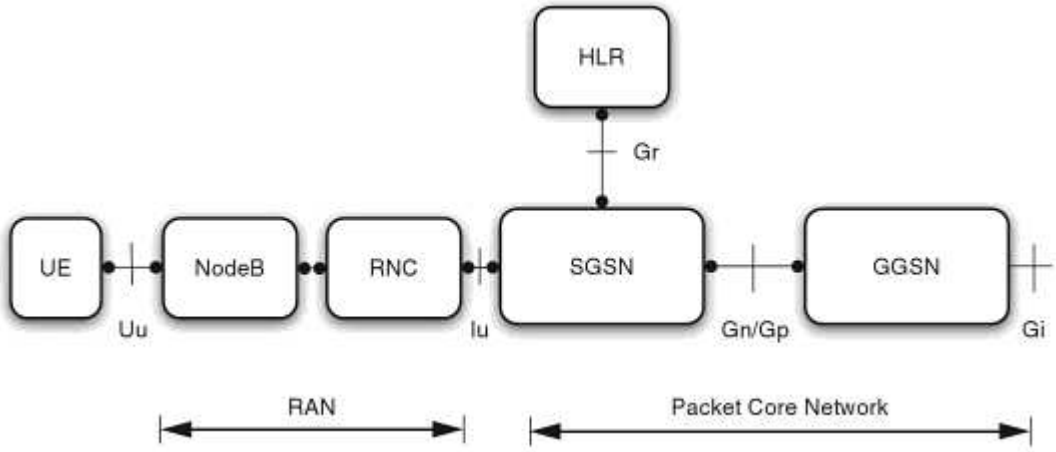
Alkuperäisen UMTS:n siirtonopeus oli 384 Kbps verkosta tilaajalle päin ja 384 Kbps tilaajalta verkkoon päin. Ensimmäinen vaiheen High Speed Download Packet Access (HSDPA):n spesifikaatio julkaistiin 3GPP release 5:ssa. Verkosta päätelaitteelle päin maksiminopeus nousi 14 Mbps:ään [22].

High Speed Upload Packet Accses (HSUPA):n spesifikaatio julkaistiin 3GPP Release 6:ssa, joka mahdollistaa 5,74 Mbps nopeuden päätelaitteelta verkkoon päin [22].

HSDPA:n toinen vaihe määriteltiin 3GPP release 7:ssa, joka mahdollistaa kahden 5 Mhz taajuuskaistan yhdistämisen. Teoreettinen maksiminopeus 2x5 MHz:n kaistalla on 42 Mbps verkosta päätelaitteelle [22].

3G GPRS perustuu samaan arkkitehtuurin kuin 2G GPRS:kin, mutta radioverkon elementit ovat vaihtuneet 2G-tukiaseman (BTS) korvaa 3G-tukiasema (NodeB) ja 2G-tukiasemaohjaimen (BSC) korvaa 3G-verkon tukiasemaohjain (RNC). [1, s. 40.]

SGSN:n ja GGSN:n välinen Gn-rajapinta pysyy samanlaisena, mutta SGSN:n ja tukiasemaohjaimen välinen protokollapino on täysin erilainen. 2G-verkossa SGSN terminoi radioprotokollapinot, kun taas 3G-verkossa tukiasemaohjain terminoi ne. Mobile Stationin nimi on myös muutettu User Equipmentiksi (UE). Kuvassa 13 on esitelty 3G GPRS-arkkitehtuuri [1, s. 40].



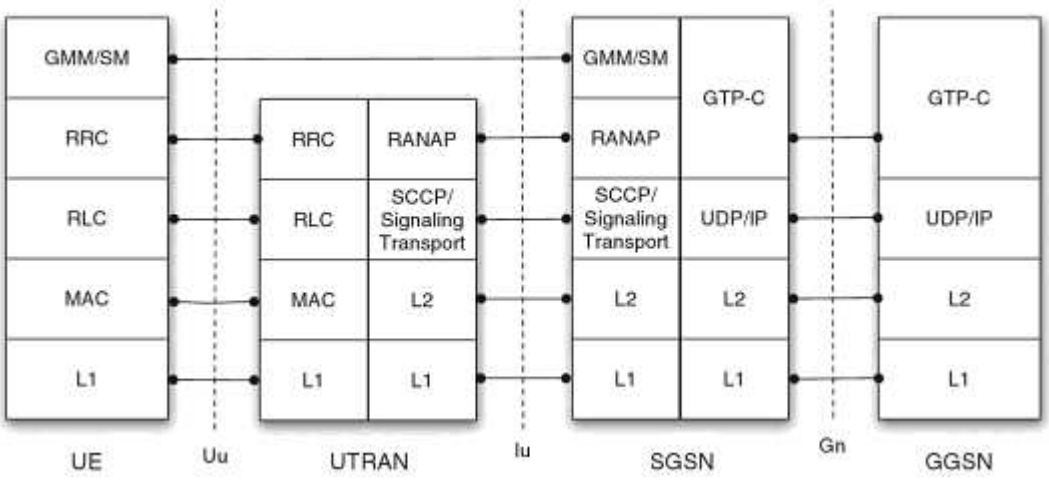
Kuva 13. 3G GPRS-verkkoarkkitehtuuri. [1, s. 39.]

3.3.5 3G GPRS-protokollat

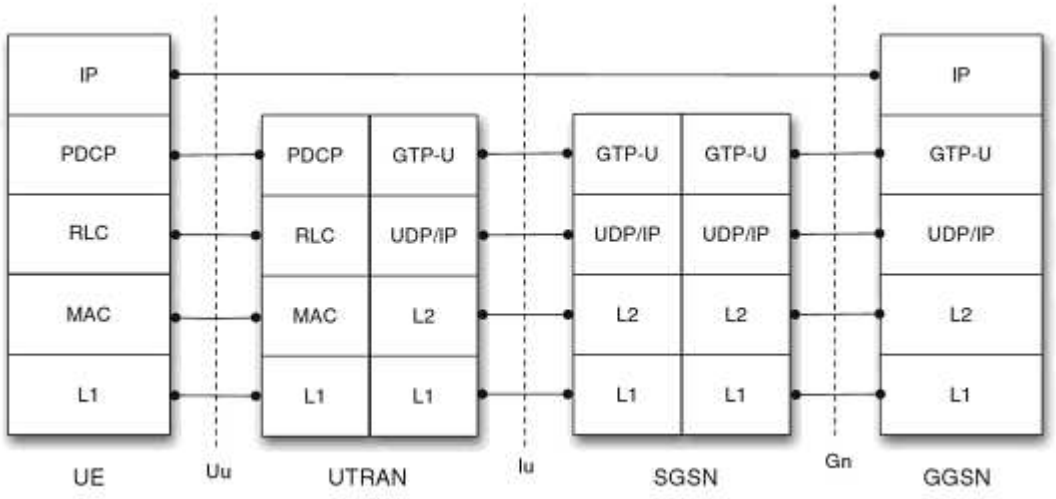
Merkittävin muutos 2G-protokolliin on se että SGSN:n ja 3G-tukiasemaohjaimen välisessä Iu-rajapinnan user-plane-protokolla on muuttunut GTP-pohjaiseksi. Iu-rajapinnan control-plane-protokolla on Signaling System no. 7 (SS7) -pohjainen Radio Access Network Application Part (RANAP). Alemman tason control-plane-protokolla on Signaling Connection Control Part (SCCP), joka on myös SS7-pohjainen [1, s. 40].

3G-tukiasemaohjaimeen on myös tullut yksi uusi protokollataso. Aikaisemmin päätelaitteen ja SGSN:n välillä ollut SNDCP on vaihtunut Packet Data Convergence Protocol (PDCP):ksi. PDCP on päätelaitteen ja 3G-tukiasemaohjaimen (RNC) välllä [1, s. 40].

PDCP:n tehtävänä on siirtää paketit radio-rajapinnan yli, hoitaa otsikkotietojen pakkaus, segmentointi ja uudelleenkokoaminen. Alemman tason Radio Link Control (RLC) yhdistää PDP-kontekstitason Radio Access Beareriin (RAB). 2G-verkossa olleet SNDCP-tason tehtävät on jaettu kahdelle protokolalle: PDCP ja RLC. GTP-U ja GTP-C protokolla toimii kuten 2G-verkossa [1, s. 55]. Kuvassa 14 on control-plane-protokollapino ja kuvassa 15 on esitelty user-plane-protokollapino.



Kuva 14. 3G GPRS control-plane-protokollat. [1, s. 41.]



Kuva 15. 3G GPRS user-plane-protokollat. [1, s. 40.]

3.3.6 Evolved Packet System (EPS)

EPS koostuu kahdesta osasta: radioliittyntäverkosta (LTE) ja pakettirunkoverkosta (Evolved Packet Core, EPC). EPS:n määritelmä julkaistiin vuonna 2008 3GPP release 8:ssa. EPS:n kehityksen motivaationa oli

- yksinkertaisempi arkkitehtuuri
- käyttäjien vaatima lisäkapasiteetin tarve
- kustannustehokkaampi
- tehokkaampi radiotaajuuksien käyttö
- pakettien välitykseen optimoitu verkko.

LTE:tä kutsutaan myös Evolved Universal Terrestial Access Network:ksi (E-UTRAN). LTE julkaistiin 3GPP release 8:ssa vuonna 2008. Sen markkinointinimi on 4G LTE.

LTE:ssä käytetään Orthogonal Frequency Division Multiple Access (OFDMA) -modulaatiota myötäsuunnassa. Paluusuunnassa käytetään Single Carrier - Frequency Division Multiple Access (SC-FDMA) modulaatiota [23].

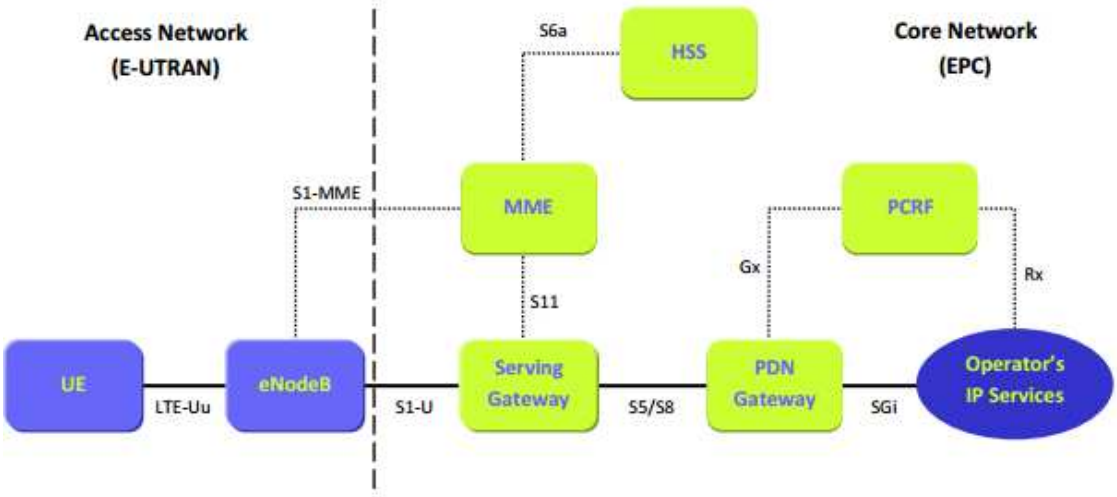
LTE-tekniikassa on joustava kaistanleveys. Siinä voidaan käyttää 1,4 MHz:n, 3 MHz:n, 5 MHz:n, 10 MHz:n, 15 MHz:n tai 20 MHz:n levyistä kaistaa. LTE on kehitetty tukemaan taajuusjakoista (FDD) ja aikajakoista (TDD) jakoa myötä- ja paluusuunnan erottelun suhteen [23].

Suomessakin yleistynyt LTE category 4 mahdollistaa 2x2 Multiple Input Multiple Output (MIMO) -tekniikkaa hyödyntäen ja 20 MHz:n kaistanleveydellä 150 Mbps myötäsuuntanopeuden ja 50 Mbps paluusuuntanopeuden [24].

3GPP release 10:ssä määritellyssä LTE Advanced -tekniikassa voidaan yhdistää eri taajuusalueilta (esim. 800MHz + 1800 MHz) kaistaa yhdeksi isoksi kaistaksi ja sen myötä saada vielä suurempia siirtonopeuksia [25].

EPS on täysin pakettipohjainen, joten puhepalvelua ei voi enää toteuttaa piirikytkennäisesti. Tämän takia on kehitetty Circuit Switched Fall Back (CSFB) -ominaisuus, jossa päätelaite ohjataan 3G- tai 2G-verkkoon vastaanottamaan tai soittamaan puhelu [26]. Suurin osa operaattoreista käyttää vielä CSFB:tä puhepalvelun toteuttamiseen. Puhepalvelu voidaan toteuttaa LTE-verkossa käyttäen pakettipohjaisia palveluita kuten IP Multimedia Subsystem (IMS) -pohjainen Voice Over LTE (VoLTE) [27]. Tekstiviestipalvelu toimii pakettipohjaisesti EPS-verkossa.

EPS:n verkkoa on yksinkertaistettu. Tukiasemaohjain puuttuu EPS-arkkitehtuurista kokonaan, tukiasemaohjaimen toiminteet on siirretty tukiasemaan ja Mobility Management Entityyn (MME) [1, s. 41]. Control-plane ja user-plane on eritelty selkeämmin eri laitteisiin, jotta operaattorit pystyvät helpommin skaalaamaan ympäristöä tarpeidensa mukaan. Kuvassa 16 on esitetty EPS:n arkkitehtuurikuva.



Kuva 16. EPS arkkitehtuurikuva. [12.]

Tärkeimmät EPS-elementit listattuna

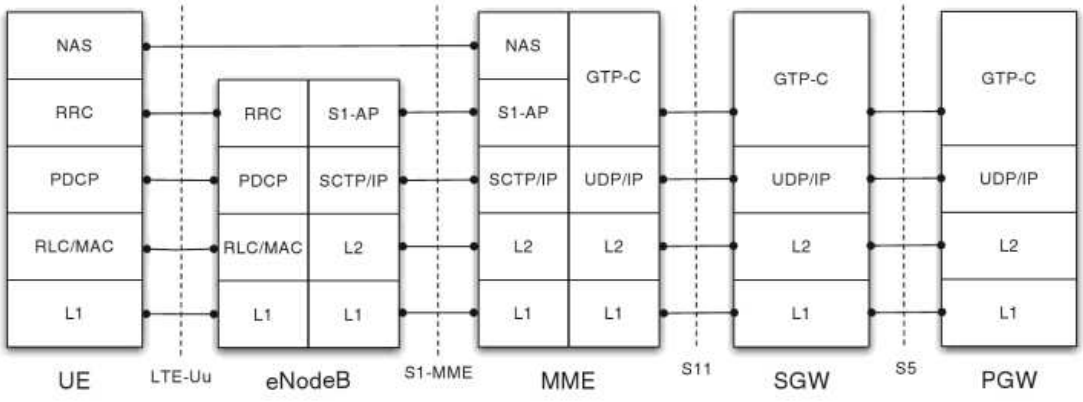
- Evolved Node B (eNodeB) on LTE-verkon tukiasema, osa tukiasemaohjaimen toiminnalisuuksista on siirretty eNodeB:n [1, s. 41].
- MME on vastuussa päätelaitteen mobiliteetin hallinnasta, autentikoinnista ja valtuutuksesta. MME on toiminnallisuudeltaan paljon vastaava kuin GPRS-arkkitehtuurin SGSN. MME ei välitä user-plane liikennettä, kuten GPRS-arkkitehtuurin SGSN [1, s. 41].
- Home Subscriber Server (HSS) on tietokanta jossa tilaajatiedot ovat, mukaan lukien autentikointitieto ja valtuutustieto. Toimii hyvin saman lailla kuin GPRS-arkkitehtuurin HLR [1, s.42].
- Serving Gateway (SGW) on mobiliteetin ankkuri kun tilaajaa siirtyy LTE-tukiasemasta toiseen LTE-tukiasemaan [1, s. 42]. SGW puskuroi tilaajalle tulevan datan verkosta päätelaitteelle päin. SGW voi vaihtua yksittäisen yhteyden aikana toiseen.
- Packet Data Network Gateway (PGW tai PDN GW) on yhdyskäytävä EPS:n ja ulkoisten IP-verkkojen välillä sekä on tilaajan IP-liikenteen terminointipiste. Se ei vaihdu koskaan yhteyden aikana [1, s. 42].
- Policy and Charging Rules Function (PCRF) on elemetti, jonka kautta voidaan ajaa dynaamisia sääntöjä verkkoon. PCRF on yhteydessä EPS-verkkooon PGW:n kautta. Säännöt voivat olla tilaajakohtaisia. Elementti voi mm. laskea tilaajan käyttämää datamäärää.

Tärkeimmät rajapinnat [1, s. 42]

- S1-MME on control-plane-rajapinta eNodeB:n ja MME:n välillä. Rajapinnassa käytetään S1AP-protokollaa.
- S1-U on user-plane rajapinta eNodeB:n ja SGW:n välillä. Rajapinnassa käytetään GTP-U protokollaa.
- S5/S8 rajapinta on SGW:n ja PGW:n välillä, S5-rajapintaa käytetään kun tilaaja on kotiverkossa, ja S8-rajapintaa kun tilaaja on toisen operaattorin verkossa. S5/S8 rajapinnoissa on control-plane ja user-plane toiminteita. Rajapinnassa käytetään GTP v2 protokollaa control-plane liikenteelle ja GTP-U protokollaa user-plane liikenteelle.
- S6a rajapinta yhdistää MME:n ja HSS:n. Rajapinnassa käytetään diameter-pohjaista protokollaa.
- S11 on control-plane-rajapinta, joka yhdistää MME:n ja SGW:n. Rajapinnasssa käytetään GTP v2 -protokollaa.
- SGi on rajapinta, jossa EPS kytketään ulkoisiin IP-verkkoihin, kuten Internetiin.

3.3.7 EPS-arkkitehtuurin protokollapinot

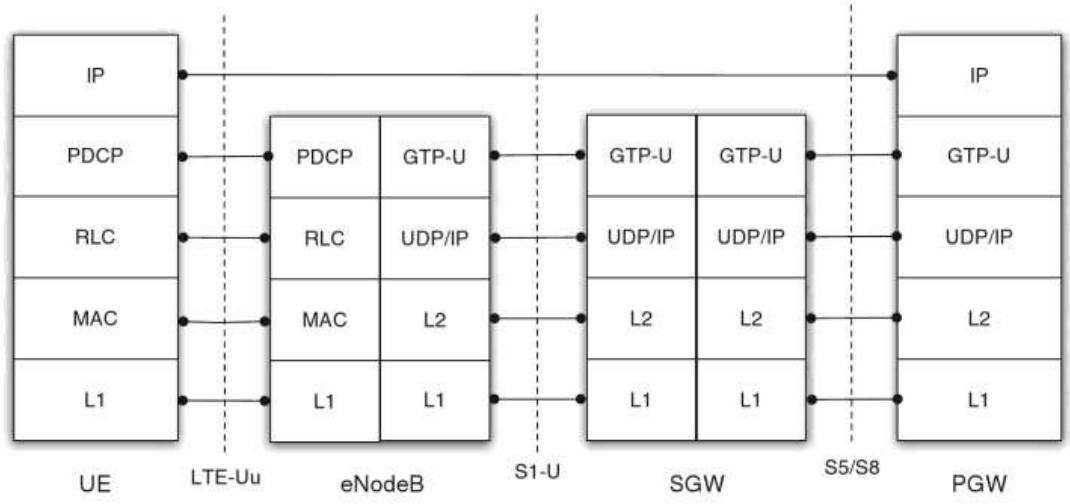
EPS control-plane on muuttunut paljon GPRS-arkkitehtuurista. SS7-pohjaiset rajapinnat ovat poistuneet. Terminaalin (UE) ja MME:n välillä käytetään Non-Access-Stratum (NAS) -protokollaa signalointiin. GTP-C on päivittynyt versio 1:stä versio 2:een. Kuvassa 17 on havainnollistettu control-plane-protokollat.



Kuva 17. EPS control-plane-protokollat [1, s. 44.]

EPS user-planessa ei ole merkittäviä eroavuuksia 3G GPRS -arkkitehtuurin user-plane- protokolliin. GTP-U -protokolla ulottuu LTE-tukiasemalta (eNodeB) pakettidata-

verkonyhdyskäytävälle (PGW) asti. PDCP:stä on uusi versio käytössä EPS:ssä. PDCP:n tehtävänä on kuljettaa käyttäjän paketit radiorajapinnan yli, pakata otsikkotiedot, salata käyttäjän paketit, tarkistaa pakettien eheys, oikea järjestys sekä tarkistaa, ettei duplikaattipaketteja tule [1, s.55]. Kuvassa 18 on esitetty user-plane-protokollat.



Kuva 18. EPS user-plane-protokollat [1, s. 43.]

4 IPv4- ja IPv6-protokollat 3GPP-matkaviestinverkoissa

Tässä luvussa esitellään pakettidataverkon yhteyspalvelu, EPS bearer ja PDP-konteksti sekä yhteydenluontiproseduuri. Tarkoituksena on tarkastella pakettidataverkon yhteyspalvelua IPv4- ja IPv6-protokollien näkökulmasta.

4.1 Pakettidataverkon (PDN) yhteyspalvelu

Packet Data Network (PDN) on yhteyspalvelu, joka tarjoaa internetprotokollan kautta yhteyden päätelaitteelta matkaviestinverkon yli ulkoiseen IP-verkkoon. Ulkoinen IP-verkko voi olla esim. internet tai yrityksen sisäverkko. PDN-yhteys on päätelaitteen ja liityntäpisteen nimen (APN) välinen assosiaatio. Jokaisella PDN-yhteydellä on IPv4-osoite ja/tai IPv6-prefiksi [1, s.163]. Päätelaitteeseen määritellään APN-asetus, johon päätelaite voi pyytää verkkoa yhdistämään.

Useampaa APN:ää voidaan käyttää samassa liittymässä. Hyvä esimerkki siitä on usein puheliittymissä käytetyt APN:t

- Internet APN (Internet-yhteyttä varten)
- MMS APN (multimediaviestejä varten)

Käyttäjä voi avata useampia PDN-yhteyksiä yhtä aikaa eri APN:iin olettaen, että päätelaite ja verkko tukevat sitä. Jokaiselta APN:ltä tulee oma IP-osoite ja oletusyhdyskäytävä PDN-yhteyteen. Esimerkiksi puhelimissa multimediaviestipalvelu voi käyttää MMS APN:ää, ja muut sovellukset voivat käyttää Internet APN:ää.

Päätelaiteen pyytäessä verkolta APN:ää, joka sen käyttämään liittymään on provisioitu, niin verkko selvittää ensin, mille GGSN:lle tai PGW:lle yhteys pitää ohjata. GGSN ja PGW ovat toiminnallisuudeltaan hyvin samanlaisia. GGSN on 2G- ja 3G-verkkojen pakettiyhdyskäytävä, ja PGW on LTE-verkon pakettiyhdyskäytävä. Useimmiten GGSN- ja PGW-toiminteet ovat fyysisesti samassa laitteessa.

Kun PDN-yhteys on luotu, niin pakettirunkoverkon laitteet tietävän sen olemassaolon. Laitteita ovat mm.

- SGSN tai MME (mikäli kyseessä EPS-yhteys)
- GGSN tai PGW (mikäli kyseessä EPS-yhteys)
- SGW (mikäli kyseessä EPS-yhteys)
- HLR tai HSS (mikäli kyseessä EPS-yhteys)
- mahdollisesti PCRF.

PDN-yhteydessä on tilatietoa kuten

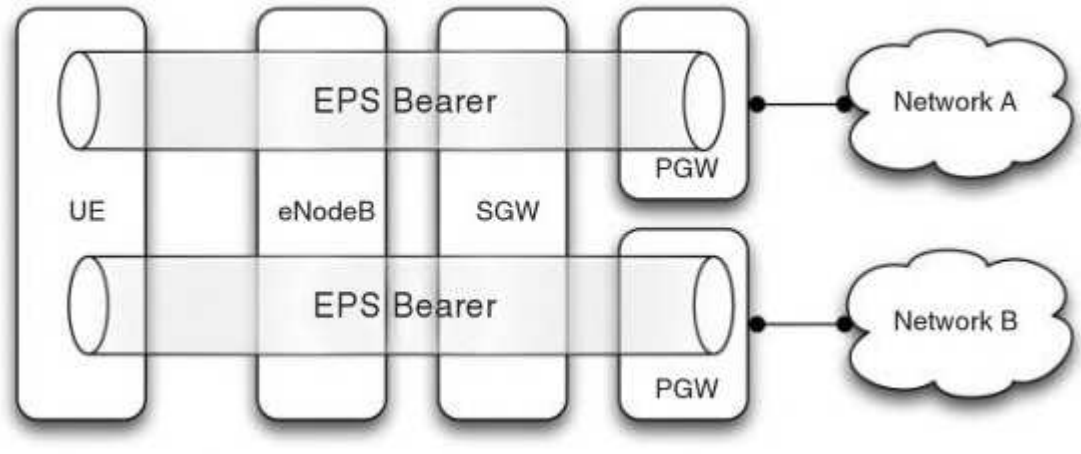
- missä SGSN laitteessa tilaaja on
- missä GGSN/PGW laitteessa tilaaja on
- tilaajan Mobile Station International ISDN Number (MSISDN), International Mobile Subscriber Identity (IMSI) ja päätelaitteen International Mobile Equipment Identity (IMEI)

- lukuisia GTP protokollaan liittyviä tunnistetietoja (kuten TEID)
- Quality of Service:een (QoS) liittyvät parametrit kuten myötäsuunnan maksiminopeus ja paluusuunnan maksiminopeus
- IPv4-osoite ja/tai IPv6-prefiksi.

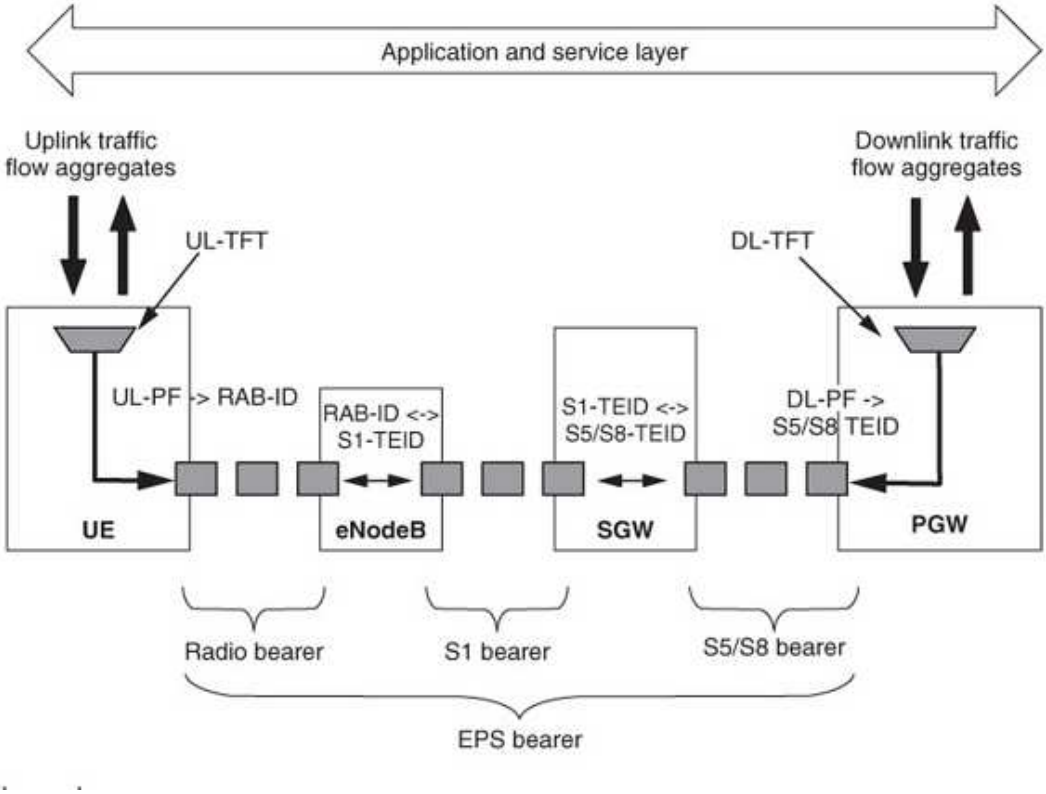
4.1.1 EPS bearer ja PDP-konteksti

Tärkeä PDN-yhteyden osa on bearer-konsepti. EPS bearer identifioi uniikisti liikennevuot, joilla on sama QoS-käsittely päätelaitteen ja PGW:n välillä. Vuot voidaan tunnistaa L3- tai L4-tasolla. Kuvassa 19 on esitetty, kuinka päätelaite on luonut kaksi EPS beareria kahteen eri ulkoiseen verkkoon.

EPS bearer koostuu radio-osasta, S1-osasta sekä S5/S8-osasta. Radio bearer muodostetaan päätelaitteen ja LTE-tukiaseman välille. S1 bearer muodostetaan LTE-tukiaseman ja SGW:n välille. S5/S8 bearer muodostetaan SGW:n ja PGW:n välille. Kuva 20 havainnollistaa EPS bearerin.



Kuva 19. Kaksi EPS beareria kahteen eri PGW:n [1, s. 63.]



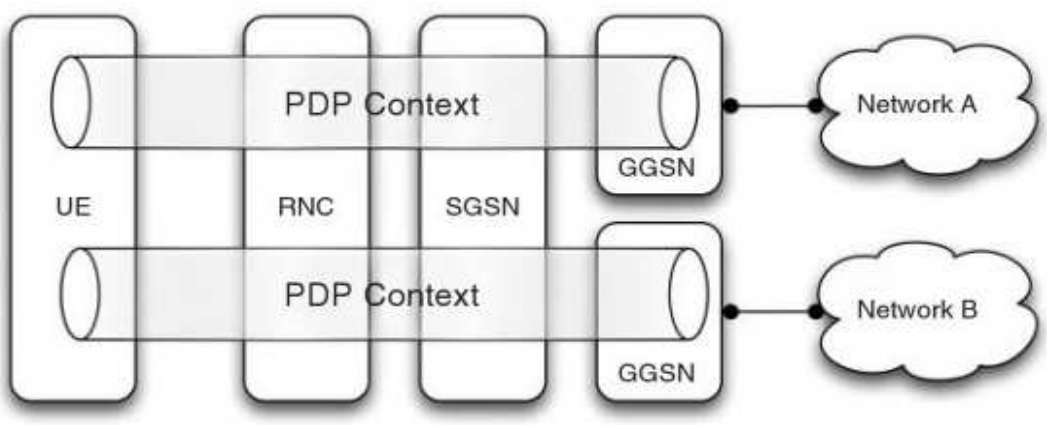
UL-TFT - Uplink Traffic Flow Template DL-TFT - Downlink Traffic Flow Template

UL-PF – Uplink Packet Filter DL-PF – Downlink Packet filter

RAB-ID – Radio Access Bearer Identifier TEID – Tunnel Endpoint Indentifier

Kuva 20. Yksinkertaistettu kuva EPS bearer:sta [1, s. 294.]

GPRS:n verkoissa EPS bearer -konseptia vastaa PDP-konteksti. On yleistä että PDN-yhteyttä ja PDP-kontekstia pidetään samana asiana, vaikka GPRS- ja EPC-arkkitehtuurissa on eroja. Kuvassa 21 on havainnollistettu, kuinka päätelaite on luonut kaksi PDP-kontekstia kahteen eri ulkoiseen verkkoon.



Kuva 21. Kaksi PDP-kontekstia kahteen eri GGSN:n [1, s. 63.]

On olemassa kahden tyyppisiä EPS beareereita: default EPS bearer ja dedicated EPS bearer. Default EPS bearer avataan aina päätelaitteen suunnasta, kun taas dedicated bearer avataan aina verkon suunnalta. Default EPS beareria luotaessa päätelaite saa aina IPv4-osoiteen ja/tai IPv6-prefiksin, mutta dedicated EPS bearerissa käytetään olemassa olevaa osoitetta, ja päätelaite sekä verkko asettaa Traffic Flow Template:n (TFT). TFT:llä saadaan identifioitua IP-vuo. Identifoidulle IP-vuolle voidaan tehdä yksilöity QoS-käsittely päätelaitteen ja PGW:n välille [1, s.165]. Sovellus joka hyödyntää dedicated beareria on esimerkiksi VoLTE. VoLTE-puhelua aloittaessa PCRF pyytää PGW:tä avaamaan dedicated bearerin tilaajan päätelaitteelle. Puhelulle pystytetään oma dedicated bearer, koska sille tehdään erilainen QoS-käsittely.

Default EPS bearer luodaan heti, kun päätelaitteeseen tulee virta. Päätelaite kiinnittyy (tekee kiinnittymisproseduurin) radioverkkoon, ja yhdistää pakettidataverkkoon (luo PDN-yhteyden) [1, s.49]. Default beareria kutsutaan GPRS-arkkitehtuurissa primääri PDP-kontekstiksi.

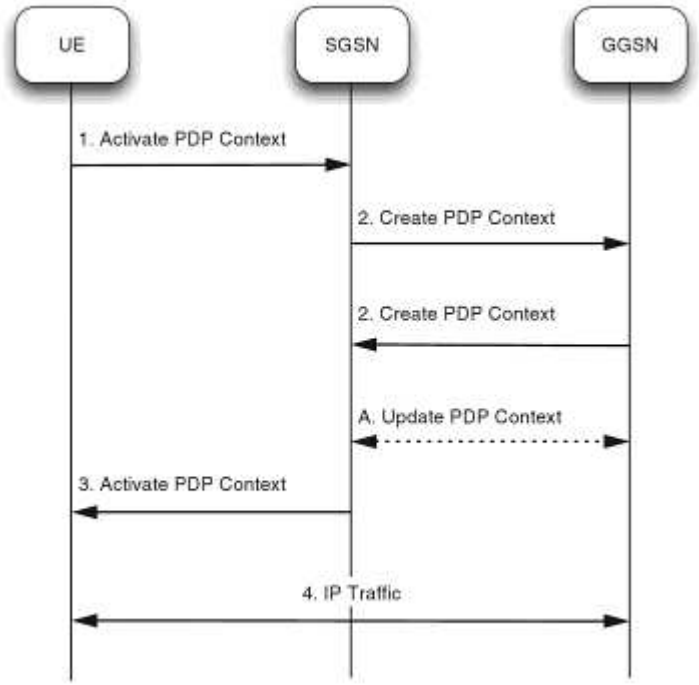
Mikäli päätelaite uudelleen käynnistetään tai se ei ole yhteydessä verkkoon, niin siltikin PDN-yhteys pysyy päällä pakettirunkoverkossa. Myös IPv4-osoite tai/tai IPv6-prefiksi pysyy samana. Tämä on yksi EPS-järjestelmän pääajatuksista, eli PDN-yhteys on signaloituna valmiiksi vaikka päätelaite tippuisi hetkellisesti pois verkosta. EPS bearer eroaa GPRS-verkon ja EPS-verkon välillä. GPRS-verkossa päätelaite voi olla kiinnittyneenä radioverkkoon, mutta sillä ei välttämättä ole vielä PDP-kontekstia, eli sen pakettidatayhteys ei vielä ole välttämättä auki [1, s.47]. Tämä onkin eräs tärkeä ero GPRS:n

ja EPS:n välillä, koska EPS-verkossa tilaajalle varataan IP-osoite heti sen kiinnittyessä radioverkkoon, kun taas GPRS:ssä täytyy avata erikseen PDP-konteksti, jotta päätelaite saa IPv4-osoitteen ja/tai IPv6-prefiksin.

Default EPS bearerin tai dedicated EPS bearerin luonti tai poisto aiheuttaa verkossa paljon signaloitavaa. Jokainen uusi bearer kuluttaa myös erillisen Radio Access Bearerin (RAB), joka vaikuttaa radioverkon resurssointiin.

4.1.2 PDP-kontekstin luontiproseduuri GPRS-arkkitehtuurissa

Päätelaitteen pitää tehdä ensin 2G- tai 3G-verkkoon kiinnittymisproseduuri (attach). Kun kiinnittymisproseduuri on valmis, niin päätelaite voi pyytää pakettidatayhteyttä auki ”Activate PDP Context” -viestin avulla. PDP-kontekstin luontiproseduuri on esitelty kuvassa 22.



Kuva 22. PDP-kontekstin luontiproseduuri GPRS-arkkitehtuurissa [1, s.48]

1. Päätelaite (UE) lähettää Activate PDP Context Requestin SGSN:lle, eli se indikoi, että haluaa avata pakettidatayhteyden. Aktivointipyynnössä on mm. APN-nimi ja haluaako päätelaite IPv4-osoitteen, IPv6-prefiksin vai kummatkin.

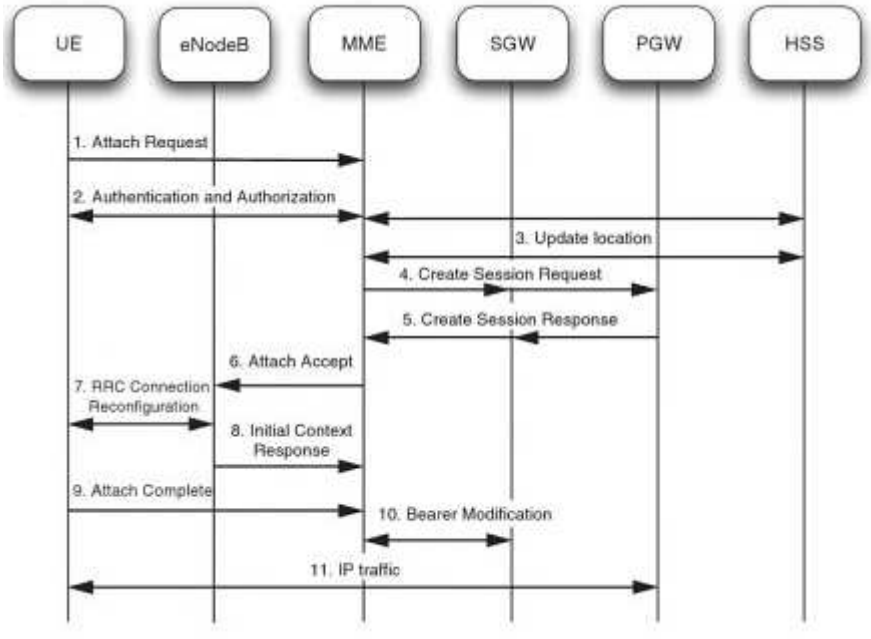
2. SGSN vertaa PDP Context Requestia tilaajaprofiiliin, ja mikäli APN on provisioitu tilaajaprofiilissa ja PDP-tyyppi täsmää, niin se selvittää DNS:n avulla, mille GGSN:lle Create PDP context Requestin viesti lähetetään ja lähettää sen. Mikäli GGSN hyväksyy pyynnön, niin se lähettää Create PDP context Response viestin SGSN:lle. Viesti sisältää mm. IP-osoitteen ja Protocol Configuration Option (PCO) -tiedot.

3. SGSN lähettää Activate PDP Context Accept:n päätelaitteelle.

4. Päätelaite voi liikennöidä pakettidatayhteydellä.

4.1.3 PDN-yhteyden muodostusproseduuri EPS-arkkitehtuurissa

EPS-arkkitehtuurissa radioverkkoon kiinnittyessä avataan aina myös pakettidatayhteys. Kuvassa 23 on esitelty LTE-verkon kiinnitysmisproseduuri ja pakettidatayhteyden aktivointiproseduuri.



Kuva 23. LTE-kiinnitymisproseduuri ja pakettidatayhteyden aktivointiproseduuri. [1, s.49.]

1. Päätelaite (UE) lähettää ”Attach Request” -viestin MME:lle.

2. Autentikointi ja tietoturva proseduurit tehdään, jotta tilaaja saadaan autentikoitua ja signalointiviestit salatuiksi.

3. MME lähettää ”Location update” viestin HSS:lle. HSS tallentaa liittymän paikkatiedon tietokantaansa.

4. MME tarkistaa tilaajaprofiilista, että tilaajalla on oikeus sen pyytämään APN:ää ja PDN-tyypit täsmäävät, jonka jälkeen MME selvittää DNS-kyselyllä, että mille PGW:lle ”Create Session Request” -viesti lähetetään. MME lähettää viestin SGW:n kautta PGW:lle.

5. PGW lähettää Create Session Response -viestin SGW:n kautta MME:lle. Viesti indikoi onnistuneesta tai epäonnistuneesta yhteyden muodostuksesta. Mikäli yhteys onnistuu, niin PGW luo uuden EPS bearerin tilatauluunsa, varaa IP-osoitteen tai osoitteet päätelaitteelle. Vastausviestiin on määritelty päätelaitteelle varattu IPv4-osoite ja/tai IPv6-prefiksi, sekä PCO:ssa on lisätietoa kuinka päätelaite määrittelee IP-pinonsa [1, s. 50].

6. MME lähettää ”Attach Accept” -viestin LTE-tukiasemalle (eNodeB). Viestissä kulkee myös päätelaitteelle varattu IPv4-osoite ja/tai IPv6-prefiksi.

7. Radio Resource Control (RRC) -yhteyden uudelleenmääritysproseduuri määrittelee radioresurssit ja toimittaa osoitteet ja PCO-tiedot päätelaitteelle.

8. LTE-tukiasema (eNodeB) lähettää ”Initial Context Response” -viestin MME:lle. Viestistä selviää mm. LTE-tukiaseman IP-osoite.

9. Päätelaite lähettää ”Attach complete” -viestin MME:lle.

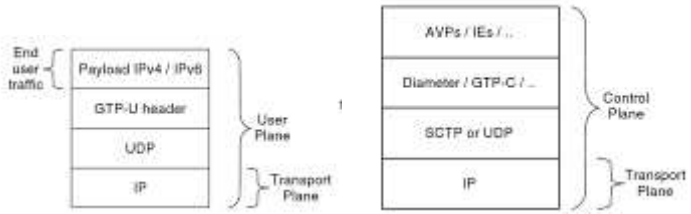
10. ”Bearer modificaation” proseduuri tehdään MME:n ja SGW:n välillä. Proseduurissa kerrotaan mm. SGW:lle LTE-tukiaseman IP-osoite.

11. Tässä vaiheessa kiinnittyminen LTE-verkkoon on onnistunut ja Default EPS bearer on muodostettu. Yhteys on valmis, paketit kulkevat tilaajalta verkkoon ja toisinpäin.

4.1.4 User-plane, control-plane ja transport plane

3GPP:n spesifikaatiossa on eroteltu selkeästi control-plane, user-plane ja transport plane [1, s.172]. Control-plane-liikenne on matkaviestinverkon sisäistä signalointia. User-plane-liikenteessä on loppukäyttäjän liikenne. Transport plane on IP-verkon siirtokerros, jonka päällä control-plane- ja user-plane-liikenne kuljetetaan.

Loppukäyttäjän IP-pakettiliikenne (user-plane) on tunneloitu GTP:n avulla. User-planessa voidaan kuljettaa IPv4 ja/tai IPv6-liikennettä, vaikka control-plane- ja/tai transport plane-liikenne olisi rakennettu IPv4:n päälle. Kuva 24 havainnollistaa user-planen, control-planen ja transport planen.



Kuva 24. User-plane, control-plane ja transport plane [1, s.172]

4.1.5 PDN- ja PDP-yhteystyypit

Jokaiseen PDN- tai PDP-yhteyteen liittyy myös IPv4-osoite ja/tai IPv6-prefiksi. PDN-yhteys voi välittää vain sen tyyppistä liikennettä, joka on neuvoteltu default EPS bearerin tai primääri PDP-kontekstin aloitusvaiheessa [1, s. 167]. Käytössä on kolme erilaista PDN-tyyppiä ja PDP-kontekstityyppiä:

- IPv4, yhteydellä on yksi IPv4-osoite, tämä on ollut 3GPP-spesifikaatiossa jo alusta asti [1, s. 167]
- IPv6, yhteydellä on yksi IPv6 /64 prefiksi, tuettuna 3GPP release 99:stä alkaen [1, s. 167].
- IPv4v6, yhteydellä on IPv4-osoite ja IPv6-prefiksi. EPS-verkossa ipv4v6 tuki tuli 3GPP release 8:ssa, mutta GPRS-verkkoarkkitehtuuriin vasta 3GPP release 9:ssä. Tätä voidaan kutsua myös dual-stack PDN/PDP:ksi [1, s. 167].

Tuki IPv6:lle on ollut jo 3GPP release 99:stä alkaen, mutta silloin pitäisi muodostaa kaksi PDN-yhteyttä, yksi IPv4:lle ja toinen IPv6:lle. Tällöin pakettirunkoverkosta ja radioverkosta pitäisi varata kaksinkertainen määrä resursseja. IPv4v6 PDN-yhteydellä ei ole tätä ongelmaa, ja sen takia se tulee yleistymään.

4.1.6 IPv4-osoitteen tai IPv6-prefiksin allokointi PDN-yhteydelle

3GPP-standardi tukee monipuolista osoitteiden jakoa tilaajille. IPv4-osoite tai IPv6-prefiksi voidaan jakaa dynaamisesti tai staattisesti. Staattinen osoitteen jako tarkoittaa että IPv4-osoite tai IPv6-prefiksi on jokaisella eri yhteydellä sama.

Seuraavat IPv4-osoitteen ja IPv6-prefiksin jakomenetelmät ovat tuettuna [1, s.198]:

- Dynaaminen osoite ja/tai prefiksi paikallisesti GGSN:stä tai PGW:stä
- Staattinen osoite ja/tai prefiksi tilaajarekisteristä (HLR ja/tai HSS)
- Dynaaminen tai staattinen osoite ja/tai prefiksi ulkoiselta Radius-palvelimelta
- Dynaaminen tai staattinen osoite ja/tai prefiksi ulkoiselta DHCP-palvelimelta

4.1.7 Nimipalvelintiedot (DNS)

Päätelaitteelle voidaan kertoa nimipalvelintiedot GTP:n PCO-viestissä, joka kulkee esim. GPRS-verkossa Create PDP context response tai Create Session Response -viestissä.

4.1.8 IPv6-pakettien välitys 3GPP-matkaviestinverkossa

Seuraavat ominaisuudet pätevät loppukäyttäjän IPv6-pakettien välitykseen 3GPP-matkaviestinverkossa [1, s. 169].

- PGW on ainoa laite, jonka kanssa päätelaite voi vaihtaa Network Discovery Protocol -viestejä .
- NDP-osoitteen kääntöä ja uudelleenohjaus toiminnetta ei tarvita, koska siellä ei ole linkkitason osoitteita ja linkki on ”point to point” -tyyppinen.
- Päätelaitteen ja PGW:n välisellä linkillä on ainoastaan yksi /64 prefiksi.
- IPv6-prefiksin uudelleennumerointi ei ole mahdollista, ilman että PDN-yhteys katkaistaan.

5 IPv6:n käyttöönotto DNA:n matkaviestinverkossa

Tässä luvussa esitellään ensin lyhyesti DNA:n matkaviestinverkko. Sen jälkeen käydään läpi kaksi eri tapaa ottaa IPv6-protokolla käyttöön. Lopuksi käydään IPv6-protokollan aiheuttamat muutokset läpi matkaviestinverkon eri elementtien näkökulmasta.

5.1 Lyhyt esittely DNA:n matkaviestinverkosta

DNA:lla on Suomen kattava (pois lukien Ahvenanmaa) radioverkko. Radioverkossa käytetyt teknologiat ja taajuudet

- 2G-radioverkko, joka on rakennettu 900 MHz:n ja 1800 MHz:n taajuuksilla.
- 3G-radioverkko, joka on rakennettu 900 MHz:n ja 2100 MHz:n taajuuksilla.
- 4G LTE-radioverkko, joka on rakennettu tätä kirjoittaessa vielä pääosin 1800 MHz:n taajuudella, 800 MHz:n verkon rakennus on alkanut vuonna 2014. Myös 2600 MHz taajuutta on käytössä.

DNA:llä on käytössä ns. triple access -mobiilipakettirunkoverkko, joka tarkoittaa, että samat laitteet palvelevat 2G-, 3G, ja 4G LTE -radioverkkoja. Kaikki rajapinnat ovat IP-pohjaisia, ja verkosta on pyritty tekemään mahdollisimman vikasietoinen. Verkko on 3GPP release 9 yhteensopiva ja rakennettu pääosin Ericssonin tekniikalla. Seuraavana on lyhyt yhteenveto käytössä olevista pakettirunkoverkon laitteista.

- Maantieteellisesti hajautetut SGSN-MME laitteet pystyvät käsittelemään miljoonia tilaajia. SGSN- ja MME-toiminteet hoidetaan siis samalla laitteella.
- Maantieteellisesti hajautetut GGSN/SGW/PGW -laitteet, jotka hoitavat PDN- ja PDP-kontekstien IP-terminoinnin. Sama laita hoitaa siis GGSN-, SGW- ja PGW-toiminteet.

- PCRF-palvelu, sijaitsee maantieteellisesti kahdessa eri paikassa ja joka on oleellinen osa EPS-arkkitehtuuria, QoS-kontrolli tapahtuu viimekädessä PCRF:ssä, kun taas GPRS-arkkitehtuurissa se tapahtuu SGSN:ssä.

DNA:n verkossa 3G Direct Tunnel on käytössä, jonka avulla SGSN:n läpi menevää user-plane-liikennettä on saatu pienemmäksi. 3G Direct Tunnelin avulla RNC pystyy lähettämään käyttäjän user-plane-liikenteen suoraan GGSN:lle, ilman että liikenne kulkee SGSN:n kautta. DNA:lla on käytössä testiverkko, josta löytyvät kaikki matkaviestinverkon elementit. Testiverkossa voidaan testata mahdollisia muutoksia hallitussa ympäristössä etukäteen.

5.2 DNA:n mobiilipakettirunkoverkon nykyinen tilanne

DNA:n IP/Multiprotocol Label Switching (MPLS) -pohjainen runkoverkko tukee IPv6:sta IPv6 Provider Edge Router (6PE) -toiminnalisuuden avulla.

DNA:n matkaviestinverkossa on satoja eri APN:iä. Pääosa niistä on yrityskohtaisia ja sen lisäksi on useita palveluoperaattoreita. Kaksi merkittävintä APN:ää ovat Internet APN, jossa on matkapuhelimien pakettidatayhteydet sekä data.dna.fi APN, jossa mokkulat ja tabletit ovat.

Internet APN:ssä on käytössä RFC1918:ssä [28] määritellyt ei julkiset IPv4-osoitteet, jotka jaetaan päätelaitteelle. NAPT-ratkaisulla käännetään ei-julkiset osoitteet julkisiksi. Useampi tilaaja käyttää samaa julkista IPv4-osoitetta. APN:ää voi käyttää 2G-, 3G- ja 4G LTE-radioverkoista. Mokkulayhteyksiä varten on data.dna.fi APN, jossa on käytössä julkiset IPv4-osoitteet. APN:ää voi käyttää 2G-, 3G- ja 4G LTE-radioverkoista.

DNA:n matkaviestinverkon pakettirunkoverkossa optimoidaan TCP-protokollan pakettikokoa, niin ettei siellä tapahdu pakettien pirstalointia. Optimointi on tehty muuttaen TCP:n kättelyvaiheessa asetettavaa Maximum Segment Size (MSS) -parametria.

5.3 IPv6:n käyttöönotto DNA:lla

DNA:lla nähdään, että internetiin liitettävien laitteiden määrä tulee kasvamaan. DNA haluaa ottaa skaalautuvan menetelmän käyttöön, jossa ei tarvitse tehdä osoitteenkääntöä, ja asiakkaiden olisi mahdollisimman helppo pystyttää erilaisia palveluita.

Suosittelen, että DNA ottaa IPv6:n käyttöön ns. dual stack -menetelmää käyttäen. Dual stackin avulla tilaajat pääsevät käyttämään IPv4-osoitteella IPv4-palveluita ja IPv6-osoitteella IPv6-palveluita

Dual stack -menetelmä voidaan ottaa käyttöön kahdella eri tavalla.

1) Otetaan rinnalle toinen IPv6 PDN/PDP-yhteys, jonka jälkeen yhdellä tilaajalla voi olla normaalitilanteessa kaksi PDN/PDP-yhteyttä auki, yksi yhteys IPv4:lle ja toinen yhteys IPv6:lle. Tätä ratkaisua ei voi suositella, koska se syö kaksinkertaiset resurssit pakettirunkoverkosta ja radioverkosta. Vaatii myös päätelaitteelta tukea.

2) Otetaan käyttöön uusi IPv4v6 PDN/PDP-tyyppi, jossa yksittäisen yhteyden kautta voidaan lähettää ja vastaanottaa IPv4- ja IPv6-liikennettä.

5.4 Loppukäytäjän IPv4v6 PDN/PDP-yhteyden vaikutus DNA:n matkaviestinverkon elemetteihin

Seuraavissa kappaleissa on listattuna matkaviestinverkkojen elementit, joista täytyy löytyä tuki IPv4v6 PDN/PDP-tyypille.

5.4.1 Tilaajarekisterit HLR ja HSS

HLR:ssä IPv6-tyyppinen PDP-yhteys on ollut tuettuna 3GPP release 99:stä alkaen [1, s.178]. IPv4v6 PDP-tyypille tuki tuli 3GPP release 9:ssä, joka julkaistiin vuoden 2009 lopussa. HSS on tukenut IPv4, IPv6 ja IPv4v6 PDN-tyyppejä 3GPP release 8:sta lähtien [1, s.178].

Tilaajalla voi olla useampi APN määriteltynä, ja jokaisella APN:llä voi olla erilainen PDP-tyyppi. Esimerkiksi MMS APN voi olla IPv4-tyyppinen ja Internet APN IPv4v6-tyyppinen.

Mikäli DNA:n tilaaja on toisen operaattorin verkossa vierailemassa (roaming), eli käyttää toisen operaattorin radioverkkoa, SGSN:ää, mutta DNA:n GGSN:ää. Mikäli tilaajan profiilissa on yksikin APN, jossa on IPv4v6 PDP-tyyppi, se voi johtaa siihen, että toisen operaattorin SGSN hylkää koko tilaajaprofiilin, joka taas johtaa siihen, että pakettidata ei toimi ollenkaan ko. operaattorin verkossa. Ongelmaa ei pitäisi esiintyä, jos operaattorin SGSN on 3GPP release 9 yhteensopiva. Tämän takia DNA:n HLR:ään tarvitaan muutos, jotta voidaan määritellä IPv4v6 yhteensopivat operaattorit. Muille operaattoreille lähetetään aina IPv4- tai IPv6-tyyppinen tilaajaprofiili.

5.4.2 Provisiointijärjestelmä

DNA:n provisiointijärjestelmä on asiakashallintajärjestelmien matkaviestinverkon elementtien välissä. Sen tehtävänä on toimittaa provisiointipyyntöjä matkaviestinverkon erilaisille elementeille kuten HLR, HSS ja PCRF. DNA:n nykyinen provisiointijärjestelmä tukee IPv4- ja IPv6-PDP-tyyppejä HLR:n provisioinneissa, mutta ei IPv4v6-PDP-tyyppiä. Provisiointiäjärjestelmään täytyy saada IPv4v6-PDP-tyypille tuki. HSS:n PDN-tyyppiin provisiointijärjestelmä ei ota mitään kantaa.

5.4.3 GGSN, PGW ja niiden tukijärjestelmät

GGSN:lle IPv4v6 PDP-tyypin tuki tuli 3GPP release 9:ssä ja PGW:ssä on ollut IPv4v6 tuettuna 3GPP release 8:sta alkaen [1, s. 177]. PDN/PDP-tyyppi voidaan määritellä APN-kohtaisesti. GGSN:ssä ja PGW:ssä on mahdollistä määritellä priorisoitu PDN/PDP-tyyppi, mikäli Dual Address Bearer (DAF) -lippu ei ole päällä SGSN:n tai MME:n lähettämässä PDN/PDP-yhteyden luontiviestissä. GGSN/PGW laitteisto ei vielä tue IPv6-protokollaa käytettäessä TCP-protokollan MSS-parametrin muuttamista.

DNA:lla on lähdetty toteuttamaan /64 IPv6-prefiksi per tilaaja -mallia, joka on myös ainoa tuettu malli. Osoitteita allokoidaan /44 IPv6-prefiksi per APN ja per GGSN tai PGW. Yhdessä /44 osoitelohkosta saadaan 20 bitin verran /64 IP prefiksiä, /64 kokoisia IPv6-prefiksejä voidaan liittää 2^{20} (1048576 kpl) yhteen APN:ään.

3GPP release 10:ssä on tullut tuki myös DHCPv6 prefiksin delegoinnille [1, s.177]. Siinä päätelaite hakee DHCPv6:lla esim. /56 IPv6-prefiksin /64 prefiksin rinnalle. DHCPv6 prefiksin delegointi ei ole tuettu vielä DNA:n GGSN:ssä tai PGW:ssä.

GGSN:ään tai PGW:n voi olla liitetty erilaisia tukijärjestelmiä, kuten Online Charging System (OCS), Roaming Cost Control (RCC) tai Policy Control and Rules Function (PCRF).

Online Charging Systemiä (OCS) käytetään yleensä reaaliaikaiseen laskutukseen. Esimerkiksi prepaid-liittymien pakettidatan raportointi voidaan hoitaa OCS-järjestelmän kautta. Laskutus voi perustua aikapohjaiseen tai siirrettyjen tavujen perusteella tehtävään hinnoitteluun. GGSN tai PGW siis jatkuvasti pyytävät OCS-järjestelmältä osuutta (quotaa), ja asiakas voi liikennöidä niin kauan, kunnes OCS ei enää myönnä osuutta (eli quota on loppunut). OCS käyttää Gy-rajapintaa keskustellessaan GGSN:n tai PGW:n kanssa. Gy-rajapinta on diameter-pohjainen, ja sen täytyy mahdollisesti tukea Framed-IPv6-Prefix AVP:ta.

Roaming Cost Controlia (RCC) käytetään EU:n verkkovierailuasetuksen mukaiseen saldorajapalveluun. RCC ja OCS käyttävät samaa Gy-rajapinta GGSN:n kanssa keskusteltaessa. DNA:n verkossa GGSN tai PGW lähettää PDP-address AVP:n kahteen kertaan (yksi IPv4:lle ja yksi IPv6:lle), mikäli PDN/PDP:n tyyppi on IPv4v6.

Policy Control and Rules Functionia (PCRF) voidaan käyttää lähes reaaliaikaiseen käytetyn datan seurantaan. PCRF käyttää diameteriin pohjautuvaa Gx-rajapintaa keskustellessaan GGSN:n tai PGW:n kanssa. Gx-rajapinnassa on enemmän mahdollisuuksia muokata tilaajayhteyden ominaisuuksia kuin Gy-rajapinnssa. EPS-arkkitehtuurissa tilaajan QoS-arvoista päättää lopulta PCRF, kun GPRS-arkkitehtuurissa QoS:n päättää SGSN. PCRF:n pitää tukea Framed-IPv6-Prefix AVP:tä, jossa GGSN tai PGW kertoo tilaajan IPv6-prefiksin PCRF:lle.

DNA:n PCRF:stä puuttuu vielä tuki Framed-IPv6-Prefix AVP:lle, jota tarvitaan IPv4v6 ja IPv6 PDN/PDP-tyypeissä. Jos yrittää muodostaa PDN/PDP-yhteyden ja yhteys ohjataan PCRF:lle, niin PCRF vastaa virheviestillä 5001 (DIAMETER_AVP_UNSUPPORTED), eikä PDN/PDP-yhteys muodostu.

5.4.4 SGSN, MME ja SGW

SGSN on tukenut IPv4:sta alusta alkaen ja IPv6:sta jo 3GPP release 99:stä alkaen. IPv4v6-tyyppi on tuettuna vasta 3GPP release 9:stä lähtien [1, s. 176]. MME ja SGW on tukenut IPv4-, IPv6- ja IPv4v6-PDN-tyyppejä 3GPP release 8:sta lähtien [1, s. 176].

Esimerkiksi SGSN on hyvin oleellinen osa PDP-tyypin neuvottelussa. Kun tilaaja kiinnittyy radioverkkoon, niin SGSN hakee Gr-rajapintaa pitkin tilaajaprofiilin HLR:stä.

Kun PDP-yhteyttä ollaan muodostamassa, niin päätelaite pyytää tiettyä PDP-tyyppiä, esim. IPv4v6:sta. SGSN vertaa pyydettyä PDP-tyyppiä ja tilaajaprofiilia, ja mikäli PDP-tyyppi on sama, niin silloin SGSN lähettää PDP context creation requestin GGSN:lle.

Mikäli PDP-tyyppi ei ole sama, niin on tekniikoita/mekanismeja, joilla voidaan vaihtaa PDP-tyyppi sellaiseksi, jota päätelaite ja verkko kummatkin tukevat. Markkinoilla on SGSN:iä sellaisilla ohjelmistoversioilla, jotka voivat hylätä HLR:ltä saadun tilaajaprofiilin, mikäli siinä on yksikin APN määritelty IPv4v6 PDP-tyyppiseksi.

5.4.5 Radioverkko

Mikäli IP-otsikkotietojen pakkaus on päällä, niin radioverkkokin voi ottaa kantaa loppukäyttäjän IP-protokollaversioon. 2G-liikenteelle IP-otsikkotietojen pakkaus tapahtuu SNDCP-tasolla, 3G-liikenteelle ja LTE-liikenteelle PDCP-tasolla. [1, s. 175.]

5.4.6 Päätelaite

Päätelaitteen pitää tukea IPv6:ta modeemissa, TCP/IP pinossa, yhteyden hallintaohjelmistossa, ohjelmistorajapinnassa (API), sekä mahdollisesti käyttöjärjestelmässä ja ohjelmistoissa [1, s. 174].

Mikäli päätelaitteeseen voi liittää useampia laitteita esimerkiksi Wireless Local Area Networkin (WLAN) tai ethernet-portin kautta, niin päätelaitteen pitää tukea NDP-välityspalvelulla (proxy) tai jotain muuta mekanismia/tekniikkaa, jolla prefiksi voidaan jakaa eteenpäin. NDP-välityspalvelulla jaetaan sama /64 prefiksi paikallisverkkoon, joka saatiin matkaviestinverkon rajapinnasta..

5.5 IPv6:n tarvitsemat tukipalvelut

5.5.1 Domain Name Service (DNS) -kääntäjänimipalvelu

DNA:n verkossa olemassa olevat kääntäjänimipalvelimet kääntävät esimerkiksi asiakkaiden osoitepyyntöjä IPv4- ja IPv6-osoitteiksi. Palvelimien IPv4-reititys on toteutettu dynaamisesti reititysprotokollan avulla hyödyntäen anycast-tekniikkaa. Verkossa on useampi nimipalvelin samalla IP-osoitteella, ja IP-verkko reitittää tilaajan paketit aina lähimmälle nimipalvelimelle. Tilatiedottoman UDP-pohjaisen nimipalvelun kanssa on turvallista käyttää anycastiä. DNA:n nimipalvelimien IPv6-osoitteet täytyy reitittää dynaamisesti reititysprotokollan avulla ja anycast-tekniikkaa käyttäen, jotta yhden palvelimen vikaantuminen ei aiheuta viiveitä kääntäjänimipalveluun. DNA:n mobiilipaketti-runkoverkko kertoo IPv4- ja IPv6-kääntäjänimipalvelimien (DNS) tiedot ipv4v6-PDP/PDN-kontekstia luotaessa PCO-viestissä.

5.5.2 DNS forward ja reverseille tietueet käytössä oleville IPv6-osoitteille

IPv6-osoitteet, jotka liikennöivät internetiin, täytyy määritellä nimipalveluun. On olemassa palveluita, jotka identifioivat esimerkiksi käyttäjän paikkatietoa perustuen nimipalvelutietoon.

DNS-palvelu voidaan jakaa forward- ja reverse-tietueisiin. Forward-tietueissa määritellään nimestä IP-osoitteeseen käännös ja reverse-tietueessa IP-osoitteesta nimeksi.

IPv6 tuo uuden haasteen osoitteiden nimipalveluun määrittämiselle. Haasteena on suuri osoiteavaruus, koska DNS-palvelimiin on yleensä staattisesti tai puolidynaamisesti määritelty, kuinka IP-osoite kääntyy nimeksi ja toisinpäin (nimi kääntyy IP-osoitteeksi).

Vanha tapa ei enää skaalaudu IPv6:n osoitteiden kanssa, koska nimipalvelimen muisti ei riitä, vaan nimipalvelukyselyn vastaus pitää luoda dynaamisesti tietyn säännön mukaan.

5.5.3 Content Delivery Network (CDN) -toimijoiden välimuistit

DNA:n runkoverkon IP-liikenteestä suurin osa on video-liikennettä. DNA:n verkossa on CDN-toimijoiden välimuisteja. Välimuisteihin täytyy saada IPv6 käyttöön, jottei käyttökokemus huonontuisi IPv6:n käyttöönoton takia. Tämä on tarpeellista vain, mikäli CDN-toimija on käyttöönottanut IPv6:n.

5.6 Yhteenveto tarvittavista muutoksista

Tarvittavat muutokset voidaan jakaa kolmeen eri vaiheeseen: ensimmäisessä vaiheessa on tehdään valmistelevat toimenpiteet, toisessa vaiheessa otetaan IPv4v6 PDP-tyyppi käyttöön kotiverkkoon ja kolmannessa vaiheessa otetaan käyttöön niiden roaming-kumppaneiden verkkoihin, jotka tukevat dual-stack:ia.

Vaihe 1 - valmistelevat toimenpiteet

- Kaikki roaming-kumppaneiden SGSN:t eivät ole vielä 3GPP release 9 yhteensopivia, joten niille ei saa lähettää IPv4v6 PDP-tyyppiä sisältävää tilaajaprofiilia, vaikka se olisi tilaajaprofiilissa määriteltynä. IPv4- tai IPv6-PDP-tyypin sisältävän tilaajaprofiilin voi lähettää ilman että pitäisi tulla epäyhteensopivuuksia. Eli käytännössä IPv4v6-PDP-tyyppi toimisi aluksi ainoastaan kotiverkossa. IPv4v6-PDP-tyyppiä on mahdollista ottaa käyttöön operaattorikohtaisesti.
- SGSN:ssä täytyy ottaa IPv6 user-plane -ominaisuus käyttöön. IPv6 user-plane on jo otettu käyttöön DNA:lla .
- MME:ssä täytyy ottaa Dual Address Bearer Flag -käyttöön, joka indikoi että PGW tukee myös IPv6-protokollaa user-planella. Dual Address Bearer Flag on jo otettu käyttöön DNA:lla.
- GGSN/PGW:lle täytyy määritellä IPv6-osoiteavaruus kaikkiin APN:iin, josta /64 IPv6-prefiksit jaetaan asiakkaille. Priorisoitu IP-versio asetetaan 4:een. Suosittelen myös, että alkuvaiheessa tilaajat, jotka vierailevat toisen operaattorin verkossa pakotetaan myös GGSN/PGW:stä käyttämään IPv4:sta.
- PCRF-järjestelmä täytyy saada tukemaan Framed-IPv6-Prefix AVP:ta
- RCC ja OCS -järjestelmien tuki täytyy vielä tarkistaa.
- Provisiointijärjestelmä täytyy saada tukemaan IPv4v6 PDP-tyyppiä
- DNS resolver -palvelun transport-plane:n täytyy tukea IPv6:sta

- CDN-toimittajien välimuistien täytyy tukea myös IPv6:sta.

Vaihe 2 - IPv4v6 PDN/PDP-tyypin käyttöönotto asiakkaiden liittymiin

- Asiakaspalvelu täytyy ohjeistaa; tarvitaan Usein Kysytyt Kysymykset (UKK) -lista, lista testatuista päätelaitteista sekä ohjeet, kuinka IPv4v6 PDN/PDP-tyyppi otetaan käyttöön päätelaitteissa.
- Provisiointijärjestelmä pitää määritellä luomaan oletuksena IPv4v6 PDP-tyyppi DNA:n tilaajille, tai vaihtoehtoisesti asiakashallintajärjestelmän provisiointikomentoihin pitää tehdä muutoksia.
- Tilaajien Internet ja data.dna.fi APN:ien PDP/PDN-tyyppi muutetaan IPv4v6:ksi.

Vaihe 3 - aktivoidaan IPv4v6 PDP-tyyppi niille roaming-kumppaneille, jotka tukevat sitä

- GSMA:n web-sivustolta voidaan hakea operaattorit, jotka tukevat IPv4v6 PDP/PDN-tyyppiä, joten HLR voidaan määritellä lähettämään niille operaattoreille IPv4v6 PDP-tyypin sisältäviä tilaajaprofiileja.
- GGSN/PGW:ssa mahdollistetaan IPv4v6 PDP-tyyppi niille operaattoreille, jotka tukevat IPv4v6:sta.

6 IPv6-protokollan testaus DNA:n tuotantoverkossa

Tässä luvussa esitellään IPv6-protokollan testaus DNA:n tuotantoverkossa. Tavoitteena oli varmistaa, että IPv6:n käyttöönotto ei heikennä merkittävästi tilaajien internetin käyttökokemusta. Käytännössä tämä tehtiin mittaamalla File Transfer Protocol (FTP) -siirtonopeutta ja muutaman suositun dual-stack-web-sivun latausaikaa. Mittaukset tehtiin käyttäen dual-stackiä sekä ainoastaan IPv4-protokollan kanssa. Insinöörityön tekijä oli käyttänyt puhelimessaan dual-stack-yhteyttä jo usean kuukauden ajan ongelmitta.

6.1.1 IPv4v6-yhteyden muodostus

Testilaitteistona oli HP:n EliteBook 8470p -kannettava tietokone, joka oli liitetty 100 Mbps ethernet-yhteydellä Huawei B593S -reitittimeen. Tietokoneen käyttöjärjestelmänä oli Windows 8 Service Pack 1. Liittymänä toimi DNA Veppi 4G, johon oli muutettu data.dna.fi APN:n PDN/PDP tyypiksi ipv4v6. Reititin oli yhteydessä DNA:n matkaviestinverkkoon 4G LTE -yhteyden avulla. Reitittimestä piti vaihtaa PDN/PDP-tyyppi IPv4:sta

IPv4v6:ksi, muuten kaikki toimi automaattisesti. Kuvasta 25 näkyy. kuinka päätelaite on saanut IPv4-osoitteen ja IPv6-prefiksin.

Internet-tila

USIM-kortin tila:	USIM-kortti normaali
Verkkotila:	4G
IPv4-tila:	Yhdistetty
IP-osoite:	10.241.163.100
IPv4-nimipalvelin:	62.241.198.245,62.241.198.246
IPv6-tila:	Yhdistetty
IPv6-osoite:	2001:14BB:20:3:5A2C:80FF:FE13:9208/64
IPv6-yhdyskäytävä:	FE80::529F:27FF:FE19:4E4F/64
IPv6-nimipalvelin:	2001:14B8:1000::1,2001:14B8:1000::2

Kuva 25. Internet-yhteyden tila Huawein B593S -reitittimestä katsottuna.

Tarkistin, että tietokoneella on IPv4-osoite ja IPv6-osoite. Huom. Windows 7 luo aina automaattisesti myös toisen väliaikaisen IPv6-osoitteen. Väliaikaista IPv6-osoitetta käytetään tietokoneesta internetiin muodostettujen yhteyksien lähdeosoitteena. Kuva 26 havainnollistaa IP-osoitteet.

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : homerouter.cpe
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : A4-4E-31-5A-71-F4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:14bb:20:3:3482:9fed:6a91:60af(Prefer
red)
   Temporary IPv6 Address. . . . . . : 2001:14bb:20:3:50ab:4cc3:d82c:379b(Prefer
red)
   Link-local IPv6 Address . . . . . : fe80::3482:9fed:6a91:60af%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 8. huhtikuuta 2014 17:40:23
   Lease Expires . . . . . . . . . . : 9. huhtikuuta 2014 17:51:42
   Default Gateway . . . . . . . . . : fe80::529f:27ff:fe19:4e4f%12
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 212094513
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1A-7B-E0-02-A0-48-1C-DB-0A-BA
   DNS Servers . . . . . . . . . . . : 62.241.198.245
                                       62.241.198.246
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Kuva 26. Testikoneen IPv4- ja IP6-osoitteet.

Huawein B593S -reitittimestä löytyi yksi ongelma. Päätelaitteen DNS-kääntäjäpalvelu vastasi tuntemattomasta syystä hitaasti AAAA-nimipalvelinkyselyihin. A-tietueen kyselyihin vastaus tuli normaalisti 400 millisekunnissa, kun taas AAAA-tietueen kysyminen kesti pääsääntöisesti yli 2 sekuntia. Kuvassa 27 on Wiresharkilla kaapattua liikennettä päätelaitteesta. Pakettinumero 587:ssa lähtee AAAA-nimipalvelukysely osoitteesta test-ipv6.com ja paketissa 676 tulee vastaus siihen. Vastausta piti odottaa 2,15 sekuntia. Ongelma korjaantui vaihtamalla tietokoneen DNS-kääntönimipalvelimiksi DNA:n omat nimipalvelimet. Ongelma oli siis Huawein reitittimen DNS-kääntönimipalvelussa. Samaa ongelmaa ei havaittu LG:n G2-puhelimen kautta jaetun yhteyden kanssa.

```
   585 28.5550540 192.168.1.3   192.168.1.1     DNS      73 Standard query 0xe50d  A test-ipv6.com
   586 28.9654910 192.168.1.1   192.168.1.3     DNS     153 Standard query response 0xe50d  A 216.218.228.119
   587 28.9661530 192.168.1.3   192.168.1.1     DNS      73 Standard query 0x11c3  AAAA test-ipv6.com
   589 29.7779160 192.168.1.3   192.168.1.1     DNS      73 Standard query 0x11c3  AAAA test-ipv6.com
   598 30.3890710 192.168.1.3   192.168.1.1     HTTP    427 GET /html/main/refresh.asp HTTP/1.1
   616 30.5899660 192.168.1.3   192.168.1.1     DNS      73 Standard query 0x11c3  AAAA test-ipv6.com
   618 30.6011830 192.168.1.1   192.168.1.3     HTTP    311 HTTP/1.1 200 OK  (text/html)
   676 32.1338440 192.168.1.1   192.168.1.3     DNS     121 Standard query response 0x11c3
   684 32.3632380 192.168.1.3   216.218.228.119 HTTP    407 GET / HTTP/1.1
   696 32.5963650 216.218.228.119 192.168.1.3   HTTP   1341 HTTP/1.1 200 OK  (text/html)
   701 32.6462710 192.168.1.3   216.218.228.119 HTTP    407 GET /index.css?version=1.0.20 HTTP/1.1
   702 32.6463460 192.168.1.3   216.218.228.119 HTTP    397 GET /site/config.js?version=1.0.20 HTTP/1.1
⊞ Frame 587: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
⊞ Ethernet II, Src: a4:4e:31:5a:71:f4 (a4:4e:31:5a:71:f4), Dst: 50:9f:27:19:4e:4f (50:9f:27:19:4e:4f)
⊞ Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: 58825 (58825), Dst Port: 53 (53)
⊟ Domain Name System (query)
    [Response In: 676]
```

Kuva 27. Wiresharkin pakettikaappauksesta näkyy, että AAAA-tietuekyselyn vastaus tulee huomattavan myöhään.

6.1.2 FTP-siirtonopeus

Halusin selvittää, että vaikuttaako käytössä oleva IP-protokollaversio merkittävästi TCP-protokollan suorituskykyyn. Vertasin siirtonopeutta IPv4-protokollan ja IPv6-protokollan välillä käyttäen FTP-protokollaa. FTP-palvelimena käytin ftp.sunet.se -palvelinta. Käytössä oli yksi FTP-yhteys. Siirsin 1,6 gigatavun tiedoston viisi kertaa kummallakin protokollalla. IPv4-protokollaa käyttäen myötäsuunnan nopeuden keskiarvo oli 8,72 Mt/s ja IPv6-protokollaa käyttäen 8,06 Mt/s. Mittaukset tehtiin 25.4.2014 klo 13-15 välisenä aikana.

6.1.3 Web-sivujen vasteaikojen mittaus

Web-sivujen lataantumisien vasteaikoja mitattiin Page Load Time –lisäosalla Chrome-selaimessa. Lisäosa mittaa, kuinka kauan web-sivu latautuu. Aina ennen latausta Windows 7:n ja selaimen DNS-puskuri sekä selaimen välimuisti tyhjennettiin. Mittauksia tehtiin 5 kpl per web-sivu. Mittaukset tehtiin 14.4.2014 klo 15-16 välisenä aikana. Mittauksista selviää, että dual-stack:iä käytettäessä web-sivut latautuvat keskimäärin 21 prosenttia hitaammin kuin pelkän IPv4:n kanssa. Dual stackiä käytettäessä keskiarvoa toi alaspäin Netflixin etusivu, muiden web-sivujen latausajat ovat hyvin lähellä toisiaan. Käytännössä web-sivujen latausnopeuksien eroja on vaikea havaita. Taulukossa 1 on esitetty web-sivujen latausajat dual-stackin ja ipv4:n kanssa.

Taulukko 1. Web-sivujen latausnopeuksien vertailu

Web-sivu	IPv4v6 (sekuntia)	IPv4 (sekuntia)
www.youtube.com	0,73	0,62
www.facebook.com	0,89	0,84

www.netflix.com	2,49	1,85
test-ipv6.com	1,59	1,39

7 Johtopäätökset

Opinnäytetyön teon aikana DNA:n matkaviestinverkon pakettirunkoverkkoon otettiin IPv6-protokolla käyttöön. Kun kaikissa matkaviestinverkon elementeissä on IPv6-protokollalle tuki, se voidaan ottaa käyttöön loppuasiakkaiden liittymiin. Tehtyjen testien perusteella IPv6:n käyttöönotto loppukäyttäjien liittymille on mahdollista ilman suurempia ongelmia. IPv6:n käyttöönotto aiheuttaa muutoksia useaan matkaviestinverkon elementtiin, joista osa on jo tehty lopputyön teon aikana.

Tavoitteena ei ollut tehdä kaiken kattavaa testausta, vaan saada perustason testit tehtyä loppukäyttäjän näkökulmasta. Tiedonsiirtonopeudessa IPv4-protokolla oli kahdeksan prosenttia nopeampi kuin IPv6-protokolla. IPv6-protokollan huonompi siirtonopeus voi johtua siitä, että PGW-laite joutuu pirstaloimaan IPv6-liikeenteen ja vastaavasti LTE-tukiasema joutuu kokoamaan pirstaleet. IPv6-pakettien pirstalointia ja kokoamista joudutaan tekemään, koska SGW-laite ei tue vielä IPv6-liikenteen TCP MSS parametrin pienentämistä. Pienentäminen on suotavaa, jotta pakettikoko saataisiin optimoitua. SGW-laitteelle on tulossa tuki IPv6-liikenteen TCP MSS parametrin pienentämiselle tämän vuoden aikana.

Web-sivujen latausnopeudessa IPv4-protokolla oli 21 prosenttia nopeampi kuin IPv6-protokolla. Web-sivujen latausnopeutta heikensi Netflixin etusivun hidas latautuminen, joka voidaan todennäköisesti korjata käyttöönottamalla IPv6-protokolla Netflix-välimuistiin. Erot ovat kuitenkin sen verran pieniä, että niillä ei ole loppukäyttäjän näkökulmasta käytännön vaikutusta.

Huawei B593S reitittimestä löytyi ohjelmointivirhe, joka hidasti IPv6 DNS-kyselyiden vastauksia. IPv6-protokollaa tukevien päätelaitteiden saatavuuden arvellaan paranevan huomattavasti vuoden 2014 aikana. Aluksi päätelaitteet saattavat tulla sellaisilla asetuksilla, että IPv6-protokolla pitää laittaa manuaalisesti päälle. IPv6:n käyttöönotto saattaa kuitenkin aiheuttaa joidenkin loppukäyttäjien internetyhteyksiin erilaisia ongelmia, jonka takia on tärkeää että asiakaspalvelu, ja muu DNA:n organisaatio on koulutettu ennen käyttöönottoa.

Tulevaisuudessa on syytä pohtia NAT64:n käyttöönottoa. NAT64:n avulla tilaaja, jolla on ainoastaan IPv6-osoite, pystyy liikennöimään myös IPv4-verkkoihin. Näin ollen sen

avulla voisi poistaa IPv4-osoitteiden jaon loppukäyttäjille kokonaan, ja IPv4-osoitteita voitaisiin vapauttaa toiseen käyttötarkoitukseen.

Lähteet

1. Jouni Korhonen, Teemu Savolainen, Jonne Soininen. Deploying IPv6 in 3GPP Networks. Wiley 2013.

2. Robustness principle. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://en.wikipedia.org/wiki/Robustness_Principle.

3. Internet Engineering Task Force. Verkkodokumentti, Luettu 25.3.2014. Saatavissa: http://en.wikipedia.org/wiki/IETF.

4. Internet Protocol. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://tools.ietf.org/html/rfc791.

5. IPv4, Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://en.wikipedia.org/wiki/IPv4.

6. RFC793 - Transmission Control Protocol. verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://tools.ietf.org/html/rfc793.

7. RFC 768 - User Datagram Protocol. verkkodokumentti. Luettu 4.4.2014. Saatavissa: https://tools.ietf.org/html/rfc768.

8. RFC 1518 - Classless Inter-Domain Routing. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://tools.ietf.org/html/rfc1518.

9. RFC 3022 - Traditional IP Network Address Translator. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: https://www.ietf.org/rfc/rfc3022.txt.

10. RFC 2460 - Internet Protocol version 6. verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://www.ietf.org/rfc/rfc2460.txt.

11. Intruduction to IPv6. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://networklessons.com/ipv6/introduction-to-ipv6/.

12. Ericsson Traffic Exploration. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://www.ericsson.com/TET/trafficView/loadBasicEditor.ericsson.

13. About 3GPP. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://www.3gpp.org/About-3GPP.

14. LTE in a Nutshell. Verkkodokumentti. Luettu 25.3.2014. Saatavissa: http://www.tsiwireless.com/docs/whitepapers/LTE%20in%20a%20Nutshell%20-%20Protocol%20Architecture.pdf.

15. First Generation. Verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://en.wikipedia.org/wiki/1G.

16. 2nd Generation. Verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://en.wikipedia.org/wiki/2G.

17. 3rd Generation. Verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://en.wikipedia.org/wiki/3G.

18. IMT-Advanced. Verkkodokumentti. Luettu 4.4.2014. Saatavissa: http://en.wikipedia.org/wiki/IMT_Advanced.

19. GPRS & EDGE. Verkkodokumentti. Luettu 4.4.2014. Saatvissa: http://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge.

20. 3GPP Releases. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://www.3gpp.org/specifications/releases.

21. UMTS. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://www.3gpp.org/technologies/keywords-acronyms/103-umts.

22. 3G UMTS HSPA - High Speed Packet Access Tutorial. Luettu 5.4.2014. Saatavissa: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/umts-high-speed-packet-access-tutorial.php.

23. LTE. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://www.3gpp.org/technologies/keywords-acronyms/98-ltC.

24. E-UTRA. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://en.wikipedia.org/wiki/E-UTRA.

25. LTE-Advanced. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced.

26. Circuit Switched Fallback. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://blog.3g4g.co.uk/2011/02/circuit-switched-fallback-csfb-quick.html.

27. Voice Over LTE. Verkkodokumentti. Luettu 5.4.2014. Saatavissa: http://www.gsma.com/technicalprojects/volte.

28. RFC1918 - Address Allocation for Private Internets. Verkkodokumentti. Luettu 8.4.2014. Saatavissa: https://tools.ietf.org/html/rfc1918.

29. RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. Verkkodokumentti. Luettu 1.5.2014. Saatavissa: https://tools.ietf.org/html/rfc4443.