LAPPEENRANNAN TEKNILLINEN KORKEAKOULU
TIETOTEKNIIKAN OSASTO

DIPLOMITYÖ

VoIP -YHDYSKÄYTÄVÄ

Diplomityön aihe on hyväksytty Lappeenrannan teknillisen korkeakoulun tietotekniikan osaston osastoneuvoston kokouksessa 21.8.2001.

Työn tarkastaja: Professori Pekka Toivanen
Työn ohjaaja: Professori Olli Martikainen

Lappeenrannassa 27.11.2001

Juha Hyttinen
Merenlahdentie 48 A 4
53 850 Lappeenranta

TIIVISTELMÄ

Tekijä: Hyttinen, Juha

Nimi: **VoIP -yhdyskäytävä**

Osasto: Tietotekniikan osasto

Vuosi: 2001

Paikka: Lappeenranta

Diplomityö. Lappeenrannan teknillinen korkeakoulu. 78 sivua, 28 kuvaa, 7 taulukkoa ja 2 liitettä.

Tarkastaja: Professori Pekka Toivanen

Hakusanat: VoIP, yhdyskäytävä, SIP, MGCP, RTP, SDP

VoIP –yhdyskäytävä toimii erilaisten verkkojen liityntäpisteissä tarjoten verkoissa olevan puhelinliikenteen integroimisen yhdeksi kokonaisuudeksi. Tällainen toiminnallisuus on tarpeellinen, koska tulevaisuudessa puhelinverkot ja Internet tulevat sulautumaan toisiinsa. Näin verkkojen väliin tarvitaan palveluita, jotka ymmärtävät molempien verkkojen arkkitehtuureja.

Tämä diplomityö pitää sisällään sekä tutkinnallisia että toteutuksellisia näkökohtia siihen miten VoIP –yhdyskäytävä voidaan toteuttaa uusimmilla kilpailukykyisillä protokollilla vaativaan ympäristöön. Työssä käsitellään IP –verkkojen puhelinpalveluiden toteuttamiseen soveltuvat protokollat tarvittavalla tasolla ja työssä käsitellään Necsom Media Switch –reitittimen sopivuutta VoIP –yhdyskäytävän alustaksi. Työssä esitellään tutkimustyön tuloksia ja erilaisia skenaarioita miten VoIP –yhdyskäytävä tulisi toteuttaa käyttämällä työssä esiintyviä teknologioita. Lopulta esitellään toteutetun VoIP –yhdyskäytävän rakenne ja toiminnallisuus.

VoIP –yhdyskäytävä tarjoaa puhelinpalveluita IP –verkoissa ja samalla mahdollistaa olemassa olevien puhelinverkkojen liikenteen yhdistämisen IP –verkkoihin. Työssä kuvatut tutkimukset ja saavutukset on tehty Necsom Oy:n ja Lappeenrannan teknillisen korkeakoulun yhteistyöhankkeessa. Tuloksia on käytetty hyväksi puntaroidessa VoIP –yhdyskäytävän toiminnallisia vaatimuksia tulevaisuuden vaatimuksien edessä.

ABSTRACT

Author: Hyttinen, Juha

Subject: **VoIP -Gateway**

Department: Information technology

Year: 2001

Place: Lappeenranta

Master's Thesis. Lappeenranta University of Technology 78 pages, 28 figures, 7 tables, and 2 appendices.

Supervisor: Professor Pekka Toivanen

Keywords: VoIP, gateway, SIP, MGCP, RTP, SDP

A VoIP gateway works in the intersection points of the different kind of networks and will integrate voice traffics to single entity. This kind functionality is needed, because in the future the telephone networks and Internet will combine and during this there is need for services that will understand the architectures of the both networks.

This thesis includes both functional and implementation aspects how the VoIP – gateway can be created to very difficult environment using new and competitive protocols. These suitable protocols for implementing telephone services in IP networks are presented and there is also handled how the Necsom Media Switch router will fit as the platform for the VoIP gateway services. Thesis will present some results of the research work and different kind of scenarios how the VoIP gateway should be implemented using the technologies presented in this document. There are introduced the structure and the functionalities of the implemented VoIP gateway.

The VoIP gateway will offer telephone services to IP networks and enables the combination of the voice traffics of the existing telephone networks and the Internet. All research and achievements are achieved in joint venture of the Necsom Ltd and Lappeenranta University of Technology. Results will give good start point for new research work.

ALKUSANAT

Diplomityö on tehty Lappeenrannassa Necsom Oy:n Voice over IP -projektissa Lappeenrannan teknillisen korkeakoulun tietotekniikan osastolle.

Projektiryhmän jäsenet Jari Kellokoski, Ossi Kauranen, Jani Tietäväinen ja Arto Hämäläinen ansaitsevat kiitoksen miellyttävän työympäristön luomisesta ja mielenkiinnosta projektia kohtaan. Nämä asiat ovat mahdollistaneet diplomityöni loppuun viemisen ja projektin mallikkaan etenemisen haluttua lopputulosta kohden.

Kiitän työni tarkastajaa professori Pekka Toivasta kuluttamastaan ajasta työtäni kohtaan ja haluankin antaa erityismaininnan hänen mielenkiinnolleen.

Kiitän työn ohjaajaa professori Olli Martikaista erityisen hyvistä neuvoista diplomityön alkuun saattamiseksi ja sekä asiantuntevista neuvoista diplomityön teon erivaiheissa, mitkä ovat auttaneet tavoitteiden saavuttamisessa.

Viimeisempänä, mutta ei vähimpänä, haluan kiittää erityisesti perhettäni ja heidän ymmärtämystään. Vaimolle erityiset kiitokset kannustuksesta.

SISÄLLYSLUETTELO

KUVAT

TAULUKOT

LIITTEET

LYHENTEET

4G	Fourth Generation
ATM	Asynchronous Transfer Mode
CA	Call Agent
FSR	Frame Synchronized Ring
Gbps	Gigabit per second (1024^3 bit / 1 second)
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
IETF	Internet Engineering Task Force
IP	Internet Protocol
Mbps	Megabit per second (1024^2 bit / 1 second)
MG	Media Gateway
MGC	Media Gateway Control
MGCP	Media Gateway Control Protocol
MS	Media Switch
NMS	Necsom Media Switch
PDA	Personal Digital Assistant
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-in User Service
RFC	Request For Comments
RTCP	Real-time Transfer Control Protocol
RTP	Real-time Transfer Protocol
SDP	Session Description Protocol
SIM	Subscriber Identify Module
SIP	Session Invitation Protocol
SQL	Structured Query Language
WLAN	Wireless Local Area Network
VoIP	Voice over Internet Protocol

1 JOHDANTO

Lähitulevaisuuden kehitysnäkymistä huomataan miten olemassa olevat piirikytkentäiset verkot pyritään muuntamaan pakettikytkentäisiksi verkoiksi, mistä hyvänä esimerkkinä voidaan pitää GSM verkkojen tilalle kaavailtua ja tulevaa GPRS verkkoa, joka on itse asiassa GSM:n laajennus. Tällöin verkot eivät ota kantaa niissä siirrettävään tietoon, vaan äänen lisäksi verkossa voidaan siirtää myös kuvaa sekä dataa. Itse asiassa kaikki verkossa liikutettava tieto näkyy samanlaisena mikä mahdollistaa myös normaalin matkapuhelimen toimenkuvan laajenemisen pelkästä äänensiirtäjästä henkilökohtaiseksi digitaaliseksi avustajaksi (engl. Personal Digital Assistant PDA), jolla on muitakin ominaisuuksia hyötykäytöstä peleihin saakka. Toisaalta olemassa oleva Internet perustuu miltei täysin Internet Protokollaan (IP), joka määrittelee miten tietoa siirretään pakettikytkentäisesti jotain siirtotietä pitkin. Siirtotie on käytännössä fyysinen laite tai keino siirtää tietoa, kuten puhelinyhteys, Ethernet verkko, langaton lähiverkko, ATM jne. Nämä näkökohdat pitää huomioida sekä liitettäessä nykyisiä puhelinverkkoja olemassa oleviin pakettikytkentäisiin verkkoihin että luodessa puhelinpalveluita tämän kaltaisiin kokonaisuuksiin. Tässä tapauksessa pakettikytkentäisellä verkolla tarkoitetaan Internet verkkoa. Tämän hetkinen kehitys on vielä välivaihe tulevaisuuteen, jossa kaikki verkot kuuluvat samaan verkkoon ja yleisesti ottaen perinteiset piirikytkentäiset verkot tulevat vähitellen sulautumaan pakettikytkentäisten verkkojen kanssa.

Tässä työssä tarkastellaan miten VoIP -palvelu saadaan kehitettyä IP –verkkoihin niin, että sen avulla voidaan yhdistää normaali puhelinverkko IP –verkkoihin ja samalla myös tarjota puhelinpalveluita puhtaaseen IP –verkkoon. Tällöin kehitys olisi murrosvaiheessa ja tulevaisuudessa mutkattomampaa, kun on olemassa teknologioita, jotka yhdistävät erilaiset verkot toisiinsa ja samalla tarjoavat pakettikytkentäisille verkoille puhelinpalveluita. VoIP –palvelulla tarkoitetaan tässä työssä lähinnä VoIP –yhdyskäytävää, joka toimii liityntäpisteessä kahden verkon välissä. Jotta VoIP –yhdyskäytävä palvelu voitaisiin toteuttaa, tarvitaan erilaisia teknologioita eri osa-alueiden kuten signaloinnin ja tiedon siirron toteuttamiseksi. Kyseisiin tehtäviin on jo pidempään ollut olemassa ratkaisuna H.323 sateenkaaristandardi, joka pitää sisällään useita eri standardeja. Tämä standardikokoelma alkaa olla suhteellisen vanha ja sen päivitys uusien vaa-

timusten mukaiseksi on lähes mahdotonta, jolloin sitä voidaankin pitää sopimattomana nykyajan tai ainakin tulevaisuuden vaateiden edessä. Toisaalta suhteellisen uusi Internet Engineering Task Force:n (IETF) kehittelemä Session Initation Protocol (SIP) mahdollistaa siirtotiestä riippumattoman signaloinnin ja IETF:n Media Gateway Control Protocol (MGCP) avulla voidaan hoitaa yhdyskäytävän sisäinen signalointi. Molempiin signalointi protokolliin liittyy myös datan siirtoon kehitetty Real-time Transfer Protocol (RTP), jonka avulla siirretään äänitietoa IP –verkoissa. Projektissamme päädyttiin tutkimaan ja käyttämään SIP ja MGCP -protokollia niiden ominaisuuksien ja dynaamisuuden takia ja ne käydään läpi kappaleessa 2.2, jonka jälkeen niitä saatetaan kuvata vielä tarkemmin työn myöhemmissä kohdissa.

Toisaalta työssä tarkastellaan myös sitä miten tämä VoIP –yhdyskäytävä saataisiin istutettua Necsom Oy:n Media Switch (NMS) reitittimeen. Alustavien arvioiden mukaan VoIP –palvelut istuisivat erittäin hyvin NMS -alustalle, koska NMS -reititin on tarkoitus sijoittaa verkkojen reunoille (engl. Edge Router), mistä palveluita voidaan jakaa sittemmin pienille verkoille. NMS -reitittimen rakenne ja toiminta tullaan kuvaamaan kappaleessa 2.

Tässä työssä asiakokonaisuus painottuu lähinnä itse VoIP –yhdyskäytävän suunnitteluun ja toteuttamiseen ja teknologiat käydään lävitse tarvittavalla tasolla. Se mitä pitää huomioida signaloinnissa ja tiedon siirrossa on jätetty tämän työ osalta vähäisemmäksi ja SIP -protokollan puolelta on tehty oma diplomityö liittyen puhelinohjaukseen Internetissä [Kel01]. Tämä työ ja edellä mainittu diplomityö eivät ole täysin erinäisiä toisistaan vaan täydentävät toisiaan, jolloin haluttaessa tietoa enemmän SIP signaloinnista kannattaa lukea myös [Kel01]. Lisäksi VoIP –yhdyskäytävän muista osa-alueista tullaan tekemään muita pienempiä tutkimusraportteja ja konferenssipapereita.

VoIP –projektimme on tehty Lappeenrannan teknillisen korkeakoulun (LTKK) ja Necsom Oy yhteistyönä. Projektijäseninä ovat toimineet Necsom Oy:n puolella Juha Hyttinen ja Jani tietäväinen ja LTKK:n puolella Jari Kellokoski, Ossi Kauranen ja Arto Hämäläinen.

2 YMPÄRISTÖ

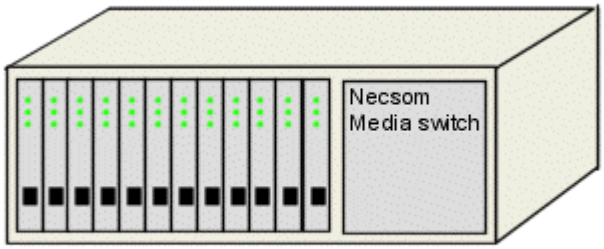
Johdannossa tulikin jo sivuttua ympäristöä, joka pitää sisällään käytettävän alustan ja käytettävät protokollat eli lyhyesti sanottuna projektissa käytetyt teknologiat. Aluksi on hyvä tutustua käytettävään laitteistoon, jolloin saadaan käsitys heti alusta asti millaisesta systeemistä on kysymys ja näin lukija voi itse miettiä, miten kulloinkin kuvailtu asia voisi istua tähän konseptiin. Työssä esitetään yksi ratkaisu, johon tutkimustyömme on päätynyt. Laitteiston kuvauksen jälkeen kuvataan käytetyt protokollat, jolloin lukija saa käsityksen mitä asioita tutkimus-, suunnittelu- ja toteutustyössä on otettu huomioon ja sen millaiseen käyttötarkoitukseen käytetyt protokollat soveltuvat.

2.1 Media Switch

Johdannossa sivutettiin Necsom Media Switch (NMS) käsitettä, jolla tarkoitettaan älykästä reititintä. NMS -reititin oli alustavasti erittäin oleellinen osa projektiamme, sen sydän, ja näin ollen se vaatiikin hiukan enemmän esittelyä. Seuraavana on kuvaus NMS -reitittimen rakenteesta, minkä jälkeen kuvaillaan millaisiin käyttötarkoituksiin NMS -reititintä voitaisiin käyttää. NMS -reitittimen käyttötarkoitukset on hyvä tietää, jotta myöhemmässä vaiheessa tutkittaessa teknologioiden yhdistämistä tiedetään hiukan millaisia vaatimuksia ympäristö asettaa VoIP –yhdyskäytävän toteutukselle.

2.1.1 Media Switch rakenne

Tutkittaessa NMS -reititintä voidaan huomata miten se poikkeaa normaalista reitittimestä, sillä se yhdistää normaalin teleliikenteen ja prosessointi mahdollisuudet käyttämällä ainutlaatuisia teknologioita [Nec01]. NMS -reitittimen rakenne on esitetty korkeammalla tasolla alhaalla olevassa kuvassa, josta saadaan hyvä lähtökohta NMS -teknologian tutkailemiseen. Kuva ei tosin ole mittasuhteiltaan aivan oikea, mutta rakenne tulee esille tarvittavalla tasolla.



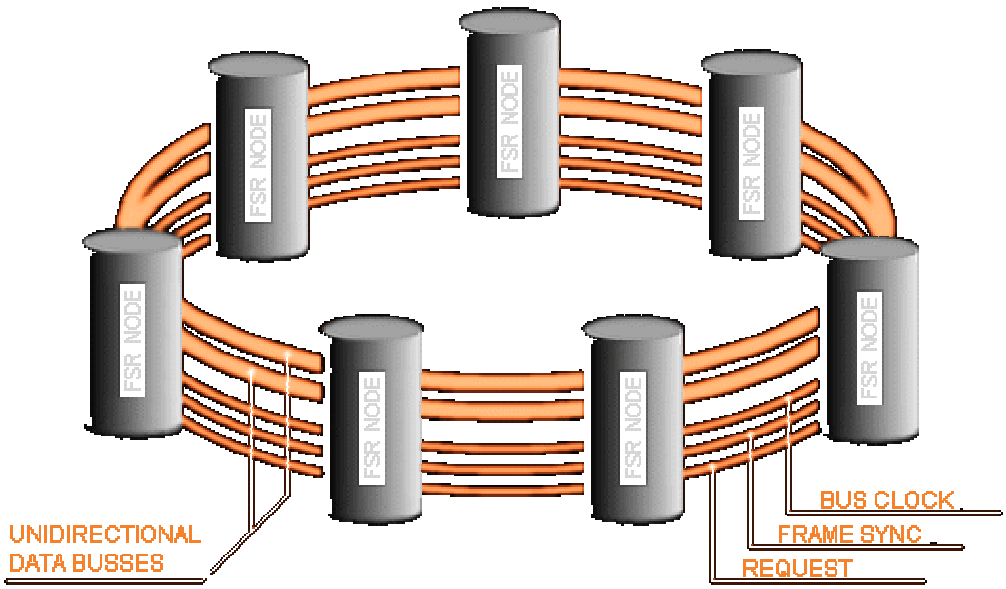
Kuva 1: Necsom Media Switch

Mitä sitten yllä oleva kuva kertoo NMS -reitittimen rakenteesta? NMS –reitittimessä on 12 korttipaikkaa eli yksi NMS -kotelo voi pitää sisällään kortteja enimmillään 12 kappaletta. Ensimmäisessä vaiheessa kortit ovat 100 Mbps Ethernet ja prosessorikortteja, mutta myöhemmin eri tyyppisiä kortteja tulee lisää kuten 1 Gbps Ethernet kortti ja 155 Mbps ATM kortti. Jokainen kortti sisältää prosessoriyksikön, jossa ajetaan Linux käyttöjärjestelmää ja näin ollen esimerkiksi IP paketin saapuessa jollekin kortille se kyetään reitittämään oikean kortin kautta ulos. Reitityspäätöksen tekoon käytetään Linuxin ominaisuuksia ja muutoinkin Linuxin pyöriessä korteilla niille on suhteellisen helppoa suunnitella ja toteuttaa palveluita [Nec01], kuten projektimme VoIP –yhdyskäytävä.

Pääsimme siihen vaiheeseen, että meillä on erilaisia kortteja, joihin on suhteellisen helppo kehittää erilaisia palveluita. Tarkemmin mietittäessä NMS -konseptia huomaamme myös sen, että se soveltuu useaan erilaiseen käyttötarkoitukseen, johtuen sen käyttämistä teknologioista. Kortit saadaan esimerkiksi toimimaan helposti halutulla tavalla, koska niissä toimii standardi Linux ja näin ollen koko NMS -reititin on ohjelmoitavissa halutunlaiseen tehtävään. Rooleja missä NMS voisi toimia on vielä tuntematon määrä, mutta tiedetään, että NMS -reititin toimii hyvin ainakin seuraavanlaisilla telekommunikaatio alueilla: ohjelmoitava reunareititin (engl. Programmable Edge Router), aktiivinen verkon piste (engl. Active Network Node), välimuistipalvelin (engl. Cache Server), näennäisissä yksityisverkoissa (engl. Virtual Private Networks), VoIP -palvelut

(engl. VoIP Services), sisällön toimitus verkoissa (engl. Content Delivery Networks), Langaton mobiliteetti (engl. Wireless Mobility) ja kolmannen ja neljännen sukupolven mobiileissa verkoissa (engl. Services in the 3rd and 4th Generation Mobile Networks) [Nec01].

Edellä esitellyt asiat ovat olleet suhteellisen korkeantasoisia kuvauksia ja päätelmiä, joten on hyvä katsoa hiukan matalammalle tasolle ja tutkia mitä NMS --reititin kätkee sisälleen. Käytännössä loppukäyttäjä huomaa vain sen, että NMS -reitittimessä on useita Linux koneita vierekkäin ja että kuhunkin niistä pääsee käsiksi verkon kautta normaalilla pääteohjelmalla (telnet) ja että kukin kone (kortti) näkee jokaisen NMS -reitittimessä olevan verkon liitynnän omanaan (vaikka käyttäjä on kirjautunut yhdelle kortille). Tämä tarkoittaa sitä, että korttien on kyettävä siirtämään tietoa keskenään jotain muuta reittiä pitkin kuin normaalia tietoliikenneyhteyttä ja NMS -reitittimessä tämän kyseisen tehtävän hoitaa Frame Synchronized Ring (FSR). Yksinkertaisuudessaan FSR sisältää kaksi data-, kello-, synkronointi- ja pyyntöväylän (katso Kuva 2 alhaalla).



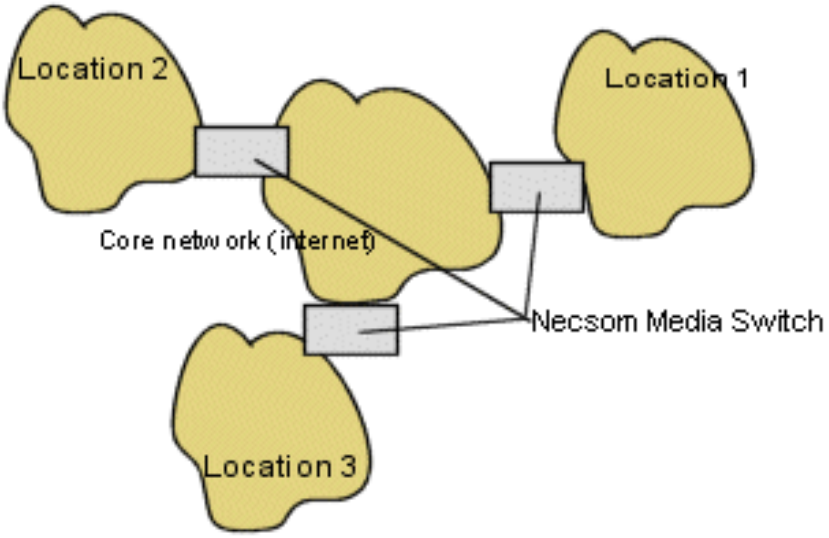
Kuva 2: Media Switch:in arkkitehtuuri

FSR teknologia tukee tiedon lähettämistä samanaikaisesti usealle kortille (engl. broadcast, multicast), mikä tarkoittaa sitä, että NMS -reititin soveltuu erittäin hyvin multime-

diatoteutusten alustaksi kuten esimerkiksi äänen ja videokuvan välitykseen. Edellä oleva kuva on matalimman tason kuvaus NMS –reitittimen toiminnasta, mitä tässä työssä tullaan esittämään. FSR:n teknologiasta ei tarvitse tietää myöhemmässä vaiheessa kuin se, että se on NMS –reitittimen sisäinen tiedonsiirtotapa. Tiedonhaluisimmille työssä on liitteenä taulukko NMS –reitittimen avainarvoista ja tiedoista (Liite 1).

2.1.2 Media Switch käyttömahdollisuuksia

Edellisessä kappaleessa listattiin rooleja missä NMS -reititin on alustavasti suunniteltu käytettävän. Lista pitää sisällään erityyppisiä NMS -reitittimen käyttömahdollisuuksia ja mietittäessä listan sisältöä tarkemmin voidaan huomata, että jokainen rooli koskee lähes poikkeuksetta reunan lähellä olevaan palvelua. ”Reunan lähellä” tarkoitetaan nyt sitä, että NMS -reititin sijaitsee lähellä loppukäyttäjää eli jossakin paikallisessa verkossa, kuten esimerkiksi jonkin kaupan verkkoliikenteen reitittäjänä. NMS -reitittimen tarkoituksena on tarjota suurimmaksi osaksi palveluita verkon reuna-alueilla ja se mitä se tekee siellä ja miten on erittäin oleellista. Jos kuvitellaan, että tällaisia NMS -reitittimiä on laajan verkon reuna-alueilla (kuten kauppojen, liikkeiden, yritysten) verkkoliikenteen reitittäjinä ja samalla ne tarjoavat palveluita verkon käyttäjille. Nämä palvelut voivat olla niin paikallisia kuin laajemman alueen kattavia, mikä tarkoittaa sitä, että keskitetyt palvelut saadaan hajautettua verkkoon sinne, missä niitä tarvitaan ja käytetään. Tässä tuli esille yksi tärkeimmistä rooleista, mitä NMS -reitittimen avulla voidaan toteuttaa eli hajautetun palvelun tarjoaminen, mutta tietysti NMS taipuu vielä monimutkaisempiin paikkoihin, koska sen saa toimimaan rakenteensa avulla halutulla tavalla. Äsken esitettyyn tapaukseen on esitetty alhaalla kuva verkon rakenteesta, jossa on 3 paikallista verkkoa ja joissa tarjotaan omia palveluita käyttäjille, kuten esimerkiksi VoIP –puheluita. Pisteet voivat tarjota myös jotain laajempaa palvelua, joka toimii joka paikassa. Työssä ei käsitellä tarkemmin miten palveluita hallinnoidaan, mutta näin lyhyesti sanottuna Necsom on rakentanut tuotteet palveluiden levittämiseen kyseenalaisissa verkoissa niin laskutus tiedon kuin muun tarvittavan tiedon keräykseen ja hallintaan.



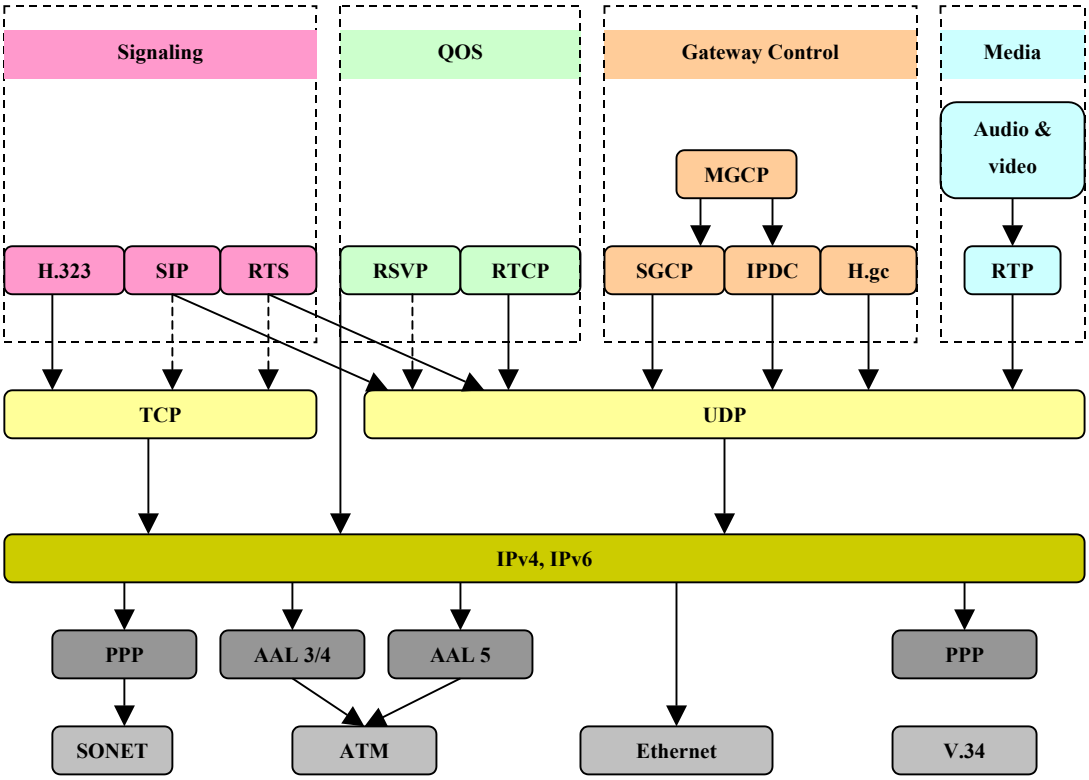
Kuva 3: NMS -verkko rakenne

Listassa on myös mainittu VoIP –palvelut itsenäisenä, mutta mietittäessä mietitään edellisessä kappaleessa esiintynyttä rakennetta voidaan sanoa, että VoIP –palvelut liittyvät oleellisesti muihin kategorioihin. Esimerkiksi neljännen sukupolven mobiiliverkot sisältävät itsestäänselvyytenä VoIP –palvelut, eikä niitä voida sivuttaa siinä tapauksessa lainkaan. NMS -reitittimen käyttämistä reuna-alueilla tarkastellaan vielä tarkemmin kappaleessa 3 ja samalla sivutaan sen erityyppisiä rooleja. Nämä on otettava huomioon kun suunnitellaan VoIP –palvelua, joka kykenee toimimaan erilaisissa paikoissa, joissa NMS -reititintä tullaan tulevaisuudessa käyttämään.

Laitteisto on nyt selvillä korkeammalla tasolla, joten tämän jälkeen on hyvä tutkia niitä tekniikoita, joilla VoIP –palvelu aiotaan tarjota ulkopuolelle. Seuraavassa kappaleessa on kuvaukset käytetyistä protokollista ja siitä miten ne toimivat.

2.2 Protokollat

Kuten johdannossa tuli jo sivuttua, projektissamme päätettiin käyttää pää-asiassa kahta protokollaa VoIP -yhdyskäytävän toteuttamiseksi. Näiden lisäksi pitää esitellä muitakin protokollia,



Kuva 4: Protokolla kerrokset

jotka ovat välttämättömiä VoIP -yhdyskäytävän toteutuksessa. Eli kaksi korkeamman tason protokollaa, jotka hoitavat signaloinnin ja yhdyskäytävän hallinnan ovat Session Initation Protocol (SIP) ja Media Gateway Control Protocol (MGCP). Näiden lisäksi on vielä Session Description Protocol (SDP) ja Real-time Transfer Protocol (RTP). SIP -protokolla hoitaa korkeamman tason signaloinnin ja MGCP yhdyskäytävän hallinnan, kun taas SDP on puhtaasti kuvausprotokolla, jolla saadaan kuvattua halutun yhteyden tyyppi sekä parametrit ja RTP on taas oleellinen itse datan reaaliaikaisessa siirrossa. Protokollat liittyvät itsenäisesti aina kuhunkin osa-alueeseen, jota VoIP -yhdyskäytävä pitää sisällään. Vaikka ne on suunniteltu toisiaan silmälläpitäen, ovat ne periaatteessa

itsenäisiä. Protokollien määrittelyt ovat "Request For Comments" (RFC) muodossa, joten ne eivät ole vielä standardeja. Määrittelyiden käyttäminen on siitä huolimatta suhteellisen turvallista ja standardin omaista, koska esimerkiksi Internetissä käytetty TCP protokolla on edelleen RFC muodossa ja on kuitenkin saavuttanut standardinomaisen aseman. Näin on oletettavissa, että RFC dokumentit tullaan jossain vaiheessa jäädyttämään standardeiksi. Seuraavaksi on tietoa käytettyjen protokollien käyttötarkoituksista ja toiminnallisuuksista.

2.2.1 SIP -protokolla

Session Initiation Protocol (SIP) on Internet Engineering Task Force ryhmittymän (IETF) kehittelemä sovellustason protokolla istuntojen luomiseen, muuttamiseen ja lopettamiseen yhden tai useamman käyttäjän välillä [RFC2543]. Istunnot voivat SIP -protokollan tapauksessa olla konferenssi-, puhelin-, tai multimediaistuntoja, joihin voidaan lisätä käyttäjiä myös istunnon ollessa ylhäällä. Yhteystyyppinä SIP -protokolla käyttää suoraa päästä - päähän yhteyttä, monilähetystä (engl. multicast) tai sitten molempia [RFC2543]. Alhaalla on listattu SIP -protokollan tärkeimmät toiminnallisuudet [RFC2543]:

- Käyttäjän paikantaminen
    - Selvitetään missä järjestelmässä käyttäjä sijaitsee
- Käyttäjän ominaisuudet
    - Selvitetään millaista ja miten koodattua dataa käyttäjä voi käsitellä
- Käyttäjän tavoitettavuus
    - Selvitetään onko käyttäjä halukas liittymään istuntoihin joihin käyttäjä on kutsuttu
- Soiton luominen
    - Luodaan yhteys soittajan ja vastaanottajan välille ja selvitetään istuntoparametrit molempien osalta
- Puhelun hallinta
    - Puhelun siirto, lopetus jne.

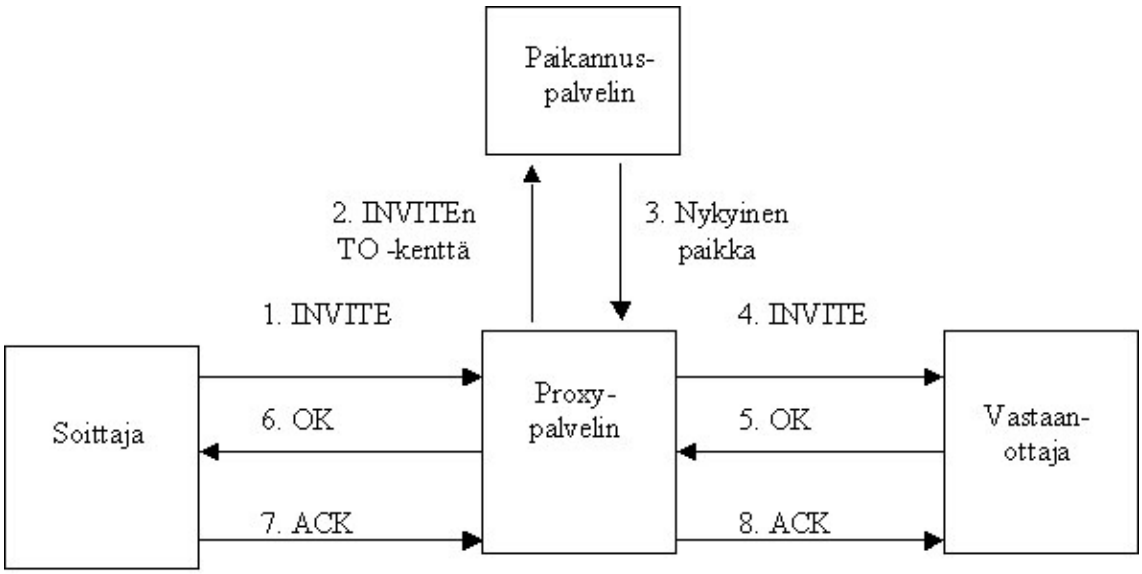
SIP –protokolla on osa IETF:n multimedian kontrollointi ja tietoarkkitehtuuria, johon liittyy kiinteästi monta protokollaa, joten rakennetta johon SIP kuuluu voitaisiin kutsua kommunikaatioperheeksi. Tästä on edellä esitetty kuva (Kuva 1), johon tosin on lisätty MGCP –protokollaan liittyvät protokollat, jotta kuvasta nähdään kokonaisuus paremmin. Joka tapauksessa SIP –protokollaan liittyy hyvin kiinteästi seuraavat protokollat: Reservation Resource Protocol (RSVP) [RFC2205] verkon kapasiteetin varaamiseksi, Real-time Transfer Protocol (RTP) [RFC1889] reaaliaikaisen datan siirtämiseen ja laatupalvelun tietojen keräämiseksi (engl. Quality of Service QoS), Real-time Streaming Protocol (RTSP) [RFC2326] tietovirran kontrolloimiseen, Session Annoucement Protocol (SAP) multimedia-istuntojen mainostamiseen monilähetyksen avulla ja Session Description Protocol (SDP) [RFC2327] multimedia-istuntojen kuvaukseen. SIP –protokolla ei ole kuitenkaan riippuvainen mistään näistä protokollista. [RFC2543]

SIP –protokollaa tarvitaan myös päätelaitteissa, joissa pyörii asiakasohjelmisto, joka hoitaa yhteyden päätelaitteen ja palvelun välillä (esim. toinen päätelaite). Asiakasohjelmisto koostuu asiakas- ja palvelinsovelluksesta, joista asiakassovellus aloittaa yhteyden muodostamisen ja palvelinsovellus ottaa vastaan viestejä ja vastaa niihin yleensä asiakkaan puolesta. Jokainen istunto, jonka asiakasohjelmistot pystyttävät erotetaan toisistaan istuntotunnuksen (Call-Id) avulla. SIP -protokolla pitää myös sisällään muita osia, joilla on erilaiset käyttötarkoitukset. Seuraavassa on kerrottu jokaisesta osasta miten se toimii ja minkälainen käyttötarkoitus sillä on. Kappaleissa ei ole esitetty kutakin tapausta varten yksityiskohtaista signalointia, mutta niissä on esitetty kuvat miten kunkin moduulin systeemi voisi rakentua.

2.2.1.1 SIP –välityspalvelin

Välityspalvelin (engl. Proxy) hoitaa näennäisesti asiakasohjelmiston ja palvelinohjelmiston tehtäviä eli se lähettää edelleen SIP –viestit ja joissain tapauksissa saattaa tehdä muutoksia niihin. SIP –välityspalvelin peittää yhteyden kahden käyttäjän välillä ja näin

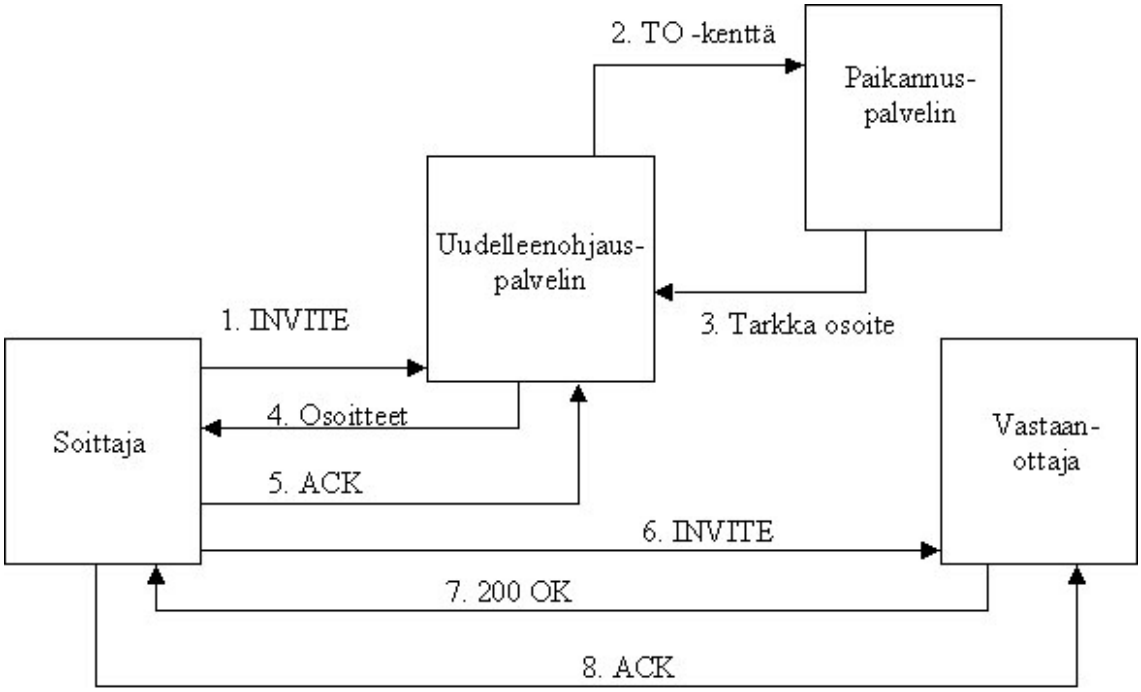
ollen oikeat asiakkaat näyttäisivät keskustelevan SIP –välityspalvelimen kanssa. Alhaalla on kuva miten SIP –välityspalvelin sijoittuu SIP maailmaan.



Kuva 5: SIP –välityspalvelin toiminnallisuus

2.2.1.2 SIP –uudelleenohjaus

SIP – uudelleenohjaus tarkoittaa sitä, että asiakasohjelmisto pyytää tietoja uudelleenohjaus palvelusta, joka sittemmin palauttaa tietoja toisesta osapuolesta. Tämän jälkeen asiakasohjelmisto osaa lähettää pyynnön oikeaan osoitteeseen. Seuraavana on kuva, jossa on esitetty SIP – uudelleenohjauksen toimintaa.



Kuva 6: SIP –uudelleenohjaus palvelun toiminnallisuus

2.2.1.3 SIP –paikannuspalvelu

SIP –paikannuspalvelu on palvelu, josta SIP –välityspalvelin ja SIP –uudelleenohjaus palvelu saavat tietoa asiakkaan sen hetkisestä sijainnista. Normaalisti paikannuspalvelin toimii SIP –välityspalvelimen tai SIP –uudelleenohjauspalvelimen ohella. SIP -protokolla ei määrittele miten paikannuspalvelu tulisi toteuttaa vaan tämä on aina toteutuskohtainen ja niin ikään rajapintaa ei ole määritelty valmiiksi siihen miten paikannuspalveluun päästään käsiksi vaan myös tämä on toteutuskohtainen. Aiemmissa kappaleissa esiintyy kuvat (Kuva 5, Kuva 4), joista nähdään hyvin miten paikannuspalvelu sijoittuu SIP –välityspalvelin ja SIP –uudelleenohjauspalvelimen kanssa.

2.2.1.4 SIP –rekisteröintipalvelu

Rekisteröintipalvelu ottaa vastaan rekisteröinti viestejä asiakasohjelmistoilta. Yleensä tämä palvelu toimii SIP –välityspalvelimen tai SIP –uudelleenohjaus palvelun ohella tarjoten tietoa paikannuspalvelulle, josta tietoja voidaan myöhemmin ammentaa esim. SIP –välityspalvelimen ja SIP –uudelleenohjauksen käyttöön.

2.2.1.5 SIP –viestit ja niiden rakenteet

SIP -viestit ovat muodoltaan pelkkää tekstiä, joka tarkoittaa sitä, että viestit voidaan siirtää millaista siirtotietä pitkin tahansa. Siirtotiellä ei ole senkään suhteen vaatimuksia, että onko se yhteydellinen vai yhteydetön, koska SIP –protokollan määritelmä määrittelee, että SIP -viestejä voidaan siirtää kummankin kaltaista siirtoteitä pitkin. Tämä siksi, koska SIP –protokollassa on käytännöt, joilla varmistetaan tai vähintään tarkistetaan, että SIP -viesti on otettu vastaan. Käytännössä se tarkoittaa, että pyyntö lähetetään uudelleen jos siihen ei ole tullut tietyn ajan kuluessa vastausviestiä. Esimerkiksi Internetissä on käytössä TCP/IP ja UDP/IP yhteydet, joista edellinen on yhteydellinen ja jälkimmäinen on yhteydetön ja SIP –protokolla toimii kummankin yhteyskäytännön päällä. Näistä UDP on normaalisti käytetty yhteyskäytäntö. Ennen kun esitellään SIP -viestejä niin käydään lävitse SIP -viestin tyypit.

SIP -viestejä on kaksi erityyppistä: pyyntö- ja vastausviestit, joista jälkimmäinen seuraa melkein aina ensimmäistä. Seuraavaksi on lista SIP -pyyntöviestien tyypeistä ja samassa on kuvaus mitä pyynnöllä tehdään.

Pyyntöviesti	Ymmärrettävä tätä viestiä
Pyyntöviestin kuvaus	
INVITE	*Välityspalvelu, Uudelleenohjaus, Asiakasohjelmisto*
Tämä metodi kertoo, että käyttäjä tai palvelin pyydetään osallistumaan istuntoon. Viestin runko-osassa voi olla SDP –protokolla (*kappale 2.2.3*), joka kuvaa istuntoon ehdotetut parametrit.	
ACK	*Välityspalvelu, Uudelleenohjaus, Asiakasohjelmisto*
Viesti on kuittaus asiakkaan puolesta INVITE –viestiin. ACK –viestejä käytettään ainoastaan INVITE –viestien kanssa. ACK –viesti voi sisältää kuvauksen istunnosta (SDP), jos esim. INVITE viesti ei sitä sisältänyt.	
OPTIONS	*Välityspalvelu, Uudelleenohjaus, Asiakasohjelmisto*
Tämän metodin avulla kysellään SIP -palvelimen ominaisuuksia.	
BYE	*Välityspalvelu*
Viesti kertoo että asiakasohjelma haluaa poistua nykyisestä istunnosta. Kumpi tahansa osapuoli (soittaja tai vastaanottaja) voi lähettää viestin. BYE –viestit välitetään kuten INVITE –viestitkin.	
CANCEL	*Välityspalvelu*
Metodin avulla voidaan perua istuntoon osallistuminen istunnon muodostamisen aikana. Mikäli istunto on jo keritty muodostaa, CANCEL viesteillä ei ole merkitystä. CANCEL –viesti peruu sen istunnon muodostuksen, jonka Call-ID, To, From ja Cseq –kentät ovat samat kuin CANCEL –viestissä.	
REGISTER	
Tämän viestin avulla asiakasohjelma rekisteröi To –kentässä olevat osoitteet SIP –palvelimelle ja niille URI –osoitteille, jotka mainitaan Contact –otsikkokentissä. Huomattavaa on että nämä URI –osoitteet voivat olla mitä tahansa URI –osoitteita ei pelkästään SIP –protokollan mukaisia osoitteita.	

Taulukko 1: SIP -pyyntöviestien tyypit

Edellä oleva taulukko esitteli kaikki pyyntöviestit, mutta niihin liittyviä vastausviestejä ei ole vielä käsitelty. Siinä missä edellä olleet pyyntöviestit määrittelevät minkälaisesta viestistä on kysymys, niin vastaus puolella vastaustyypit ovat määritelty numeroilla seuraavan taulukon mukaisesti.

Vastaus koodit	Kuvaus
1XX	Informointi, viesti on vastaanotettu ja käsittely jatkuu
2XX	Hyväksyntä, viesti on vastaanotettu, ymmärretty ja hyväksytty
3XX	Uudelleen ohjaus, viestin käsitteleminen vaatii uusia toimenpiteitä
4XX	Asiakasohjelmiston virhe, viestin syntaksi on väärä tai viestiä ei voi käsitellä tällä palvelimella
5XX	Palvelinohjelman virhe, viestin käsittelyssä palvelimella tapahtui virhe, viesti on oletettavasti oikeanlainen.
6XX	Yleinen virhe, viestiä ei voida käsitellä millään palvelimella

Taulukko 2: SIP -vastausviestien tyypit

Edellä listatuista vastausviesteistä normaalisti ja useimmiten esiintyvä vastausviesti on 200, joka on ”ok” –viesti ja tarkoittaa, että kaikki on mennyt oikealla tavalla. RFC2543 [RFC2543] esittelee tarkemmin kaikki vastausviestit. Kuten aiemmin tuli mainittua SDP liittyy SIP -protokollaan ja se voi olla minkä SIP –viestin mukana tahansa, niin pyyntö- kuin vastausviestissä. SDP –protokollan ja SIP –protokollan yhteen toimivuudesta on kerrottu lisää kappaleessa 2.2.3.1. Seuraavaksi on kuva SIP -viestistä.

```
INVITE sip:watson@boston.bell-tel.com SIP/2.0
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip:a.g.bell@bell-
tel.com>;tag=3pcc
To: T. Watson <sip:watson@bell-tel.com>
Call-ID: 662606876@kton.bell-tel.com
CSeq: 1 INVITE
Contact: <sip:a.g.bell@kton.bell-tel.com>
Subject: Mr. Watson, come here.
Content-Type: application/sdp
Content-Length: ...

v=0
o=bell 53655765 2353687637 IN IP4 128.3.4.5
s=Mr. Watson, come here.
t=3149328600 0
c=IN IP4 kton.bell-tel.com
m=audio 3456 RTP/AVP 0 3 4 5
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:4 G723/8000
a=rtpmap:5 DVI4/8000
```

Kuva 7: SIP -viesti

Edellä olevassa kuvassa on esitetty INVITE –viesti, jossa kulkee mukana SDP -kuvaus. SIP –viesti muistuttaa ulkonäöltään HTTP:n syntaksia (HyperText Transfer Protocol), joka johtuu siitä, että SIP -protokollan syntaksi on suunniteltu käyttämällä HTTP:stä tuttua rakennetta hyväksi. Näin on saatu käytettyä uudelleen jo olemassa olevaa tietoutta ja ohjelmoijat tietävät jo tutuksi tulleen rakenteen hyvin, jolloin opetteleminen ei ole niin paljon työtä vaativaa. Toisaalta on olemassa valmiita kokoojia (engl. parser), jotka ymmärtävät HTTP:n tapaista syntaksia ja nämä kokoojat saadaan uusilla määrittelyillä toimimaan myös SIP -viestin parsimisessa. Eli yksinkertaisesti vanhaa hyvää teknologiaa on käytetty uudelleen hyväksi.

2.2.2 MGCP –protokolla

Media Gateway Control Protocol (MGCP) on Internet Engineering Task Force (IETF) kehittelemä protokolla, jonka avulla hallinnoidaan yhdyskäytävän sisäisiä toimintoja. Seuraavana on muutama kappale, jotka selostavat pääpiirteittäin MGCP -protokollan toiminnallisuutta ja kappaleet on kategorisoitu pieniin kokonaisuuksiin.

2.2.2.1 MGCP perustietoa

Media Gateway Control Protocol -protokollan (MGCP) avulla ulkoinen mediayhdyskäytävän kontrolloija (engl. Media Gateway Controller, MGC), toiselta nimeltään Puhelu Agentti (engl. Call Agent, CA), kykenee hallinnoimaan puhelinyhdyskäytäviä, jotka tarjoavat tiedonmuuntamispalvelun piirikytkentäisten äänisignaalien ja pakettiverkkojen pakettien välillä [RFC2705]. RFC 2705 luettelee esimerkkinä muutamia yhdyskäytävän tyyppejä, mutta ne on laitettu ainoastaan esimerkiksi, koska RFC:ssä ei haluta rajata MGCP -protokollan käyttömahdollisuuksia. Näin ollen MGCP -protokollaa on mahdollista käyttää mitä erilaisimmissa paikoissa ja mitä erilaisimpiin tarkoituksiin, kunhan sen käyttö pysyy RFC2705 määrittelemissä puitteissa. Seuraavassa luetellaan muutamia erilaisia RFC2705:stä löytyviä yhdyskäytävätyyppejä, jotta lukija saisi käsityksen siitä millaisia yhdyskäytäviä MGCP -protokollan avulla voidaan hallinnoida.

- Trunking gateway

  Yhdistää puhelinverkon Voice over IP verkkoon.
- Voice over ATM gateway

  Toimintaperiaate sama kuin edellisessä, mutta tieto liikkuu ATM verkkojen kautta.
- Residental gateway

  Tarjoaa perinteisen analogisen (RJ11) liitännän Voice over IP verkkoon
- Access gateway

  Tarjoaa perinteisen analogisen (RJ11) liitännän tai digitaalisen PBX liitännän Voice over IP verkkoon .

- Business gateway

  Tarjoaa perinteisen digitaalisen PBX liitännän tai integroidun "pehmeän PBX" (pehmeä tarkoittaa ohjelmistolla toteutettua) liitännän Voice over IP verkkoon
- Network Access Servers

  Pystyvät tarjoamaan modeemin puhelinverkkoon (piiriin) ja samalla tarjoamaan pääsyn Internetiin.
- Circuit switches or packet switches

  Tarjoaa hallinnointi rajapinnan ulkoiselle kontrollointi elementille.

Edellä esiteltiin valmiiksi mietittyjä ja jo olemassa olevia yhdyskäytävätyyppejä, mutta mikään edellä oleva ei kuvaa projektissamme suunniteltua yhdyskäytävän rakennetta, joka tullaan selvittämään tarkemmin kappaleessa 3. Seuraavana tutkitaan MGCP -protokollan rakennetta matalammalla tasolla.

2.2.2.2 MGCP hallinnoimat päätepisteet

Tutkittaessa MGCP –protokollan rakennetta huomataan, että se luo, tuhoaa ja hallitsee päätepisteitä(engl. endpoint, EP) ja niissä olevia yhteyksiä. Nämä päätepisteet ovat normaalisti yhteyksiä puhelimeen, josta sittemmin luodaan yhteyksiä toisessa yhdyskäytävässä tai sitten samassa yhdyskäytävässä oleviin päätepisteisiin. Päätepisteet määrittelevät toiminnallisuuden jokaiselle yhteydelle ja soitolle, jolloin yhdyskäytävässä voi tapahtua tiedon muuntaminen erityyppisestä koodauksesta toiseksi (esim. mu-law <--> G.723). RFC 2705 esittelee erityyppisiä yhdyskäytävätyyppejä ja erilaisia päätepisteitä, mutta tämä voi olla harhaan johtavaa, sillä valmistajat ja ohjelmoijat voivat itse määritellä erityyppisiä yhdyskäytäviä ja erityyppisiä päätepisteitä yhdyskäytävään [RFC2705]. Kuten aiemmin ja nyt tuli esille RFC 2705 esittelemät asiat ovat lähinnä triviaaleja esimerkkejä ja se ei pakota käyttämään mitään tiettyjä vaan antaa vapauden tekijöille määritellä uusia erilaisia yhdyskäytäviä erilaisineen päätepisteineen.

RFC 2705 esittelemät päätepisteet:

- Digital channel (DS0)
- Analog line
- Announcement server access point
- Interactive Voice Response access point
- Conference bridge access point
- Packet relay
- Wiretap access point
- ATM "trunk side" interface.

Päätepisteitä on kahdenlaisia: normaaleja päätepisteitä ja näennäisiä päätepisteitä, joista edelliset tarkoittavat rautatason ratkaisuja ja jälkimmäiset ohjelmistolla toteutettuja ratkaisuja. Tässä vaiheeseen riittää tietää, että yhdyskäytävä sisältää päätepisteitä, joita MGCP -protokollan avulla hallinnoidaan MGC:ltä, ja että päätepisteet määrittelevät yhdyskäytävän toiminnallisuuden kullekin yhteydelle ja loppukädessä puhelulle.

2.2.2.3 MGCP -viestien tyypit

MGCP -protokolla sisältää yhdeksän erilaista viestityyppiä, joilla pyyntöjä lähetetään joko MGC:ltä MG:lle tai toisin päin. Kaikki viestit eivät kulje molempiin suuntiin vaan MGC lähinnä hallinnoi MG:tä, jolloin MG:n lähettämät viestit MGC:lle ovat vastauksia tai sitten ilmoituksia tapahtumista. Seuraavassa taulukossa on esitetty viestityypit ja se mitä niillä tehdään. Siinä kerrotaan myös mihin suuntaan viestit kulkevat eli kulkevatko ne MGC:ltä MG:lle, MG:ltä MGC:lle vai molempiin suuntiin.

Pyyntöviesti	**Suunta**
Pyyntöviestin kuvaus	
EndpointConfiguration	**MGC → MG**
Pyynnöllä voidaan muuttaa koodaus tapaa puhelinlinjan puolella. (a-law tai mu-law koodaus)	
NotificationRequest	**MGC → MG**

Pyynnöllä pyydetään yhdyskäytävään tarkkailemaan tiettyjä tapahtumia, kuten puhelimen luurin ylös nostoja/ alas laittoja , DTMF sointuja (DTMF Tone) jne.	
Notify	**MGC ← MG**
Yhdyskäytävä käyttää tätä pyyntöä ilmoittaakseen MGC:lle tapahtumista, joita ollaan pyydetty tarkkailemaan.	
CreateConnection	**MGC → MG**
Pyynnöllä pyydetään yhdyskäytävää luomaan yhteys, joka päätyy johonkin päätepisteeseen yhdyskäytävän sisällä.	
ModifyConnection	**MGC → MG**
Pyynnöllä muokataan aiemmin luodun yhteyden parametreja.	
DeleteConnection	**MGC ←→ MG**
Pyynnöllä pyydetään yhdyskäytävää tuhoamaan olemassa oleva yhteys. Yhdyskäytävä voi myös itse ilmoittaa MGC:lle tällä pyynnöllä, kun jotain yhteyttä ei enää ole olemassa.	
AuditEndpoint ja AuditConnection	**MGC → MG**
MGC käyttää näitä pyyntöjä saadakseen tietoa päätepisteistä ja yhteyksistä.	
RestartInProgress	**MGC ← MG**
Yhdyskäytävä ilmoittaa MGC:lle tällä komennolla, että jokin ryhmä päätepisteitä on otettu pois päältä ja laitettua takaisin päälle.	

Taulukko 3: MGCP -viestien tyypit

Viestien toiminnallisuudet viittaavat hyvin paljon siihen, että tarkoituksena on yhdistää piirikytkentäinen verkko pakettikytkentäiseen verkkoon. Aiemmin kuvailtu NMS –reititin on taas oma konseptinsa, jolloin MGCP -protokollan istuttaminen on jokseenkin hankalaa ja vaatii paljon miettimistä. Tätä seikkaa mietitään tarkemmin kappaleessa 3.

Vastaus koodit	Kuvaus
000 – 099	Vastauksen hyväksyminen / kuittaus
100 – 199	Tilapäinen vastaus
200 – 299	Onnistunut suoritus

400 – 499	Hetkellinen virhe
500 – 599	Pysyvä virhe
800 – 899	Paketille ominaiset vastaus koodit

Taulukko 4: MGCP -vastauskoodien tyypit

Taulukko 3 esitti MGCP -protokollan pyyntöviestien tyypit ja Taulukko 4 esittää taas vastaavasti vastausviestien tyypit korkealla tasolla. Vastaus viestejä ei ole lueteltu kattavasti tässä vaan ne löytyvät RFC2705:sta [RFC2705]. Kuten huomataan MGCP -protokollassa on erilaisia vastauksia, jotka indikoivat erityyppisiin tapauksiin. Vastaukset voivat olla pysyviä virheitä tai sitten väliaikaisia. Esimerkiksi jos puhelimen luuri on ylhäällä MGCP -protokolla luo tällöin väliaikaisen viestin tai sitten jos yhteyksien siirtokapasiteetti on varattu täyteen niin tällöin vastauksena tulee pysyvä virhe. Mutta siihen mitä vastauksia itse asiassa syntyy emme puutu ainakaan nyt, koska se ei ole vielä tässä vaiheessa olennaista.

2.2.2.4 MGCP - viestien rakenne

MGCP -viesti rakentuu puhtaasta tekstistä eli viestin käsittelyssä ei tarvitse huomioida alustaa, jossa käsittely tapahtuu. Kyseessä voi olla esimerkiksi Big Endian tai Little Endian käyttöjärjestelmä (Esimerkiksi PowerPC ympäristö käyttää Big Endian muistihierarkiaa ja Intel taas Little Endian muistihierarkiaa). Tarkemmin Big Endian ja Little Endian tyypeistä voi lukea vaikka Richard Stevens:in "Unix -Networkin Programming" -kirjasta [Ste98]. Tekstimuotoinen viesti mahdollistaa käytännössä sen, että viesti voidaan siirtää käyttäen millaista siirtotietä tahansa joten MGCP -protokolla ei ole riippuvainen fyysisestä alustasta tai siirtotiestä, jolloin se toimii myös mitä erilaisemmissa paikoissa. Viesti rakentuu periaatteessa kolmesta erilaisesta kohdasta, jotka on seuraavaksi selitetty lyhyesti.

- Otsake

Kertoo onko kyseessä pyyntö- vai vastausviesti ja sen minkä tyyppinen viesti on kyseessä.

- Parametrit

  Parametreja on olemassa useita jotka on määritelty kirjaimilla. Esimerkiksi "C:" tarkoittaa, että kyseessä on ”Call-Id” -parametri. Parametreja voi olla monta, kuten usein onkin, ja kukin parametri sijaitsee omalla rivillään.

- SDP

  Parametrien jälkeen voi tulla Session Description Protocol (SDP), joka tullaan kuvailemaan kappaleessa 2.2.3

Viestin rakenne ja muoto mahdollistavat MGCP -protokollan jatkokehitystyön sillä siihen on helppo rakentaa tarvittaessa lisää erilaisia parametreja tai muokata vanhoja määrittelyitä. Tosin määrittelymuutokset vaikuttavat jo olemassa oleviin ratkaisuihin, mutta näihin tulevat muutokset on yleensä helppo toteuttaa. Seuraavassa esitellään esimerkki viestiparista eli pyynnöstä ja vastauksesta (Kuva 8 ja Kuva 9).

```
CRCX 1204 aaln/1@rgw-2567.whatever.net MGCP 1.0
C: A3C47F21456789F0
L: p:10, a:PCMU
```

Kuva 8: MGCP -pyyntöviesti

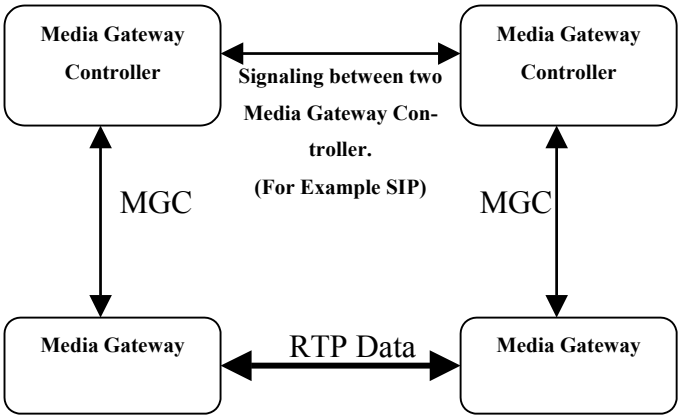
```
200 1204 OK
I: FDE234C8

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP
```

Kuva 9: MGCP -vastausviesti

Edellä oleva esimerkki luo uuden yhteyden Media Yhdyskäytävään (engl. Media Gateway, MG). Siinä lähetetään aluksi yhteyden luomispyyntö, johon odotetaan vastausta. Kun vastaus saapuu niin se sisältää SDP -kuvauksen luodusta yhteydestä. SDP -protokollasta tullaan selittämään kappaleessa 2.2.3 tarkemmin.

2.2.2.5 MGCP - viestien kulku

Viestin kulkeminen on suhteellisen yksinkertainen tapahtumaketju, mutta ketju nimitys on nyt tässä tapauksessa hieman harhaanjohtava, koska MGCP -protokolla ei oleta, että jokin viesti tyyppi tulee aluksi vaan sen avulla voidaan komentaa alhaalla olevaa yhdyskäytävään miten halutaan. Luonnollisestihan yhteyden pitää olla luotu aluksi ennen kuin sitä voidaan muokata. Eli MGCP -protokollan avulla yhdyskäytävää komennetaan yksiselitteisillä käskyillä ja se miten mihinkin viestiin reagoidaan riippuu täysin sovelluksesta.



Kuva 10: Kaksi MGCP yhdyskäytävää

Jos soitossa on kaksi erillistä MGC:tä, jotka hallinnoivat kahta erillistä yhdyskäytävää, niin on huomioitava se, että RFC2705:n mukaan nämä MGC:t ovat synkronoitava niin, että ne lähettävät yhtenäisiä viestejä yhdyskäytävälle. RFC2705 ei puutu siihen miten MGC:t synkronoidaan, mutta siinä on mainittu, että SIP -protokolla sopii yhtenä vaihtoehtona kyseiseen tehtävään.

2.2.3 SDP –protokolla

Session Description Protocol (SDP) on IETF:n määrittelemä protokolla kuten aiemmin esitellyt SIP –protokolla ja MGCP –protokolla. SDP -protokollaa voidaan pitää suhteellisen itsenäisenä, koska sen tehtävä on vain kuvata pyydetyn istunnon ominaisuuksia. Se ei puutu siihen miten tieto siirretään paikasta toiseen vaan tämä on jätetty toisen protokollan hoidettavaksi (SIP, MGCP). Toisaalta SDP -protokollan käyttäminen on häilyväistä, koska SIP –protokollan puolella SDP –protokollalla on joissain tapauksissa tarpeellinen rooli signaloinnissa. SIP –ja SDP –protokollien suhteesta kerrotaan lisää kappaleessa 2.2.3.1. Seuraavaksi on esitetty SDP -kuvauksesta kuva, jotta SDP -viestin rakenne olisi alusta asti selvillä ja että asiat, joita tullaan myöhemmin tässä kappaleessa mainitsemaan, olisi helpompi ymmärtää.[RFC2327]

```
v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

Kuva 11: SDP -kuvauksen esimerkki

Edellä olevasta kuvasta huomataan helposti, että SDP –kuvauksen rakenne on erittäin yksinkertainen. Se on muotoa: <Viestin tyyppi>=<Arvo>. Ensimmäinen kirjain kullakin rivillä ilmaisee mitä tietoa sillä rivillä on eli mikä parametri on kyseessä, minkä jälkeen seuraa itse parametrin arvo määritellyssä muodossa. Rivin rakenteelle on oleellista se, että ”=” –merkin kummallakaan puolella ei saa olla välilyöntiä. SDP –protokollan toimivuuden kannalta on väliä missä järjestyksessä parametrit ovat. Esimerkiksi ”v=” –parametri on aina SDP -kuvauksen ensimmäinen parametri ja jos SDP -kuvauksia on useita peräkkäin ”v=” aloittaa aina uuden SDP -kuvauksen. SDP -kuvauksen rakenne on määritelty liitteessä 2 yleisellä tasolla ja siinä on myös esitelty edellä oleva SDP -kuvaus.[RFC2327]

SDP -kuvaus kuvaa yhteydestä seuraavanlaisia asioita: istunnon nimi, istunnon tarkoitus, aika tai ajat jolloin istunto on aktiivinen, käytettävä media ja tarvittava tieto median kuvaamiseksi. Näistä mediankuvaukset ovat oleellisimpia, koska niitä käytetään itse

yhteyksien luomiseen ja ne kertovat myös käytettävät siirtoprotokollat. Seuraavassa on tietoa SDP -protokollan mediankuvauksen parametreista ja siitä mitä ne sisältävät:

Tieto	Tiedon sisältö	Esimerkki
Median tyyppi	Audio, video	m=**audio** 49170 RTP/AVP 0 m=**video** 51372 RTP/AVP 31
Siirtoprotokolla	RTP /UDP/IP, H.320	m=audio 49170 **RTP/AVP** 0 m=video 51372 **RTP/AVP** 31
Median formaatti	H.261, video, MPEG video	m=audio 49170 RTP/AVP **0** m=video 51372 RTP/AVP **31**
Monilähetyksissä	Monilähetysosoite ja portti	c=IN IP4 **224.2.17.12/127** m=audio **49170** RTP/AVP 0 m=video **51372** RTP/AVP 31
Yksilähetyksessä	IP -osoite ja portti	c=IN IP4 **128.96.41.1** m=audio **49170** RTP/AVP 0 m=video **51372** RTP/AVP 31

Esimerkki sarakkeessa kulloinkin tarkasteltu asia on piirretty vahvistettuna

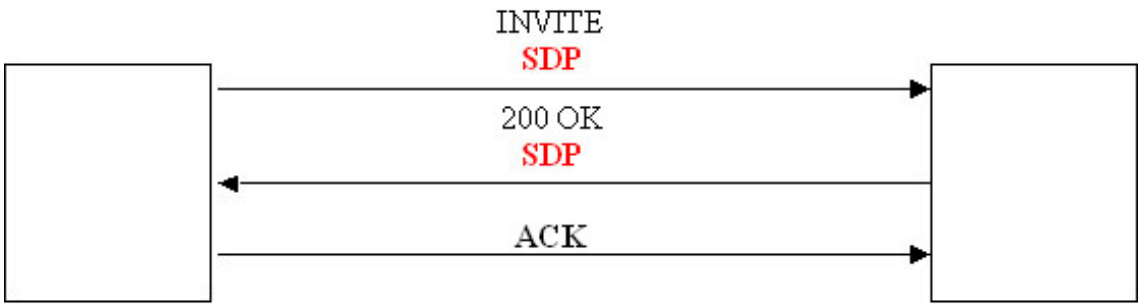
Taulukko 5: SDP -viestin median tiedot

Edellä olevassa taulukossa on kerrottu mitä asioista SDP -kuvauksen media-osio kertoo ja asioita on havainnollistettu ottamalla aiemmin esiintyneestä kuvasta (Kuva 11) kenttiä esimerkiksi. Mediaformaatissa huomataan, että esimerkissä formaattina on pelkkä numero, joka on itse asiassa lyhenne formaatille. RTP:n RFC:n taulukko 2:ssa on luetteltu valmiiksi määriteltyjä arvoja standardeja formaatteja varten [RFC1890].

2.2.3.1 SDP –protokolla ja SIP –protokolla

SIP –protokolla hoitaa signaloinnin ja sen jokaisen viestityypin lastina voi olla SDP -kuvaus. SDP –protokollaa tarvitaan istunnon parametrien kuvaukseen, kuten äskeisessä SDP –protokollan kappaleessa tulikin esille. SIP –protokollassa SDP -protokollaa käy-

tetään eniten istunnon luontivaiheessa, jolloin tietoa vaihdetaan päätepisteiden välillä. Seuraavassa on kaksi tapausta, joissa SDP -protokollaa käytetään istunnon luomisvaiheessa.



Kuva 12: SDP kulkeutuu INVITE - ja vastausviestin mukana

Edellä olevassa esimerkissä SDP -kuvaus kulkeutuu soittajalta INVITE viestin mukana, mikä tarkoittaa sitä, että vastaanottaja on heti tietoinen soittajan istunnon parametreista. Näin ollen vastaanottaja vastaa vastausviestillä ja lähettää sen mukana oman SDP –kuvauksen, minkä jälkeen soittaja vielä kuittaa yhteyden muodostamisen. Tämän jälkeen tietoa voidaan siirtää SDP -kuvauksien kuvaamien ominaisuuksien mukaan.

Kuva 13: SDP kulkeutuu vastausviestin ja ACK –viestin mukana

Edellä olevassa esimerkissä ensimmäinen SDP -kuvaus kulkee vasta vastaanottajan vastausviestissä, mikä tarkoittaa sitä, että soittajan pitää lähettää oma SDP -kuvaus ACK –viestin mukana. Nämä edellä olevat tapaukset ovat toisensa pois sulkevia. Tosin SIP -

protokollan määritykset eivät ota kantaa missä viesteissä SDP –kuvaus kulkee vaan se voidaan liittää jokaiseen viestiin, mutta on toinen asia miten tämä tieto käsitellään.

2.2.3.2 SDP -protokolla ja MGCP -protokolla

SDP -protokollan suhde MGCP -protokollaan on suoraviivainen sillä MGCP -protokolla käyttää SDP -protokollaa vain kuvatakseen yhteyden osapuolien tiedot. MGCP -protokollassa SDP -kuvaus liikkuu ainoastaan yhteyden luontiviestin (CRCX) ja yhteyden muokkausviestin (MDCX) mukana. SDP -kuvaus liitetään suoraan MGCP -viestin perään eikä se kuulu minkään MGCP -viestin parametrin taakse (kts. Kuva 9). Seuraavassa on yksinkertainen esimerkki, jossa yhteys luodaan kahden päätepisteen välille.

1) MGC eli Call Agent pyytää yhdyskäytävää 1 luomaan uuden yhteyden päätepisteeseen, mihin käytetään MGCP -protokollan yhteyden luomispyyntöä (CRCX). Yhdyskäytävä luo uuden yhteyden CRCX -viestin tullessa ja palauttaa vastausviestissä oman paikallisen SDP -kuvauksen, joka siis kuvaa yhteyden. Nyt tämän ensimmäisen päätepisteen yhteys on vastaanotto asennossa, koska se ei vielä tiedä minne tietoa pitäisi lähettää.

2) Edellisen vaiheen jälkeen MGC eli Call Agent pyytää toista yhdyskäytävää (tai samaa) luomaan uuden yhteyden toisen päätepisteen sisään, mihin jälleen käytetään MGCP -protokollan yhteyden luomispyyntöä (CRCX), mutta sillä erotuksella, että tähän pyyntöön laitetaan sisään edellisestä yhteyden luomisesta saatu SDP -kuvaus. Nyt yhdyskäytävä saa luotua uuden yhteyden ja tietää myös samalla toisen eli ensimmäisen päätepisteen yhteyden kuvauksen, jolloin yhteydestä saadaan kumpaankin suuntaan toimiva (vastaanottava ja lähettävä). Yhteyden luomispyyntö palauttaa nyt vastauksena toisen päätepisteen paikallisen SDP -kuvauksen.

3) MGC eli Call Agent tietää nyt myös toisen päätepisteen yhteyden tiedot, jolloin se käyttää yhteyden muokkaamispyyntöä asettaakseen ensimmäisen päätepisteen

yhteyden toimimaan täysin. Eli Call Agent lähettää yhteyden muokkauspyynnön (MDCX) yhdyskäytävälle. Muokkauspyynnössä kulkee yhdyskäytävälle toisen päätepisteen paikallinen SDP -kuvaus. Nyt molemmat päätepisteet kykenevät sekä lähettämään että vastaanottamaan tietoa, mikä tarkoittaa, että yhteys toimii molempiin suuntiin.

Esimerkki on otettu suoraan MGCP -protokollan RFC:stä [RFC2705] ja se esittää todella yksinkertaisesti miten SDP -protokolla suhteutuu MGCP -protokollaan.

	Yhteyden luomisviesti (CRCX)		**Yhteyden muokkaamisviesti (MDCX)**	
	Pyyntö	***Vastaus***	***Pyyntö***	***Vastaus***
Vieras SDP	Vapaa-ehtoinen	EI	Vapaaehtoinen	EI
Paikallinen SDP	EI	Vapaaehtoinen*	EI	Vapaaehtoinen
* Paikallinen SDP pitäisi lähettää CRCX viestin vastauksessa, mutta se voidaan myös lähettää MDCX viestin vastauksessa. SDP viesti erotetaan MGCP -viestistä tyhjällä rivillä.				

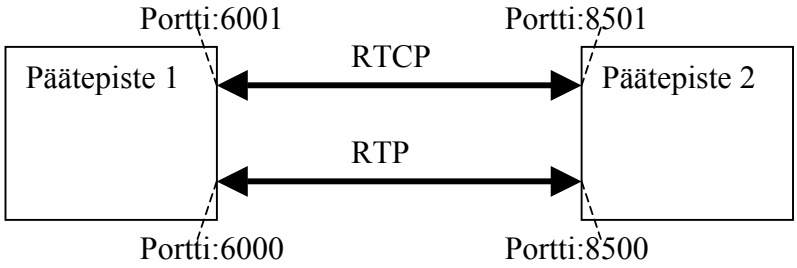
Taulukko 6: SDP- ja MGCP -viestien suhdetaulukko

Edellä olevassa taulukossa (Taulukko 6) esitellään SDP -protokollan suhde MGCP -protokollan yhteyden luomis- ja muokkauspyyntöihin. SDP -protokollalla ei olekaan suhdetta muihin MGCP -protokollan viestityyppeihin, koska se ei liity niihin millään tavalla. Yksinkertaistettuna MGCP -protokolla käyttää SDP -protokollaa kuten sitä on tarkoitettua käytettävän eli yhteyksien kuvaamiseen. Itse MGCP -protokolla hoitaa signaloinnin ja näin ollen SDP -kuvauksen siirron paikasta toiseen, missä SDP -protokollalla ei ole minkäänlaista valtaa signalointiin vaan kaikki päätelmät tehdään MGCP -protokollan tietojen mukaan.

2.2.4 RTP –protokolla

Kuten aiemmin esitellyt protokollat myös Real-time Transfer Protocol (RTP) on IETF:n kehittelemä protokolla. RTP –protokolla tarjoaa päästä päähän siirtopalvelua tiedoille, joille on ominaista reaaliaikaisuus, kuten vuorovaikutteisella äänellä ja videolla. Palvelu pitävät sisällään hyötykuorman tyypin tunnistamisen (engl. payload type identification), sekvenssi numeroinnin (engl. sequence numbering), aikaleimaamisen (engl. timestamping) ja siirron monitoroinnin (engl. delivery monitoring). RTP –protokolla on riippumaton siirtotiestä, mutta normaalisti se käyttää siirtotienä UDP:tä, joka tarjoaa multipleksauksen ja tarkistussumma palvelun RTP –protokollalle. RTP –protokolla tukee tiedon siirtämistä useisiin kohteisiin käyttämällä monilähetystä (engl. multicast), jos alhaalla oleva siirtotie vain tukee sitä. [RFC1889]

RTP –protokolla rakentuu itse asiassa kahdesta osasta, joista toinen hoitaa tiedon liikuttamisen ja toinen hoitaa RTP -yhteyden kontrolloinnin ja monitoroinnin. Itse Real-time Transfer Protocol (RTP) hoitaa tiedon siirtämisen kun taas Real-time Transfer Control Protocol (RTCP) hoitaa kontrolloinnin ja monitoroinnin. RTP -yhteys voidaan luoda myös ilman RTCP –protokollaa, jolloin ei saada tietoa yhteydestä, mutta joissain tapauksissa tämä ei ole edes välttämätöntä. RTP –yhteyksien luonnissa on sellainen ominaisuus, että parilliset portit varataan tiedon siirtämistä (RTP) ja sitä seuraava pariton portti kontrollointia varten (RTCP). Esim. portti 6000 RTP -yhteyttä ja portti 6001 RTCP –yhteyttä varten.



Kuva 14: RTP ja RTCP tietovirrat

RTP –protokollasta on huomioitava sellainen asia, että se ei itsessään tarjoa laatupalvelua (Quality of Service, QoS), vaan tämä on toteutettava muulla tavoin. Laatupalvelun toteuttamiseksi voidaan käyttää esimerkiksi Resource Reservation Protocol -protokollaa (RSVP). Tietysti siirron monitorointi on osa laatupalvelua, mutta sen avulla ei voida taata kaistaa tai saati sitten varaamaan. Joka tapauksessa monitorointi on tarvittava osa VoIP –palveluissa eli äänen siirrossa, mitä varten RTP –protokolla on alunperin myös kehitetty.

RTP –protokollaa ei käsitellä työssä tarkemmin, koska projekti itsessään käytti RTP –protokollan ominaisuuksia, eikä tutkimukset liittyneet mitenkään RTP –protokollan tutkimiseen vaan suurempaan kokonaisuuteen, jossa RTP oli vain siirtotapa tiedolle. Työn myöhemmässä vaiheessa RTP –protokollaa tullaan kylläkin sivuamaan lisää, mutta silloin tarkastelu jää ainoastaan korkeammalle tasolle. Jos lukija haluaa tietää lisää RTP –protokollasta, niin kuvaukset RTP –protokollan ominaisuuksista ja sen määrittelyt löytyvät RFC1889:stä [RFC1889] ja hiukan lisätietoutta löytyy RFC1890:stä [RFC1890].

2.3 NAT

Network Address Translation (NAT) eli verkon IP -osoitteen muuttaminen toisesta IP -osoitteesta toiseksi ei liity suoraan VoIP –projektiin, mutta se on huomioitava erinäisiä rakenteellisia ratkaisuja tehdessä. NAT tulee hyvin esille silloin, kun kaksi toisistaan erillään olevaa verkkoa liitetään, joka tarkoittaa IP verkoissa julkisen ja yksityisen verkon liittämistä. Tällöin yksityisestä verkosta tulevien kutsujen lähde IP –osoitteet kartoitetaan karttaan ja NAT muuntaa sisäisen verkon IP:n julkisen verkon IP:ksi. Kun julkisesta verkosta tulee pyyntö julkiseen IP:hen se muutetaan yksityisen verkon vastaavaksi IP:ksi, mutta nyt on huomioitavaa, että NAT palvelimen kartassa on oltava jo tiedot kartoitusta varten. Muunnoksia on kahdenlaisia: monta – yhdeksi ja monta – moneksi.

Monta-yhdeksi tarkoittaa lähinnä sitä, että on olemassa vain yksi julkinen IP -osoite, jota kaikki yksityisen verkon koneet käyttävät. Tämä tarkoittaa sitä, että aluksi yksityinen verkko lähettää pyyntöjä tiettyyn IP osoitteeseen ja porttiin tietystä omasta IP:stä ja portista, jolloin NAT palvelin muuntaa kutsut niin, että ne näyttävät tulevan julkisesta IP:stä. Kun julkisesta verkosta tulee tietoa taas NAT palvelimen julkiseen IP –osoitteeseen ja porttiin niin NAT osaa välittää tiedot oikealle yksityisen verkon koneelle ja oikeaan porttiin. Tällöin tietysti tämä yksi julkinen IP –osoite kuormittuu paljon ja siitä saattaa suuressa kuormitustilanteessa loppua resurssit (käytännössä portit)

Monta–moneksi tarkoittaa sitä, että yksityisen verkon koneet varaavat yhden julkisen IP –osoitteen itselleen, jolloin NAT –palvelin lähettää kaikki julkiseen IP –osoitteeseen tulleet kutsut uudelleen yksityiseen IP –osoitteeseen. Tässä on suurimpana erona se, että julkisia IP:tä pitää olla useita käytössä. Voihan tietysti kuvitella, että on useita julkisia IP osoitteita, joihin sisäisen liikenteen IP –paketit kartoitetaan samalla tavalla kuin monta – yhdeksi tapauksessa.

Molemmille tapauksille on yhtenäistä se, että julkinen IP ei suoranaisesti näe yksityisen verkon koneita vaan tieto liikkuu välikäsien kautta ja tällöin suoranainen signalointi julkisesta verkosta suoraan yksityiseen verkkoon ei onnistu. Normaalisti tällaisia pisteitä on yritysten verkoissa, jolloin syntyy säästöä verkkokustannuksissa. Tämä onkin erittäin hyvä piste VoIP –yhdyskäytävälle, joka osaa reitittää ääntä niin yrityksen sisällä kuin sieltä ulos. Ulos menevä liikenne kulkee VoIP –yhdyskäytävän kautta, jolloin kukin päätelaite näyttäisi olevan yhteydessä tähän kyseiseen VoIP –yhdyskäytävään.

Edellä olevasta kuvauksesta saadaan irti se, että NAT -muunnoksen huomioiminen VoIP –yhdyskäytävän toteutuksessa on tärkeää ja sitä paitsi pitäähän yhdyskäytävä itsessäänkin sisällään käsitteen kahden verkon liittämisestä, olivat ne sitten normaalin piirikytkentäisen puhelinverkon ja IP verkon liittäminen tai sitten kahden toisilleen näennäisesti näkymättömän IP verkon liittäminen.

3 TEKNIIKOIDEN YHDISTÄMINEN

Edellinen kappale kertoi kustakin käytetystä teknologista perusteet korkeammalla tasolla, jonka pitäisi riittää suhteellisen pitkälle, mutta tarpeen vaatiessa tässä kappaleessa selvitetään asioita myös matalammalla tasolla. Itse kunkin protokollan käyttäminen yksistään on suhteellisen yksinkertainen asia eikä vaadi sinällään mitään suurempaa tutkimusta, mutta kun protokollia halutaan käyttää kokonaisuutena, niin se aiheuttaa enemmän miettimistä. Nyt tarkoitetaan lähinnä SIP- ja MGCP -protokollien käyttämissä yhdessä sillä SDP- ja RTP -protokollat liittyvät molempiin suhteellisen kiinteästi. Protokollien yhdessä käyttäminen on vain osa ongelmaa ja toinen on itse alusta eli Necsom Media Switch (NMS). Se miten protokollat saadaan toimimaan tässä hajautetun laskentakapasiteetin ympäristössä on mielenkiintoinen ongelma, joka jouduttiin huomioimaan koko projektin ajan.

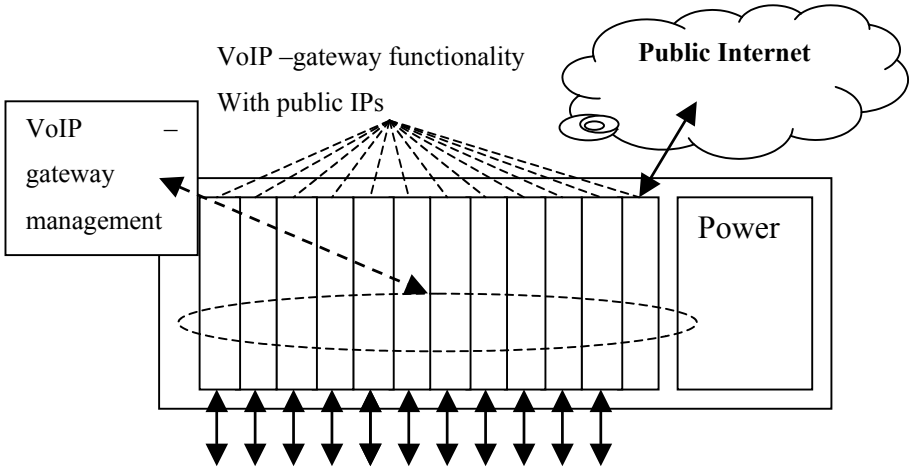
3.1 Media Switch ympäristö

Laitteisto itsessään asetti omat vaatimuksensa niin ominaisuuksien puolesta kuin sopivuudestaan VoIP –yhdyskäytävän toteutukseen. Kyseessä on konsepti, jossa toimii itsenäisenä monta Linux -konetta, joiden laskentakapasiteetti ja muutoinkin tehokkuus ei ole normaalien palvelimien luokkaa. Tämä tarkoittaa sitä, että ainakaan normaaleilla liityntäkorteilla ei voi olla suurta tehoa vaativia toimintoja tai liian useaa vähemmän resursseja vaativaa tehtävää. Muutoinkin mietittäessä konseptia huomataan, että jos NMS -reitittimen lävitse reititetään tarpeeksi tietoa niin korttien kapasiteettia tarvitaan tämän tiedon reititykseen, jolloin palvelu ohjelmistot saavat vielä vähemmän ajo-aikaa käytettäväkseen. Nämä seikat johtavat siihen, että palvelua (tapauksessamme VoIP –yhdyskäytävää) suunniteltaessa pitää huomioida korttien rajoitukset ja miettiä voisiko osa ohjelmasta toimia erillisellä koneella tai sitten prosessorikortilla, jolloin kuorma liityntäkorteilla saataisiin laskemaan.

Olettaessa, että meillä on NMS -reititin, jossa on 12 Ethernet liityntäkorttia ja että kussakin kortissa on toimimassa pieni osa VoIP –yhdyskäytävää ja kukin niistä prosessoisi

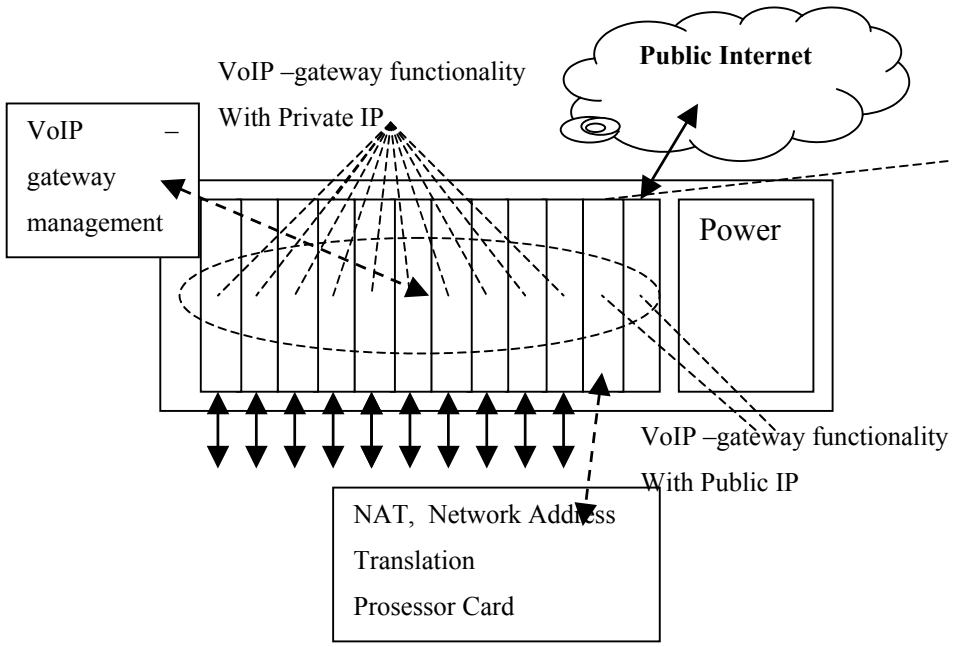
korttien läpi kulkevaa äänitietoa. Tämä tarkoittaa sitä että korteilla tehdään itse VoIP –yhdyskäytävä toiminnallisuus ja hallinnointi hoidetaan jossain muualla. Otetaan esille yksinkertainen IP ← → IP liikenne, jossa ääni tieto liikkuu IP verkosta IP verkkoon ja välillä ei tarvitse tehdä muunnosta piirikytkentäisestä pakettikytkentäiseen eikä päinvastoin. Tällöin tieto pitää ottaa vastaan ja lähettää edelleen, sekä tarvittaessa voitaisiin vaikka tehdä tiedon koodauksen (engl. codec) muunnos toisesta tyypistä toiseksi. Pelkän IP -liikenteen reititys VoIP -yhdyskäytävän lävitse on kyseenalaista ellei tietovirtaa haluta tarkkailla, muuntaa tiedon koodausta tai sitten yhdistää kahta verkkoa toisiinsa (huomio NAT kappaleessa 2.3).

Tarkempaa tutkimusta on siis turha tehdä tapausta varten, jossa kaikki IP:t olisivat julkisia, koska tällöin tieto voidaan siirtää suoraan verkon läpi ilman mitään välikäsiä. Sen sijaan VoIP –yhdyskäytävän odotetaankin toimivan juuri sellaisessa pisteessä, jossa eri verkot yhdistyvät, oli kyseessä sitten kahden toisilleen näkymättömän verkon tai perinteisen piirikytkentäisen ja pakettikytkentäisen yhdistäminen. Suoritetaan muutamia suuntaa antavia mietteitä tapaukselle, jossa ääni reititetään VoIP –yhdyskäytävän läpi julkisesta IP –verkosta yksityiseen IP –verkkoon. Tällöin korteille luotaisiin päätepisteitä, jotka pitäisivät sisällään yhteyksien tiedot ja kortit suorittaisivat yhteyksien tietojen vastaanoton ja lähetyksen. Tapauksesta on muutama erilainen toteutusmahdollisuus, jotka esitetään seuraavaksi kuvien kera.



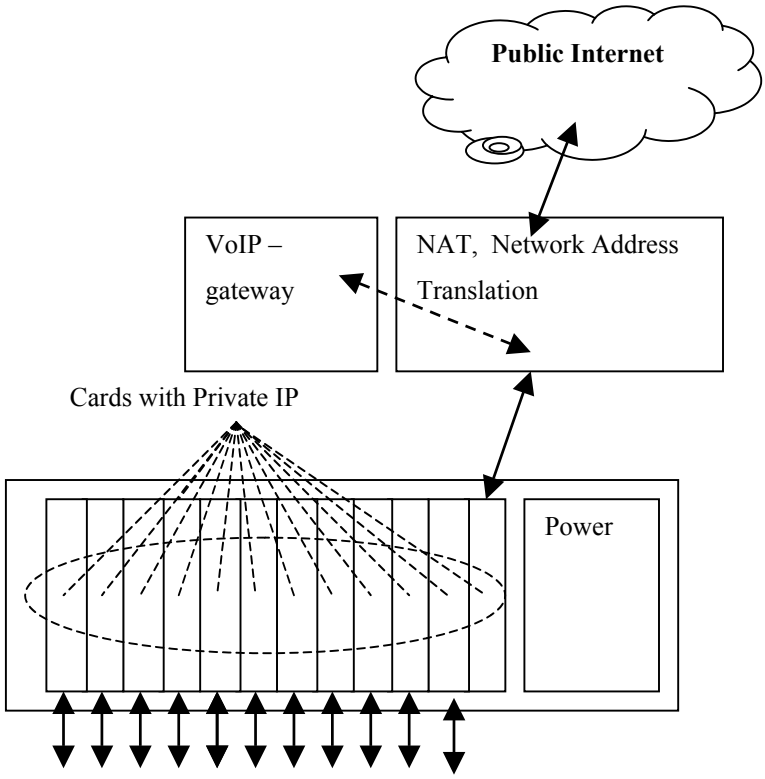
Kuva 15: VoIP –yhdyskäytävä kun kaikilla NMS -korteilla on julkinen IP

Tässä tapauksessa jokaisella NMS -kortilla olisi julkinen IP –osoite, jolloin ulkoa tuleva yhteys VoIP –yhdyskäytävään voi päätyä mille kortille tahansa. Näin kaikki luotavat päätepisteet voitaisiin luoda tasaisesti jokaiselle kortille vuorollaan, koska kaikkien korttien IP:t näkyvät kaikkialle ja tällöin kuormaa saataisiin jaettua. Nyt on oletettu vielä sellainen asia, että jokaisen kortin takana on yksityinen verkko, joka ei näy julkiseen verkkoon vaan ainoastaan kullekin kortille. Tällöin normaalin verkon oma IP –liikenne pitäisi myös pystyä ajamaan NAT -muunnoksen lävitse, mikä tarkoittaisi sitä, että NAT muunnos pitäisi suorittaa korteilla. Mutta kuten aiemmin tuli esille NMS -liityntäkorttien kapasiteetti ei ole rajaton jolloin NAT -muunnos tekeminen korteilla saattaisi kuormittaa niitä liikaa. Huomioimatta tämän ongelman tai jättämällä NAT –osuus kokonaan pois, voisi ratkaisu sopia hyvin VoIP –yhdyskäytävän toteuttamiseksi.



Kuva 16: VoIP –yhdyskäytävä kun muutamalla NMS -kortilla on julkinen IP

Jos taas oletetaan, että kyseessä on edellä olevassa kuvassa esitetty tapaus, jossa yksi liityntäkortti olisi ainoastaan yhteydessä julkiseen verkkoon, tilanne on aivan erilainen edelliseen tapaukseen verrattuna. Tällöin julkisesta verkosta tuleva liikenne näkee ainoastaan yhden liityntäkortin ja voi lähettää tietoa ainoastaan tähän osoitteeseen. Tällöin muun normaalin IP –liikenteen NAT -muunnos voisi tapahtua vaikka prosessorikortilla, joka on NMS -reitittimessä. Tähän tapaukseen on muutama ratkaisu, jotka voisivat toimia VoIP –yhdyskäytävän tapauksessa. Yksi näistä vaihtoehdoista olisi, että päätepiste luodaan aina liityntäkortille tai sitten prosessorikortille, jossa NAT -muunnos tapahtuisi. Tästä saadaan muodostettua erikoistapaus, jossa päätepiste jaettaisiin vielä puoliksi niin, että päätepisteen toiminnallisuus jaettaisiin kahdelle kortille, jolloin esim. mahdollinen tiedon muutos (engl. codec) tapahtuisi kulloinkin ulos menevällä kortilla. Kummassakin tapauksessa kuormitettaisiin muutamaa korttia suhteellisesti enemmän kuin muita ympäristön kortteja. Toisaalta NAT kartoitukseen voitaisiin signaloinnin aikana lisätä uusia tietoja, joiden avulla NAT osaisi ohjata VoIP –palvelulle tulevat tiedot uuteen osoitteeseen. Tämä olisi varmasti jokseenkin toimiva ratkaisu, mutta vaatisi lisää hallinnointia ja näin systeemistä muodostuisi monimutkaisempi ja VoIP –yhdyskäytävä olisi tällöin aika riippuvainen alustastaan.



Kuva 17: Kaikkien NMS -korttien IP osoitteet ovat yksityisiä

Tietysti koko NMS -reititin voitaisiin peittää palomuurilla, jossa NAT -muunnos tehtäisiin, mutta tällöin NMS -reitittimen perusidea itsenäisenä laitteena kärsisi. Tässä tapauksessa VoIP –yhdyskäytävän pitäisi periaatteessa sijaita tässä palomuurissa tai takana, jolloin VoIP –yhdyskäytävä päivittäisi palomuurin tietoja jolloin VoIP –yhdyskäytävälle tulevat paketit ohjattaisiin oikeaan paikkaan (vastaavalla tavalla kuin edellisessä tulkinnassa).

Edellä oli muutamia ajatuksia miten VoIP –yhdyskäytävä voitaisiin rakentaa NMS -ympäristöön, joista muutamat voidaan melkein heti unohtaa, koska VoIP –yhdyskäytävän itsessään on tarkoitus toimia sellaisessa pisteessä, jossa kaksi verkko kohtaa toisensa. Tällöin konseptista saadaan helpompi eikä tarvita lisäominaisuuksia muiden moduulien hallitsemista varten. Jo itsessään VoIP –yhdyskäytävän toiminnallisuuksien jakaminen NMS -reitittimen ja hallinnointi palikan kesken on ongelma ja tämän takia konseptiin ei ole hyvä lisätä ylimääräistä toiminnallisuutta, koska asiat voidaan tehdä ilman niitäkin.

Edellä ei mainittu lainkaan tapausta, jossa NMS -liityntäkorteilla ei olisikaan VoIP –yhdyskäytävä toiminnallisuutta, vaan tämä suoritettaisiin erillisellä koneella tai pelkästään prosessorikortilla. Tätä tapausta puntaroidaan enemmän protokollien sopivuuden tutkimuksen jälkeen.

3.2 Protokollien sopivuus

Projektin aikana syntyi monia kysymyksiä ja ajatuksia miten protokollat sopisivat VoIP –yhdyskäytävän toteuttamiseksi. SIP -protokollan toiminnallisuus on tärkeä toteutuksessa, koska sen avulla osapuolet voivat sopia keskenään yhteyden tiedoista ja muutoinkin hoitaa yhteyden signaloinnin ulkopuolelle. MGCP -protokollan rooli oli useaan otteeseen epäselvä ja sen sopivuutta VoIP -toteutukseemme mietittiin usein. Lopulta tulimme siihen tulokseen, että voimme omassa ympäristössämme (NMS) toteuttaa VoIP -yhdyskäytävän kahdella eri tavalla, joissa toisessa käytetään MGCP -protokollaa ja toisessa ei. Seuraavana on siitä miten protokollat sopisivat.

3.2.1 SIP -protokollan sopivuus

SIP -protokollan sopivuutta VoIP –yhdyskäytävän toteuttamisessa pitää miettiä siten, että miten yleinen SIP on ja miten se soveltuu palveluiden toteuttamiseen ja miten tulevaisuus suhteutuu tähän teknologiaan. SIP -protokolla on suhteellisen uusi protokolla, mutta sitä tuetaan yhä enemmän erilaisissa toteutuksissa ja laitteissa ja nykyinen tilanne osoittaa, että se on nousemassa oleelliseksi teknologiaksi. Tietysti sopivuutta ei voida määritellä ainoastaan sen perusteella, että se on yleistymässä ja että sen käyttö on tällä hetkellä hienoa vaan pitää olla joitain perusteita nykyisten ja tulevaisuuden näkymien perusteella.

Projektin alkuaikana ei ollut sinällään tietoa miten SIP -teknologiaan pitäisi suhteutua vaan se oli uutuus, josta voisi olla johonkin. SIP -protokollan perustoiminnallisuus on selostettu korkealla tasolla kappaleessa 2.2.1, missä myös kerrotaan miksi se on noussut

pinnalle. Kappaleessa kerrotaan muun muassa sen olevan tekstipohjainen ja tämän takia siirtotiestä riippumaton ja että se on dynaaminen ja sitä voidaan laajentaa vaatimusten muuttuessa. Tämä tukee sitä, että tulevaisuuden vaatimusten edessä SIP -teknologia pystyy muuttumaan ja on siten pitkä-aikainen. SIP -protokollaa verratessa jo suhteellisen vanhaan H.323:seen huomataan, että se on suhteellisen yksinkertainen ja taipuvainen. H.323 ja SIP vertailusta voi lukea hieman tarkemmin [Kau01]. SIP -protokollan avulla on mahdollista liittää erilaisia palveluita yhtenäiseen kokonaisuuteen, kuten esimerkiksi SIP -muuntajien avulla voidaan H.323 ja MGCP -signaloinnit muuntaa SIP –signaloinniksi. Tällainen mahdollisuus osoittaa sen , että SIP -protokolla taipuu erittäin monien protokollien tilalle tai ainakin voi liittää ne samaan kokonaisuuteen. Edellä lueteltujen ominaisuuksiensa takia on perusteltua käyttää SIP –protokollaa, mutta päätöksiä tehdessä on hyvä huomioida myös olemassa oleva teknologia ja kohde missä protokollaa suunnitellaan käytettävän.

SIP -toiminnallisuus on se osa, jonka systeemin ulkopuolella olevat päätepisteet näkevät ensimmäisenä, koska signalointi hoidetaan SIP -protokollan avulla. Tällöin SIP - toiminnallisuuden pitää sijaita sellaisessa paikassa, josta se näkyy kummallekin soiton osapuolelle eli VoIP –yhdyskäytävän tapauksessa SIP –toiminnallisuuden pitää sijaita verkkojen risteyskohdassa tai vähintäänkin osa SIP - toiminnallisuudesta. SIP -osio toimii välityspalvelimen kaltaisesti ja peittää oikeat SIP -yhteydet toisiltaan ja kykenee samalla muuttamaan SIP –viestin tietoja kuten SDP -kuvauksen arvoja. Tällöin soiton päätepisteet saavat sellaista tietoa, jota SIP -välityspalvelu haluaa antaa. VoIP –yhdyskäytävän toimiessa NMS -ympäristössä SIP -toiminnallisuuden pitäisi tällöin periaatteessa sijaita korteilla, mutta SIP -protokollan rakenteen takia SIP –toiminnallisuutta on vaikea jakaa korteille rinnakkaisesti toimivaksi ja oman SIP –toiminnallisuuden laittaminen jokaiselle kortille olisi taas resurssien tuhlausta. Tähän on ratkaisuna pienet SIP –moduulit, jotka peittävät oikean SIP –toiminnallisuuden ja tarjoavat yksinkertaisesti vain SIP –palvelun jokaisen kortin takana olevalle verkolle. Ne toimivat pieninä SIP –välityspalvelimina ohjaamalla SIP –viestit uudelleen oikealle SIP –palvelulle. Tosin nämä pienet SIP –moduulit voivat pitää sisällään joitain pieniä toiminnallisuuksia kuten esimerkiksi tunnistus voidaan suorittaa jo korteilla tai vaihtoehtoisesti jättää itse SIP –palvelun tehtäväksi ja muutonkin joitain pieniä tehtäviä voidaan antaa hoidettavaksi

tälle pienemmälle SIP –moduulille. Näin SIP -viestit kulkevat pienien SIP –osion lävitse ja itse SIP –palvelu ei näy ulos. Haluttaessa NMS -reititin voidaan poistaa kokonaan välistä ja kutsut lähetetään tällöin suoraan itse VoIP –yhdyskäytävän SIP -osioille, jolloin pienet SIP –moduulit jäisivät yksinkertaisesti pois välistä, mitä loppukäyttäjä ei tosin huomaisi.

3.2.2 MGCP -protokollan sopivuus

Kuten aiemmin tuli esille niin MGCP -protokollan sopivuudesta oli monenlaista mielipidettä projektin edetessä. MGCP -protokollan avulla hallinnoidaan päätepisteitä, jotka yhdistävät yhteyden IP –verkkoon. Yhteydellä tarkoitetaan nyt yhteyttä päätepisteeseen kuten esimerkiksi puhelimesta tulevaa puhelua. Kuten MGCP -protokollan kuvauskappaleessa tuli esille, niin päätepisteet voivat olla rautatason ratkaisuja tai sitten ohjelmistotason ratkaisuja. MGCP -protokollan avulla voidaan tarkkailla ja ottaa huomioon SS7 -signalointi, jota käytetään PSTN –verkoissa. Tämä tarkoittaa sitä, että MGCP –protokolla on suuntautunut lähinnä erilaisten verkkojen yhdistämiseen (piirikytkentäiset ← → pakettikytkentäiset).

Tapauksessamme MGCP -protokollasta olisi lähinnä hyötyä, kun NMS -reitittimeen saadaan kortti, jolla voidaan liittyä perinteisiin PSTN –verkkoihin. Tällöin MGCP -protokolla kykenee ottamaan signalointia vastaan myös piirikytkentäisestä verkosta. Näin VoIP –yhdyskäytävämme kykenisi yhdistämään PSTN -liikenteen IP verkkoon. Asia kuulostaa kirjoitettuna triviaalilta, mutta sitä se ei ole ja vaatii paljon ponnisteluja, jotta MGCP -protokolla voidaan liittää konseptiimme. Asiasta lisää seuraavissa kappaleissa.

MGCP -protokolla hallitsee yhteyksiä, jotka tulevat päätepisteiden kautta MGCP –protokollan tietoisuuteen. Esimerkiksi rautatasolla PSTN -kytkimen piirit voisivat olla tällaisia päätepisteitä. Tällöin piiristä tuleva tieto voidaan muuntaa IP –verkkoon sopivaksi MGCP -signaloinnin avulla (Hallinnoija, MGC, hallitsee yhdyskäytävää, MG). Alustavasti NMS -reitittimen ominaisuudet PSTN –liitynnän osalta eivät ole ajankohtai-

sia, joka tarkoittaa, että VoIP –yhdyskäytävämme tapauksessa IP –verkon liittäminen IP -verkkoon on tärkeää. Tällöin tieto tulee IP –verkon yhteyden kautta ja lähtee IP –yhteyden kautta eli päätepisteiden pitäisi ottaa sisään tuleva tieto IP –yhteydestä ja lähettää se sitten IP –yhteyden kautta toiselle päätepisteelle. Nyt päätepisteen pitäisi olla ohjelmistolla toteutettu, jolloin se pitäisi myös luoda jotenkin, mutta tietysti päätepiste voitaisiin luoda aina silloin, kun tieto (MGCP -viesti) tulee ei vielä olemassa olevalle päätepisteelle. Luomisvaiheessa pitäisi myös tietää mistä sisään tuleva tieto tulee, joka ei ole helppoa, koska alustavastihan MGCP -protokolla hallinnoi päätepisteitä, joissa tieto tulee jo jostakin (piiristä tai sitten jostain muualta). MGCP -protokollan valjastaminen VoIP –yhdyskäytävän käyttöön ei ole helppoa ja osa-alue sisältää paljon ongelmia. Tosin MGCP –protokollaan onnistutaan kyllä upottamaan VoIP –yhdyskäytävämme käyttöön, mutta tällöin sitä voidaan vahingossa käyttää myös RFC2705 [RFC2705] määrittelyn vastaisesti.

Millainen tarve sitten MGCP –protokollan käytölle on, koska nykyään on jo saatavissa valmiita ja hyvin toimivia PSTN –yhdyskäytäviä, jotka itsessään käyttävät MGCP -protokollaa sisäisessä signaloinnissa ja tarjoavat ulkoiseen signalointiin SIP -protokolla rajapinnan. Tällöin voitaisiinkin pitää järkevänä, että PSTN –kytkin voisi olla erillinen kokonaisuus, joka voidaan sittemmin liittää VoIP –yhdyskäytävä konseptiin. Tällöin kokonaisuus rakennettaisiin palasista ja konseptissa käytettäisiin jo valmiiksi kehitettyjä osia ja näin VoIP –yhdyskäytävämme saisi automaattisesti ilman lisätyötä liitynnän PSTN –verkkoihin.

3.3 Kokonaisuus

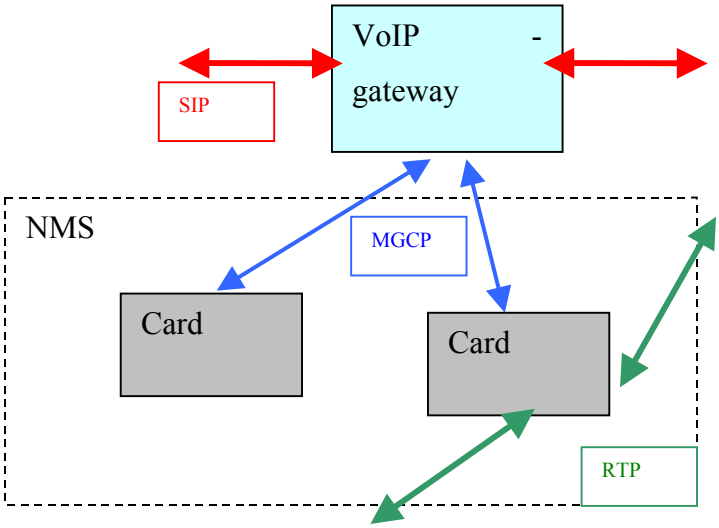
Edellä olleet mietteet teknologioista osoittavat hyvin sen, että kokonaisuuden rakentaminen on tutkimusta vaativa prosessi. Ensinkin se miten MGCP- ja SIP –protokollat suhtautuvat toisiinsa ja se miten kokonaisuus saadaan toimimaan NMS -ympäristössä ovat ongelmallisia kohtia. MGCP -protokolla on suuntautunut erilaiseen tehtävään kuin SIP –protokolla eli ne eivät ole vertaisia vaan voivat olla molemmat käytössä yhtenevässä verkossa samaan aikaan. SIP - MGCP muuntajan avulla yksittäinen MG voidaan

liittää SIP -signalointiin ja toisaalta SIP -protokollaa voidaan esimerkiksi tarvita kahden erillisen MGC:n väliseen synkronointiin [RFC2705], koska MGCP -protokollassa ei olla puututtu siihen miten kaksi osapuolta voivat vaihtaa tietoa keskenään. Eli jos SIP -protokolla tuo signalointi tietoa systeemiin, niin MGCP -protokollan avulla voidaan kontrolloida itse yhdyskäytävää.

Kootessa asiat yhteen voidaan huomata, että VoIP -yhdyskäytävän toteutukseen on kaksi suurempaa linjaa, joista toisessa käytetään NMS –kortteja, joihin hajautetaan yhdyskäytävän toiminnallisuutta ja toisena linjana on se, että yhdyskäytävä toiminnallisuutta ei hajauteta laisinkaan korteilla, jolloin MGCP -protokollaa ei tarvita. Toisaalta jälkimmäisessä tapauksessa yhdyskäytävä voidaan laittaa toimimaan vaikkapa prosessorikortille, jolloin se toimisi NMS -reitittimen sisällä.

3.3.1 VoIP –yhdyskäytävä hajautetusti (käytetään MGCP -protokollaa)

Siinä tapauksessa, kun yhdyskäytävä toiminnallisuutta jaetaan korteille, tapahtuisi kontrollointi MGCP -protokollan avulla. Tällöin MGCP -viestejä voitaisiin ottaa vastaan jokaisella kortilla, jolloin jokainen kortti nähtäisiin yksittäisenä yhdyskäytävänä tai sitten MGCP -viestejä otettaisiin vastaan yhdellä kortilla, joka sitten komentaisi toisia kortteja. Siinä missä SIP -pinon laittaminen jokaiselle kortille on resursseja hukkaavaa niin myös MGCP -pinon laittaminen niille aiheuttaa saman. Projektissa tehdyn tutkimustyön perusteella parhaalta vaihtoehdolta tuntui MGCP –pinon sijoittaminen yhdelle korteille, josta käskyt sittemmin jaetaan muille korteille. Kummatkin konseptit ovat toiminnallisuudeltaan suhteellisen samankaltaiset, paitsi että toisessa nähdään koko NMS -reititin yhdyskäytävänä kun taas toisessa nähdään monta pientä yhdyskäytävää.



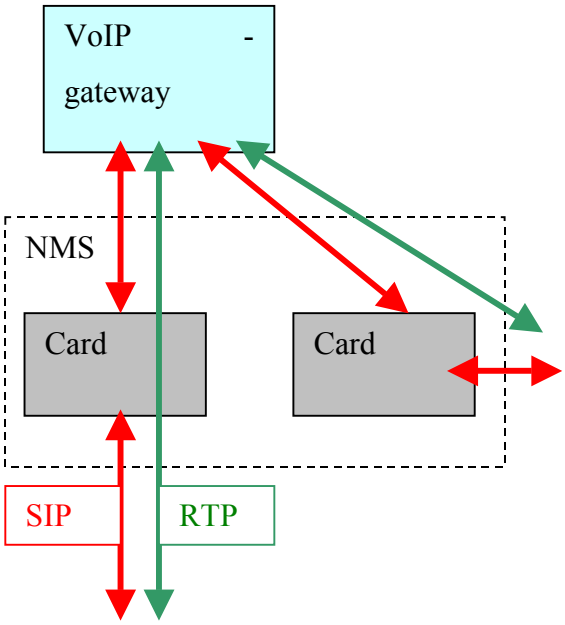
Kuva 18: VoIP –yhdyskäytävä MGCP -protokollan kanssa

Ottamalla edellä olevasta kuvasta toinen MGCP viiva pois saadaan tapaus, jossa koko NMS -reititin nähdään yhtenä yhdyskäytävänä. Se miten liikenne taas liikkuu systeemin sisällä on mielenkiintoinen asia, koska MGCP -protokolla hallinnoi päätepisteitä ja siinä olevaa tai olevia yhteyksiä, pitää kyseiset päätepisteet luoda jotenkin. Luominen voisi tapahtua vaikka yhteyden luomispyynnön yhteydessä, jos päätepistettä ei ole olemassa. Tällöin pitäisi myös pystyä rakentamaan yhteys, josta soittajan tieto tulee, koska normaalistihan MGCP –protokollan käyttötapauksessa tieto tulee PSTN -verkosta. Tämähän tarkoittaa sitä, että päätepisteeseen pitää luoda kaksi yhteyttä, joista toinen olisi soittajalle ja toinen vastaanottajan päädylle ja näin ollen soitto toimisi niin kuin pitäisi. Mitäpä jos soitto halutaan odotus tilaan ja ottaa väliin uusi puhelu toiseen numeroon? Tällöin tulee ongelmia, koska MGCP -protokolla on toteutettu monomediaa varten, mikä tarkoittaa, että tietoa tulee vain yksittäisestä pisteestä eli tässä tapauksessa soittajalta. Nyt MGCP -protokollan pitää kyetä laittamaan toinen soitto odotustilaan ja muuttamaan yhteys, käytännössä päätepiste, uuden soiton vaatimiin asetuksiin. Tällöin tulee ongelmia MGCP -protokollan määritysten kanssa, koska se olettaa tiedon tulevan periaatteessa jostain muulta, kuten verkosta tai sitten joltain palvelimelta, eikä näin osaa varautua siihen, että soittajan yhteyttä pitää myös osata hallinnoida. Ratkaisimme ongelman projektissa useaan otteeseen eri tavoilla ja aina tuntui, että jokin asia ei toimi halutulla tai sitten määritysten mukaisella tavalla. Lopulta saimme rakennettua määrityksen jonka

avulla MGCP -protokolla olisi toiminut jotenkin, mutta sekin ratkaisu tuntui vääränlaiselta.

3.3.2 VoIP –yhdyskäytävä yhdessä paikassa (ei käytetä MGCP:tä)

VoIP –yhdyskäytävän ollessa oma kokonaisuus siinä ei tarvita mitään hallinnointia hajautettuja osia varten, koska niitä ei ole. Tällöin MGCP -protokollaa ei tarvita ja rakenne yksinkertaistuu paljon, mutta haittapuolena on, että NMS -reitittimen ominaisuuksien käyttäminen jää vähäisemmälle. Kuitenkin tässä tapauksessa VoIP –yhdyskäytävä voidaan sijoittaa NMS -reitittimen taakse jollekin prosessorikortille tai sitten ihan jonkin liityntäkortin takana olevalle itsenäiselle palvelimelle.



Kuva 19: VoIP –yhdyskäytävä ilman MGCP -protokollaa

Tämä ratkaisu on hyvä siitä, että tähän konseptiin saadaan rakennettua toiminnallisuutta huomattavasti helpommin ja enemmän kuin edelliseen. Nyt soiton päätepisteitä on helppo hallita, koska ne sijaitsevat yhdessä keskitetyssä paikassa ja koska hallinnointi on helpompaa niin myös erilaisten ominaisuuksien rakentaminen on huomattavasti helpompaa. Tällä konseptilla voidaan erottaa vaikka yksityinen ja julkinen Internet toisis-

taan niin, että VoIP –puhelut tulevat yhdyskäytävän lävitse, koska VoIP –yhdyskäytävä tarjoaa liitynnän kahden eri verkon välillä. Tällöin voitaisiinkin mieltää, että välissä olisi VoIP –välityspalvelin, joka käyttää signalointiin SIP -protokollaa ja tiedon siirtämiseen RTP -protokollaa. Tällaiseen pisteeseen voitaisiin lisätä ominaisuus, joka mahdollistaisi soittamisen yrityksen sisällä suoraan ilman VoIP –yhdyskäytävää, mikä tarkoittaisi sitä, että puhelinyhteyden luonnissa tarkastetaan vain soittajan verkon osoite ja vastaajan verkon osoite ja niiden ollessa toisilleen näkyvässä verkossa voidaan soiton tiedon antaa liikkua suoraan toisesta päätepisteestä toiseen. Tämä suorayhteys on suoraan SIP -maailmasta tuttu, jossa päätelaitteet hakevat saatavuus tietoa toisista ja itse yhteys kulkee suoraan.

Konseptista on muutakin etua, sillä jos yhdyskäytävä rakenteeseen tehdään oikeanlaiset tilarakenteet, saadaan VoIP –yhdyskäytävä signaloimaan erillisen MGC:n kanssa SIP -protokollan avulla, jolloin MGC synkronoi oman MG:n päätepisteen VoIP –yhdyskäytävän päätepisteen kanssa. Tällöin esimerkiksi PSTN –yhdyskäytävä, joka käyttää MGCP -protokollaa sisäiseen signalointiin ja ulkoiseen signalointiin SIP -protokollaa, kykenee näennäisesti synkronoimaan soiton päätepisteet VoIP –yhdyskäytävän kanssa huomaamatta, että toisessa päässä ei olekaan normaalia MGC:tä.

3.3.3 Vaihtoehtojen vertailu

Verratessa edellä olleita vaihtoehtoja on helppo huomata kumman puoleen tulee käännyttyä. Ensimmäinen on rakenteeltaan monimutkaisempi, mutta kykenee käyttämään NMS -reitittimen rakennetta paremmin hyväksi, mutta toisaalta samalla se on virheille alttiimpi, koska siinä on niin paljon hallinnoitavaa tehtävää. Jälkimmäinen taas ei käytä NMS -reitittimen rakennetta niin paljon hyväksi, mutta rakenteeltaan se on yksinkertainen ja sitä saadaan tarvittaessa laajennettua helpommin eikä erillisen PSTN –yhdyskäytävän liittäminen ole ongelma. Toisaalta nykyään on jo olemassa hyviä ratkaisuja PSTN –yhdyskäytävästä, jolloin sellaista ei välttämättä ole viisasta itse rakentaa vaan on helpointa käyttää jo valmista rakennetta. Muutoinkin MGCP -protokollan sopi-

vuus projektimme tapauksessa oli kyseenalaisena, jolloin jälkimmäistä vaihtoehtoa voidaan pitää senkin suhteen parempana.

Kappaleessa 3.1 ilmennyt NAT asia pitää myös huomioida. Kappaleessa puntaroitiin tapauksia, joissa yhdyskäytävästä osa on korteilla ja sellaista tapausta jossa yhdyskäytävä on kokonaisuus. Jos NAT tapahtuu NMS -reitittimen sisällä niin tällöin yhdyskäytävän toiminnan hajottaminen korteille voisi olla erittäin hyvä ratkaisu, koska tällöin liityntäpisteet voisivat olla joko yksityisessä tai julkisessa verkossa ja tiedon siirtäminen julkisesta yksityiseen ja toisin päin tapahtuisi NMS -reitittimen FSR -renkaan kautta. Näin ollen NMS -teknologia mahdollistaisi sen, että verkot olisivat näkymättömissä toisilleen, mutta VoIP –yhdyskäytävän ”päätepisteet” näkisivät toisensa. Tässä tapauksessa päätepisteet luotaisiin julkiseen ja yksityiseen verkkoon ja kaksi pistettä muodostaisi aina soiton. Mutta jos NAT -muunnos tehtäisiin ennen NMS –reititintä, niin tällöin yhtenäinen VoIP –yhdyskäytävä olisi parempi ratkaisu, koska näin se voitaisiin sijoittaa siihen koneeseen jossa tehdään itse NAT ja VoIP –yhdyskäytävä olisi kahden verkon liityntäpisteessä. Kaikki muut tapaukset ovat ongelmallisia, kuten esimerkiksi se, että yhtenäinen VoIP –yhdyskäytävä sijaitsisi NMS -reitittimen takana omalla koneella ja NMS -reitittimen sisällä tehtäisiin NAT muunnos. Tällöin olisi ongelmallista saada tietovirta kulkemaan oikealla tavalla VoIP –yhdyskäytävälle, koska yhdyskäytävä saattaisi sijaita yksityisessä verkossa, joka ei näy julkiseen verkkoon päin. Toisaalta VoIP –yhdyskäytävä voisi omistaa julkisen IP:n, jolloin ongelma olisi taas toisin päin eli VoIP –yhdyskäytävä ei näkisi yksityistä verkkoa , mihin sen piti olla yhdyskäytävänä.

Projektimme toteutti aluksi rakennetta, jossa käytettiin MGCP –protokollaa eli osa yhdyskäytävästä olisi sijainnut korteilla, mutta myöhemmässä vaiheessa suuntaus muutettiin yhtenäiseen VoIP –yhdyskäytävään sen vuoksi, koska sitä voidaan käyttää ilman NMS -reititintä ja sen upottaminen NMS -reitittimen rakenteeseen on helpompaa alkuvaiheessa. Toisaalta ratkaisu myös yksinkertaisti projektia, vaikka ei vähentänyt työmäärää, koska samat asiat pitää toteuttaa joka tapauksessa riippumatta siitä missä ne sijaitsevat. NAT ongelmat tulevat siinä vaiheessa eteen kun NMS -reitittimen rakennetta aletaan oikeasti peittämään NAT:in taakse niin, että VoIP –yhdyskäytävä halutaan olevan myös NMS -reitittimessä.

4 TOTEUTUS

VoIP –yhdyskäytävän toteuttaminen SIP- , MGCP-, SDP- ja RTP –protokollien avulla NMS -ympäristöön oli erittäin mielenkiintoista. Aiemmin esitettiin muuttamia vaihtoehtoja miten VoIP –yhdyskäytävä voitaisiin ehkä toteuttaa ja millaisia ongelmia esiintyy kun eri vaihtoehtoja pyritään saamaan toimivaksi ratkaisuksi. VoIP -projektin ensimmäisessä vaiheessa suunniteltiin VoIP –yhdyskäytävä NMS -ympäristöön ja suunnitelmissa käytettiin rakennetta, jossa osa yhdyskäytävän toiminnallisuudesta sijaitsi NMS -reitittimen sisällä ja näin ollen samalla hyödynnettiin MGCP –protokollan ominaisuuksia. Ensimmäinen prototyyppi toteutettiin suunnitelmien mukaan, mutta sillä erotuksella, että se toimi ainoastaan Linux alustalla. Prototyyppi toimi halutulla tavalla, mutta siinä ei vielä huomioitu MGCP -protokollan käyttämisestä syntyviä epäkohtia. Yleisesti ottaen vaihe antoi paljon palautetta protokollista ja VoIP –yhdyskäytävän toiminnallisuudesta ja seuraava vaihe, joka toimisi NMS ympäristössä, aloitettiinkin ensimmäisestä vaiheesta saatujen kokemusten perusteella.

Jatkossa huomattiin, että VoIP –yhdyskäytävän toteuttaminen ilman osien hajautusta NMS -alustalle voisi olla parempi ja yksinkertaisempi ratkaisu, jolloin myös MGCP -protokolla jäisi kokonaan pois ja VoIP –yhdyskäytävän kaikki toiminnallisuus toimisi yhdessä kokonaisessa paketissa. Osaltaan tähän päätökseen vaikutti myös se, että yhtenäinen toteutus ei olisi enää riippuvainen NMS -alustasta vaan sitä voitaisiin käyttää myös pelkällä Linux alustalla. Tämä olisi ollut muutoinkin tarpeellista alussa, koska NMS -reititin piti sisällään vain Ethernet –liityntäkortteja, jolloin hajautetussa versiossa suurin osa VoiP –yhdyskäytävän toiminnallisuutta olisi sijainnut erillisellä koneella. Muutoinkin rakenteen suunnittelu ja toteuttamisvaiheet yksinkertaistuvat niin paljon, että se säästi aikaa ja samalla jatkokehitys helpottui.

Seuraavaksi kuvaillaan VoIP –yhdyskäytävä, jossa ei ole käytetty lainkaan MGCP –protokollaa ja tämä kuvaus on tehty toiminnallisilta ja rakenteellisilta näkökohdilta erikseen omissa kappaleissaan. Toisaalta kuvausten jälkeen mietitään millaisissa pisteissä toteuttamaamme VoIP -yhdyskäytävää tarvitaan ja millaisia tekijöitä pitää huomioida sen suorituskykyä mietittäessä.

4.1 Menetelmät ja työvälineet

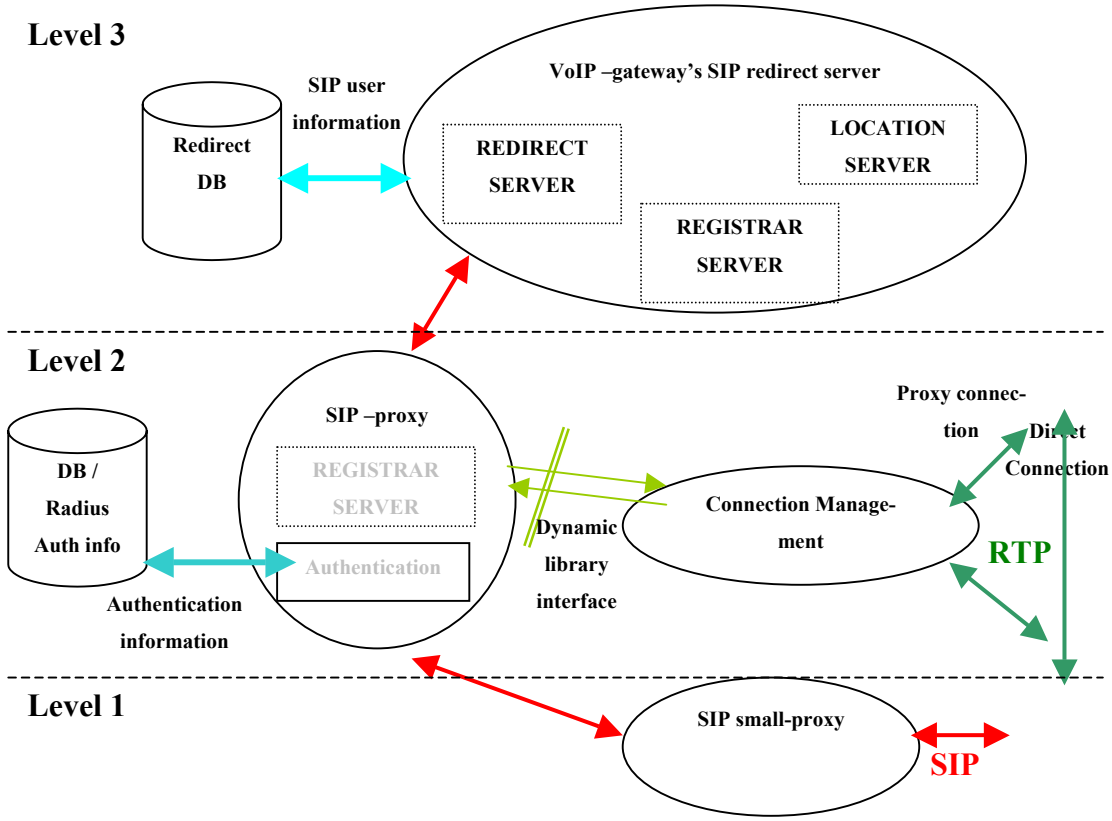
Projektin alkaessa päädyttiin käyttämään Vovida.org [Vovida] tarjoamia protokollapinoja VoIP –yhdyskäytävän toteuttamiseksi. Pinot on tehty C++ kielellä joten päätettiin, että C++ tullaan käyttämään kaikkialla missä se on mahdollista. Kaikki mitä NMS -alustalle tarvittaisiin toteuttaa päätettiin toteuttaa C:llä johtuen alustan teknisestä rakenteesta. Suosioon noussut JAVA kieli oli VoIP –projektiin sopimaton sen hitauden ja vaatimusten takia. Javahan vaatii koodille välitulkkauksen ja näin ollen tämä olisi ollut hidastava tekijä ja kaiken lisäksi ympäristöön oltaisiin tarvittu myös Java paketit, jotta koodia oltaisiin saatu ajettua. Projektissa hyödynnettiin C++ kirjallisuutta[Str00] ja sen antamia hyviä ohjeita. Koodaus pyrittiin tekemään Design Pattern –tyylin [Gam00] mukaisesti niissä paikoissa missä se on mahdollista, mutta niiden käyttäminen tahtoi unohtua usein.

Työtehtävät jaettiin projektiryhmän kesken niin, että yhdessä mietittiin mitä tarvitsee tehdä ja sitten määriteltiin osa-alueelle vastuuhenkilö, jonka tehtäväksi jäi suunnitella ja toteuttaa osa-alueeseen liittyvät asiat. Kaikki tapahtui projektiryhmän myötämielisellä avustuksella ja näin kaikki auttoivat toisiaan vaikka pohjimmiltaan projektin työjako olikin hajoita ja hallitse tyyliä.

4.2 VoIP –yhdyskäytävän toiminnallisuus

VoIP –yhdyskäytävä koostuu useasta moduulista, joilla kullakin on oma tehtävä. VoIP –yhdyskäytävä koostuu kolmesta isommasta osasta, jotka jakautuvat kaikkiaan yhdeksään pienempään osaan. Jokainen osa on itsenäinen, mutta esimerkiksi VoIP –yhdyskäytävän yhteyden hallinta osion ja SIP –välityspalvelu (SIP -välityspalvelin) osion välillä on vaadittu erityisiä ratkaisuja, jolloin SIP -osio on riippuvainen yhteyden hallinta osioista ja päinvastoin. Seuraava kuva esittelee VoIP –yhdyskäytävän toiminnalliset palikat.

Seuraava kuva on jaettu kolmeen tasoon, jotka ilmaisevat edellä mainittuja kolmea suurempaa osaa. Näiden sisällä on lisää moduuleja, jotka tarkentavat tasojen toiminnallisuutta enemmän. Kuvaa seuraavat kappaleet määrittelevät kuvassa esiintyneet osat tarkemmin.



Kuva 20: Toiminnallinen kuva VoIP –yhdyskäytävästä

4.2.1 Taso 1 (Level 1)

Tason 1 toiminnallisuus pitää sisällään NMS -ympäristöön tulevat osat, joita ainakin aluksi on vain yksi eli pienempi SIP –välityspalvelin. Lisäksi NMS -ympäristöön saattaa olla tarvetta lisätä ulosmenevän kortin ratkaisija, joka tekee ratkaisun jonkin IP osoitteen perusteella siitä minkä kortin kautta IP liikenne kulkee ulos kyseistä IP:tä var-

ten. Tällainen ratkaisija käyttää ratkaisun tekemiseen hyväksi NMS –reitittimen reititystaulua.

4.2.1.1 SIP –välityspalvelin, pieni (SIP -smallproxy)

Pienemmän välityspalvelimen tarkoituksena on tarjota SIP -rajapinta jokaisen kortin takana oleville asiakkaille, mikä tarkoittaa sitä, että asiakas näkee NMS –reitittimen tukevan SIP -protokollaa. Tällöin asiakas näkee vain sen, että NMS -reititin tarjoaa SIP -rajapinnan, muttei itse asiassa tiedä minne SIP -liikenne oikeasti menee. Alussa tämä pienempi välityspalvelin ohjaa liikenteen kohti VoIP –yhdyskäytävää eikä itse tee mitään suurempia toiminnallisuuksia. Pienempi välityspalvelin lisää kuitenkin SIP -viestiin tiedon reitistä, jota pitkin SIP -viesti on liikkunut eli VIA -kentän, joka osoittaa pienemmän SIP –välityspalvelimen omaan osoitteeseen. Myöhemmin, jos on tarvetta, tähän osaan voidaan lisätä toiminnallisuuksia. Esimerkiksi langattomat mobiiliverkot saatavat tarvita tähän pisteeseen enemmän toiminnallisuutta, jotta esim. juuri mobiiliverkoissa tuttu ”roaming” saataisiin toimimaan SIP -protokollan avulla. Tätä aihetta ei ole vielä tutkittu enempää, mutta alustavat näkymät ja ajatukset tuntuvat siltä.

4.2.2 Taso 2 (Level 2)

Taso 2 pitää sisällään itse VoIP –yhdyskäytävän ja sisältää näin ollen useita pienempiä osioita. Kokonaisuudessaan taso pitää sisällään SIP -viestien vastaanoton, niiden jatkokäsittelyn, SIP -viestien tunnistamisen ja VoIP -yhteyksien luomisen. Jokainen edellä mainittu asia liittyy omaan kokonaisuuteen ja on näin ollen selostettu paremmin seuraavissa kappaleissa.

4.2.2.1 SIP –välityspalvelin

SIP –välityspalvelin on osa, joka pitää sisällään SIP -pinon ja SIP -protokollaan liittyvät toiminnallisuudet. Moduuli on erityistapaus välityspalvelimesta ja välittää viestejä VoIP –yhdyskäytävä osioille ja ottaa myös vastaan niitä sieltä. Tähän osaan kuuluu myös läpinäkyvä SIP –rekisteröijä ja käyttäjän tunnistus, mikä on määritelty SIP -protokollan RFC:ssä [RFC2543]. Välityspalvelu käyttää ulkoista uudelleenohjauspalvelinta käyttäjien paikantamiseen ja ulkoista rekisteröijää rekisteröidäkseen käyttäjät systeemiin.

Moduuli on toteutettu niin, että se voidaan ladata dynaamisesti, jolloin SIP –välityspalvelin tarjoaa vain yksinkertaisen rajapinnan SIP –viestien noutoon ja lähettämiseen. Tämä yksinkertainen rajapinta on riittävä, koska VoIP –yhdyskäytävä (yhteyksien hallinta osa) ei tee itsessään mitään suurempia liittyen SIP -protokollan määrityksiin vaan käsittelee viestejä omaa käyttöä varten. Näin SIP- ja VoIP –osiot ovat näennäisesti toisistaan riippumattomat, vaikka tarvitsevatkin toistensa ominaisuuksia.

4.2.2.2 Tunnistus (Authentication)

Tässä konseptissa SIP -viestien tunnistus on sijoitettu SIP –välityspalvelimeen. Tunnistuksessa tarvitaan käyttäjän tunnistetietoja, jotka voidaan hakea omasta tietokannasta tai sitten jostain ulkoisesta systeemistä kuten Radiuksesta. Tällöin tunnistus-osioon pitää toteuttaa vain pieni rajapinta kutakin ulkoista systeemiä varten, jolloin tunnistus osaa hakea tiedot oikealla tavalla.

4.2.2.3 Tunnistus Tietokanta

Tietokanta voi olla tässä tapauksessa pelkkä tietokanta, jossa sijaitsee käyttäjän tunnus, salasana ja muuta SIP -tunnistukseen liittyvää tietoa. Tietokannan tiedot voidaan myös saada ulkoisesta systeemistä kuten Radiuksesta, joka pitää itsessään sisällä jonkinlaisen tietokannan. Jos tunnistukseen käytetään ulkoista käyttäjätunnus, salasana paria, pitää

tällöin SIP –protokollan muut tarvitsemat tunnistustiedot saada tallennettua johonkin väliaikaiseen välimuistiin, jotta SIP -tunnistus toimisi oikealla tavalla. Toteutuksemme käyttää alustavasti SQL –tietokantaa tunnistustietojen tallennukseen.

4.2.2.4 SIP –Rekisteröijä

Tason 2 tapauksessa rekisteröijä on vain pelkkä käsite, koska SIP –välityspalvelin välittää rekisteröinti tiedot vain eteenpäin toisaalle, jossa itse rekisteröityminen tapahtuu, vaikkakin välityspalvelin suorittaa tarvittaessa tunnistamisen. Tapauksessamme rekisteröintipyynnöt lähetetään SIP –uudelleenohjauspalvelulle.

4.2.2.5 Yhteyden hallinta (Connection Management)

Tämä moduuli on VoIP -yhdyskäytävä kokonaisuuden sydän eli tässä osioissa on tiedot yhteyksistä ja niiden tiloista. Alustavasti on kahdenlaisia yhteyksiä: suoria ja välitettyjä yhteyksiä. Tämä tarkoittaa sitä, että suorassa yhteydessä tietovirta kulkee suoraan päätepisteiden välillä (käyttäjien päätelaitteet), kun taas välitetyssä yhteydessä tieto kulkee yhdyskäytävän lävitse. Nämä kaksi yhteystyyppiä on identtiset tilojensa suhteen ja ainoana erona on tietovirran kulku. Välitetyssä yhteydessä tietovirran tietoa voidaan käsitellä välissä esimerkiksi muuttamalla tiedon koodaus tyypistä toiseen.

Moduulin tehtävä on luoda, tuhota ja hallita yhteyksiä, jakaa aikaa SIP –osioilta saatujen viestien käsittelyyn ja jakaa aikaa tietovirran tiedon prosessointia varten. Moduulin ominaisuuksia on helppo kehittää eteenpäin tekemällä erilaisia päätepisteitä, joilla on erilaisia tilakoneita. Se miten päätöksenteko luotavasta päätepisteen tyypistä tehdään tullaan selvittämään myöhemmin, kun käsitellään systeemin sijoituspaikkaa ja miten VoIP –yhdyskäytävä voidaan asentaa (asennustiedot, engl. configuring).

4.2.3 Taso 3 (Level 3)

Tällä tasolla on lähinnä ne moduulit, jotka eivät ole riippuvaisia systeemistämme vaan voivat toimia myös itsenäisesti SIP -protokollan määrittelemällä tavalla. Eli muutkin, kuin pelkästään tämän työn esittelemä VoIP –yhdyskäytävä, voisivat käyttää tämän tason palveluita.

4.2.3.1 SIP –uudelleenohjaus

Uudelleenohjauspalvelun tarkoituksena on etsiä uudelleenohjaustietokannasta käyttäjän sen hetkistä sijaintia vaastaava SIP –yhteystieto. Esimerkiksi jos käyttäjän kotipaikka on verkossa ”***necsom.com”*** ja käyttäjätunnus on ”***juupe”*** , niin tällöin käyttäjän SIP -osoite voisi olla esimerkiksi ”***sip:juupe@necsom.com***”. Käyttäjän käynnistäessä asiakasohjelmiston vaikkapa koneesta ”***lyijy.necsom.com”*** hän rekisteröityy uudelleenohjauspalvelimeen. Tämän jälkeen käyttäjälle ”**juupe@necsom.com**” soittavat lähettävät SIP –viestin uudelleenohjauspalvelimelle, johon vastaanottava käyttäjä rekisteröityi. Uudellenohjauspalvelin etsii rekisteröityneelle käyttäjälle (”***sip:juupe@necsom.com”***) vastaavan osoiteen ”***sip:juupe@lyijy.necsom.com”*** ja palauttaa sen alkuperäisen SIP –viestin lähettäjälle**.** Vastaavia osoitteita saataa olla myös ennemmän kuin yksi. Nyt alkuperäinen uudelleenohjauspalvelimelle lähetetty viesti lähetetään uuteen saatuun osoitteeseen. Huomattavaa on se, että to -kentän osoite pysyy samana eli ”***sip:juupe@necsom.com”***, mutta osoite johon pyyntö lähetetään (request url) muutetaan ”***sip:juupe@lyijy.necsom.com”*** –osoitteeksi. Tämä on yksinkertainen tapaus ja uudelleenohjaukseen liittyy paljon muita erilaisia tapauksia, mutta tämän työn puitteissa niitä ei ole mahdollista käsitellä.

4.2.3.2 SIP –Rekisteröijä

Rekisteröijä on yksinkertainen osio, joka osaa rekisteröidä käyttäjän uudet paikkatiedot tietokantaan, jonka jälkeen uudelleenohjauspalvelu voi käyttää niitä. Rekisteröijän teh-

täviin kuuluu rekisteröidä, muuttaa ja poistaa käyttäjien tietoja. Tämä ominaisuus on upotettu uudelleenohjauspalveluumme.

4.2.3.3 Paikannuspalvelin

Paikannuspalvelinta ei ole toteutettu toteutuksessamme vielä mitenkään, mutta yksinkertaisuudessaan se tarjoaa paikannustietoa SIP –osoitteen jatkokäsittelyä varten. Tässä vaiheessa tätä ominaisuutta ei tarvita, mutta tulevaisuudessa sen tarve voi tulla ajankohtaiseksi.

4.2.3.4 SIP –tietokanta

Tietokanta pitää sisällään käyttäjän avaintiedot eli milloin käyttäjän tiedot vanhenevat ja tiedot käyttäjän kontaktitiedoista. Esimerkiksi uudelleenohjauspalvelu käyttää kontaktitietoja. Yhdelle käyttäjälle voi olla useita kontaktitietoja, mutta on erittäin suositeltavaa, että esimerkiksi SIP -osoitteita olisi vain yksi, mutta jos niitä löytyy useita pitää tällöin kaikki palauttaa. Toteutuksemme käyttää SQL –tietokantaa käyttäjän SIP –tietojen tallennukseen.

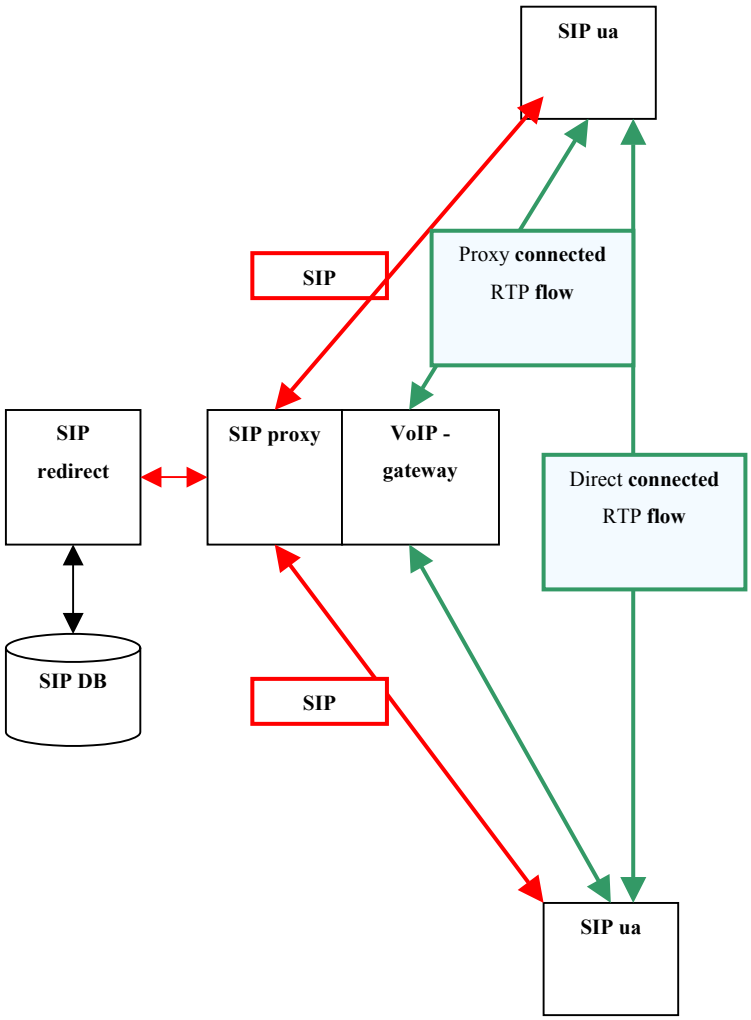
4.3 VoIP –yhdyskäytävän rakenne ja sen sijoitus

Rakenteellisesti toteuttamaamme VoIP –yhdyskäytävää voidaan käyttää ainakin kahdella tavalla. Tämäkin puntarointi ja mietintä on tehty siitä näkökulmasta, että NMS -reitittimessä ei vielä ole kapasiteettia pyörittää VoIP –palvelua itsensä sisällä. Käsitellään aluksi tapaus jossa NMS -reititintä ei esiinny lainkaan. Tämän jälkeen tutkitaan miten VoIP –yhdyskäytävä voisi toimia yhdessä NMS -ympäristön kanssa.

4.3.1 Ilman Necsom Media Switch reititintä

On harhaan johtavaa puhua, että tapauksessa ei ole NMS -reititintä lainkaan, vaan asia on paremminkin niin, että tässä tapauksessa VoIP –yhdyskäytävä toimii ilman NMS -reititintä ja NMS -reititin voi olla VoIP –yhdyskäytävän takana. NMS –reititin voi sijaita yleisessä tai yksityisessä verkossa, mutta jälkimmäisessä tapauksessa VoIP –yhdyskäytävä koneessa pitää toimia myös NAT –muunnospalvelu (yhdyskäytävä hahmottaa molemmat verkot).

Aiemmin on esiintynyt erilaisia kuvia eri mahdollisuuksista miten VoIP –yhdyskäytävä voisi toimia, mutta seuraava kuva esittää tapauksen, jossa yhdyskäytävämme toimii. Yhdyskäytävä toimii yhdessä koneessa ja käyttää tietokantaa tunnistustietojen hakemiseen ja tallennukseen sekä ulkoista SIP –uudelleenohjauspalvelinta käyttäjätietojen hakemiseen. Systeemi voi sijaita sellaisessa pisteessä, jossa julkinen ja yksityinen verkko yhdistyvät toisiinsa eli pisteessä, jossa tehdään muutoksia IP osoitteisiin.

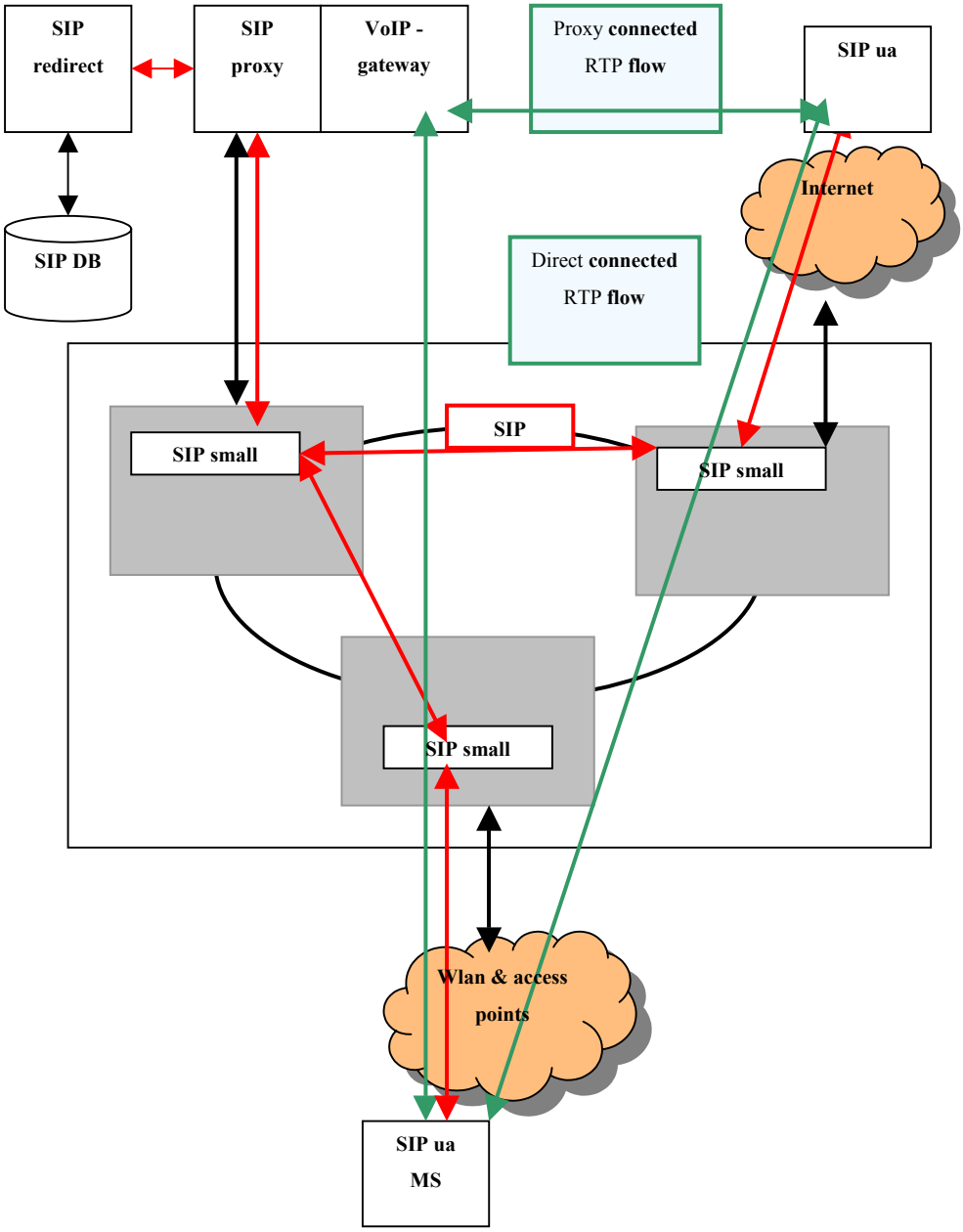


Kuva 21: VoIP –yhdyskäytävä toteutus ilman NMS –ympäristöä

Jos yhdyskäytävä sijaitsee kahden toisilleen näkymättömän verkon yhdistymispisteessä, pitää tietovirtojen myös tällöin kulkea VoIP –yhdyskäytävä toteutuksen kautta. Tällöin ulkoa tuleva soitto päätyy VoIP –yhdyskäytävään ja näin mahdollistetaan soittaminen, koska julkinen verkkohan ei voi lähettää tietoa suoraan yksityisen verkon osoitteisiin. Sinä tapauksessa, että soitto tulee yksityisestä verkosta ja että se on suunnattu yksityiseen verkkoon, voidaan yhteydeksi luoda suora yhteys, jolloin yhdyskäytävä itse ei kuormitu niin paljoa, koska osa tietovirrasta kulkee suoraa tietä päätepisteiden välillä.

4.3.2 VoIP –yhdyskäytävä NMS -reitittimen takana

Tässä tapauksessa VoIP –yhdyskäytävä pitää sijoittaa sellaiseen pisteeseen, että se näkyy sekä julkiseen että yksityiseen verkkoon päin (tarkoittaa että yhdyskäytävällä on sekä julkinen että yksityinen IP -osoite). Muutoin sijoituspaikalla ei ole väliä.



Kuva 22: VoIP –yhdyskäytävä NMS –reitittimen kanssa

Edellä olevassa kuvassa VoIP –yhdyskäytävä sijaitsee yhden kortin takana ja näin kaikki SIP -liikenne kulkee korttien SIP –välityspalvelimien kautta itse VoIP –yhdyskäytävän SIP -osiolle ja tietovirta liikkuu joko suoraan päätelaitteelta päätelaitteelle tai VoIP –yhdyskäytävän lävitse. Tässä tapauksessa NAT aiheuttaa ongelmia ja ainakin osa VoIP –yhdyskäytävästä pitäisi sijaita siellä missä NAT –muunnos tehdään, mutta tämä hajautettu vaihtoehtohan jätettiin huomioimatta ja VoIP –yhdyskäytävä pidetään kokonaisena ohjelmana. Jos VoIP –yhdyskäytävä sijaitsee NAT –koneen takana niin tällöin yhtenä vaihtoehtona olisi reikien muodostaminen dynaamisesti NAT -koneeseen, jolloin julkisesta verkosta tuleva tieto lähetettäisiin edelleen VoIP –yhdyskäytävälle. Tätä mahdollisuutta ei olla kuitenkaan ehditty tutkia ja joten sitä ei käsitellä enempää.

4.3.3 Ominaisuudet

VoIP –yhdyskäytävän rakenteelliset ominaisuudet mahdollistavat pidemmän aikavälin jatkokehityksen, koska siinä voidaan määritellä toiminnallisuuksia osoiteryhmien avulla. Mitä nämä osoiteryhmät sitten tarkoittavat? Alussa osoiteryhmällä sidotaan ominaisuuksia vain omaan verkkoliityntään. Esimerkiksi jonkin verkkokortin ryhmään voidaan lisätä tai poistaa IP –osoitteita ja IP –aliverkkoja. Jos molempien sekä soittajan että vastaajan IP:t kuuluvat samaan ryhmään, niin tällöin heidän välilleen on mahdollista muodostaa suora yhteys (molemmat saman verkkokortin takana). Rakenne perustuu oikeuksiin jolloin jokin aliverkko voi kuulua ryhmään, mutta kyseisen aliverkon jokin IP voidaan asettaan kielto asentoon, mikä tarkoittaa, että kyseisestä IP:stä tulevat tiedot reititetään VoIP –yhdyskäytävän lävitse eikä suorayhteys ole tällöin mahdollinen.

Osoiteryhmät pitää määritellä ainakin VoIP –yhdyskäytävän jokaista verkkokorttia varten, jotta yhdyskäytävä tietää millaisia verkkokortti liitäntöjä on käytettävissä. Nyt toinen kortti voi olla vaikka liityntä julkiseen verkkoon ja toinen yksityiseen verkkoon. Näin VoIP –yhdyskäytävä osaa rakentaa tarvittavat RTP yhteydet oikeaan verkkoon päin ja osaa samalla antaa lupia suorille yhteyksille. Toisaalta voidaan tehdä lisäryhmiä joille voidaan määritellä ominaisuuksia. Ominaisuutena voisi olla esimerkiksi, että jonkin ryhmän osoitteet ovat itse asiassa PSTN –yhdyskäytävän omistamia IP -osoitteita.

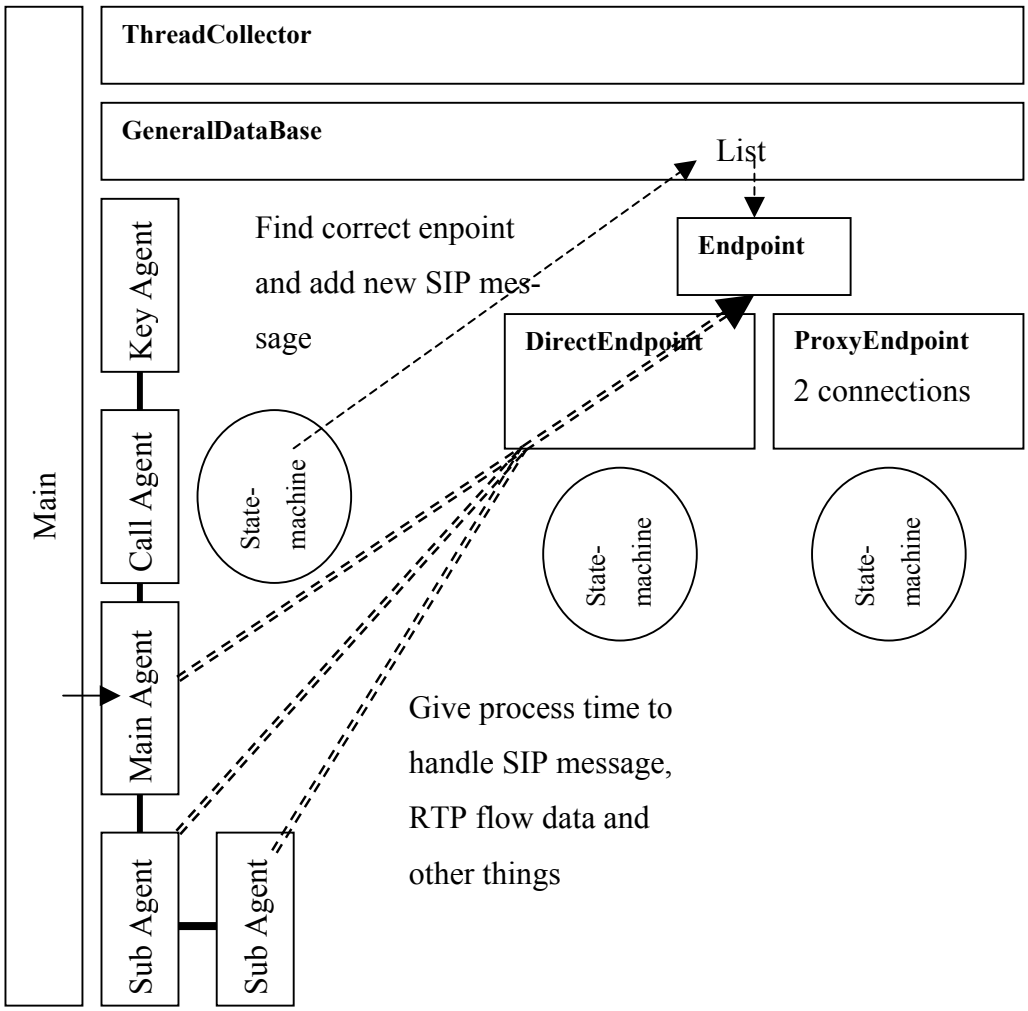
Sitten kun kyseiselle PSTN –yhdyskäytävä tyypille on toteutettu (ohjelmoitu uudenlainen päätepiste) tarvittavat toiminnallisuudet, VoIP –yhdyskäytävämme saadaan toimimaan kyseisen PSTN -yhdyskäytävän kanssa. Yleisesti ottaen rakenne mahdollistaa VoIP –yhdyskäytävän toimimisen mitä erilaisimpien SIP -systeemien kanssa.

Muutoin VoIP –yhdyskäytävän parametrien asetus on lähinnä SIP -tietojen määritystä ja tietoliikenne porttien määrityksiä. Tärkein osio toiminnallisuuden kannalta onkin juuri osoiteryhmien määritteleminen oikealla tavalla. SIP -tietojen määritykseen liittyy tietokantojen IP -osoitetietojen määritteleminen ja uudelleenohjauspalvelun IP –osoitteen määritteleminen. VoIP –yhdyskäytävän osion parametreista tärkein toiminnallisuuden kannalta on säikeiden lukumäärän määritys, koska VoIP –yhdyskäytävässä on mahdollista ajaa useaa rinnakkaista säiettä, jotka jakavat ajoaikaa itse tehtävien suorituksille. Rakenteesta on hyötyä, kun alustana toimii Linux kone, joka on varustettu usealla prosessorilla.

4.3.4 Toteutuksen fyysinen rakenne

SIP -osion rakenteesta kerrotaan enemmän toisessa diplomityössä [Kel01] ja nyt onkin tarkoituksenmukaista kertoa ainoastaan yhdyskäytävän yhteyden hallintapalikan rakenteesta, koska se määrittelee lopulta yhdyskäytävän toiminnallisuuden.

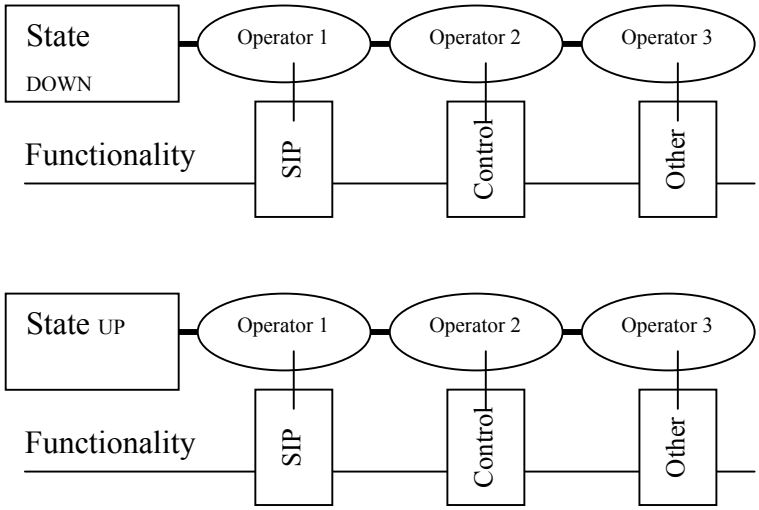
Rakenteellisesti yhteyden hallintapalikk rakentuu signalointi, tilakone ja päätepiste osista. Signalointi tieto otetaan vastaan erityisessä ”callagent” osioissa, joka hoitaa kaiken ulkoisen signaloinnin kuten rajapinan SIP –osioon. Hallintapalikkaan on myös mahdollista lisätä näppäinkomentokuuntelija ”keyagent”, jonka avulla VoiP –yhdyskäytävää voidaan komentaa suoraan shell -ruudulta. Itse prosessointi suoritetaan ”mainagent” osioissa. Jokainen osa toimii omassa säikeessä (engl. Thread) ja ”mainagent” osioilla voi olla rinnakkaisia säikeitä, jotka jakavat myös aikaa tiedon prosessointiin. Näin systeemi saadaan toimiaan tehokkaasti myös moniprosessointi ympäristössä. Seuraava kuva esittää miten hallintapalikka rakentuu.



Kuva 23: Toteutuksen rakenne (yhteyden hallinta osa)

Kokonaisuudessaan rakenteeseen voidaan toteuttaa (ohjelmoida) erilaisia päätepisteitä lisää, jotta VoIP –yhdyskäytävä saadaan toimimaan muiden systeemien kanssa. Tähän voitaisiin rakentaa vaikka uusi päätepiste PSTN –yhdyskäytävää varten. Nyt pitää huomata, että päätepiste pitää sisällään vain toiminnallisuuden yhteydelle, mikä tarkoittaa sitä, että jokaista yhteyttä varten on oma päätepiste. Toisaalta kun huomioidaan VoIP –yhdyskäytävän ominaisuudet niin tiedetään, että parametrien määritysvaiheessa voidaan määritellä päätepisteen tyyppi jollekin osoiteryhmälle, jolloin esim. PSTN –yhdyskäytävän osoite voidaan asentaa sellaiseen moodiin, että viestin tullessa PSTN –

yhdyskäytävän osoitteesta tai mennessä sinne suuntaan luodaan PSTN –yhdyskäytävän tyyppinen päätepiste.



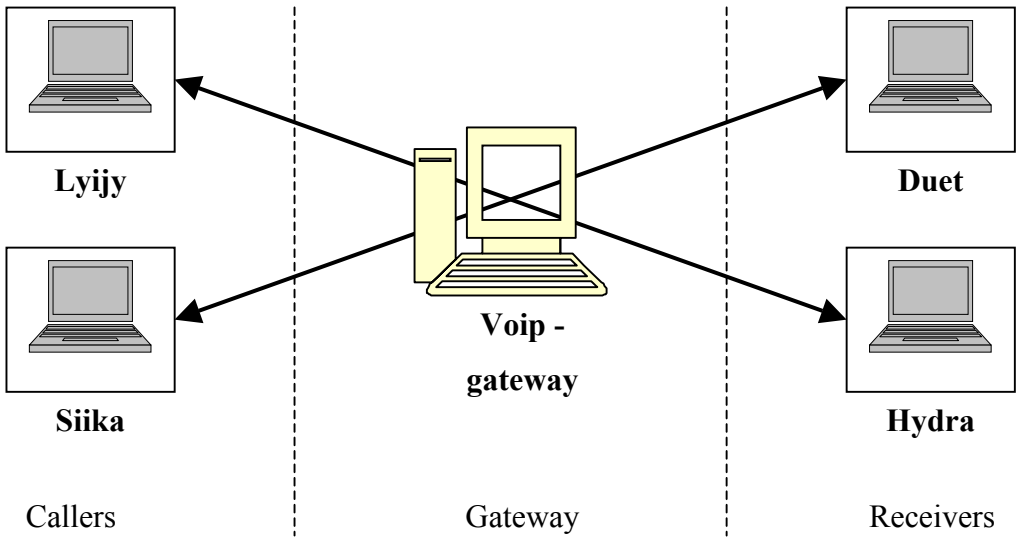
Kuva 24: Tilakoneen toimintaperiaate (yhteyden hallinta osa)

Päätepistettä varten on omanlainen tilakone, jonka avulla päätepisteelle tehdään toiminnallisuuksia. Tilakone on sellainen, että se on yhteinen jokaiselle samantyyppiselle päätepisteelle, milloin tilakoneet eivät vie muistia jokaista luotua päätepistettä kohden vaan jokaista päätepiste tyyppiä kohden. Tilakone rakentuu niin, että päätepistetyypin tilakoneeseen ladataan halutunlaisia operaattoreita ja viestin tullessa operaattoreita kutsutaan vuorollaan ja kutsun onnistuessa tiedetään, että kyseessä oli oikea operaattori. Rakenne on sen takia tällainen, että tilakoneeseen voidaan toteuttaa operaattoreita erilaisia viestityyppejä varten, jolloin tilakonetta voidaan helposti laajentaa ymmärtämään myös muunlaisia viestityyppejä. Nyt tilakoneet ymmärtävät lähinnä vain SIP -viestejä, jotka nekin ovat VoIP –yhdyskäytävämme käyttämässä muodossa, koska virallinen SIP –viestin käsittely tehdään SIP –välityspalvelin moduulissa.

Tietämys yhteydenhallintaosan rakenteesta tällä tasolla riittää tämän työn osalta. Nyt on perustietoa siitä miten systeemi toimii ja miksi se voidaan helposti laajentaa toimimaan useiden erilaisten muiden SIP -systeemien kanssa. Vaikka sovitustyö erilaisiin systeemeihin on helppoa, voi se silti joissain tapauksissa vaatia enemmän työtä, koska ei ole taattua että SIP –välityspalvelin ja ”yhteyden hallinta” -osat toimivat jokaisessa tapauksessa juuri halutulla tavalla.

4.4 VoIP –yhdyskäytävän suorituskyky

Tässä kappaleessa esitetyt mittaukset on tehty rajatulle osalle VoIP –yhdyskäytävän ominaisuuksia. VoIP –yhdyskäytävä prosessoi ainoastaan signalointitietoa eli sen lävitse ei reititetty laisinkaan tietovirtaa (itse ääntä). Ajon aikana ainoastaan yksi säie prosessoi käsiteltävää tietoa eli tässä testissä pelkästään signalointia ja näin ollen kaikki muut säikeet olivat joko protokollapinon tai VoIP –yhdyskäytävän muun toiminnallisuuden omistamia. Mittaustuloksissa esitettyjä arvoja olisi varmasti saatu parannettua jos tietoa prosessoivien säikeiden määrää olisi nostettu, mutta esitetyt tiedot riittävät vallan hyvin esittämään VoIP –yhdyskäytävän toiminnallisuuden arvoja.



Kuva 25: Testausjärjestely

Koejärjestelyt olivat edellä esitetyn kuvan kaltaiset. VoIP –yhdyskäytävän toimimiseen tarvittavat kaikki moduulit (tietokanta, SIP –uudelleenohjauspalvelu ja itse VoIP -yhdyskäytävä) toimivat yhdellä koneella ja VoIP -yhdyskäytävää kuormitettiin neljällä erilliseltä koneella seuraavanlaisesti: Kaksi koneista toimi lähettävänä osapuolena ja kaksi vastaavasti vastaanottavana osapuolen. Kumpikin lähettävä osapuoli loi rinnak-

kaisesti useita puheluita, jolloin VoIP –yhdyskäytävä signaloi useita puheluita yhtä aikaa. VoIP –yhdyskäytävä toimi koneessa, jossa toimi Linux –käyttöjärjestelmästä Debianin jakeluversio. Kone oli Celeron 700 Mhz ja koneessa oli käytettävissä keskusmuistia 155 Mt. Toisaalta kone olisi voinut olla moni prosessori kone, jolloin tulokset olisivat parantuneet paremman rinnakkaisen ajon myötä.

Kuvaus	**Ensimmäinen yhteys (lyijy ← → hydra)**	**Toinen yhteys (siika ← → duet)**
Puheluiden viive (kahden puhelun välillä)	1000 millisekuntia	1000 millisekuntia
Puhelun kesto	1000 millisekuntia	1000 millisekuntia
Puheluiden määrä	100 puhelua	100 puhelua
Rinnakkaisten puheluiden määrä	6 kappaletta	6 kappaletta

Taulukko 7: Testauksessa käytetyt arvot

Edellä esitetyssä taulukossa on esitetty avainarvoja mittaustapahtumasta, joiden perusteella puhelinliikennettä simuloitiin. Lähettävät osapuolet laskivat kauan puhelun pystyyn laittamiseen ja sen sulkemiseen kuluu aikaa ja näiden tietojen perusteella kyettiin laskemaan läpi menevien puheluiden lukumäärä sekuntia kohden. Simuloitavissa yhteyksistä (ensimmäinen ja toinen yhteys) laskettiin keskiarvot kaikkien rinnakkaisten puheluiden tuottamille arvoille. Avain arvoksi saatiin 200 puhelua 35 sekuntia kohden mikä tarkoittaa siis 5.7 puhelua sekuntia kohden.

Tulokset olivat halutunlaiset, koska systeemin lävitse kyettiin välittämään sekunnissa useita yhtäaikaisia istuntoja. Testauksessa pyrittiin saamaan hiukan kuvaa systeemin toimivuudesta ja eikä kyseessä ollut nopeustestaus. Aiemmin esitetty koejärjestely kertookin, että testaamisessa oltaisiin voitu käyttää rinnakkaisia säikeitä ja ajoalustana olisi voinut olla rinnakkaiseen ajoon paremmin skaalauntuva ympäristö, jolloin tulokset olisivat parantuneet. Saavutettu tulos ylsi haluttuihin vaatimuksiin.

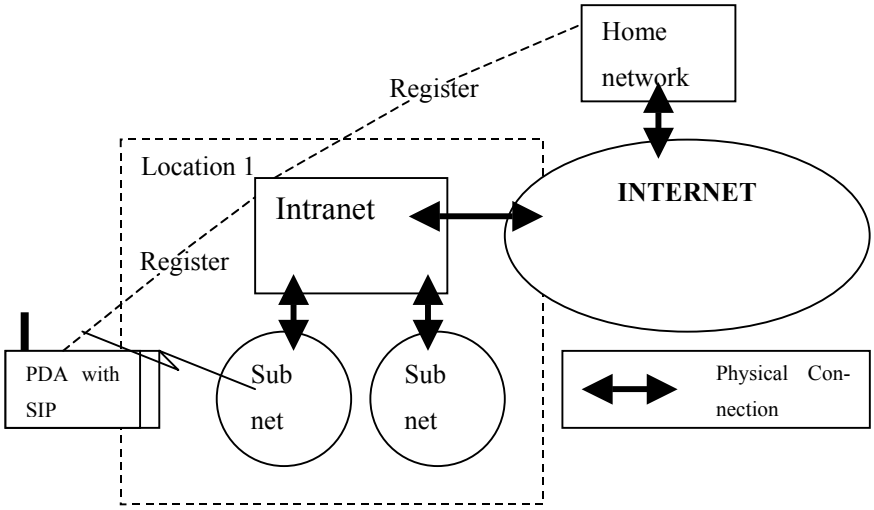
5 VoIP –YHDYSKÄYTÄVÄN TULEVAISUUS

Tulevaisuutta mietittäessä pitää huomioida useita erilaisia asioita, jotka voivat vaikuttaa omalta osaltaan niin VoIP –systeemin kokonaisuuteen kuin sen yksittäisiin kohtiin. Kaiken lisäksi kurkottaessa tulevaisuuteen sinne voidaan päätyä useita eri polkuja pitkin, jolloin nämä polut itsessään asettavat vaatimuksia.

Jo tälläkin hetkellä on tarvetta sellaisille systeemeille, joilla voitaisiin säästää esimerkiksi yritysten sisäisissä puhelinkuluissa ja lähitulevaisuudessa ratkaisuiden tarve lisääntyy yhä enemmän. Toisaalta nykyisellä mobiili-aikakaudella yritysten tärkeimpänä viestintävälineenä on matkapuhelin ja yleisesti se on vielä ainoa puhelin mitä henkilökunta käyttää eikä rinnakkaisen lankapuhelimen hankintaa ole katsottu tarpeelliseksi, vaikka lankapuhelimella soittaminen on ainakin vielä tällä hetkellä huomattavasti halvempaa kuin matkapuhelimella. Matkapuhelimien yleistyessä tämä saattaa tietysti lähitulevaisuudessa kääntyä päälaelleen. Toisaalta kaikilla yrityksillä ei ole varaa hankkia omaa puhelinkeskusta, jonka avulla yrityksen sisäiset puhelut olisivat ilmaisia. Mikäpä olisi parempi ratkaisu yritysten sisäisen puhelinliikenteen alustaksi kuin yrityksessä valmiiksi oleva tietoliikenneverkko, jolloin jokaisen työpöydällä oleva tietokone toimisi päätelaitteena. Tietysti tavoitettavuus on huonompi kuin matkapuhelimessa (sama kuin lankapuhelimessa), mutta ratkaisuna se olisi huomattavasti halvempi kuin oman puhelinkeskuksen hankkiminen, koska tällöin kaikki puhelinliikenne voitaisiin reitittää ohjelmistojen avulla verkossa. Toisaalta langattomuus on toinen tekijä, joka lisää kiinnostusta yritysten sisäisen puhelinliikenteen siirtämisestä tietoliikenneverkossa, mutta tästä on näkemyksiä hieman myöhemmin. Toteutuksemme yhtenä mahdollisena sijoituspisteenä on alusta asti pidetty juuri sisäistä puhelinliikenettä.

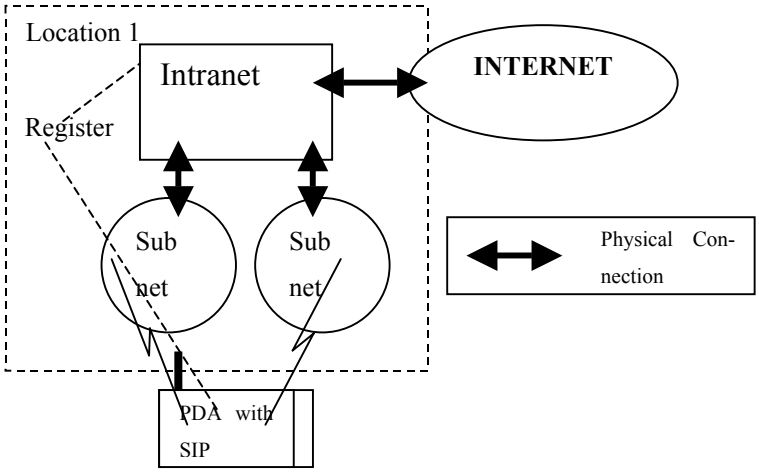
Yksi tärkeä asia on mobiliteetti (langattomuus), mikä tarkoittaa mobiililaitteiden liikutettavuutta. Useasti asiasta puhutaan käsitteellä 4G: ”Neljännen sukupolven mobiiliverkot kokoaa kaikki tietoliikenneverkot ja palvelut internetin ympärille” [Ikk01]. Tässä tapauksessa VoIP -yhdyskäytävä olisi 4G -verkkojen yksi palvelu ja tietysti äänen siirtäminen sisältyy itsessään 4G -käsitteeseen, koska se on perusosio koko tietoliikenneverkon rakenteessa. Näin VoIP –palveluita tarvitaan mobiiliverkoissa siinä missä äänen

siirtoa tarvitaan puhelinverkoissa. Tällä hetkellä esille on noussut WLAN käsite, joka tarjoaa langattoman tiedonsiirron IP –verkoissa ja näin se voi liittää mobiileja laitteita IP –verkkoon. Kuten aiemmin tuli esille niin käyttämämme SIP -protokolla ei puutu siirtotiehen ja näin sen käyttö sopii ilman mitään erityisiä muutoksia myös WLAN verkkoon. Tietysti ainoa tarvittava seikka on SIP -protokollaa ymmärtävä ohjelmisto mobiiliin laitteeseen. Ongelmana ei ole yksittäinen systeemi vaan kokonaisuus, koska yhdessä paikassa päätelaitteella on kiinteä osoite, mutta siirryttäesä systeemistä toiseen päätelaite saa uuden osoitteen, jolloin puhelinyhteys katkeaa jos mitään ei tehdä. Tällöin pitää suorittaa roaming toiminnallisuuksia, jotta päätepisteet tietävät asentaa esimerkiksi käynnissä olevaan puheluun uudet parametrit. Tämä alue on vielä tutkimuksen alla eikä siitä ole olemassa mitään jäädytettyä määritystä ja on vaikea toteuttaa mitään standardinomaista ratkaisua. Mobiliteetti rakentuu kolmesta vaiheesta, joista on seuraavaksi pienet selostukset ja kuvat.



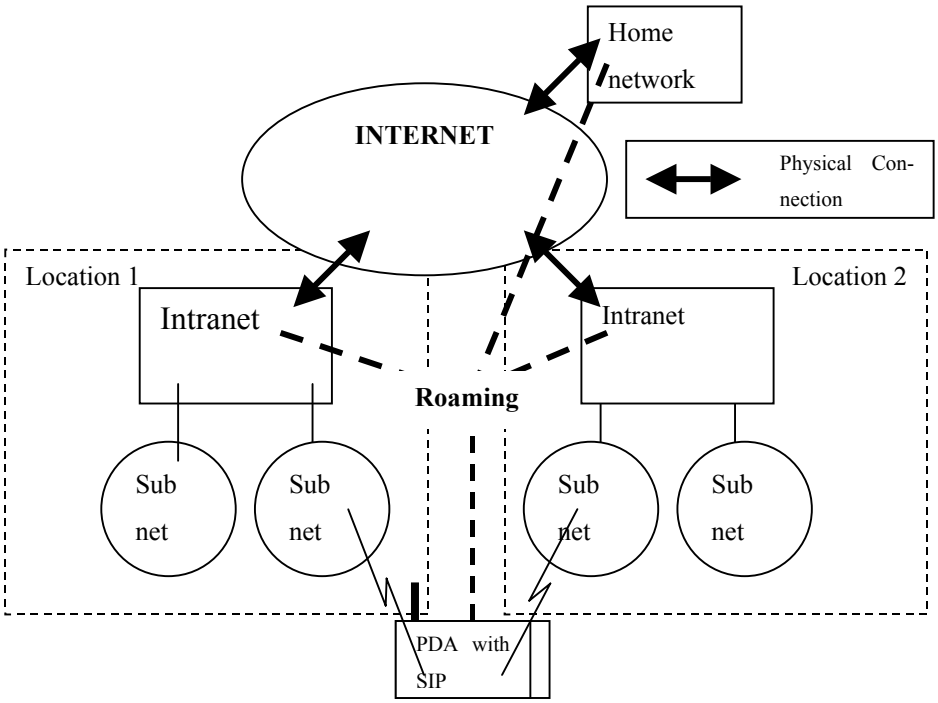
Kuva 26: Mobiliteetti: Rekisteröityminen vieras verkossa

Edellä oleva kuva kuvaa päätelaitteen tulemista systeemin sisälle jolloin se rekisteröityy siihen ja samalla systeemi ilmoittaa päätelaitteen kotiverkolle (omalle verkolle) uuden paikan, jossa päätelaite sijaitsee. Näin kotiverkkoon tulevat kutsut ohjataan uudelleen oikeaan paikkaan.



Kuva 27: Mobiliteetti: Aliverkon vaihto

Tässä tapauksessa päätelaite siirtyy systeemin sisällä toisesta aliverkosta toiseen jolloin sen osoite muuttuu toiseksi eli sellaiseksi osoitteeksi, joka kuuluu uuteen aliverkkoon. Tällöin on tarpeellista ilmoittaa systeemin sisällä uusi paikka, jossa päätelaite on, mutta nyt ei ole tarpeellista ilmoittaa kotiverkolle mitään, koska systeemi ei vaihdu. Englannin kielessä tätä tapausta kutsutaan ”terminal mobility” nimikkeellä.



Kuva 28: Mobiliteetti: Järjestelmän vaihto

Viimeisin kuvasarjan kuva taas kuvaa tapausta, jossa päätelaite siirtyy kokonaisuudessa systeemistä toiseen, jolloin on myös tarpeellista ilmoittaa uudesta paikasta kotiverkkoon. Tätä tapausta kutsutaan nimikkeellä roaming.

Näistä kolmesta tapauksesta huomataan millaisia asioita tulevaisuus tuo tullessaan ja millaisia asioita pitää huomioida VoIP –palvelua kehittäessä mobiilia ympäristöä varten. Kaikkien ongelmien ratkaiseminen ei ole aivan helppoa ja jos tällainen systeemi olisi jo jollain olemassa niin hänellä olisi erittäin suuri etumatka kilpailijoihin. SIP -protokollan puolella on useita ratkaisuja mobiliteetin hallintaan ja rekisteröintiin ja näitä on kuvattu enemmän [Scu01] dokumentaatiossa. Asiasta on kerrottu tätä kappaletta hiukan tarkemmin diplomityössä [Kel01].

IPv4 tilalle kaavailtu IPv6 tarjoaa huomattavasti enemmän osoitteita eikä tällöin olisi enää tarpeellista tehdä NAT -muunnoksia, koska IP -osoitteita olisi tarpeeksi käyttöön kuin käyttöön. Miksi siis kehittää systeemiä, joka kykenee toimimaan yksityisen verkon ja julkisen verkon välillä? Tässä kappaleessa ei ole esitelty sitä asiaa mikä on myös erittäin oleellinen eli VoIP –palvelun yhdistäminen jo olemassa olemaan puhelinsysteemiin PSTN –yhdyskäytävän avulla. Jotta yhdistäminen on mahdollista tarvitaan sellainen toteutus, joka ymmärtää PSTN –yhdyskäytävän vaatimukset ja pystyy näin ollen keskustelemaan sen kanssa. Vaikka PSTN –yhdyskäytävä hoitaisikin signaloinnin SIP -protokollan avulla niin ei ole sanottua, että päätelaite kykenisi suoraan keskustelemaan sen kanssa, vaan on oletettava, että VoIP –yhdyskäytävä pitää sisällään sellaista tietoutta minkä avulla yhteyden ottaminen onnistuu (Esimerkiksi tilakoneet ja niiden synkronisuus PSTN –yhdyskäytävän omien tilojen kanssa). Tällöinhän PSTN -liikenne muutetaan PSTN -yhdyskäytävä → VoIP –yhdyskäytävä systeemin kautta IP -verkkoon.

Tulevaisuuden näkymissä pitää myös huomioida VoIP –palvelun käyttäjän tunnistus ja samalla systeemin turvallisuus näkökohdat. Miten käyttäjä voidaan tunnistaa tarpeeksi luotettavalla tasolla ja miten tiedonsiirto saadaan turvalliseksi? Sinällään SIP protokollassa on huomioita turvallisuus tekijöitä erilaisilla salaus- ja sähköisillä allekirjoitus teknologioilla, mutta kysymykseksi nouseekin se, että miten voimme olla varmoja, että

käyttäjä on todellakin oikea. Käyttäjän saapuessa systeemiin hänet voidaan tunnistaa SIP -protokollan avulla, mutta miten luotettavaa tämä on ja miten tämän jälkeen toimitaan ja miten seuraavat SIP -viestit voidaan tunnistaa niin, että niiden tiedetään tulevat oikealta käyttäjältä. Pitäisikö jokainen SIP -viesti tunnistaa, jolloin turvallisuus paranisi? Esimerkkinä GSM -verkoissa puhelimessa on SIM kortti, jonka avulla käyttäjä voidaan tunnistaa tarkasti, mutta nykyisissä pakettikytkentäisissä verkoissa vastaavaa systeemiä ei vielä ole ja pelkkä tunnus-salasana pari ei ole luotettava ratkaisu, koska se antaa käyttäjälle mahdollisuuden vähentää tiedostamattaan tietoturvaa antamalla omat tunnukset vaikkapa toiselle henkilölle. Tämähän on suhteellisen mahdotonta esimerkiksi GSM verkoissa, koska harvempi ihminen on halukas antamaan oman SIM korttinsa toisen käyttöön. Tietysti vanhan tunnistuskeinon sijaan voitaisiin käyttää biometrisiä tunnisteita kuten sormenjälkiä tai sitten voitaisiin käyttää sirukorttia (GSM verkon SIM kortti on myös sirukortti) myös IP -verkoissa (sähköinen henkilökortti), mutta tämä taas vaatii lisälaitteistoa päätelaitteisiin eli käytännössä kortinlukijan. Toisena osana on itse tiedon siirtämisen turva. Kun äänitietoa siirretään niin nykyään se kulkee suhteellisen normaalissa muodossa eli sellaisena, että ulkopuoliset voivat poimia tietoa verkosta ja kuunnella mitä siellä kulkee. Tällöin pitäisi tiedolle tehdä salaus, jolloin sen lukeminen olisi mahdotonta. Tietysti voidaan käyttää ”Virtual Private Network” –tunneleita (engl. VPN tunnel) tiedonsiirrossa vaikka yrityksen sisällä, mutta tämä ei ole yleispätevä ratkaisu ja tällöin VoIP –systeemi olisi osaksi riippuvainen VPN ratkaisuista. ’Alku vaiheissa tullaan varmasti toimeen tällaisellakin ratkaisulla, mutta erilaisia ratkaisuja pitää miettiä tulevaisuutta varten, kuten vaikkapa jotain muunnos tapaa (engl. codec), joka osaa tehdä tiedolle salauksen.

Tulevaisuus tuo monia haasteita mukana niin palvelun sijainnin, verkon rakenteen ja turvallisuuden suhteen. Kootessa kaikki yhteen kokonaisuuteen huomataan, että paljon on vielä työtä edessä ja oikeanlaisten ratkaisujen hakeminen vaatii pitkäjänteistä tutkimusta ja opiskelua. Voisimme kuitenkin uskoa, että loppujen lopuksi maaliin päästään oikeiden ja väärien ratkaisuiden viitoittamana.

6 JOHTOPÄÄTÖKSET

Nykykehityksen mukaisesti tietoliikenne on siirtymässä kokoajan olemassa olevista piirikytkentäisistä verkoista pakettikytkentäisiin verkkoihin, mistä hyvänä esimerkkinä on GSM verkkojen laajennus GPRS, joka tarkoittaa sitä, että matkapuhelin liikenne liikkuu paketteina. Toisaalta päätelaiteet voivat toimia monipuolisesti niin olemassa olevissa matkapuhelinverkoissa kuin IP –verkoissa, mikä tarkoittaa, että verkot ovat näennäisesti yhdistymässä. Tällöin on tarpeellista kehittää palveluita äänen siirtämiseksi IP verkoissa. Toisaalta nykyisin on jo tarvetta sisäisen puhelinliikenteen siirtämiseen IP –verkoissa, joka toisi paljon hyötyä kustannusten kurissa pitämiseksi. Nämä seikat vaikuttavat siihen, että tulevaisuudessa tarvitaan yhä enemmän VoIP –palveluita IP –verkoissa ja muutoinkin Internetissä.

Työ esittelee VoIP –yhdyskäytävän toteuttamisen ongelmia, käytetyt SIP- ja MGCP -protokollat ja laitteistoalustan, johon VoIP –yhdyskäytävä alustavasti suunniteltiin. VoIP –yhdyskäytävä ratkaisee osaltaan tulevaisuuden ongelmia tai ainakin helpottaa niiden ratkaisemisessa, koska toteutus voidaan sijoittaa juuri sellaisiin paikkoihin missä yritysten verkot voivat hyödyntää palvelua tehokkaasti, ja missä neljännen sukupolven (4G) [Myl01] verkot voivat hyödyntää VoIP –palvelua yhdistäessään erityyppisiä verkkoja yhdeksi tai sitten sellaisessa pisteessä, jossa PSTN –liikenne voidaan ohjata IP –verkkoon.

Omalta osaltaan toteutettu ratkaisua voidaan laajentaa tarpeen vaatiessa niin, että sen yhteensopivuus on mahdollisimman kattava, jolloin VoIP –yhdyskäytävä ei ole riippuvainen systeemin ominaisuuksista niin paljon eli tällöin VoIP –yhdyskäytävä voi toimia mitä erilaisempien systeemien kanssa.

Lähitulevaisuus näyttää sen onko VoIP –palveluiden tarve niin suuri kuin tällä hetkellä kuvitellaan, mutta yleisesti kehityksen suunta näyttää kulkevan juuri sinne missä kaikki tietoliikenne on pakettiliikennettä ja näin VoIP –palveluille on myös oma paikkansa.

LÄHTEET

[RFC2705] Arango, M., Dugan, A., Elliott, I., Huitema, C., Pickett, S., MGCP: Media Gateway Control Protocol RFC 2705 [Verkkodokumentti], Lokakuu 1999, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc2705.txt

[RFC1889] Schulzrinne, H., Casner, S., Frederick, R., and Jacobson, V., Real-Time Transfer Protocol RFC 1889 [Verkkodokumentti], Tammikuu 1996, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc1889.txt

[RFC1890] Schulzrinne, H., RTP Profile for Audio and Video Conferences with Minimal Control RFC 1890 [Verkkodokumentti], Tammikuu 1996, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc1890.txt

[RFC2543] Handley, M., Schulzrinne, H., Schooler, E., and Rosenberg, J. Session Initation Protocol, RFC 2543 [Verkkodokumentti], Maaliskuu 1999, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc2543.txt

[RFC2326] Schulzrinne H., Rao A., Lanphier R. Real Time Streaming Protocol (RTPS), RFC 2326 [Verkkodokumentti], Huhtikuu 1998, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc2326.txt

[RFC2327] Handley, M. and Jacobson, V. Session Description Protocol, RFC 2327 [Verkkodokumentti], Huhtikuu 1998, [Viitattu 9.10.2001]. Saatavissa: ftp://ftp.ietf.org/rfc/rfc2327.txt

[Ste98] Stevens, R. 1998. Unix Network Programming Vol. 1 second edition. London: Prentice Hall. ISBN 0-13-490012-X

[Kel01] Kellokoski, J. Puhelunohjaus Internetissä, Diplomityö, Lappeenrannan teknillinen korkeakoulu. Syyskuu 2001. (Julkaisematta)

[Ikk01] Ikkelä, K. Local Services In A Fourth Generation Mobile Networks, Diplomityö, Lappeenrannan teknillinen korkeakoulu. Heinäkuu 2001.

[Myl01] Myllynen, M. The Architecture Of A Fourth Generation Mobile Network, Diplomityö, Lappeenrannan teknillinen korkeakoulu. Kesäkuu 2001.

[Kau01] Kauranen, O., Kellokoski, J., Voice Over IP Implementation Using Session Initiation and Media Gateway Control Protocols. Personal Wireless Conference PWC 2001.

[Scu01]. Schulzrinne H. SIP Registeration . Internet Draft. Huhtikuu 2001 (työn alla)

[Str00] Stroustrup, B., C++ -ohjelmointi, 2000, Teknolit Oy, ISBN: 951-846-026-4

[Gam00] Gamma, E., Helm, R., Johnson, R., Vlissides, J., Design Patterns, 1995, Addisson-Wesley, ISBN: 0-201-63361-2

[Vovida] Vovida.org, Kotisivut [Verkkodokumentti], Syyskuu 2001, [Viitattu 20.09.2001]. Saatavissa: http://www.vovida.org

[Nec01] Necsom Oy, Kotisivut [Verkkodokumentti], Syyskuu 2001, [Viitattu 20.09.2001]. Saatavissa: http://www.necsom.com

MEDIA SWITCH TECHNICAL DETAILS

MEDIA SWITCH TECHNICAL DETAILS	
Switching Fabric	Non blocking FSR architecture
Switch Throughput	2 Gbit/s (typical)
Line Interface Units (LIU)	100/100 Mbit/s Ethernet STM1 ATM (one physical port per unit)
Processor Unit (Availability mid 2001)	Plug in with a powerful processor and USB interface
Power unit	220/240 VAC @ 500Hz
Nominal power consumption	100 W
Operating system on interface cards	Linux
Operating system on control computer	Sun Solaris on SPARC Linux Win32
Chassis dimensions	48,2 cm x 32,4 cm x16,0 cm (W x D x H)
Weight	5 kg maximum

SDP MESSAGE FORMAT

Next is shown the SDP messages general format. First we describe the general format of parameters. Parameter fields (lines) are format:

Parameter-type>=<Value>

Next is listed all parameter types of the SDP messages and those are in that order that RFC 2327 defines. So the parameters must be in the same order where the appear below. Parameter is optional if their value is * character.

v= (protocol version)
o= (owner/creator and session identifier).
s= (session name)
i=* (session information)
u=* (URI of description)
e=* (email address)
p=* (phone number)
c=* (connection information - not required if included in all media)
b=* (bandwidth information)
One or more time descriptions (see below)
z=* (time zone adjustments)
k=* (encryption key)
a=* (zero or more session attribute lines)
Zero or more media descriptions (see below)

Time description
t= (time the session is active)
r=* (zero or more repeat times)

Media description
m= (media name and transport address)

i=* (media title)
c=* (connection information - optional if included at session-level)
b=* (bandwidth information)
k=* (encryption key)
a=* (zero or more media attribute lines)

Next is shown simple example of the SDP message and there is also shown parameter field formats. As you can see SDP parameter and message format is very simple to understand.

v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait