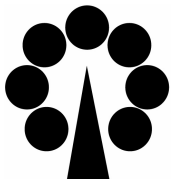


Satakunnan ammattikorkeakoulu

Antti Peurakoski

HAJAUTETTU TESTAUSYMPÄRISTÖ

Tekniikan Porin yksikkö

Tietotekniikan koulutusohjelma

Ohjelmistotekniikan suuntautumisvaihtoehto

2008

TIIVISTELMÄ

HAJAUTETTU TESTAUSYMPÄRISTÖ
Antti Peurakoski

SATAKUNNAN AMMATTIKORKEAKOULU
Tekniikan Porin yksikkö
Tekniikantie 2
28600 Pori

Tietotekniikan koulutusohjelma
Ohjelmistotekniikan suuntautumisvaihtoehto
Työn valvoja: Juha Aromaa, DI
Päättötyö: 37 sivua, 1 liite
Tammikuu 2008
UDK: 004.73, 621.395

Asiasanat: merkinanto, SIGTRAN, IP-puhelu, Media Gateway

Concilio Mobile Gateway Suite on järjestelmä, jonka avulla pystytään yhdistämään osia sekä mobiili- että VoIP-verkoista. Sen avulla voidaan soittaa normaali IP-puhelu tavallisella dataominaisuuksia vailla olevasta 2G/3G-puhelimesta, ilman mitään erillisiä lisälaitteita tai –ohjelmia.

Työssä kuvataan kyseisen tuotteen systeemitestaukseen rakennettu hajautettu testausympäristö. Se sisälsi Espoossa sijaitsevat Concilio Mobile Gateway Suite:n komponentit yhteydessä Satakunnan Ammattikorkeakoulun NGN-laboratorion mobiiliverkkoon. Työ sisälsi monien uusien tekniikoiden käyttöönottoa, kuten SIGTRAN-linkit ja CESoPSN-protokolla.

ABSTRACT

DECENTRALIZED TESTING ENVINROMENT
Antti Peurakoski

SATAKUNTA UNIVERSITY OF APPLIED SCIENCES
Unit of Technology in Pori
Tekniikantie 2
28600 Pori

Degree Program of Information Technology
Programming Technology
Supervisor: Juha Aromaa, M.Sc
Bachelor's Thesis: 37 pages, 1 annex
January 2008
UDC: 004.73, 621.395

Key Words: signaling, SIGTRAN, Voice over IP, Media Gateway

Concilio Mobile Gateway Suite is a solution which connects parts of GSM and VoIP networks. It allows normal 2G/3G handset to make a basic VoIP call without any accessories or separate software.

A decentralized testing environment for system testing is described in this thesis. Testing environment included components of Concilio Mobile Gateway Suite connected to Satakunta University of Applied Science NGN-laboratory's mobile network. Components were located in Espoo and Pori. Work involved many new technologies as SIGTRAN and CESoPSN protocol.

SISÄLLYS

LYHENTEET

AIS	Alarm Indication Signal
BSS	Base Station Subsystem
BSC	Base Station Controller
BTS	Base Transceiver Station
CAS	Channel Associated Signaling
CEM	Customer Experience Management
CES	Circuit Emulation Services
CESoPSN	Circuit Emulation Services over Packet Switching Network
CEM	Concilio Element Manager
CEPT	European Conference of Postal and Telecommunications Administrations
CMS	Concilio Mobile Gateway Suite
DNS	Domain Name System
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
GAGW	Concilio Access Gateway
CRGW	Concilio Roaming Gateway
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GW	Gateway
HDSL	High bit-rate Digital Subscriber Line
HLR	Home Location Register
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force

IP	Internet Protocol
IPDC	Internet Protocol Device Control
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
LAN	Local Area Network
MAP	Mobile Application Part
MEGACO	Media Gateway Control Protocol
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MOC	Mobile Originating Call
MSC	Mobile Switching Center
MTC	Mobile Terminating Call
MTP	Message Transfer Part
NGN	Next Generation Network
OSI	Open Systems Interconnection
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
PW	Pseudo-Wire
PSTN	Public Switched Telephone Network
RAN	Radio Access Network
RNS	Radio Network System
RTP	Real-time Transport Protocol
SCCP	Signaling Connection and Control Part
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol

SG	Signaling Gateway
SGCP	Simple Gateway Control Protocol
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SP	Signaling Point
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexed
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
VDSL	Very High Speed Digital Subscriber Line
VLR	Visitor Location Register
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

1 JOHDANTO

VoIP (Voice over IP) on muuttanut suuresti yritysten viestintää helpompaan ja halvempaan suuntaan. Nyt tämä muutos tekee tuloaan mobiiliympäristöön. Ennen sen käyttö matkapuhelimessa oli rajoitettua pienen kaistan ja kalliin hinnan vuoksi. Wi-Fi-yhteyksiä käyttävät matkapuhelimet ja 3G muuttavat tilanteen toiseksi.

VoIP on osoittautunut hyväksi tuotteeksi myös yksityisellä sektorilla. Halvat ja jopa ilmaiset puhelut houkuttelevat suuresti kuluttajia. Jos nuo ominaisuudet yhdistettäisiin mobiiliverkkoon, internet puhelut leviäisivät asiakkaiden normaalikäyttöön myös työpaikan ulkopuolella.

Operaattorit ovat aina hallinneet mobiiliverkkoja ja –markkinoita. 2G/3G-verkkojen lisenssien ja laitteiden suuren hinnan vuoksi uusien yritysten mukaantulo markkinoille on ollut todella hankalaa. Internet on kuitenkin kaikkien käytössä, joten luonnollisesti se on suunta, johon matkapuhelinyhteyksiä kannattaa viedä. Tässä työssä tutustutaan yhden vaihtoehdon, Concilio Mobile Gateway Suite:n järjestelmän rakentamiseen ja testausvaiheeseen.

Concilio Mobile Gateway Suite:n testaus Satakunnan ammattikorkeakoulun kanssa alkoi kesällä 2007. NGN-laboratorion laitteet ovat olleet välttämättömiä systeemitestauksessa. Työssä perehdytään tarkemmin tämän testausympäristön rakentamiseen, laitteisiin, yhteyksiin ja itse testaukseen.

2 CONCILIO MOBILE GATEWAY SUITE

2.1 Yleistä

Concilio Networks tuo VoIP-ympäristön edut ja ominaisuudet kaikkiin GSM/3G-päätelaitteisiin, myös ilman kehittyneitä dataominaisuuksia vailla oleviin vanhoihin puhelimiin yhdistämällä normaalit mobiiliverkot internettiin. Concilio Mobile Gateway Suite (CMS) toimii Radio Access Network:in (RAN) ja VoIP-ympäristön välissä eräänlaisena rajapintana. [1]

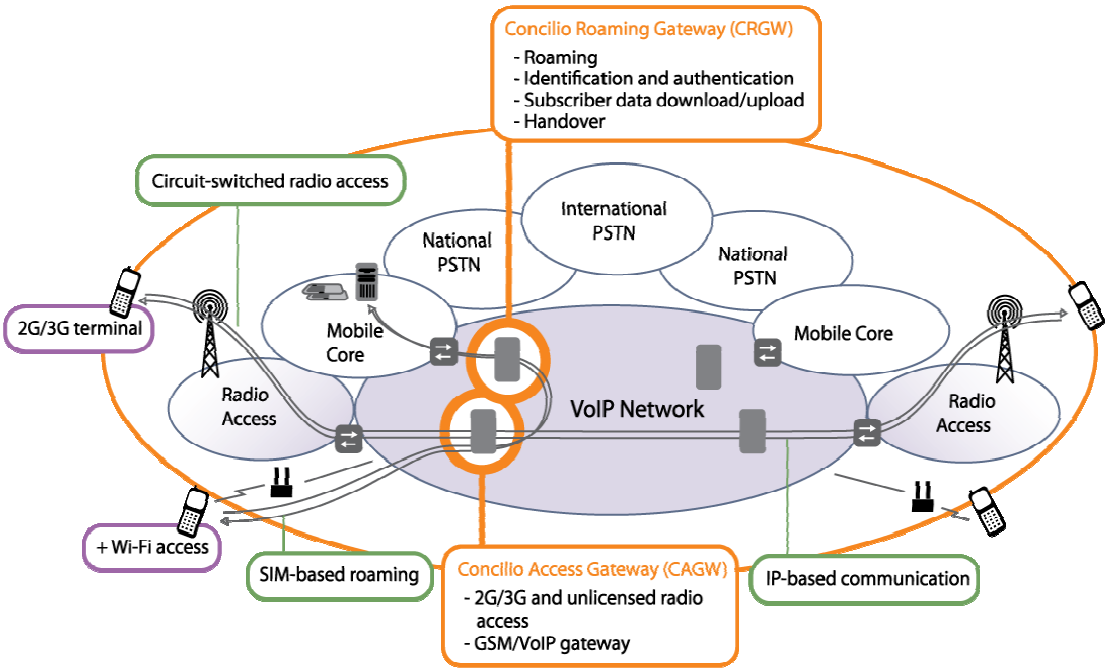
Concilion tuotteet tekevät mahdolliseksi WiFi-verkkoja tukevien puhelimien vierailut GSM/3G- ja WiFi-verkkojen välillä. Matkapuhelimet toimivat VoIP-päätelaitteina käyttäen samaa numeroa kuin normaaleissa GSM-verkoissa ilman mitään erillisiä asiakasohjelmia. WiFi- ja mobiiliverkot yhdistyvät yhdeksi suureksi verkoksi. [1]

Concilio Mobile Gateway Suite:n hyödyt:

- Edullisemmat puhelut
- Helppo ja halpa tapa yhdistää mobiili- ja WiFi-verkot
- Käyttää yhtä ja samaa GSM-numeroa kaikissa verkoissa
- Loppukäyttäjän näkökulmasta mikään ei muutu, käyttö samanlaista kuin ennenkin

2.2 Arkkitehtuuri

Concilio Mobile Gateway Suite:n ideana on käyttää hyväksi jo olemassa olevia matkapuhelin- ja IP-verkkoja (Internet Protocol). Se yhdistää sekä piirikytkentäisen- että VoIP-verkon piirteitä yhteen. [3]



Kuva 1. Concilio Mobile Gateway Suite:n arkkitehtuuri. [3]

Kokonaisuus rakentuu VoIP-, mobiili- ja muista verkoista (esim. WiFi), jonka kautta yhteys CMS:ään on mahdollista. Kaksi tärkeintä komponenttia ovat Concilio Access Gateway (CAGW) ja Concilio Roaming Gateway (CRGW). CAGW yhdistää kaikki eri verkot VoIP-ympäristöön ja GRGW yhdistää VoIP:in mobiiliverkkoon mahdollistaen mm. sijainnin päivitykset, autentikoinnit, jne. [3]

Ympäristössä on yleensä yksi GRGW ja useita Access Gateway:tä. Asennus on helppoa, GAGW:hen konfiguroidaan vain verkkoasetukset ja GRGW:n osoite jolloin se hakee kaikki asetuksensa automaattisesti. [3]

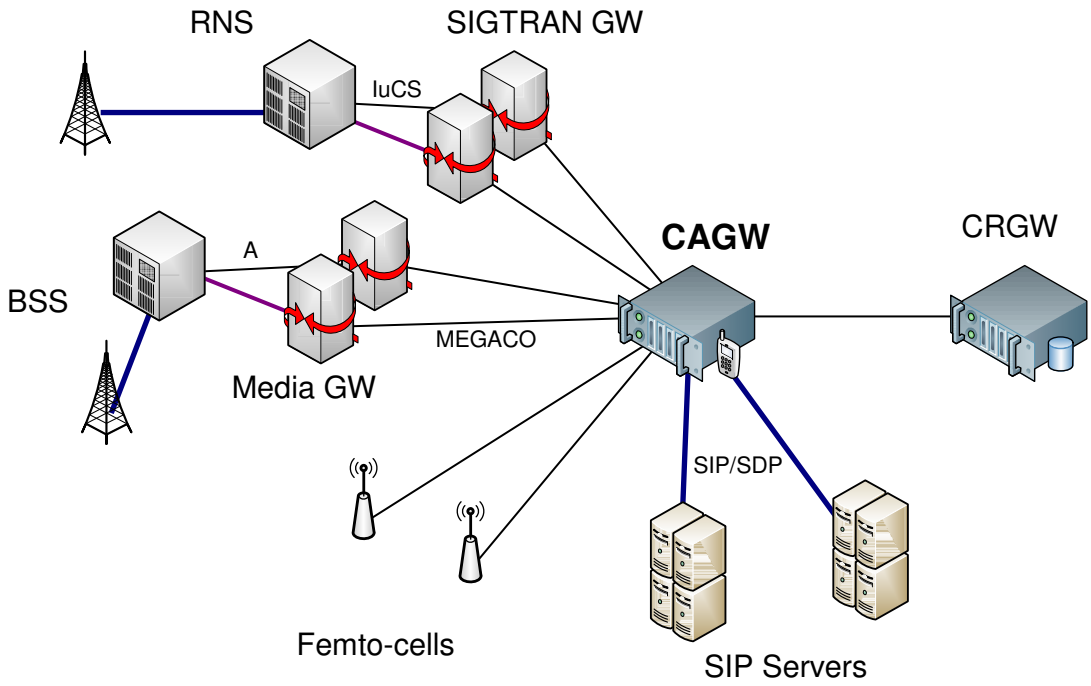
2.3 Concilio Access Gateway

Concilio Access Gateway yhdistää WiFi- ja mobiiliverkot yhteen VoIP-ympäristöön. Mobiiliverkon puolelta CAGW näyttää normaalilta MSC:ltä (Mobile Switching Center) ja VoIP:n puolelta SIP-palvelimelta (Session Initiation Protocol). Siihen voidaan yhdistää yksi tai useampia tukiasemaohjaimia ja SIP-palvelimia. MOC- (Mobile Originating Call) ja MTC- (Mobile Terminating Call) puhelut kulkevat ensin CAGW:hen, jossa se setup-sanomien mukaan välittää puhelut ja tekstiviestit eteen-

päin 2G/3G- ja VoIP-verkon välillä ja ohjaa MGW:tä (Media Gateway) antamalla sille oikeat parametrit yhteyttä varten. [2]

Puhelimen kytkeytyessä verkkoon, se ensin autentikoidaan CAGW:ssä SIM-kortin (Subscriber Identity Module) avulla. GRGW:n palveluita hyväksikäyttäen, autentikointi viedään loppuun normaaliin tapaan mobiilipuolella. Kun autentikointi on tehty onnistuneesti, CAGW rekisteröi päätelaitteen puhelinnumerolla VoIP- ja mobiiliverkkoon CRGW:n avulla suorittamalla location updaten HLR:ään (Home Location Register). Tämän jälkeen kaikki verkot tietävät, miten kyseiseen päätelaitteeseen saa yhteyden. [2]

Normaalisti CMS sisältää yhden tai useamman CAGW:n, jotka yhdistyvät yhteen Concilio Roaming Gateway:hin.[2]



Kuva 2. Concilio Access Gateway:n mahdolliset yhteydet.

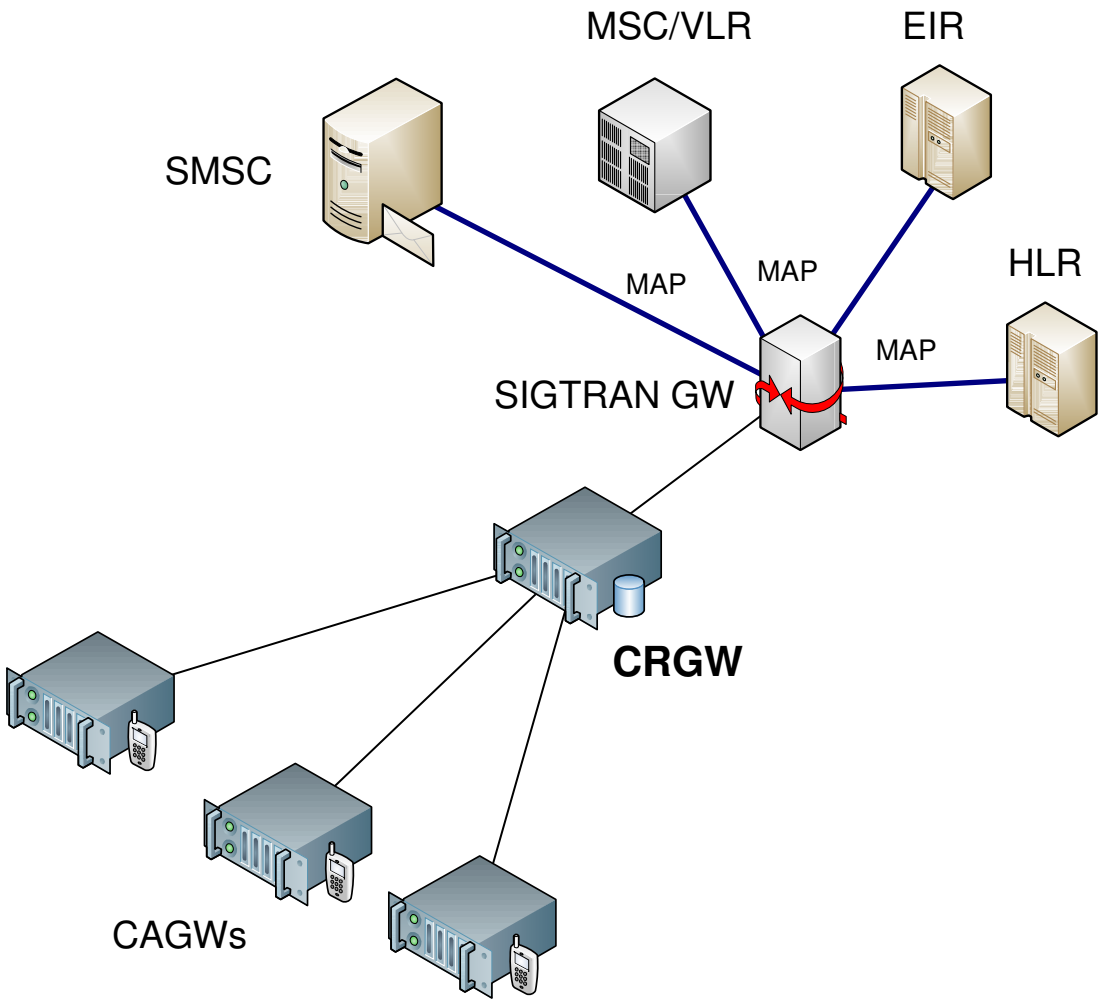
2.4 Concilio Roaming Gateway

Concilio Roaming Gateway:n päätehtävä on pitää mobiiliverkko ajantasalla päätelaitteiden suhteen ja välittää palveluita ja informaatiota mobiiliverkon puolelta muuhun järjestelmään. Se pitää yhteyttä kaikkiin mobiiliverkon rekistereihin, kuten HLR:ään, VLR:ään ja EIR:iin (Equipment Identity Register) MAP-protokollaa (Mobile Application Part) käyttäen. Gateway-tehtävän lisäksi GRGW sisältää myös kaikkien tilaajien tiedot ja jokaisen GAGW:n asetuksen ja parametrit. [2]

Mobiiliverkon näkökulmasta GRGW toimii kuin VLR, joka palvelee CMS:ään kuuluvia puhelimia. GRGW huolehtii sijaintien päivityksistä HLR:lle, jolloin puhelimien sijainti on aina tiedossa. [2]

Kun päätelaite poistuu Concilio Mobile Gateway Suite:n vaikutusalueelta, GRGW informoi GAGW:tä tästä. GAGW informoi edelleen VoIP-verkkoa joka nyt tietää että puhelin ei ole enää järjestelmässä, vaan puhelut täytyy reitittää PSTN:n puolelle. [2]

CRGW pitää tietoa ja logeja kaikista järjestelmän laitteista. Yksittäiset laitteet tallentavat loginsa suoraan CRGW:lle. Logit pitävät tiedon myös kaikista puheluista jne.[2]



Kuva 3. Concilio Roaming Gateway:n mahdolliset yhteydet.

3 TESTAUSYMPÄRISTÖ

3.1 Työssä käytettävät teknologiat

3.1.1 IP, UDP ja TCP

IP eli Internet Protokolla on OSI-mallin (Open Systems Interconnection Basic Reference Model) kerroksen 3 protokolla (verkkokerros). Sen päätehtävä on kuljettaa dataa pakettikytkentäisessä verkossa. Paketit kulkevat perille IP-osoitteiden perusteella. Yhteyttä voidaan pitää epäluotettavana, koska verkko ei varmista mitenkään paketin perillemenoa ja eheyttä. IP-paketti rakentuu otsikko- (header) ja dataosiosta. Otsikko sisältää 13 kenttää, joista 12 on pakollisia. Viimeinen kenttä sisältää valinnaisia kohtia, joita ei yleensä käytetä (esim. ohjeita paketin reititykseen jne.). Pakollisissa kentissä ilmenee mm. versionumero, protokollan numero, pituus, lähdeosoite, kohdeosoite, jne. Otsikkokenttien jälkeen alkaa data, joka alkaa yleensä ylemmän tason protokollan otsikolla.[8]

UDP (User Datagram Protocol) on yksi OSI-mallin kuljetuskerroksen pääprotokollista. Sitä yleensä käytetään esim. reaaliaikaisen kuvan ja äänen siirtoon ja DNS-pyyntöjen (Domain Name System) lähettämiseen. Pakettien perillemenoa ei varmisteta millään tavoin. Koska UDP ei suorita alkukättelyjä, kuittailuja eikä yhteyden lopettamisia, se on huomattavasti kevyempi yhteystapa verrattuna TCP:hen.[9]

+	Bitit 0 - 15	16 - 31
0	Lähdeosoitteen portti	Kohdeosoitteen portti
32	Datan koko	Tarkistussumma
64	Data	

Kuva 4. UDP-paketti. [9]

Kuvassa 4 punaisella merkityt kentät eivät ole pakollisia. Datan koko –kenttään tulee koko UPD-paketin koko (Otsikkokentät + data). 16-bittistä tarkistussumma-kenttää käytetään otsikon ja datan virheentarkistuksessa.[9]

TCP (Transmission Control Protocol) on UDP:n kanssa samalla kuljetuskerroksella toimiva siirtoprotokolla. TCP-paketissa lähetetään kerralla yksi tavujono ja se myös huolehtii niiden oikeasta järjestyksestä. TCP:hen on kehitetty erilaisia mekanismeja (vuonvalvonta ja ruuhkanhallinta), joiden avulla esim. kadonnut tai korruptoitunut paketti voidaan lähettää uudestaan. Suurin osa internetin liikenteestä on TCP-liikennettä.[10][11]

TCP yhteys luodaan kolmiosaisen ”kättelyn” avulla. Asiakas lähettää ensin serverille SYN-paketin. Serveri vastaa siihen SYN/ACK-paketilla. Viimeiseksi asiakas vielä vastaa ACK-paketilla ja datan siirto voi alkaa. Tiedon siirrossa toimivat useat mekanismit. Ajastimet kertovat viiveistä ja hukatuista paketeista. Kun yhteys muodostetaan, sille annetaan sekvenssinumero, jolla eri yhteyksien paketit tunnistetaan. Paketeilla on myös numerointi, joilla tunnistetaan niiden oikea järjestys. Tarkistussummat varmistavat, että tieto ei ole korruptoitunutta. Lisäksi jokaisesta perilletulleesta paketista lähetetään kuittaus lähettäjälle. Jos kuittausta ei kuulu, paketti lähetetään uudestaan. Yhteys päätetään ns. ”nelitiekättelyllä”. Molemmat osapuolet lähettävät erikseen FIN-paketin ja vastaavat toisilleen FIN/ACK-paketilla.[10][11]

Liukuva ikkuna (window scaling) on yksi TCP:n hyödyllisistä ominaisuuksista. Siinä dataa lähetetään juuri niin paljon kuin vastapuoli sitä kykenee ottamaan vastaan. Yhteydessä on käytössä 4 liukuvaa ikkunaa, molempien osapuolten lähetys- ja vastaanottoikkuna. Näiden koko muuttuu dynaamisesti yhteyden aikana. Serveri voi lähettää ikkunan verran dataa toiselle ennen edellisen paketin kuittauksen saapumista. Vaikka TCP on paljon monimutkaisempi kuin UDP, se voi näiden liukuvien ikkunoiden avulla siirtää paketteja sitä nopeammin. [10][11]

3.1.2 SIGTRAN

SIGTRAN (Signaling Transport) on IETF-työryhmän nimi, joka on tuottanut spesifikaatiot useaan protokollaan. SIGTRAN protokollapinon tarkoitus on siirtää piirikytkentäisen puhelinverkon (PSTN) paketteja IP:n yli. SIGTRAN arkkitehtuuri muodostuu kolmesta osasta:

- Normaali muokkaamaton Internet Protokolla (IP)
- Stream Control Transmission Protocol (SCTP) on IETF-työryhmän (Internet Engineering Task Force) määrittelemä uusi protokolla, joka toimii TCP- ja UDP–protokollien tilalla merkinannon siirrossa IP-verkossa.
- Sovitusprotokollakerros, joka tukee esim. tiettyjä hallinnallisia toimintoja, joita tietyt piirikytkentäisen verkon sovellusprotokollat tarvitsevat. Tätä varten IETF on myös luonut uusia protokollia, näistä vain yksi voi olla aktiivisena kerralla:
    - MTP2 User Peer-to-Peer Adaptation Layer (M2PA)
    - MTP2 User Adaptation Layer (M2UA)
    - MTP3 User Adaptation Layer(M3UA)
    - SCCP User Adaption (SUA)
    - ISDN User Adaption (IUA)

[4][5][6]

Protokollan kehitys sai alkunsa, kun VoIP-verkkoja yritettiin sulauttaa puhelinverkkoon ja tähän tarvittiin uusia keinoja. SIGTRAN:in päätarkoitus on vain siirtää protokollia, joten sanomat eivät muutu matkalla millään tavoin. Tämä tekee protokollasta läpinäkyvän. TCP on hyvin luotettava ja hyödyllinen protokolla siirrettäessä dataa pakettikytkentäisissä verkoissa, mutta piirikytkentäisen verkon sanomien siirtoon siitä ei ollut. Oli tarve kehittää uusi siirtoprotokolla, SCTP. [4][5][6]

Stream Control Transmission on luotettava siirtoprotokolla, joka toimii yhteydettömän ja pakettipohjaisen IP:n päällä. SCTP:n on luonut IETF ja se on standartoitu

vuonna 2000 (RFC2960). Alunperin se luotiin luotettavaksi siirtoprotokollaksi välittämään viestejä SCTP:n eri käyttäjien välillä. [4][5][6]

SCTP:n PDU:ita (Protocol Data Unit) kutsutaan SCTP-paketeiksi. SCTP-paketeista muodostuu IP-paketin hyötykuorma. Paketti muodostuu osoitekentästä (Common Header, kuvassa 5 sinisenä), joka vie ensimmäiset 12 tavua ja datakentistä (Chunk, ensimmäinen datakenttä kuvassa 5 vihreänä, loput punaisena), jotka vievät loput paketista. Jokaisen datakentän alussa on yhden tavun kokoinen tunniste (maksimissaan 255 eri tyyppistä datakenttää), josta se identifioidaan. Tunnisteita on tällä hetkellä määritelty 15 kappaletta. Loput kentästä vie 2 tavua ja tähän datan viemä tila päälle. [4][5][6]

Bits	Bits 0 - 7	8 - 15	16 -23	24 -31
+0	Source port		Destination port	
32	Verification tag			
64	Checksum			
96	Chunk 1 type	Chunk 1 flags	Chunk 1 length	
128	Chunk 1 data			
...	...			
...	Chuk n type	Chunk n flags	Chunk n length	
...	Chunk n data			

Kuva 5. SCTP-paketin rakenne. [7]

Suurimmat erot TCP:hen ovat multihoming ja multistreaming. TCP-virta (stream) määritellään jonoksi bittejä, joiden täytyy saapua kohteeseensa tietyssä järjestyksessä. SCTP-virta koostuu viestijonoista, eli bittien sijaan käsitellään kerralla kokonaisia sanomia. Multistreaming tarkoittaa SCTP:n kykyä lähettää rinnakkaisia viestivirtoja samaan aikaan. Esim. PCM:ssä (Pulse Code Modulation) useat samanaikaiset puhelut kulkevat eri aikaväleissä. SCTP-yhteydeltä vaaditaan myös, että usean puhelun data voidaan siirtää samanaikaisesti. Multihoming tarkoittaa ominaisuutta, joka mahdollistaa SCTP-päätepisteeseen osoittamisen eri IP-osoitteilla. Esim. jos päätepisteet ja verkko on konfiguroitu oikein, viestit matkaavat kohteeseensa eri fyysisiä siirtoteitä pitkin eri osoitteilla. Näin tiedonsiirto on paljon varmempaa mahdollisten verkkojen häiriöiden suhteen. [4][5][6]

Jos SCTP-päätepisteellä on useita eri IP-osoitteita, niin se ilmoittaa niistä kaikista käyttämällä INIT-datakentän (Chunk type 1) osoite –parametriä. Serveri ilmoittaa omista osoitteistaan INIT-ACK-datakentässä (Chunk type 2). Jos sanomien INIT- tai INIT-ACK-datakentissä ei ole IP-osoitteita, niin käytetään IP-paketin (joka kantaa SCTP-paketin) kohdeosoitetta. SCTP monitoroi yhteyksiä lähettämällä HEARTBEAT–datakenttiä kaikkiin käyttämättömiin siirtoteihin. Vastaanottaja vastaa HEARTBEAT-ACK–datakentällä. Näin jokaisen siirtotien tila on joko aktiivinen (active) tai toimimaton (inactive). [4][5][6]

Liitteessä 1 on esitelty kaappaus tyypillisestä SCTP-vuosta.

3.1.3 SIP

Session Initiation Protocol (SIP) on sovelluskerroksen protokolla, jonka avulla toteutetaan kommunikointia IP-verkoissa. Viimeisin versio spesifikaatiosta on IETF:n SIP Working Group:n määrittämä RFC 3261. SIP:in avulla kaksi tai useampi osapuolta pystyy suorittamaan Internet-puhelun, videopuhelun, välittämään multimediaa toisilleen, ym. SIP on tällä hetkellä suosituimpia IP-puhelujen signalointiprotokollia H.323:sen ohella. [21]

SIP:ssä on useita normaalin puhelinverkon ominaisuuksia ja vaikutteita. Tarkoitus on luoda mahdollisimman tuttu konsepti vaikka tekniikaltaan systeemi on erilainen. Esimerkiksi soitto suoritetaan valitsemalla numero, puhelin soi, soittoäänet, hälytys- ja varattua ilmaavat äänet. SS7 (Signaling System 7), eli protokollakokoelma, jolla kuljetetaan puhelinverkon merkinanto, on hyvin monimutkainen ja laaja järjestelmä, jossa puhelut väylöittyvät monen mutkan kautta. SIP perustuu peer-to-peer protokollaan, jossa päätelaitteet ovat suoraan yhteydessä toisiinsa. Eli SIP:n ominaisuudet sijaitsevat päätelaitteissa kun taas SS7:n ominaisuudet sijaitsevat itse verkossa. [21]

SIP on suhteellisen kevyt protokolla, koska sitä voidaan siirtää niin UDP:n, TCP:n ja myös SCTP:n päällä. SIP on pelkästään signaloinnin ja puhelujen ohjausprotokolla. Sen päällä kulkee Session Description Protokolla (SDP), josta selviää mm. oikea

portti, tarvittavat koodekit jne. Tämän jälkeen itse puhe tai video siirretään erikseen RTP-protokollaa käyttäen. [21]

Järjestelmässä on kahden tyyppisiä komponentteja, User Agent (UA) ja SIP-server.

1. User Agent
   User Agent Client (UAC) lähettää pyyntöjä ja saa niihin vastauksia User Agent Serveriltä (UAS). Molemmat tyypit ovat läsnä SIP-päätepisteessä, jotta kommunikaatio toimii molempiin suuntiin.
2. SIP palvelimia on kolmea tyyppiä
   Proxy Server välittää sanomia eteenpäin seuraavaan SIP-serveriin. Se toimii yhteyspisteenä kahden asiakkaan välissä. Toiminta on hyvin lähellä normaalia HTTP- (Hypertext Trasfer Protocol) proxyn toimintaa.
   Registrar Server on laite, joka hyväksyy SIP-asiakkaat verkkoon. Se myös pitää yllä tietoa asiakkaiden sijainneista ja osoitteista.
   Redirect Server ainoastaan välittää sanomia eteenpäin.
   Kaikki edellämainitut serverityypit voivat sijaita samassa palvelimessa.

[13]

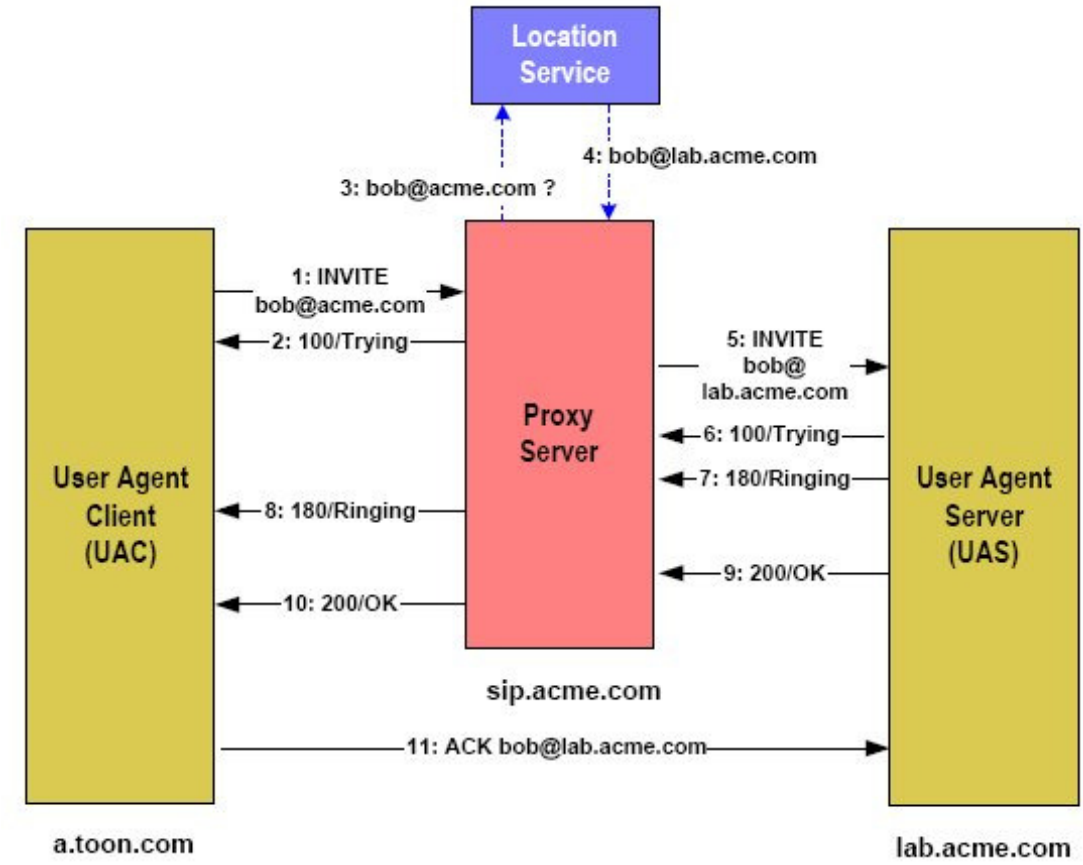
SIP-viestit koostuvat tekstipohjaisista pyynnöistä (request) ja vastauksista (answer). UAC lähettää pyynnön ja UAS vastaa siihen. Tärkeimmät pyynnöt ovat:

- INVITE (kutsuu toista käyttäjää yhteyden aikaansaamiseksi)
- ACK (vastaus yhteyspyyntöön)
- OPTION (pyytää erinäisiä tietoja serveriltä, esim. saatavuus)
- BYE (lopetetaan yhteys)
- CANCEL (kumoaa lähetetyn invite sanoman)
- REGISTER (käyttäjä rekisteröityy SIP-palvelimelle)

[13]

SIP-vastaussanomia on kuutta erilaista, ne kertovat yksinkertaisesti pyynnön ymmärtämisen. Vastauksessa on virhekoodi ja SIP-versionumero. [13]

- 1xx Tilapäinen vastaus (pyyntö vastaanotettu, mutta vielä kesken)
- 2xx Onnistuminen (pyyntö vastaanotettu ja toteutettu)
- 3xx Uudelleenohjaus (lisätoimenpiteitä vaaditaan pyynnön suorittamiseen.)
- 4xx Asiakaspuolen virhe (pyyntöä ei voida suorittaa)
- 5xx Palvelinvirhe (palvelin ei voinut suorittaa pyyntöä)
- 6xx Globaali virhe (mikään palvelin ei voi suorittaa pyyntöä)



Kuva 6. Yhteyden muodostus käyttäen välityspalvelinta. [15]

3.1.4 E1 ja CES

European Conference of Postal and Telecommunications Administrations (CEPT) aluperin lanseerasi E-carrier järjestelmän, jonka myöhemmin ITU-T (International Telecommunication Union Standardization Sector) otti haltuunsa. E1 on maailman-

laajuinen (poislukien USA ja Japani) järjestelmä, jolla digitaalisen puhelinverkon yhdessä fyysisessä siirtotiessä voidaan kuljettaa samaan aikaan useita eri puheluja. [14]

E1:ssä on 32 eri aikaväliä, joista 30 on varattu puheen siirtoon. Yksi aikaväli on merkinannolle ja yksi on varattu kehyslukitukselle. Vastaanottaja tietää tämän perusteella milloin uusi kehys alkaa. Aikavälit siirtävät 8 bittiä dataa omalla vuorollaan, joita on 8000 sekunnissa. Linkki toimii yleensä kahdella erillisellä kaapelilla, joiden tiedonsiirtonopeus on 2.048Mbit/s. [14]

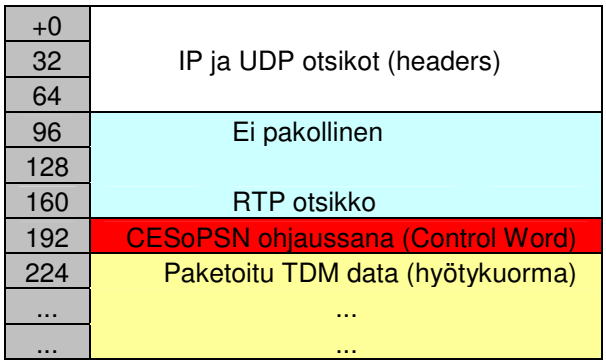
CES tai CESoPSN (Circuit Emulation Services over Packet Switching Network) mahdollistaa piirikytkentäisen verkon palveluiden siirtämisen Internetin yli. Se siirtää aikajaettua signaalia luomalla eräänlaisen virtuaalisen siirtotien pakettiverkon yli. Tätä emuloitua siirtotietä IP:n yli kutsutaan nimeltä pseudowire (PW). Tämä palvelu täyttää harvoin samat edellytykset kuin oikea E1-linja, verkkojen viiveistä yms. johtuen. [16]

CESoPSN:n kehityksessä se määriteltiin täyttämään nämä edellytykset:

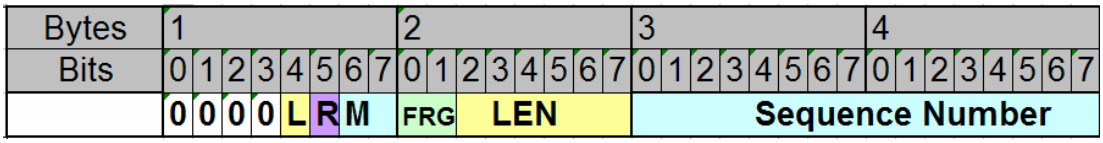
- Jokainen paketti sisältää saman verran "korvaavaa" TDM-dataa (Time Division Multiplexing), tämä helpottaa kadonneitten pakettien käsittelyä. Eli jokainen paketti sisältää yhtä pitkän ajan jakson aikajaettua signaalia.
- Aika tiedon kulkemiseen päästä päähän tulee olla kiinteä (end-to-end delay).

- Pakettien muodostamiseen kuuluva aika: a) Viive pakettien muodostamiseen kuuluu olla 1-5ms b) Järjestelmä joka sallii muuttaa tätä viivettä, täytyy tukea viiveen muuttamista sellaisessa skaalassa, joka on 125 mikrosekunnin monikerta.
- Jos siirretään esim kanavamerkinantoa (CAS), tämä data siirretään omissa paketeissaan erillään muusta TDM-datasta.

Bits	0 - 7	8 - 15	16 - 23	24 - 31



Kuva 7. CESoPSN-paketti käytettäessä UDP:tä. [16]



Kuva 8. CESoPSN Control Word. [16]

CESoPSN ohjaussanomat ensimmäiset 4 bittiä ovat nollia. L asetetaan, jos kytkennässä (circuit) havaitaan jotain virheitä. M–kenttä toimii L–kentän jatkeena (toimivat 3-bittisenä koodina, josta lisää taulukossa 1). R–kenttä asetetaan, jos toiminto, joka suorittaa TDM-datan pakkauksen CESoPSN-paketteihin, kadottaa peräkkäisten pakettien numerojärjestyksen. FRG-kenttää käytetään todella harvoin. Sillä määritellään, esim. jos osa datasta kuuluu lähettää PW:n toisessa päässä eri porttiin. LEN–kentässä on paketin koko, jos se on alle 64 tavua, niin se asetetaan nollaksi. Viimeisessä kentässä on paketin järjestysnumero, joka helpottaa havaitsemaan kadonneita paketteja. [16]

L	M	TULKINTA
0	00	Normaali tilanne, ei virheitä.

0	10	Tilanne jossa vastaanottava osapuoli havaitsee TDM-virrassa bittikuvioita, jotka kertovat katkoksista lähetyksessä (Remote Defect Indication). Tämän jälkeen se yrittää katkoksista huolimatta asettaa ulosmenevän portin (trunk) virhettä vastaavaan tilaan.
0	11	Varattu CESoPSN:n signalointi-paketeille.
1	00	TDM-data on epäkelpoa. Yrittää asettaa ulosmenevän portin AIS-tilaan (Alarm Indication Signal).

Taulukko 1. CESoPSN-ohjaussanoman L- ja M-kenttien selitykset. [16]

Yhteyden laatu ei kokeilujen perusteella ole aina ollut kovinkaan vakaata, johtuen esim. pakettiverkkojen viiveistä jne. Viivettä on yritetty eliminoida asettamalla puskurit (jitter buffer). Vastaanottaja ottaa vastaan CESoPSN-paketin ja siirtää sen puskuriinsa, josta se tietyn ajan välein purkaa niitä TDM-dataksi. [17]

Synkronisaation pitäminen on myös hankalaa. Mahdolista on käyttää molemmissa päissä samaa ulkopuolista kelloa, mikä on usein mahdotonta pitkien välimatkojen takia. Yleisesti CESoPSN yrittää pitää kelloa yllä pakettien järjestysnumeroiden ja niiden aikaleimojen avulla. [17]

3.1.5 MEGACO arkkitehtuuri

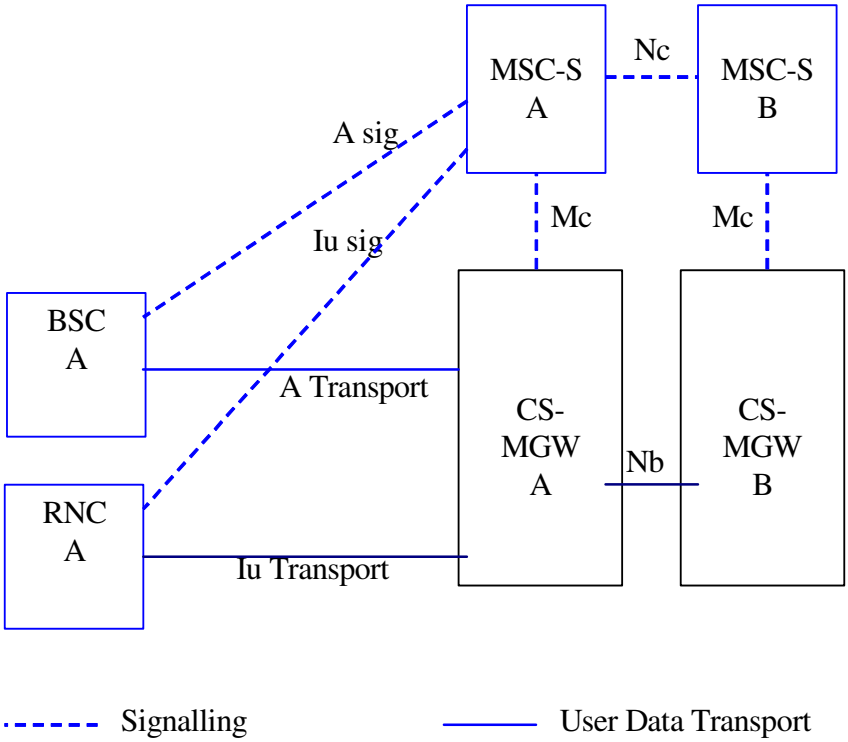
MEGACO tai Gateway Control Protocol, on protokolla, jota käytetään MGC:n (Media Gateway Controller) ja MGW:n (Media Gateway) välissä. Se tarjoaa tarvitut ohjausmekanismit MGW:n hallintaan puhelujen välittämiseksi IP- ja puhelinverkkojen välillä. [18]

Historia alkaa vuodesta 1997, jolloin aloitettiin projekti nimeltään ETSI-TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks). Sen tarkoituksena oli mahdollistaa puhelujen kulkeminen piirikytkentäisistä verkoista IP-verkkoihin ja toisinpäin. Uutena ajatuksena oli toteteutuksen hajoittaminen useampiin komponentteihin, kuten MGC, MGW ja SG (Signalling Gateway). Vuonna 1998 ETSI ja IETF julkaisivat ensimmäisen laitteen ohjaamiseen tarkoitetun protokollan IPDC:n (Internet Protocol Device Control). Samana vuonna Telcordia julkaisi

samantyylisen protokollan SGCP:n (Simple Gateway Control Protocol), jotka molemmat yhdistettiin pian MGCP:ksi (Media Gateway Control Protocol). Kahden kilpailevan protokollan vaikutuksesta MGCP uudistui ja viimein yhdistyi kilpailijaansa ITU:n ja IETF:n toimesta MEGACO:ksi. [18]

Megacon pääidea on hajauttaa puhelujenvälitystoiminnot eri laitteisiin (MGW ja MGC). Keskeistä on, että puhelujen ohjaus tapahtuu MGC:ssä. MEGACO määrittelee:

- Yhteysmalli: Päätepisteet, mediavirrat ja konteksi
- Päätepisteiden, mediavirtojen ja kontekstien ominaisuudet
- Paketit
- Tapahtumat ja signaalit



Kuva 9. 3GPP Release 4-arkkitehtuuri. [19]

3GPP Rel4:n arkkitehtuurissa on suuria yhdennäköisyyksiä MEGACO:on. 3GPP on työryhmä, joka koostuu useista suurista telekommunikaatiolan järjestöistä kuten ARIB, CCSA, ETSI, TTA ja TTC. Sen tehtävänä on kehittää kolmannen sukupolven matkapuhelinverkkoja. Rel4:n (kuva 9) perusideana on jakaa MSC kahteen osaan, jotka ovat MSC-server (MSC-S) ja Media Gateway (CS-MGW). Serveri suorittaa kaiken puhelujenhallinnan ja ohjaa signaloinnin eteenpäin. Media Gateway:n hallintaan se käyttää MEGACO–protokollaa. [19]

Media Gateway:n tehtävä on muuttaa eri verkkojen mediat vastaamaan toisisaan. Esimerkiksi muuttaa piirikytkentäisen verkon RTP-virrat IP-verkkoon sopivaksi ja toisinpäin. Kaiken tämän toiminnan äly sijaitsee MGC:ssä. Signalling Gateway (SG) tekee saman signaloinnin siirron suorittaville protokollille, mitä MGW tekee puhevirralle, eli se muuttaa ne sopiviksi eri verkkoihin. SG ei muuta itse ylempia sovellusprotokollia. [18]

Kuva 10. Testauksessa käytimme Audiocodes:n valmistamaa Mediant 2000 Media Gateway:tä. [24]

Megacon yhteysmallissa tärkeimmät käsitteet ovat päätepisteet (termination) ja yhteydet (context). Context kuvaa yhteyttä päätepisteiden välissä. Päätepisteitä voi olla kaksi (point-to-point) tai useampia yhteyttä kohti. Yhteyttä kuvataan attribuuteilla ja descriptoreilla. ContextID kertoo yhteyden nimen. Muodostettaessa yhteyttä kerrotaan päätepisteiden välisen median suunta. Yhteys on luotu, kun siihen on lisätty ensimmäinen päätepiste ja tuhottu, kun viimeinen päätepiste poistetaan. [18]

Päätepiste on looginen toiminto, joka lähettää ja vastaaanottaa signalointia ja mediavirtaa. Päätepisteillä on tunniste TerminationID, joka annetaan sen luonnin yhteydessä. Se ilmoittaa MGC:lle erilaisista tapahtumista, esimerkiksi tulevasta puhelusta. Päätepisteitä on kahta eri lajia, puolikiinteitä, jotka edustavat fyysistä yhteyttä toiseen toiseen MGW:hen ja lyhytaikaisia, joita käytetään esim. yksittäisen puhelun mediavirran siirtoon. MGC hallitsee kaikki näitä yhteyksiä ja päätepisteitä, määrittää niiden ominaisuudet, luo, poistaa muokkaa, jne. [18]

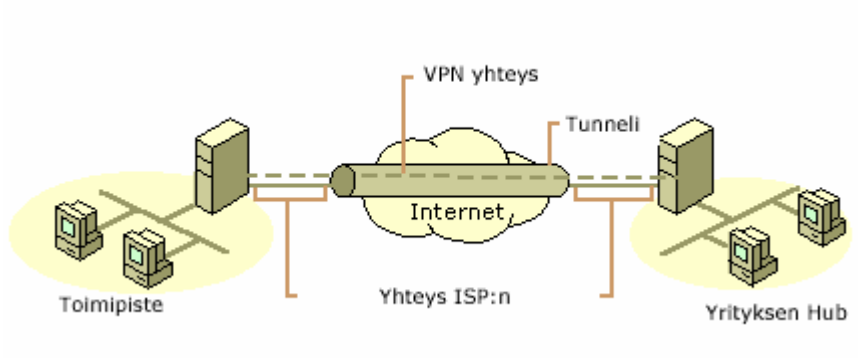
3.1.6 Muut

Järjestelmän monen yhteydet, kuten SIGTRAN-linkit ja tukiasemien siirto IP:n yli vaativat nopeita internet yhteyksiä. Käytössä oli kaksi eri tekniikkaa, Porissa SHDSL ja Espoossa VDSL.

SHDSL-tekniikka eli "Symmetric High-speed DSL" on ADSL-tekniikan edeltäjä. Se siirtää noin kaksi megabittiä sekunnissa molempiin suuntiin yhdellä johtoparilla ja noin 4 megabittiä kahdella parilla. Tämä vastaa puhelinjärjestelmän klassista niin sanottua T1- tai E1-linjaa. Sitä käytetään moniin perinteisen puhelinverkon sovelluksiin, kuten keskuksien liittämiseen puhelinverkkoon. Usean kupariparin tarpeesta johtuen SHDSL ei sovi kotikäyttäjälle. Maksimietäisyys on noin 3 – 4 km. [20]

VDSL (Very High Speed Digital Subscriber Line) on nopein DSL-tekniikoista. Toisen sukupolven VDSL-järjestelmillä pystytään saavuttamaan samanaikaisesti jopa 100Mbit/s lähetys- ja latausnopeus yhdellä johtoparilla. Miinuspuolena on todella pieni toimintaetäisyys, se on maksimissaan vain reilun kilometrin, joten sitä voidaan käyttää vain suurempien keskuksien läheisyydessä. [20]

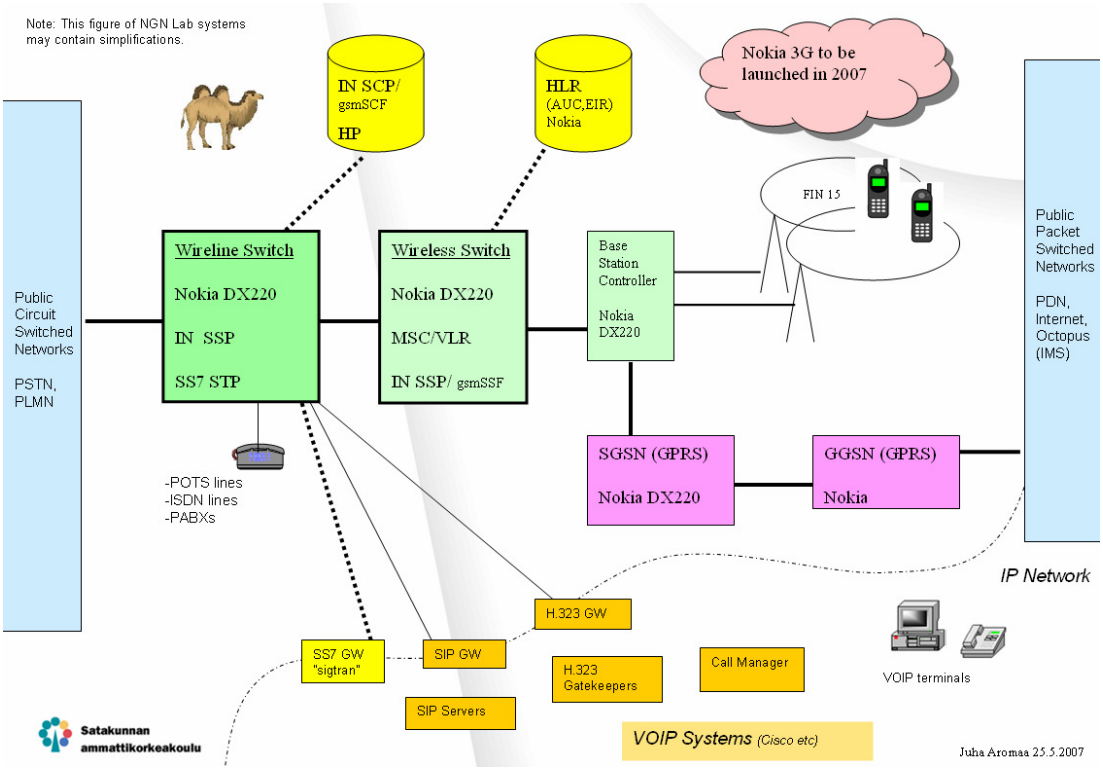
Testausympäristön eri verkot yhdistettiin käyttäen VPN-tekniikkaa. Virtual Private Network on keino, jolla kaksi tai useampaa verkkoa yhdistetään virtuaalisesti toisiinsa julkisen IP-verkon yli. Tieto turvataan salauksella, jonka erilliset VPN-päätelaitteet sitten purkavat. Kyseisessä tapauksessa käytimme IPSec-salausta. [21]



Kuva 11. Reitittimien välinen VPN-yhteys. [22]

Tässä testausympäristössä käytimme kuvan 11 mukaista ratkaisua. VPN-palvelin tuottaa reititetyn yhteyden verkkoon, johon VPN-palvelin on yhteydessä. Reititetyssä VPN-yhteydessä lähetetyt paketit eivät kerro reitittimien alkuperää. Kutsuva reititin (VPN-client) todistaa itsensä vastaanottavalle reitittimelle (VPN-palvelin). Vastavuoroisesti vastaanottava reititin todentaa itsensä kutsuvalle reitittimelle.

3.2 NGN-laboratorio



Kuva 12. Satakunnan ammattikorkeakoulun NGN-laboratorio. [29]

NGN-laboratorio (Next Generation Networks Laboratory) , aiemmalta nimeltään älyverkkolaboratorio (Intelligent Networks Laboratory, IN), on tietotekniikan koulutusohjelman oppimisympäristö, jossa on operaattoritason televerkkojärjestelmiä, lanka- ja matkapuhelinverkon (GSM, GPRS, 3G) laitteistoja, älyverkkolaitteita ja IP- ja puhelintekniikan laitteita. [29]

Laboratorio on laatuyksikkönä Tekniikan ja merenkulun toimialan strateginen painopiste. Se on maailmanlaajuisesti hyvin ainutlaatuinen oppimis- ja testausympäristö. Laitteiden hankintaa ovat tukeneet monet tahot lahjoituksin, luovuttamalla laitteita laboratorion käytettäväksi, myöntämällä alennuksia hankintoihin, myöntämälä ohjelmistolisenssejä ilmaiseksi, antamalla käyttötukea, jne. Eli NGN-laboratorio on onnistunut verkostumaan ja saamaan luottamusta usealta alan toimijoilta. Tämä on johtanut siihen, että useat eri yrityksen suorittavat tuotetestauksiaan laboratorion avulla. [29]

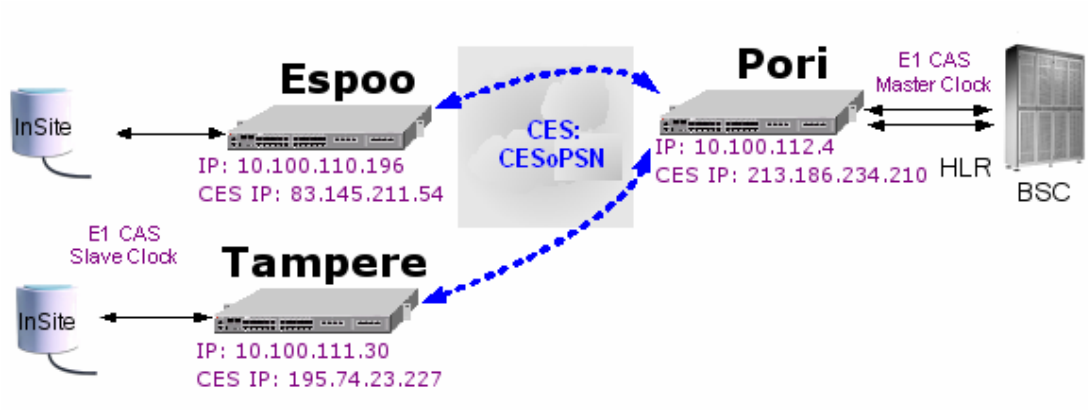
NGN-laboratorio mahdollistaa useiden erillaisten puhelinverkkojen yhteyksien luonnin, niiden protokollien anylysonnin, puhelinverkkojen laitteiden operoinnin, jne. [29]

3.3 Telco T-Marc ja Nokia Insite BTS

Testauksen kannalta oleellinen tukiasemaohjain (BSC) sijaitsi Porissa NGN-laboratoriossa. Tarvetta oli kuitenkin saada laitetestausta tehdyksi muuallakin kuin Porissa. Eli tarvitsi keksiä keino saada tukiasemat viedyksi Espooseen ja Tampereelle. Yksi keino tähän on viedä E1-signaali IP:n yli CESoPSN-protokollaa käyttäen. Laitteena tähän käytimme Telco System:in T-Marc:ia ja Nokia InSite-tukiasemia.

Nokia InSite-tukiasema on maailman pieninpiä tukiasemia painaessaan vain 2,5kg ja se on suunniteltu monipuoliseen sisätilakäyttöön. Se tukee kaikkia GSM-taajuuksia (900/1800/1900) ja GPRS:ää. Asennus on helppoa, tukiasemaohjaimen tarvittavien asetusten laiton jälkeen otetaan yhteys tukiasemaan sarjaportin avulla. Nokian oman hallintaohjelmiston avulla tukiaseman käyttöönotto sujuu vaivattomasti, jonka jälkeen se on toimintakunnossa. [23].

Telco T-Marc:in tehtävä on siirtää E1-signaali IP-verkon yli tukiasemalle Concilio Networksin toimipaikkaan Espooseen. Laitteessa on 4 TDM-porttia, WAN-portti ja 4-porttinen kytkin. Siirtoon käytettiin CESoPSN-protokollaa. Jokaisella laitteella oli 2 eri IP-osoitetta. Toinen on CES-portin osoite, johon paketoitu TDM-data saapuu ja toinen hallintaa varten oleva IP. Hallinta tapahtui telnetin välityksellä ja käyttöliittymä oli hyvin paljon Cisco:n laitteiden tapaan toimiva.



Kuva 13. CESoPSN yhteydet testausympäristössä. [28]

Siirtoa varten pakollisia asetuksia olivat mm. kohdeosoitteet ja portit, käytettävä protokolla, linjan tyyppi, synkronointipuskurin (jitter buffer) koko, TDM-datan määrä paketeissa (aggregation, frames per packet), jne. Vastaanottava laite päätteli tulevien pakettien aikaleimoista kellon (synkronointi). Mahdollista oli siirtää koko linja, tai vain halutut aikavälit. Suurimmat vaikuttajat kaistan tarvittavuuteen ovat siirrettävien aikavälien määrä ja datan määrä paketeissa. Miksi siirtää käyttämättömiä aikavälejä. Koska E1-linjassa yksi aikaväli lähettää 8-bittisen näytteen 8000 kertaa sekunnissa, saadaan tarvittavien pakettien määrä (packets) jakamalla se aggregation-arvolla (TDM-datan määrä pakettia kohti, frames per packet). Siirrettävän paketin koko saadaan kertomalla tarvittavien aikavälien määrä aggregation-arvolla ja lisäämällä otsikkotietojen (headers) tarvitsema tila. Tulos kerrotaan vielä, jotta vastaus saadaan biteissä.

$$\text{Packet/s} \qquad \text{Full Packet Size}$$

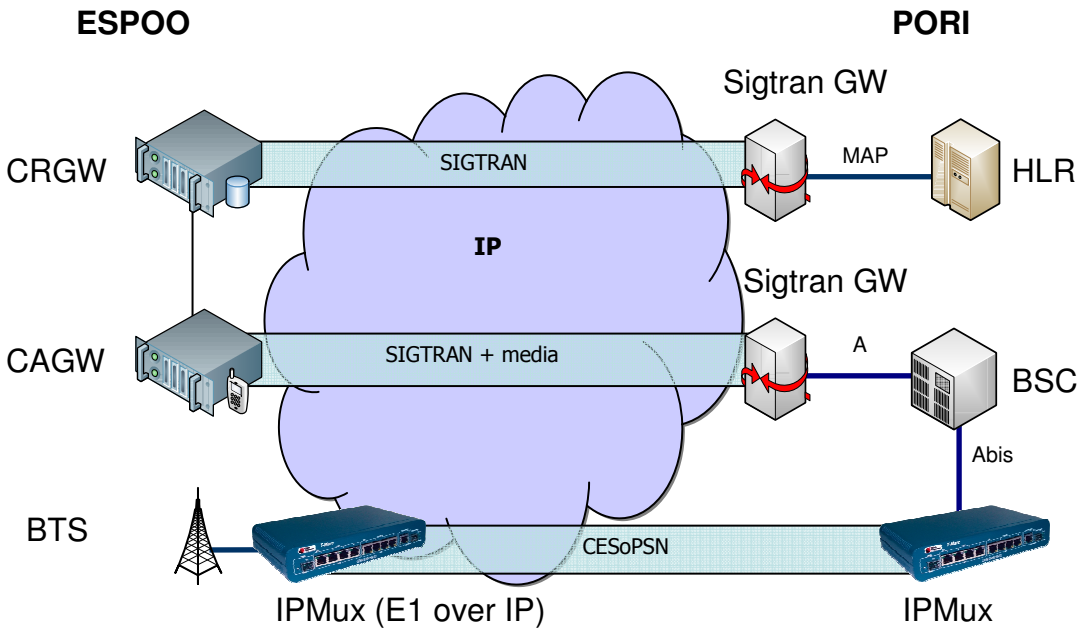
$$\frac{8000}{\text{Aggregation}} \quad \mathbf{X} \quad (\text{Timeslots} \times \text{Aggregation} + \text{Header Size}) \times 8 = \text{bit/s}$$

Teoriassa koko konsepti vaikutti hyvinkin toimivalta, mutta totuus oli toinen. Konfiguroiminen osottautui hyvinkin aikaavieväksi ja jos yksikin parametri oli poikkeava toiseen laitteeseen verrattuna, yhteyttä ei syntynyt. Ja näiden eroavaisuuksien löytäminen oli myös hankalaa. Toinen negatiivinen asia oli suuri kaistantarve. Siirrettävät aikavälimme vaativat kaistaa noin 400kb/s, minkä vuoksi jouduimme hetken kokeilemisen jälkeen päivittämään internet-yhteyksiämme nopeampiin. Kolmantena haittana oli kellon siirto. Se ei yksinkertaisesti siirtynyt tarpeeksi tarkasti. Tämä ilmeni muun muassa puhelujen katkeamisena jne. Esim. yli 10 minuutin puhelut olivat todella harvinaisia. Kokeilimme myös siirtää SS7-signalointia IP:n yli MGW-laitteeseen, mikä ei toiminut lainkaan. Yhteys nousi ja laski jatkuvasti. Kaikesta tästä huolimatta, kun laitteet kerran sai konfiguroitua kunnolla, se myös toimi yllättävän varmasti ja puhelut toimivat riittävästi testauksen tarpeisiin.

4 TESTAUS

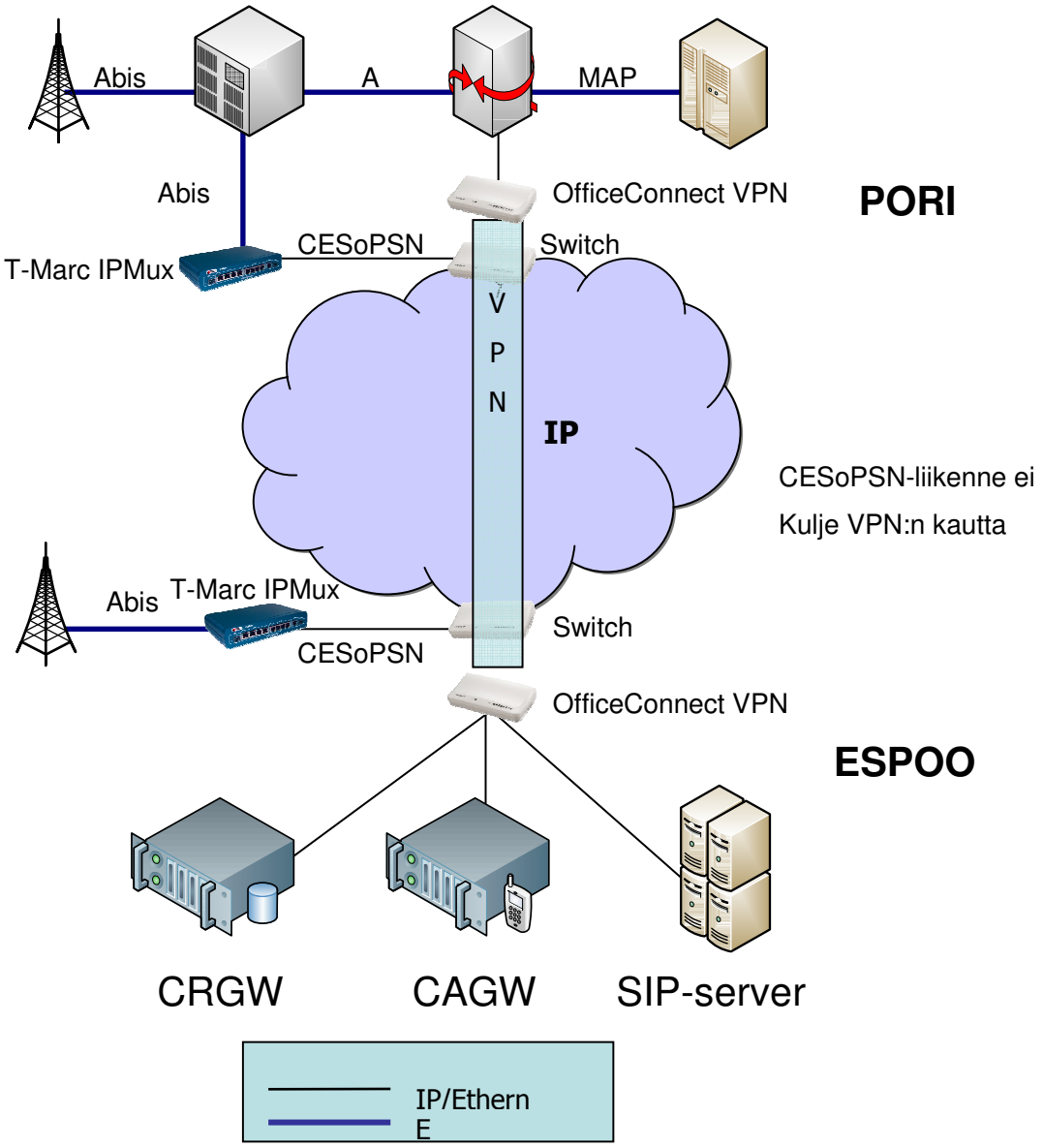
4.1 Systeemitestaus

Testausympäristön rakentaminen alkoi kesällä 2007. Ensimmäinen vaihe oli SIGTRAN-yhteyksien konfigurointi Porista Espooseen. Media Gateway:nä käytettiin Audiocodes:n valmistamaa Mediant 2000:sta. Yhteydet kulkivat VPN:n läpi. Seuraavaksi loimme linkin HLR:stä MGW:hen. Määrittelimme MGW:lle uniikin signalointipisteen (SP) ja loimme yhteydelle link:n, link-set:in ja route-set:in. HLR oli SIGTRAN-linkin kautta yhteydessä Concilio Roaming Gateway:hyn, joka vastaa HLR:n näkökulmasta normaalia VLR:ää.



Kuva 14. Testausympäristön looginen arkkitehtuuri.

Tukiasemaohjaimen liittäminen järjestelmään vaati enemmän työtä. Tarkoitus oli liittää BSC SIGTRAN-linkillä Concilio Acces Gateway:hyn, joka vastaa tukiasemaohjaimen näkökulmasta MSC:tä. BSC voi olla kerrallaan kiinni vain yhdessä MSC:ssä, ja Porin NGN-laboratorion BSC oli jo kytketty omaan Mobile Switch Center:iin. Ratkaisuna annoimme MGW:lle saman signalointipisteen kuin Porin MSC:llä, eli korvasimme Porin MSC:n CAGW:llä. Tämän muutoksen takia NGN-laboratorion oma GSM-verkko ei toiminut, joten sovimme erikseen testausajoista, milloin kumpikin verkko oli toiminnassa. Vaihto oli helposti toteutettavissa. Vaihdoimme vain BSC:ltä lähtevän E1-kaapelin MSC:stä Media Gateway:hyn ja toisinpäin.



Kuva 15. Testausympäristön fyysiset yhteydet.

Viimeinen vaihe testausympäristön rakentamisessa oli tukiaseman asennus Espooseen. Tukiasemaohjain sijaitsi Porissa, joten vienti jouduttiin toteuttamaan IP-verkon yli. Tähän käytimme Telco Systems:in valmistamia T-Marc laitteita, jotka käyttivät CESoPSN-protokollaa. Näin myös Espoossa pystyttiin suorittamaan koesoittoja järjestelmään.

Testausympäristö toimi hienosti ja ensimmäiset toimivat puhelut CMS-järjestelmässä Porin ja Epoon välillä soitettiin. Systeemitestaus piti sisällään lähinnä erilaisten puhelutapauksien toimivuuden selvittämistä. Koesoittoja suoritettiin niin matka- kuin SIP-puhelimienkin välillä. Erilaisia tapauksia oli kymmeniä, esimerkiksi A soittaa – B vastaa, A soittaa – B hylkää puhelun, A soittaa – B katoaa verkosta, jne. Merkinantoa monitoroitiin ja kaapattiin ja häiriöiden ilmentyessä niistä raportoitiin eteenpäin.

4.2 Ohjelmistot

4.2.1 Nethawk M5 ja Wireshark

Nethawk on erikoistunut langattomien verkkojen (mm. GSM, GPRS, EDGE, WiMAX) ja niiden protokollien (SS7, VoIP) analysointi- ja testaustuotteisiin. Nethawk M5 on tarkoitettu juuri puhelinverkkojen protokollien monitoroimiseen. Mahdollista on analysoidaan useaa linjaa ja aikaväliä samalla kertaa. [25]

Testauksessa ohjelmalla analysoitiin Media Gateway:n ja HLR:n välillä olevaa liikennettä sekä MGW:n ja BSC:n välistä A-rajapintaa. A-rajapinta osottautui erittäin herkäksi monitoroinnin kannalta, esim. liian pitkä Nethawk:in kaapeli sai aikaan toisen siirtosuunnan katkeamisen. Eniten ohjelmaa käytettiin varmistamaan yhteyksien toimivuutta. Esimerkiksi tapaus, jossa sanomien kulkeminen SS7-verkosta SIGTRAN:in läpi CAGW:lle kesti huomattavia aikoja. Nethawk:lla oli mahdollista monitoroida sanomien lähtemistä ja ottaa ylös niiden aikaleimat, joita myöhemmin verrattiin perilletulleiden pakettien aikaleimoihin.

Wireshark on Windows- ja Linux-käyttöjärjestelmissä toimiva ilmainen pakettianalysaattori, joka näyttää paketin eri protokollakerrokset hierarkkisesti. Se tunnettiin aiemmin nimellä Ethereal. Se näyttää kirjaimellisesti satoja protokollia, myös SIGTRAN:n protokollapinon. Analysoitavia paketteja on mahdollista suodattaa, jotta tietyn protokollan tai sanoman hakeminen helpottuu. [26]

Wireshark oli testauksessa Porin NGN-laboratoriossa eniten käytetty apuväline. Sen avulla pystyi vaivattomasti seuraamaan SIGTRAN-liikennettä ja näkemään heti, jos jokin oli vialla. Esimerkiksi systeemitestauksessa testasin puhelujen toimivuutta Concilio Mobile Suite-järjestelmässä. Suoritin koesoittoja GSM-puhelimien sekä SIP:n ja GSM:n välillä. Wireshark:lla sai GSM- ja SIP-puolen sanomat näkyviin yhdellä kertaa, joka auttoi epäonnistuneisiin puheluihin johtaineiden syiden etsinnässä. Liitteessä 1 olevat SCTP-paketit on kaapattu Wireshark-analysaattorilla.

4.2.2 TWiki ja Trac

Hajautetussa ympäristössä on tärkeää hyvä yhteydenpito ja raportointi, joilla kaikki osapuolet pysyvät ajan tasalla luotettavasti. Ratkaisu tähän on yleensä jokin webpohjainen järjestelmä, johon jokaisella osapuolella on pääsy. Käytössämme oli TWiki-niminen online-yhteistyöalusta. Se on yrityskäyttöön soveltuva Wikipedian kaltainen järjestelmä.

TWiki sijaitsi sisäverkossa, joten ulkopuolisten pääsy sinne evättiin. Jokaisen käyttäjän oli mahdollista luoda uusia ja editoida olemassa olevia sivuja ja dokumenttejä. Käyttöliittymä oli täysin selainpohjainen, joten muutoksien tekeminen ei vaatinut ohjelmointitaitoja. Käytössä on satoja erilaisia plugineja, joilla sivuille oli mahdollista luoda kalentereja, taulukoita, jne. Järjestelmä sisälsi myös käyttäjähallinnan, jolla pystyttiin käyttäjäkohtaisesti estämään tiettyjen sivujen muutokset. TWiki mahdollisti myös tiedostojen tallentamisen. Järjestelmä sisälsi manuaaleja, yhteystietoja, raportteja, tiedotteita, testausaikatauluja, testausraportteja, dokumentaatioita, logeja, jne.

Trac on vapaaseen lähdekoodiin perustuva ohjelmistokehityksen virheiden (bug) jäljitysjärjestelmä. Sen tarkoituksena on helpottaa ohjelmiston testaajien ja ohjelmoijien kommunikaatiota ja yhteistyötä virheidenkorjauksessa. [27]

Trac on web-pohjainen ja sitä hallitaan täysin selaimen kautta. Virheen havaitsemisen jälkeen käyttäjä luo eräänlaisen ”lipukkeen” (ticket). Siihen laitetaan lyhyt selostus virheestä, mahdollista on myös liittää tiedosto (esim. kaappaus ilmenneestä ongelmasta). Valittavissa on myös virheen korjauksen tärkeys (priority), ohjelman versionumero, ohjelman komponentti, jossa virhe ilmeni, hakusanoja, jne. Ticket osoitetaan yleensä tietylle henkilölle, joka saa sähköpostilla tiedon virheestä. Kun ongelma on ratkaistu, osoitettu henkilö merkitseen virheen korjatuksi. Seuraavaksi alkuperäinen ticket:n luoja saa tiedon sähköpostilla asiasta. Kun hän varmistanut ongelman poistuneet, voi hän sulkea ticket:in.

5 YHTEENVETO

Puhelut ovat hiljalleen siirtymässä kokonaan Internettiin. Muutos tulee viemään paljon aikaa ja se ei tapahdu kerralla. Concilio Networks:n tuote toimii eräänlaisena väliratkaisuna tähän verkkojen sulautumiseen. Se yhdistää mobiili- ja VoIP-ympäristöt saumattomasti toisiinsa, mikä pienentää kynnystä IP-maailmaan siirtymisessä.

Luomani testausympäristö toimi niin kuin oli tarkoituskin. Suurimmiksi ongelmiksi tunnistin hankaluudet E1-linjojen viennissä IP:n yli. Yhteydet olivat yksinkertaisesti liian epävakaat, satunaisia katkoksia ja heittelyitä ilmeni koko ajan. SIGTRAN-linkit sitä vastoin toimivat moitteetta.

Testausympäristön rakentaminen lopulliseen muotoonsa oli mielenkiintoinen prosessi. Se sisälsi paljon tutustumista uusiin tekniikoihin ja laitteisiin. Aloittaessani työni NGN-laboratoriossa, tietämykseni mobiiliverkon järjestelmistä oli hyvin vähäinen. Olemalla mukana Concilio Mobile Gateway Suite:n testausympäristön luomisessa ja itse testauksessa, opin suuria määriä uutta tietoa mobiilijärjestelmien arkkitehtuureista ja protokollista.

Kokemuksieni perusteella sekä merkinantoa että mediaa voidaan onnistuneesti siirtää hajautetussa testiympäristössä IP:n yli. Kustannusmielessä tämä on hyvin edullista. Merkittävää on myös maantieteellisten etäisyyksien häviäminen. Suosittelen silti tarpeeksi riittävän ajan varausta yhteyksien luotettavuuden ja toimivuuden varrmistamiseksi.

LÄHTEET

[1] Concilio Networks kotisivu. [verkkodokumentti]. [viitattu 6.11.2007]. Saatavissa: http://www.concilionetworks.com/index.php?id=30

[2] Concilio Mobile Gateway Suite for Enterprises, Solution Description.

[3] Concilio Mobile Gateway Suite for Corporate Use, White Paper.

[4] WikiPedia – SIGTRAN. [verkkodokumentti]. [viitattu 27.11.2007]. Saatavissa: http://en.wikipedia.org/wiki/SIGTRAN

[5] RFC 2719 Framework Architecture for Signaling Transport. [verkkodokumentti]. [viitattu 27.11.2007]. Saatavissa: http://tools.ietf.org/html/rfc2719

[6] International Engineering Consortium. SS7 over IP Signaling Transport & SCTP [verkkodokumentti]. [viitattu 28.11.2007]. Saatavissa: http://www.iec.org/online/tutorials/ss7_over/

[7] WikiPedia – Stream Control Transmission Protocol. [verkkodokumentti]. [viitattu 28.11.2007]. Saatavissa: http://en.wikipedia.org/wiki/SCTP

[8] WikiPedia – Internet Protocol. [verkkodokumentti]. [viitattu 4.12.2007]. Saatavissa: http://en.wikipedia.org/wiki/Internet_Protocol

[9] WikiPedia – User Datagram Protocol. [verkkodokumentti]. [viitattu 4.12.2007]. Saatavissa: http://en.wikipedia.org/wiki/User_Datagram_Protocol

[10] Wikipedia – Transmission Control Protocol. [verkkodokumentti]. [viitattu 4.12.2007]. Saatavissa: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

[11] Matti Rintala – TCP/IP protokollat. [verkkodokumentti]. [viitattu 4.12.2007]. Saatavissa: http://koti.mbnet.fi/mrin/paattotyo/index.html

[12] VoIP Foro – SIP architecture: Session Initiation Protocol – RFC 3261. [verkkodokumentti]. [viitattu 11.12.2007]. Saatavissa: http://www.en.voipforo.com/SIP/SIP_architecture.php

[13] Petri Kankaanpää – Opinnäytetyö: SIP lisäpalvelut OCSC-ympäristössä, SAMK 2004.

[14] WikiPedia – E-carrier. [verkkodokumentti]. [viitattu 11.12.2007]. Saatavissa: http://en.wikipedia.org/wiki/E-carrier

[15] Radvision – SIP: Protocol overview. [pdf dokumentti].

[16] Network Working Group – RFC5086, TDM Circuit Emulation Service over PSN. [verkkodokumentti]. [viitattu 2.1.2008]. Saatavissa: http://www.ietf.org/rfc/rfc5086.txt

[17] Network Working Group – TDM Circuit Emulation Service over Packet Switched Network (CESoPSN). [verkkodokumentti]. [viitattu 2.1.2008]. Saatavissa: ftp://ftp.axerra.com/sasha/draft-vainshtein-cesopsn-01.txt

[18] Luentomateriaali: Jani Peltola – Media Gateway Control – Megaco/H.248. SAMK 2002

[19] Etsi Mobile Competence Centre - Overview of 3GPP Release 4 v.1.1.0 (draft).

[20] PC Technology Guide – Digital Communications – Other xDSL Variants. [verkkodokumentti]. [viitattu 3.1.2008]. Saatavissa: http://www.pctechguide.com/62DigitalComms_Other_xDSL_variants.htm

[21] WikiPedia – VPN. [verkkodokumentti]. [viitattu 3.1.2008]. Saatavissa: http://fi.wikipedia.org/wiki/VPN

[22] Tietoverkot opas – VPN verkot. [verkkodokumentti]. [viitattu 3.1.2008]. Saatavissa: http://www.2kmediat.com/vpn/

[23] Nokia – New Nokia InSite Base Station – Press Release. [verkkodokumentti]. [viitattu 6.1.2008]. Saatavissa: http://press.nokia.com/PR/199902/777263_5.html

[24] Audiocodes Mediant 2000 VoIP Media Gateway. [verkkodokumentti]. [viitattu 10.1.2008]. Saatavissa: http://www.audiocodes.com/objects/LTRM-40003_DS_M2K_2000.pdf

[25] Nethawk – Nethawk M5 Product Page. [verkkodokumentti]. [viitattu 11.1.2008]. Saatavissa: https://www.nethawk.fi/products/nethawk_analyser/nethawk_m5

[26] Wireshark – About Wireshark. [verkkodokumentti]. [viitattu 11.1.2008]. Saatavissa: http://www.wireshark.org/about.html

[27] The Trac Project Home Page. [verkkodokumentti]. [viitattu 11.1.2008]. Saatavissa: http://trac.edgewall.org/

[28] Telco Systems – Telco T-Marc 254 Product Documentation.

[29] Juha Aromaa – NGN-laboratorion yleiskuvauksia. SAMK 2007.

LIITE 1. Kaappaus SCTP-sanomista

```
No.     Time        Source                Destination           Protocol Info
```

```
77      4682.717807 1024                    900                     BSSAP    CR (BSSMAP)
Complete Layer 3 Information (DTAP) (MM) Location Updating Request

Frame 77 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: AudioCod_0e:11:0e (00:90:8f:0e:11:0e), Dst: 3comEuro_71:cb:08
(00:18:6e:71:cb:08)
Internet Protocol, Src: 10.100.112.2 (10.100.112.2), Dst: 10.100.110.189
(10.100.110.189)
Stream Control Transmission Protocol, Src Port: 2900 (2900), Dst Port: 2900 (2900)
    Source port: 2900
    Destination port: 2900
    Verification tag: 0x7e5bee1a
    Checksum: 0xde9f1b92 [correct CRC32C]
    DATA chunk(ordered, complete segment, TSN: 350, SID: 1, SSN: 3, PPID: 3, payload
length: 84 bytes)
        Chunk type: DATA (0)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x03
            .... ...1 = E-Bit: Last segment
            .... ..1. = B-Bit: First segment
            .... .0.. = U-Bit: Ordered deliviery
        Chunk length: 100
        TSN: 350
        Stream Identifier: 0x0001
        Stream sequence number: 3
        Payload protocol identifier: M3UA (3)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
BSSAP
GSM A-I/F BSSMAP - Complete Layer 3 Information
GSM A-I/F DTAP - Location Updating Request
```

```
No.     Time        Source                Destination           Protocol Info
82      4682.776076 300                   80                    GSM MAP  invoke sen-
dAuthenticationInfo

Frame 82 (166 bytes on wire, 166 bytes captured)
Ethernet II, Src: 3comEuro_71:cb:08 (00:18:6e:71:cb:08), Dst: AudioCod_0e:11:0e
(00:90:8f:0e:11:0e)
Internet Protocol, Src: 10.100.110.184 (10.100.110.184), Dst: 10.100.112.2
(10.100.112.2)
Stream Control Transmission Protocol, Src Port: 2905 (2905), Dst Port: 2905 (2905)
    Source port: 2905
    Destination port: 2905
    Verification tag: 0x00000f46
    Checksum: 0xd2eae006 [correct CRC32C]
    DATA chunk(ordered, complete segment, TSN: 3877764462, SID: 1, SSN: 1, PPID: 3,
payload length: 104 bytes)
        Chunk type: DATA (0)
```

```
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x03
            .... ...1 = E-Bit: Last segment
            .... ..1. = B-Bit: First segment
            .... .0.. = U-Bit: Ordered deliviery
        Chunk length: 120
        TSN: 3877764462
        Stream Identifier: 0x0001
        Stream sequence number: 1
        Payload protocol identifier: M3UA (3)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
```

```
No.     Time        Source                Destination           Protocol Info
92 4682.962842      80                    300                   GSM MAP  invoke in-
sertSubscriberData

Frame 92 (234 bytes on wire, 234 bytes captured)
Ethernet II, Src: AudioCod_0e:11:0e (00:90:8f:0e:11:0e), Dst: 3comEuro_71:cb:08
(00:18:6e:71:cb:08)
Internet Protocol, Src: 10.100.112.2 (10.100.112.2), Dst: 10.100.110.189
(10.100.110.189)
Stream Control Transmission Protocol, Src Port: 2900 (2900), Dst Port: 2900 (2900)
    Source port: 2900
    Destination port: 2900
    Verification tag: 0x7e5bee1a
    Checksum: 0xc96faa57 [correct CRC32C]
    DATA chunk(ordered, complete segment, TSN: 353, SID: 1, SSN: 6, PPID: 3, payload
length: 172 bytes)
        Chunk type: DATA (0)
            0... .... = Bit: Stop processing of the packet
            .0.. .... = Bit: Do not report
        Chunk flags: 0x03
            .... ...1 = E-Bit: Last segment
            .... ..1. = B-Bit: First segment
            .... .0.. = U-Bit: Ordered deliviery
        Chunk length: 188
        TSN: 353
        Stream Identifier: 0x0001
        Stream sequence number: 6
        Payload protocol identifier: M3UA (3)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
```